

---

## 취약성 점검항목 및 가이드

---

2014. 12.

※ 본 가이드는 웹하드 업체의 취약성 점검에 대한 이해를 돕기 위하여 작성된 예시 이며, 본 가이드의 적용 시 업체의 현황에 맞도록 적용할 것을 권고함

## 목 차

|                                                 |    |
|-------------------------------------------------|----|
| 1. UNIX 시스템 취약성 점검항목 및 가이드 .....                | 3  |
| 1.1. 계정 관리 .....                                | 3  |
| 1.1.1. 취약한 패스워드 사용 .....                        | 3  |
| 1.1.2. Shadow 패스워드 정책 .....                     | 4  |
| 1.1.3. 계정 잠금 임계값 설정 .....                       | 6  |
| 1.1.4. root 이외의 UID '0' 사용 금지 .....             | 7  |
| 1.1.5. 패스워드 최소 길이 설정 .....                      | 8  |
| 1.1.6. 패스워드 최대 사용 기간 설정 .....                   | 9  |
| 1.1.7. 패스워드 최소 사용 기간 설정 .....                   | 11 |
| 1.1.8. su 명령어 사용 제한 .....                       | 13 |
| 1.1.9. 불필요한 계정 제거 .....                         | 17 |
| 1.1.10. 로그인에 필요하지 않은 계정 shell 제한 .....          | 18 |
| 1.2. 파일 및 디렉터리 관리 .....                         | 19 |
| 1.2.1. root PATH의 환경변수에 현재 디렉터리(".") 제한 .....   | 19 |
| 1.2.2. /etc/passwd 파일 소유자 및 권한 설정 .....         | 20 |
| 1.2.3. /etc/shadow 파일 소유자 및 권한 설정 .....         | 21 |
| 1.2.4. /etc/hosts 파일 소유자 및 권한 설정 .....          | 23 |
| 1.2.5. /etc/(x)inetd.conf 파일 소유자 및 권한 설정 .....  | 24 |
| 1.2.6. /etc/(r)syslog.conf 파일 소유자 및 권한 설정 ..... | 25 |
| 1.2.7. /etc/services 파일 소유자 및 권한 설정 .....       | 26 |
| 1.3. 서비스 관리 .....                               | 27 |
| 1.3.1. root 계정의 telnet, ssh 접근 제한 .....         | 27 |
| 1.3.2. Session Timeout 설정 .....                 | 29 |
| 1.3.3. 원격 접속 IP 제한 .....                        | 31 |
| 1.3.4. rhosts, hosts.equiv 사용 금지 .....          | 33 |
| 1.3.5. finger 서비스 비활성화 .....                    | 35 |
| 1.3.6. r 계열 서비스 비활성화 .....                      | 37 |
| 1.3.7. Dos 공격에 취약한 서비스 비활성화 .....               | 39 |
| 1.3.8. RPC 서비스 비활성화 .....                       | 42 |
| 1.3.9. tftp, talk 서비스 비활성화 .....                | 45 |
| 1.3.10. NFS 서비스 비활성화 .....                      | 47 |
| 1.3.11. NFS 접근 통제 .....                         | 48 |
| 1.3.12. automount 제거 .....                      | 49 |
| 1.3.13. Sendmail 버전 점검 .....                    | 51 |
| 1.3.14. 인증받지 않은 사용자의 Sendmail q옵션 사용 .....      | 53 |
| 1.3.15. Sendmail expn, vrfy 명령어 제한 .....        | 54 |
| 1.3.16. DNS 버전 점검 .....                         | 55 |
| 1.3.17. DNS recursion 제한 설정 .....               | 57 |
| 1.3.18. DNS Zone Transfer 제한 설정 .....           | 59 |

|                                                |            |
|------------------------------------------------|------------|
| 1.3.19. ftp 서비스 비활성화 .....                     | 60         |
| 1.3.20. Anonymous FTP 접근 제한 .....              | 62         |
| 1.3.21. root 및 불필요한 계정의 ftp 접근 제한 .....        | 63         |
| 1.3.22. SNMP 서비스 비활성화 .....                    | 65         |
| 1.3.23. SNMP Default Community String 변경 ..... | 67         |
| 1.3.24. 서비스 배너설정 및 불필요한 OS 정보 제거 .....         | 68         |
| <b>1.4. 로그 및 패치관리 .....</b>                    | <b>72</b>  |
| 1.4.1. 최신 보안패치 및 벤더 권고사항 적용 .....              | 72         |
| 1.4.2. 로그 기록 설정 .....                          | 73         |
| 1.4.3. 로그의 정기적 검토 및 보고 .....                   | 75         |
| <b>2. Windows 시스템 취약성 점검항목 및 가이드 .....</b>     | <b>76</b>  |
| <b>2.1. 계정 관리 .....</b>                        | <b>76</b>  |
| 2.1.1. Administrator 계정 이름 바꾸기 .....           | 76         |
| 2.1.2. Guest 계정 상태 .....                       | 78         |
| 2.1.3. 불필요한 계정 제거 .....                        | 80         |
| 2.1.4. 해독 가능한 암호화를 사용하여 암호 저장 .....            | 82         |
| 2.1.5. 계정 잠금 임계값 설정 .....                      | 84         |
| 2.1.6. 비밀번호 사용 만기 설정 .....                     | 86         |
| 2.1.7. 비밀번호 복잡성 설정 .....                       | 88         |
| 2.1.8. 비밀번호 최소 암호 길이 .....                     | 90         |
| 2.1.9. 비밀번호 최대 사용 기간 .....                     | 92         |
| 2.1.10. 비밀번호 최소 사용 기간 .....                    | 94         |
| 2.1.11. 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 .....      | 96         |
| <b>2.2. 서비스 관리 .....</b>                       | <b>99</b>  |
| 2.2.1. 공유 권한 및 사용자 그룹 설정 .....                 | 99         |
| 2.2.2. 하드디스크 기본 공유 제거 .....                    | 101        |
| 2.2.3. FTP 서비스 구동 점검 .....                     | 103        |
| 2.2.4. FTP 접근 통제 설정 .....                      | 105        |
| 2.2.5. Anonymous FTP 접속 제한 .....               | 108        |
| 2.2.6. DNS 서비스 구동 점검 .....                     | 110        |
| 2.2.7. DNS Zone Transfer 설정 .....              | 113        |
| 2.2.8. 터미널 서비스 암호화 수준 설정 .....                 | 115        |
| 2.2.9. SNMP 서비스 구동 점검 .....                    | 117        |
| 2.2.10. SNMP Default Community String 변경 ..... | 119        |
| <b>2.3. 기타 보안설정 .....</b>                      | <b>121</b> |
| 2.3.1. 백신 프로그램 설치 .....                        | 121        |
| 2.3.2. SAM 파일 접근 통제 설정 .....                   | 122        |
| 2.3.3. 화면보호기 설정 .....                          | 124        |

|                                             |            |
|---------------------------------------------|------------|
| 2.3.4. 로그온 하지 않고 시스템 종료 허용 .....            | 126        |
| 2.3.5. Null Session 접근 점검 .....             | 128        |
| 2.3.6. 원격 시스템에서 강제로 시스템 종료 .....            | 130        |
| 2.3.7. Autologon 사용 제한 .....                | 132        |
| 2.3.8. 이동식 미디어 포맷 및 꺼내기 허용 .....            | 134        |
| <b>2.4. 로그 및 패치관리 .....</b>                 | <b>136</b> |
| 2.4.1. 최신 서비스 팩 적용 .....                    | 136        |
| 2.4.2. 최신 HOT FIX 적용 .....                  | 138        |
| 2.4.3. 백신 프로그램 업데이트 .....                   | 139        |
| 2.4.4. FTP 로깅 설정 .....                      | 140        |
| 2.4.5. 이벤트 로그 관리 설정 .....                   | 143        |
| 2.4.6. 감사 정책 설정 .....                       | 147        |
| <b>3. 네트워크 취약성 점검항목 및 가이드 .....</b>         | <b>149</b> |
| <b>3.1. 계정관리 .....</b>                      | <b>149</b> |
| 3.1.1. 패스워드 설정 .....                        | 149        |
| 3.1.2. 패스워드 복잡성 설정 .....                    | 152        |
| 3.1.3. 암호화된 패스워드 사용 .....                   | 153        |
| <b>3.2. 접근관리 .....</b>                      | <b>155</b> |
| 3.2.1. VTY 접근(ACL) 설정 .....                 | 155        |
| 3.2.2. Session Timeout 설정 .....             | 157        |
| 3.2.3. VTY 접속 시 안전한 프로토콜 사용 .....           | 159        |
| 3.2.4. 불필요한 보조 입·출력 포트 사용 금지 .....          | 161        |
| <b>3.3. 패치관리 .....</b>                      | <b>162</b> |
| 3.3.1. 최신 보안 패치 및 벤더 권고사항 적용 .....          | 162        |
| <b>3.4. 기능관리 .....</b>                      | <b>163</b> |
| 3.4.1. SNMP 서비스 확인 .....                    | 163        |
| 3.4.2. SNMP community string 복잡성 설정 .....   | 165        |
| 3.4.3. TFTP 서비스 차단 .....                    | 167        |
| 3.4.4. Spoofing 방지 필터링 적용 .....             | 168        |
| 3.4.5. 사용하지 않는 인터페이스의 shutdown 설정 .....     | 170        |
| 3.4.6. Finger 서비스 차단 .....                  | 172        |
| 3.4.7. 웹 서비스 차단 .....                       | 173        |
| 3.4.8. TCP/UDP Small 서비스 차단 .....           | 174        |
| 3.4.9. IP BOOTP 서비스 제한 .....                | 175        |
| 3.4.10. Source 라우팅 차단 .....                 | 177        |
| 3.4.11. arp proxy 제거 .....                  | 178        |
| 3.4.12. ICMP unreachable, Redirect 차단 ..... | 180        |

|                                                |     |
|------------------------------------------------|-----|
| <b>3.5. 로그관리</b>                               | 182 |
| 3.5.1. 로깅 버퍼 크기 설정                             | 182 |
| 3.5.2. 정책에 따른 로깅 설정                            | 183 |
| 3.5.3. NTP 서버 연동                               | 185 |
| <b>4. 정보보호시스템 취약성 점검항목 및 가이드</b>               | 187 |
| <b>4.1. 장비 SW/HW 관련 진단</b>                     | 187 |
| 4.1.1. 최신 패치 적용 여부                             | 187 |
| <b>4.2. 계정 관리</b>                              | 188 |
| 4.2.1. 보안장비 Default 패스워드 변경                    | 188 |
| <b>4.3. 네트워크 원격 관리</b>                         | 189 |
| 4.3.1. 보안장비 원격관리 접근통제                          | 189 |
| 4.3.2. SNMP community string 복잡성 설정            | 190 |
| <b>4.4. 정책 관리 관련 진단</b>                        | 191 |
| 4.4.1. Any(src) to Any(dst), Any 서비스 정책 제한     | 191 |
| 4.4.2. Any(src) to Group(dst), Any 서비스 정책 제한   | 192 |
| 4.4.3. Group(src) to Any(dst), Any 서비스 정책 제한   | 193 |
| 4.4.4. Group(src) to Group(dst), Any 서비스 정책 제한 | 194 |
| 4.4.5. Any(src) to Group(dst), CML 서비스 정책 제한   | 195 |
| 4.4.6. Group(src) to Any(dst), CML 서비스 정책 제한   | 196 |
| 4.4.7. Group(src) to Group(dst), CML 서비스 정책 제한 | 197 |
| 4.4.8. Internal Outbound                       | 198 |
| 4.4.9. Drop All                                | 199 |
| 4.4.10. 침입탐지 룰 적용                              | 200 |
| 4.4.11. False Positive 관리                      | 201 |
| <b>4.5. 로그 관리 관련 진단</b>                        | 202 |
| 4.5.1. 보안장비 로그 설정                              | 202 |
| 4.5.2. 보안장비 로그 정기적 검토                          | 203 |
| <b>4.6. 보안기능 설정관련 진단</b>                       | 204 |
| 4.6.1. ICMP Flooding 차단 설정                     | 204 |
| 4.6.2. Port-Scan 차단 설정                         | 205 |
| 4.6.3. Winnuke 차단설정                            | 206 |
| 4.6.4. Session-threshold 설정                    | 207 |
| 4.6.5. Source Routing 차단 옵션                    | 208 |
| 4.6.6. 장비 리셋 기능 비활성화 여부                        | 209 |
| 4.6.7. Alert & Monitoring 활성화                  | 210 |
| 4.6.8. TCP/UDP Session Timeout 활성화             | 211 |

|                                                                             |            |
|-----------------------------------------------------------------------------|------------|
| 4.6.9. Agent Activity Check .....                                           | 212        |
| 4.6.10. Agent, Console 통신 암호화 .....                                         | 213        |
| <b>5. DBMS 취약성 점검항목 및 가이드 .....</b>                                         | <b>214</b> |
| <b>5.1. 계정관리 .....</b>                                                      | <b>214</b> |
| 5.1.1. 기본 계정의 패스워드, 정책 등을 변경하여 사용 .....                                     | 214        |
| 5.1.2. Scott 등 Demonstration 및 불필요한 계정을 제거하거나 잠금 설정 후 사용 .....              | 216        |
| 5.1.3. 패스워드의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정 .....                               | 218        |
| 5.1.4. 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용 .....                          | 221        |
| 5.1.5. 패스워드 재사용에 대한 제약 설정 .....                                             | 224        |
| 5.1.6. DB 사용자 계정을 개별적으로 부여하여 사용 .....                                       | 227        |
| 5.1.7. Guest 계정의 관리 .....                                                   | 229        |
| <b>5.2. 권한관리 .....</b>                                                      | <b>230</b> |
| 5.2.1. 원격에서 DB 서버로의 접속 제한 .....                                             | 230        |
| 5.2.2. DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정 .....                      | 232        |
| 5.2.3. Listener의 패스워드 설정 및 디폴트 포트 변경 .....                                  | 234        |
| 5.2.4. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 .....                               | 236        |
| 5.2.5. 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 설정 .....                                  | 237        |
| 5.2.6. 데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정 .....          | 238        |
| 5.2.7. Application 사용자의 권한의 최소화 .....                                       | 240        |
| 5.2.8. Registry procedure permission .....                                  | 242        |
| 5.2.9. Fixed server 및 DB Role 부여 .....                                      | 244        |
| <b>5.3. 보안 관리 .....</b>                                                     | <b>246</b> |
| 5.3.1. 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정 .....                   | 246        |
| 5.3.2. OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정 ..... | 248        |
| 5.3.3. 세션 Idle timeout 설정 .....                                             | 249        |
| 5.3.4. SYSDBA 로그인 제한 설정 .....                                               | 250        |
| 5.3.5. OS 명령 수행 제한 .....                                                    | 251        |
| 5.3.6. XP_cmdshell procedure 사용 .....                                       | 252        |
| 5.3.7. Sample DB 사용 .....                                                   | 253        |
| 5.3.8. 외부 DB와의 연동 .....                                                     | 254        |
| 5.3.9. My SQL 설치 시 제공된 test 데이터베이스 제거 .....                                 | 255        |
| <b>5.4. 운영관리 .....</b>                                                      | <b>256</b> |
| 5.4.1. Listener 감사 설정 .....                                                 | 256        |
| 5.4.2. 로그 관련 디렉터리 접근권한 .....                                                | 257        |
| 5.4.3. Control File의 물리적 DISK 관리 .....                                      | 258        |
| 5.4.4. 백업 및 복구 설정 .....                                                     | 259        |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| <b>5.5. 패치관리</b>                                                  | 260 |
| 5.5.1. 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용                         | 260 |
| 5.5.2. 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정          | 263 |
| 5.5.3. Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정                      | 265 |
| 5.5.4. Show processlist 기능 제거                                     | 266 |
| <b>6. PC 취약성 점검항목 및 가이드</b>                                       | 267 |
| <b>6.1. 계정관리</b>                                                  | 267 |
| 6.1.1. 패스워드의 주기적 변경                                               | 267 |
| 6.1.2. 패스워드 정책이 해당 조직의 보안 정책에 적합하게 설정                             | 270 |
| 6.1.3. 복구 콘솔 자동 로그인 금지 설정                                         | 273 |
| <b>6.2. 서비스관리</b>                                                 | 276 |
| 6.2.1. 공유 폴더 제거                                                   | 276 |
| 6.2.2. 불필요한 서비스 제거                                                | 282 |
| 6.2.3. Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지       | 285 |
| 6.2.4. 파일 시스템을 NTFS로 포맷                                           | 288 |
| <b>6.3. 패치관리</b>                                                  | 290 |
| 6.3.1. HOT FIX 등 최신 보안패치                                          | 290 |
| 6.3.2. 최신 서비스팩 적용                                                 | 292 |
| <b>6.4. 보안관리</b>                                                  | 293 |
| 6.4.1. 바이러스 백신 프로그램 설치 및 주기적 업데이트                                 | 293 |
| 6.4.2. 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화                          | 295 |
| 6.4.3. OS에서 제공하는 침입차단 기능 활성화                                      | 296 |
| 6.4.4. 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정                            | 299 |
| 6.4.5. CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립 | 301 |
| 6.4.6. 시스템 부팅 시 Windows Messenger 자동시작 금지                         | 304 |
| 6.4.7. 원격 지원 금지 정책 설정                                             | 306 |
| <b>7. 웹 취약성 점검항목 및 가이드</b>                                        | 309 |
| <b>7.1. 중요 정보 노출</b>                                              | 309 |
| 7.1.1. SQL Injection.                                             | 309 |
| 7.1.2. 부적절한 에러 처리                                                 | 310 |
| 7.1.3. 백업 페이지 존재                                                  | 311 |
| 7.1.4. 디폴트 페이지 존재                                                 | 312 |
| 7.1.5. 관리자 페이지 접근                                                 | 313 |
| 7.1.6. 디렉터리 리스팅                                                   | 314 |

|                                 |            |
|---------------------------------|------------|
| 7.1.7. 소스코드 노출 .....            | 315        |
| 7.1.8. 파일 다운로드 .....            | 316        |
| 7.1.9. 중요정보 전송구간 암호화 .....      | 317        |
| <b>7.2. 취약한 인증 권한 .....</b>     | <b>318</b> |
| 7.2.1. XSS(크로스 사이트 스크립트) .....  | 318        |
| 7.2.2. 디폴트/취약한 계정 사용 .....      | 319        |
| 7.2.3. URL 직접 접근 .....          | 320        |
| 7.2.4. 히든필드 조작 .....            | 321        |
| 7.2.5. 쿠키 인증 취약점 .....          | 322        |
| 7.2.6. 세션/쿠키 타임아웃 설정 .....      | 323        |
| 7.2.7. 다중 세션 허용 .....           | 324        |
| 7.2.8. 파라미터 변조 .....            | 325        |
| 7.2.9. 검증되지 않은 리다이렉트와 포워드 ..... | 326        |
| 7.2.10. 불충분한 인증 .....           | 327        |
| <b>7.3. 원격명령실행 .....</b>        | <b>328</b> |
| 7.3.1. 파일 업로드 .....             | 328        |



## 1. UNIX 시스템 취약성 점검항목 및 가이드

### 1.1. 계정 관리

#### 1.1.1. 취약한 패스워드 사용

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | US1-01 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | 사용자 계정(root 및 일반계정 모두)의 암호 설정 시, 일반적으로 유추하기 쉬운 암호를 설정하여, 비인가 사용자의 시스템 접근을 허용할 수 있다.<br>따라서 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 패스워드로 설정하여 공격자가 추측하기 어려운 패스워드를 사용해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 진단 기준 | 양호 - 패스워드를 영문, 숫자, 특수문자를 혼합 사용하여 복잡하게 설정한 경우<br>취약 - 패스워드가 존재하지 않거나, 패스워드를 영문, 숫자, 특수문자를 혼합 사용하지 않고 간단하게 설정한 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | 패스워드 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인.<br>존 더 립퍼는 사전에 있는 모든 단어와 그 변화형을 패스워드로 시도하고, 단어 하나 하나를 암호화하면서 이미 암호화된 패스워드와 비교하는 방식으로, 취약한 패스워드로 설정되어 있는 사용자들을 찾아서 미리 알려줄 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 조치 방법 | <p>기업의 보안정책에 상응하는 수준의 패스워드로 수정해야 하며, 일반적으로 권장하는 패스워드 설정은 다음과 같다.</p> <ol style="list-style-type: none"> <li>1. 패스워드의 길이는 최소 8자 이상으로 설정</li> <li>2. 영문(대문자, 소문자), 숫자, 특수문자를 혼합하여 패스워드 설정</li> <li>3. 패스워드는 주기적으로 변경하고, 재사용 금지</li> <li>4. 사전에 있는 단어나 누구나 유추 가능한 간단한 패스워드 사용 금지</li> </ol> <p>[Linux, AIX, HP-UX, Solaris]</p> <ol style="list-style-type: none"> <li>1. 다른 사용자 계정 패스워드 변경(Root 권한일 때) <ul style="list-style-type: none"> <li># passwd <u>변경할 ID</u></li> <li>New password : <u>변경할 Passwd</u></li> <li>Retype new passwd : <u>변경할 Passwd (위와 동일)</u></li> </ul> </li> <li>2. 접속중인 자신의 계정 패스워드 변경 <ul style="list-style-type: none"> <li># passwd</li> <li>(current) UNIX passwd : <u>현재 Passwd</u></li> <li>New password : <u>변경할 Passwd</u></li> <li>Retype new passwd : <u>변경할 Passwd</u></li> </ul> </li> </ol> <p>※ 다음과 같은 패스워드는 피해야 한다.<br/>지역명, 부서명, 담당자, 성명, 대표, 업무명, "root", "root123", "admin", "123admin" 등</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |

### 1.1.2. Shadow 패스워드 정책

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | US1-02 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | /etc/passwd 파일은 일반 사용자도 읽기권한이 있으므로 passwd 파일에 계정의 비밀번호가 포함되어 있을 경우 크랙을 통해 root 비밀번호를 취득할 수 있다, 따라서 보안에 취약한 passwd 파일에 저장되어 있는 암호 필드를 특별 권한이 있는 사용자만 접근 가능한 shadow 파일에 패스워드를 저장하여 관리해야 한다.                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | 암호 - 패스워드를 /etc/shadow 파일에 저장되어 있는 경우<br>취약 - 패스워드를 /etc/passwd 파일에 저장되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 점검 방법 | /etc/shadow 파일의 존재 유무를 확인하고, /etc/passwd 파일의 2번째 필드에 비밀번호가 포함되어 있지 않은지 확인<br><br>[Linux, Solaris]<br>1. /etc/shadow 파일 존재 확인<br># ls -l /etc/shadow<br>2. /etc/passwd 파일내 두 번째 필드가 "x"표시가 되어 있는지 확인<br># cat /etc/passwd<br>root:x:0:0:root:/root:/bin/bash<br><br>[AIX]<br>1. /etc/security/passwd 파일 존재 확인<br># ls -l /etc/security/passwd<br>2. /etc/passwd 파일내 두 번째 필드가 "x"표시가 되어 있는지 확인<br># cat /etc/passwd<br>root:x:0:0:root:/root:/bin/bash<br><br>[HP-UX]<br>1. /tcb 디렉터리 존재 확인<br>2. /etc/passwd 파일내 두 번째 필드가 "x"표시가 되어 있는지 확인 |       |        |     |   |
| 조치 방법 | 아래의 보안설정 방법에 따라 설정을 변경<br><br>[Linux, Solaris]<br>1. 쉘도우 패스워드 정책 적용 방법<br># pwconv<br>2. 일반 패스워드 정책 적용 방법<br>#pwunconv<br>[AIX]<br>AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장 · 관리함                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                          |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>[HP-UX]</p> <p>HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 "/tcb/files/auth" 디렉터리에 계정 이니셜과 계정 이름에 따라 파일로 저장·관리할 수 있으므로 Trusted Mode인지 확인 후 UnTrusted Mode인 경우 모드를 전환함</p> <p>1. Trusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행<br/>#/etc/tsconvert</p> <p>2. UnTrusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행<br/>#/etc/tsconvert -r</p> |
| 비고 | <p>[HP-UX]</p> <p>Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환 필요</p>                                                                                                                                                                                                                     |

### 1.1.3. 계정 잠금 임계값 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | US1-03 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | 침입자에 의한 패스워드 무작위 공격(Brute Forceing)이나 패스워드 추측(Geussing) 공격 시 시간을 지체하게 하거나 자동공격에 시간을 끌기 위해 패스워드 입력 횟수를 적정하게 제한하는 것이 좋다.                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | 양호 - 패스워드 입력 횟수를 적정하게 제한했을 경우<br>취약 - 패스워드 입력 횟수를 적정하게 제한하지 않았을 경우                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>패스워드 입력 횟수가 제한되어 있는지 해당 설정파일에서 설정 값 확인</p> <p>[Linux]<br/># cat /etc/pam.d/system-auth<br/>auth required pam_tally2.so deny=5 no_magic_root</p> <p>[Solaris]<br/># cat /etc/default/login<br/>RETRIES = 10</p> <p>[HP-UX]<br/># cat /etc/default/security<br/>maxtries = 5</p> <p>[AIX]<br/># cat /etc/security/user<br/>loginretries = 5</p>                                                         |       |        |     |   |
| 조치 방법 | <p>해당 설정파일에 패스워드 입력 횟수를 제한하는 내용 추가 (예. 5회)</p> <p>[Linux]<br/># vi /etc/pam.d/system-auth<br/>auth required pam_tally2.so deny=5 no_magic_root<br/>account required pam_tally2.so onerr=fail no_magic_root</p> <p>[Solaris]<br/># vi /etc/default/login<br/>RETRIES = 5</p> <p>[HP-UX]<br/># vi /etc/default/security<br/>Maxtries = 5</p> <p>[AIX]<br/># vi /etc/security/user<br/>loginretries = 5</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |

#### 1.1.4. root 이외의 UID '0' 사용 금지

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | US1-04 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 설명    | <p>root(UID=0)와 동일한 *UID(User Identification)를 가진 계정 존재 시 root 권한으로 시스템 접근이 가능하므로 root의 UID를 가진 계정이 존재하지 않도록 확인하여야 한다. root뿐만 아니라 사용자 간 UID 중복 시에도 권한 중복으로 인한 사용자 감사 추적에 어렵게 되는 문제가 발생하므로 계정 및 UID 확인이 필요하다.</p> <p>*UID(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름.</p>                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - root 계정과 동일한 UID를 갖는 계정이 존재하지 않을 경우</p> <p>취약 - UID가 '0'인 계정이 두 개 이상 존재할 경우</p>                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 점검 방법 | <p>시스템 내 root 계정과 동일한 UID('0') 를 갖는 계정이 존재하는지 확인</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <pre># cat /etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin ...생략...</pre> <p>※ /etc/passwd 파일 구조<br/>         ①loginID : ②x : ③UID : ④GID : ⑤comment : ⑥home_directory : ⑦login_shell<br/>         ID ② 패스워드 ③ UID ④ GID ⑤ 사용자정보 ⑥ 홈 디렉터리 ⑦ 로그인 셸</p> |       |        |     |   |
| 조치 방법 | <p>root계정과 UID중복 시에 새로운 UID로 변경</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <pre># usermod -u '새로 부여할 UID' 'UID를 변경할 ID'</pre> <p>ex) # usermod -u 600 snoopy<br/>         → snoopy 계정의 UID를 600으로 변경</p> <p>※ UID를 변경할 계정이 현재 사용 중일 경우에는 vi를 이용하여 조치</p> <pre># vi /etc/passwd snoopy:x:600:501:snoopy:/root:/bin/bash</pre>                                                   |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |

### 1.1.5. 패스워드 최소 길이 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                             | 항목 코드 | US1-05 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | <p>일반적으로 모든 계정은 패스워드가 존재하도록 권장한다. 만약 패스워드가 없는 계정이 있다면 조치를 취해야 하며, 공격자가 쉽게 유추 할 수 없는 패스워드를 만들도록 패스워드 규칙을 정해 주는 것이 좋다.</p> <p>패스워드의 최소 길이를 특정수치 이상으로 설정하여 패스워드 무작위 공격(Brute Forceing)이나 패스워드 추측(Geussing) 공격 등에 대처할 수 있다.</p>                                                                                                                                                       |       |        |     |   |
| 진단 기준 | <p>양호 - 패스워드 최소 길이가 8 이상으로 설정되어 있는 경우</p> <p>취약 - 패스워드 최소 길이가 8 미만으로 설정되어 있는 경우</p>                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 점검 방법 | <p>패스워드 정책 설정파일에서 패스워드 최소 길이의 설정 값 확인</p><br><p>[Linux]</p> <pre># cat /etc/login.defs PASS_MIN_LEN      0</pre> <p>[Solaris]</p> <pre># cat /etc/default/passwd PASSLENGTH = 0</pre> <p>[HP-UX]</p> <pre># cat /etc/default/security MIN_PASSWORD_LENGTH = 0</pre> <p>[AIX]</p> <pre># cat /etc/security/user     minlen = 0</pre>                                               |       |        |     |   |
| 조치 방법 | <p>최소 패스워드 길이는 기업의 보안정책마다 다르지만, 일반적으로 8자리 이상을 권고 해당 파일을 수정하여 패스워드 최소 길이를 최소 8자리 이상으로 설정</p><br><p>[Linux]</p> <pre># vi /etc/login.defs PASS_MIN_LEN      8</pre> <p>[Solaris]</p> <pre># vi /etc/default/passwd PASSLENGTH = 8</pre> <p>[HP-UX]</p> <pre># vi /etc/default/security MIN_PASSWORD_LENGTH = 8</pre> <p>[AIX]</p> <pre># vi /etc/security/user     minlen = 8</pre> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |

### 1.1.6. 패스워드 최대 사용 기간 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | US1-06 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | <p>일반적으로 모든 계정은 패스워드가 존재하도록 권장하며, 만약 패스워드가 없는 계정이 있다면 조치를 취해야 한다.</p> <p>유닉스 시스템을 관리하다 보면 사용자들의 패스워드를 관리하는 것이 중요한 문제이다. 이럴 경우 패스워드 정책을 설정하여 특정 기간이 지나면 패스워드를 새로 변경해야 한다거나, 몇 일 이내에는 패스워드를 변경할 수 없게 하는 것이 가능하다.</p> <p>예를 들어 공격자가 암호화된 패스워드 파일과 암호화 함수를 얻어도, 패스워드 정책에 따라 주기적으로 패스워드를 변경하면 원하는 정보를 얻을 수 없게 된다.</p> <p>따라서 패스워드 정책을 사용하면 공격자는 패스워드를 추측하기 어려울 뿐만 아니라, 주기에 따라 패스워드가 변경되므로 더 안전하게 보호 할 수 있다.</p> <p>또한, 주기를 단기간으로 주면 보호성을 높일 수 있으나 너무 자주 패스워드를 변경하게 되면, 계정 사용자의 불편을 초래할 수 있으므로 보호 정도와 이용 특성에 따라 적절하게 패스워드 정책을 세워야 한다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 보안정책에 따른 최대 사용 기간이 설정되어 있는 경우</p> <p>취약 - 보안정책에 따른 최대 사용 기간이 설정되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>해당 설정파일에서 패스워드 최대 사용 기간의 설정 값 확인</p> <p>[Linux]<br/># cat /etc/login.defs<br/>PASS_MAX_DAYS      0</p> <p>[Solaris]<br/># cat /etc/default/passwd<br/>MAXWEEKS = 0</p> <p>[HP-UX]<br/># cat /etc/default/security<br/>PASSWORD_MAXDAYS = 0</p> <p>[AIX]<br/># cat /etc/security/user<br/>default:<br/>    maxage = 0</p>                                                                                                                                                                                                         |       |        |     |   |
| 조치 방법 | <p>패스워드 최대 사용 기간은 기업의 보안정책에 맞게 설정 (예. 90일)</p> <p>[Linux]<br/># vi /etc/login.defs<br/>PASS_MAX_DAYS      90</p>                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |

|    |                                                                                                                                                                                                                        |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>[Solaris]</p> <pre># vi /etc/default/passwd MAXWEEKS = 12</pre> <p>[HP-UX]</p> <pre># vi /etc/default/security PASSWORD_MAXDAYS = 90</pre> <p>[AIX]</p> <pre># vi /etc/security/user default:     maxage = 90</pre> |
| 비고 |                                                                                                                                                                                                                        |



### 1.1.7. 패스워드 최소 사용 기간 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                    | 항목 코드 | US1-07 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | 패스워드 최소 사용기간을 설정하지 않은 경우 사용자에게 익숙한 패스워드로 변경이 가능하며, 이를 재사용함으로써 패스워드의 정기적인 변경은 무의미해질 수 있다. 이전 암호를 그대로 재사용하는 것을 방지하기 위해 최근 암호 기억 설정을 함께 적용하여 패스워드를 보호해야 한다.                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | 양호 - 보안정책에 따른 패스워드 최소 사용 기간이 설정되어 있는 경우<br>취약 - 보안정책에 따른 패스워드 최소 사용 기간이 설정되어 있지 않은 경우                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | 해당 설정파일에서 패스워드 최소 사용 기간의 설정 값 확인<br><br>[Linux]<br><pre># cat /etc/login.defs PASS_MIN_DAYS      0</pre><br>[Solaris]<br><pre># cat /etc/default/passwd MINWEEKS = 0</pre><br>[HP-UX]<br><pre># cat /etc/default/security PASSWORD_MINDAYS = 0</pre><br>[AIX]<br><pre># cat /etc/security/user default: minage = 0</pre> |       |        |     |   |
| 조치 방법 | 패스워드 최소 사용 기간은 기업의 보안정책에 맞게 설정<br><br>[Linux]<br><pre># vi /etc/login.defs PASS_MIN_DAYS      1</pre><br>[Solaris]<br><pre># vi /etc/default/passwd MINWEEKS = 1</pre><br>[HP-UX]<br><pre># vi /etc/default/security PASSWORD_MINDAYS = 1</pre>                                                                          |       |        |     |   |

|    |                                                            |
|----|------------------------------------------------------------|
|    | [AIX]<br># vi /etc/security/user<br>default:<br>minage = 1 |
| 비고 |                                                            |

### 1.1.8. su 명령어 사용 제한

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | US1-08 | 중요도 | L |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | <p>root계정에 접속할 때 일반 사용자로 로그인한 후 root 사용자로 전환하는 것을 권장하는데 이때 su명령어를 사용한다.</p> <p>su 명령어는 로그아웃 하지 않고 다른 사용자의 권한으로 셸을 실행하게 된다. 따라서 su 명령어를 통해 root 계정으로 접속 시 모든 권한을 획득 할 수 있으므로 허용하는 계정만 su 명령어를 통해 root 계정으로 접속 할 수 있도록 해야 한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 진단 기준 | <p>양호 - su 명령어를 특정 그룹에 속한 사용자만 사용하도록 제한이 되어 있을 경우</p> <p>취약 - su 명령어를 모든 사용자가 사용하도록 되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 점검 방법 | <p>SU 권한이 필요한 특정한 계정들이 한정된 별도의 그룹에 속해 관리되고 있는지 점검</p> <p>[Linux]</p> <p>&lt;방법 1&gt;</p> <ol style="list-style-type: none"> <li>1. /bin/su 파일에 일반 사용자의 접근권한이 제거되어 있는지 확인<br/> <pre># ls -al /bin/su</pre> <pre>-rwsr-x-. 1 root user 34188 Nov 22 07:31 /bin/su</pre> </li> <li>2. “wheel” 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인<br/> <pre># cat /etc/group</pre> <pre>wheel:x:10:root,admin</pre> </li> </ol> <p>&lt;방법 2&gt; LINUX PAM 모듈 이용시</p> <ol style="list-style-type: none"> <li>1. “wheel” 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인<br/> <pre>#cat /etc/group</pre> <pre>wheel:x:10:root,admin</pre> </li> <li>2. 허용 그룹(su 명령어 사용 그룹) 설정 여부 확인<br/> <pre># cat /etc/pam.d/su</pre> <pre>auth required /lib/security/pam_wheel.so group=wheel</pre> </li> </ol> <p>[Solaris]</p> <ol style="list-style-type: none"> <li>1. /usr/bin/su 파일에 일반 사용자의 접근권한이 제거되어 있는지 확인<br/> <pre># ls -al /usr/bin/su</pre> <pre>-rwsr-x-. 1 root user 34200 Dec 12 12:14 /usr/bin/su</pre> </li> <li>2. “wheel” 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인<br/> <pre># cat /etc/group</pre> <pre>wheel:x:10:root,admin</pre> </li> </ol> <p>[AIX]</p> <p>&lt;방법 1&gt; /etc/security/user 파일에 su 명령어를 사용할 그룹이 지정되어 있는지 확인<br/> <pre># cat /etc/security/user</pre> </p> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>예) default :</p> <pre>sugroups = wheel</pre> <p>&lt;방법 2&gt;</p> <ol style="list-style-type: none"> <li>1. /usr/bin/su 파일에 일반 사용자의 접근권한이 제거되어 있는지 확인<br/># ls -al /usr/bin/su<br/>-rwsr-x-. 1 root user 34200 Dec 12 12:14 /usr/bin/su</li> <li>2. “wheel” 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인<br/># cat /etc/group<br/>wheel:x:10:root,admin</li> </ol> <p>[HP-UX]</p> <p>&lt;방법 1&gt; /etc/default/security 파일에 su 명령어를 사용할 그룹이 지정되어 있는지 확인<br/># cat /etc/default/security</p> <p>예) SU_ROOT_GROUP=wheel (su 명령어를 사용할 그룹 지정)</p> <p>&lt;방법 2&gt;</p> <ol style="list-style-type: none"> <li>1. /usr/bin/su 파일에 일반 사용자의 접근권한이 제거되어 있는지 확인<br/># ls -al /usr/bin/su<br/>-rwsr-x-. 1 root user 34200 Dec 12 12:14 /usr/bin/su</li> <li>2. “wheel” 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인<br/># cat /etc/group<br/>wheel:x:10:root,admin</li> </ol> |
| 조치 방법 | <p>일반 사용자의 su 명령 사용 제한</p> <ol style="list-style-type: none"> <li>1. Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용)</li> <li>2. su 명령어의 그룹을 요청받은 그룹으로 변경</li> <li>3. su 명령어의 권한 변경(4750)</li> <li>4. su 명령어 사용이 필요한 계정을 새로 생성한 그룹에 추가(추가할 계정 요청)</li> </ol> <p>※ LINUX의 경우, *PAM(Pluggable Authentication Module)을 이용한 설정 가능</p> <p>*PAM(Pluggable Authentication Module): 사용자를 인증하고 그 사용자의 서비스에 대한 액세스를 제어하는 모듈화된 방법을 말하며, PAM은 관리자가 응용프로그램들의 사용자 인증 방법을 선택할 수 있도록 해준다.</p> <p>[Linux]</p> <p>&lt;방법 1&gt;</p> <ol style="list-style-type: none"> <li>1. wheel group 생성 (wheel 그룹이 존재하지 않는 경우)<br/># groupadd wheel</li> <li>2. su 명령어 그룹 변경<br/># chgrp wheel /bin/su</li> <li>3. su 명령어 사용권한 변경<br/># chmod 4750 /bin/su</li> <li>4. wheel 그룹에 su 명령 허용 계정 등록</li> </ol>                                                                                     |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <pre># usermod -G wheel [계정 명]</pre> <p>또는, 직접 /etc/group 파일을 수정하여 필요한 계정 등록</p> <pre>wheel:x:10: -&gt; wheel:x:10:root,admin</pre> <p>&lt;방법 2&gt; PAM 모듈을 이용한 설정 방법</p> <ol style="list-style-type: none"> <li>1. wheel group 생성 (wheel 그룹이 존재하지 않는 경우) <pre># groupadd wheel</pre> </li> <li>2. wheel 그룹에 su 명령 허용 계정 등록 <pre># useradd -G wheel [계정 명]</pre> </li> <li>3. /etc/pam.d/su 파일을 수정 <pre># vi /etc/pam.d/su</pre> <pre>auth required /lib/security/pam_wheel.so group=wheel</pre> </li> <li>4. /etc/login.defs 수정 <pre># vi /etc/login.defs</pre> <pre>SU_WHEEL_ONLY yes</pre> </li> </ol> <p>[Solaris]</p> <ol style="list-style-type: none"> <li>1. wheel group 생성 (wheel 그룹이 존재하지 않는 경우) <pre># groupadd wheel</pre> </li> <li>2. su 명령어 그룹 변경 <pre># chgrp wheel /usr/bin/su</pre> </li> <li>3. su 명령어 사용권한 변경 <pre># chmod 4750 /usr/bin/su</pre> </li> <li>4. wheel 그룹에 su 명령 허용 계정 등록 <pre># usermod -G wheel [계정 명]</pre> <p>또는, 직접 /etc/group 파일을 수정하여 필요한 계정 등록</p> <pre>wheel:x:10: -&gt; wheel:x:10:root,admin</pre> </li> </ol> <p>[AIX]</p> <p>&lt;방법 1&gt; vi /etc/security/user 파일에서 su 명령어를 사용할 그룹을 지정</p> <pre># vi /etc/security/user</pre> <p>예) default :</p> <pre>sugroups = wheel (su 명령어를 사용할 그룹 지정)</pre> <p>&lt;방법 2&gt;</p> <ol style="list-style-type: none"> <li>1. group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) <pre># mkgroup wheel</pre> </li> <li>2. /usr/bin/su 파일의 그룹을 wheel 그룹으로 변경 <pre># chgrp wheel /usr/bin/su</pre> </li> <li>3. /usr/bin/su 파일의 권한변경(4750) <pre># chmod 4750 /usr/bin/su</pre> </li> <li>4. su 명령어 사용이 필요한 계정을 wheel 그룹에 추가 <pre># chgroup users=[계정 명] wheel</pre> </li> </ol> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <p>[HP-UX]</p> <p>&lt;방법 1&gt; /etc/default/security 파일에서 su 명령어를 사용할 그룹을 지정</p> <pre># vi /etc/default/security</pre> <p>SU_ROOT_GROUP=wheel (su 명령어를 사용할 그룹 지정)</p> <p>&lt;방법 2&gt;</p> <ol style="list-style-type: none"> <li>1. group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) <pre># groupadd wheel</pre> </li> <li>2. /usr/bin/su 파일의 그룹을 wheel 그룹으로 변경 <pre># chgrp wheel /usr/bin/su</pre> </li> <li>3. /usr/bin/su 파일의 권한변경 (4750) <pre># chmod 4750 /usr/bin/su</pre> </li> <li>4. su 명령어 사용이 필요한 계정을 wheel 그룹에 추가 <pre># usermod -G wheel [계정명]</pre> </li> </ol> |
| <b>비고</b> | 그룹에 추가된 계정들은 모든 Session 종료 후 재로그인 시 su 명령어 사용 가능                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### 1.1.9. 불필요한 계정 제거

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | US1-09 | 중요도 | L |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | OS나 Package 설치 시 Default로 생성되는 계정은 대부분 Default 패스워드를 사용하는 경우가 많으며 패스워드 추측공격에 악용될 수 있으므로 시스템에서 이용하지 않는 "lp, uucp, nuucp" 등의 Default 계정 및 의심스러운 특이한 계정의 존재 유무를 확인 후 삭제해야 한다. 또한, 관리되지 않은 불필요한 계정으로 인해 시스템 접속이 가능하므로 퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정은 제거해야 한다. 특히, 장기간 패스워드가 변경되지 않은 미사용 계정은 반복적인 패스워드 추측 공격(Password Guessing)이 가능하고 해당 계정 정보의 유출 여부 확인이 어렵다.                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 진단 기준 | 양호 - 불필요한 계정을 삭제, 변경 했을 경우<br>취약 - 불필요한 계정을 삭제하지 않고, 존재하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>OS설치 시 제공되는 기본 계정과 오랫동안 로그인하지 않은 계정 또는 한번도 로그인하지 않은 계정의 존재 여부를 아래의 명령어를 통해 확인한다.</p> <p># cat /etc/passwd : 현재 불필요한 계정이 존재하는지 확인</p> <p>또한 각 계정들의 로그인 정보 등의 분석</p> <p># last : 계정들의 로그인, 로그아웃, 시스템 재부팅 등의 정보</p> <p># lastlog : 계정들의 최근 로그인 정보</p> <p># lastb : 계정들의 실패한 로그인 정보로서, 반복된 로그인 실패는 사용하지 않는 계정의 불법적인 로그인 시도를 의심해볼 수 있음 (root 권한으로 실행)</p>                                                                                                                                                                                                                                                                         |       |        |     |   |
| 조치 방법 | <p>불필요한 계정 발견 시 아래의 보안설정 방법에 따라 조치</p> <p>[Linux, HP-UX, Solaris]</p> <ol style="list-style-type: none"> <li>1. 서버에 등록된 불필요한 사용자 계정 확인</li> <li>2. userdel 명령으로 불필요한 사용자 계정 삭제</li> </ol> <p># userdel [계정 명]</p> <p>※ /etc/passwd 파일에서 계정 앞에 #을 삽입하여도 주석처리가 되지 않으므로 조치 시에는 반드시 계정을 삭제하도록 권고함</p> <p>[AIX]</p> <ol style="list-style-type: none"> <li>1. 서버에 등록된 불필요한 사용자 계정 확인</li> <li>2. rmuser 명령으로 불필요한 사용자 계정 삭제</li> </ol> <p># rmuser [계정 명]</p> <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>기본적으로 차단하는 Default 계정</p> <p>adm, lp, sync, shutdown, halt, news, uucp, operator, games, gopher, nfsnobody, squid 등</p> </div> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |

### 1.1.10. 로그인 필요하지 않은 계정 shell 제한

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | US1-10 | 중요도 | L |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | <p>로그인이 필요 없는 계정을 이용해 시스템에 접근하여 사용자의 명령어를 해석하고 악용할 가능성이 있으므로, /bin/false *셸(Shell)을 부여해 로그인을 금지한다.</p> <p>*셸(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | <p>양호 - 로그인 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되어 있는 경우</p> <p>취약 - 로그인 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | <p>/etc/passwd 파일의 내용을 확인하여 shell 제한 여부 확인</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <pre># vi /etc/passwd</pre> <p>root:x:0:0:root:/root:/bin/bash : root 계정은 bash 셸이 부여됨</p> <p>bin:x:1:1:bin:/bin:/bin/false : bin 계정은 셸이 부여되지 않음</p>                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 조치 방법 | <p>로그인이 필요 없는 계정의 셸을 /bin/false, /noshell, /sbin/nologin 설정</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <p>&lt;방법 1&gt;</p> <p>/etc/passwd 파일의 bin계정의 셸을 /bin/false로 수정</p> <pre># vi /etc/passwd</pre> <p>root:x:0:0:root:/root:/bin/false</p> <p>&lt;방법2&gt;</p> <p>shell 제한 명령어</p> <p>bin 계정의 셸을 /noshell로 수정</p> <pre># usermod -s /noshell bin</pre> <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>일반적으로 로그인이 불필요한 계정</p> </div> <div style="margin-top: 5px;"> <p>daemon, bin, sys, adm, listen, nobody, nobody4, noaccess, diag, listen, operator, games, gopher 등 일반적으로 UID 100 이하 60000 이상의 시스템 계정 해당</p> </div> |       |        |     |   |
| 비고    | 모호한 경우 “/etc/shadow” 파일에서 해당 계정에 패스워드 존재 여부로 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |



## 1.2. 파일 및 디렉터리 관리

### 1.2.1. root PATH의 환경변수에 현재 디렉터리(".") 제한

| 분류                                       | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | US2-01 | 중요도 | H |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|------------------------|--|---------|-------------------------------|----------|-------------------------------------------|----------|---------------------------------------------|-----------|------------------------------------|------------------------------------------|--|
| 대상                                       | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| 설명                                       | <p>root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 위치하고 있는 명령어가 실행될 수 있다. 즉 "."이 /usr/bin이나 /bin, /sbin 등 명령어들이 위치하고 있는 디렉터리보다 우선하여 위치하고 있을 경우, root 계정의 인가자가 특정 명령을 실행하면, 비인가자가 불법적으로 위치시킨 파일을 실행하여 예기치 않은 결과를 가져올 수 있다.</p> <p>잘못된 PATH의 우선순위 등이 침해사고에 이용될 수 있으므로 "." 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가리키지 않도록 설정한다.</p>                                                                                                                                                                                                                                                                                                |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| 진단 기준                                    | <p>양호 – PATH 환경변수에 “.”이 맨 앞이나 중간에 포함되지 않은 경우</p> <p>취약 – PATH 환경변수에 “.”이 맨 앞이나 중간에 포함되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| 점검 방법                                    | <div>[Linux, AIX, HP-UX, Solaris]</div> <div>1. echo \$PATH로 현재 설정된 PATH 값 확인</div> <div># echo \$PATH</div> <div>/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin</div> <div>위와 같이 출력되는 PATH 변수 내에 “.” 포함 여부 확인</div> <table><tr><th colspan="2">SHELL에 따라 참조되는 환경 설정파일</th></tr><tr><td>/bin/sh</td><td>/etc/profile, \$HOME/.profile</td></tr><tr><td>/bin/csh</td><td>\$HOME/.cshrc, \$HOME/.login, /etc/.login</td></tr><tr><td>/bin/ksh</td><td>/etc/profile, \$HOME/.profile, \$HOME/kshrc</td></tr><tr><td>/bin/bash</td><td>/etc/profile, \$HOME/.bash_profile</td></tr><tr><td colspan="2">※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨</td></tr></table> |       |        |     |   | SHELL에 따라 참조되는 환경 설정파일 |  | /bin/sh | /etc/profile, \$HOME/.profile | /bin/csh | \$HOME/.cshrc, \$HOME/.login, /etc/.login | /bin/ksh | /etc/profile, \$HOME/.profile, \$HOME/kshrc | /bin/bash | /etc/profile, \$HOME/.bash_profile | ※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨 |  |
| SHELL에 따라 참조되는 환경 설정파일                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| /bin/sh                                  | /etc/profile, \$HOME/.profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| /bin/csh                                 | \$HOME/.cshrc, \$HOME/.login, /etc/.login                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| /bin/ksh                                 | /etc/profile, \$HOME/.profile, \$HOME/kshrc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| /bin/bash                                | /etc/profile, \$HOME/.bash_profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| ※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| 조치 방법                                    | <p>PATH 변수 내에 “.”, 이 맨 앞에 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경</p> <div>[Linux, AIX, HP-UX, Solaris]</div> <div>1. vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile)을 연 후</div> <div># vi /etc/profile</div> <div>2. 아래와 같이 수정</div> <div>(수정 전) PATH=.:\$PATH:\$HOME/bin</div> <div>(수정 후) PATH=\$PATH:\$HOME/bin</div> <div>※ 환경변수 파일은 OS별로 약간씩 다를 수 있음</div>                                                                                                                                                                                                                                                                                                 |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |
| 비고                                       | 애플리케이션 구성상 “.” 을 사용해야 하는 경우에는 “.”을 PATH 환경변수의 마지막으로 이동하도록 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |                        |  |         |                               |          |                                           |          |                                             |           |                                    |                                          |  |

### 1.2.2. /etc/passwd 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | US2-02 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 설명    | /etc/passwd 파일은 사용자의 ID, 패스워드(보안상 'x'로 표시), UID, GID, 홈 디렉터리, shell 정보를 담고 있는 중요 파일이다. 이 파일이 노출되면 보안상 심각한 문제를 발생할 수 있어 관리자 이외의 사용자는 접근 제한이 필요하다. 따라서 /etc/passwd 파일의 소유자와 퍼미션 지정여부를 확인해야 한다.                                                                                                                                                                                                                            |       |        |     |   |
| 진단 기준 | 양호 - /etc/passwd 파일의 소유자가 root이고, 권한이 644이하인 경우<br>취약 - /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | [Linux, AIX, Solaris]<br>1. /etc/passwd 파일의 퍼미션과 소유자를 확인<br># ls -l /etc/passwd<br>-rw-r--r-. 1 root root 1839 2014-03-04 23:27 /etc/passwd<br><br>[HP-UX]<br><Standard Mode, Trusted Mode><br>1. /etc/passwd 파일의 퍼미션과 소유자를 확인<br># ls -l /etc/passwd                                                                                                                                                                   |       |        |     |   |
| 조치 방법 | [Linux, AIX, Solaris]<br>1. /etc/passwd 파일의 퍼미션을 644(또는 444)로, 소유자를 root로 변경<br># chmod 644 /etc/passwd<br># chown root /etc/passwd<br><br>[HP-UX]<br><Standard Mode><br>1. /etc/passwd 파일의 퍼미션을 600(또는 400)로, 소유자를 root로 변경<br># chmod 644 /etc/passwd<br># chown root /etc/passwd<br><br><Trusted Mode><br>1. /etc/passwd 파일의 퍼미션을 644(또는 444)로, 소유자를 root로 변경<br># chmod 644 /etc/passwd<br># chown root /etc/passwd |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |

### 1.2.3. /etc/shadow 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | US2-03 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 설명    | <p>/etc/passwd 파일에서 패스워드의 보안을 위해 표시하지 않는 패스워드를 따로 관리하는 파일이 /etc/shadow 파일이며, 암호화된 패스워드 정보를 담고 있다. 이 파일은 root를 제외한 사용자의 접근이 허용되면 보안상 문제가 발생할 수 있다.</p> <p>예를 들어 /etc/shadow 파일의 퍼미션을 644로 설정하여 일반 사용자가 접근 할 수 있다면 이 파일을 가지고 암호를 유추할 수 있으므로 /etc/shadow 파일의 소유자와 퍼미션 설정이 중요하다.</p>                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | <p>양호 - /etc/shadow 파일의 소유자가 root이고, 권한이 400이하인 경우</p> <p>취약 - /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400 이하가 아닌 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>[Linux, Solaris]</p> <p>1. /etc/shadow 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/shadow</pre> <pre>-r-----. 1 root root 1270 2014-03-03 09:52 /etc/shadow</pre> <p>[AIX]</p> <p>1. /etc/security/passwd 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/security/passwd</pre> <p>[HP-UX]</p> <p>&lt;Standard Mode&gt;</p> <p>Standard Mode 일 경우는 패스워드를 /etc/passwd 파일에 저장하므로 해당사항 없음</p> <p>&lt;Trusted Mode&gt;</p> <p>1. /tcb/files/auth/계정이니셜/계정명 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /tcb/files/auth/계정이니셜/계정명</pre> <p>&lt;Shadow Password&gt;</p> <p>1. /etc/shadow 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/shadow</pre> |       |        |     |   |
| 조치 방법 | <p>[Linux, Solaris]</p> <p>1. /etc/shadow 파일의 퍼미션을 600(또는 400)로, 소유자를 root로 변경</p> <pre># chmod 600 /etc/shadow</pre> <pre># chown root /etc/shadow</pre> <p>[AIX]</p> <p>1. /etc/security/passwd 파일의 퍼미션을 600(또는 400)로, 소유자를 root로 변경</p> <pre># chmod 600 /etc/security/passwd</pre> <pre># chown root /etc/security/passwd</pre>                                                                                                                                                                                                                                                                                |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>[HP-UX]</p> <p>&lt;Standard Mode&gt;</p> <p>Standard Mode 일 경우는 패스워드를 /etc/passwd 파일에 저장하므로 해당사항 없음</p> <p>&lt;Trusted Mode&gt;</p> <p>1. /tcb/files/auth/계정이니셜/계정명 파일들 중 시스템 계정을 제외한 로그인 가능한 계정의 권한도 root 소유의 “400”으로 설정</p> <pre># chmod 400 /tcb/files/auth/계정이니셜/계정명</pre> <pre># chown root /tcb/files/auth/계정이니셜/계정명</pre> <p>&lt;Shadow Password 사용시&gt;</p> <p>1. /etc/shadow 파일의 퍼미션을 600(또는 400)로, 소유자를 root로 변경</p> <pre># chmod 600 /etc/shadow</pre> <pre># chown root /etc/shadow</pre> |
| 비고 | <ul style="list-style-type: none"> <li>• HP-UX_11.11의 경우 Shadow Password Bundle 설치 후 pwconv를 실행하면 shadow 파일이 생성</li> <li>• HP-UX_11.23의 경우 Shadow Password product가 기본적으로 설치되어 있음</li> </ul>                                                                                                                                                                                                                                                                                                             |

#### 1.2.4. /etc/hosts 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                       | 항목 코드 | US2-04 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                         |       |        |     |   |
| 설명    | /etc/hosts 파일은 IP address 와 Host name 을 매핑하는데 사용되는 파일이며, 이 파일의 접근권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 된다. 따라서 /etc/hosts 파일을 일반 사용자가 접근 할 수 있다면 이 파일을 가지고 host 파일에 접근하여 spoof 공격을 할 수 있으므로 /etc/hosts 파일의 소유자와 퍼미션 설정이 중요하다.                                                        |       |        |     |   |
| 진단 기준 | 양호 - /etc/hosts 파일의 소유자가 root이고, 권한이 644이하인 경우<br>취약 - /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우                                                                                                                                                                           |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX]<br>1. /etc/hosts 파일의 퍼미션과 소유자를 확인<br># ls -l /etc/hosts<br>-rw-r--r--. 1 root root 158 2010-01-12 05:28 /etc/hosts<br><br>[Solaris]<br>1. /etc/inet/hosts 파일의 퍼미션과 소유자를 확인<br># ls -l /etc/inet/hosts<br>-rw-r--r-- 1 root sys 500 Nov 23 2010 /etc/inet/hosts |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX]<br>1. /etc/hosts 파일의 퍼미션을 644로, 소유자를 root로 변경<br># chmod 644 /etc/hosts<br># chown root /etc/hosts<br><br>[Solaris]<br>1. /etc/inet/hosts 파일의 퍼미션을 644로, 소유자를 root로 변경<br># chmod 644 /etc/inet/hosts<br># chown root /etc/inet/hosts                          |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                    |       |        |     |   |

### 1.2.5. /etc/(x)inetd.conf 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | US2-05 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | 인터넷 수퍼데몬은 외부 네트워크의 요청이 있을 때, /etc/(x)inetd.conf에 등록되어 있는 내부 프로그램인 인터넷 서비스들의 데몬을 실행시켜주는 역할을 한다.<br>inetd.conf(xinetd.d)의 접근권한 설정이 잘못 설정되어 있을 경우 비인가자가 악의적인 프로그램을 이 파일에 등록하여 root의 권한으로 실행하게 할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 진단 기준 | 양호 - /etc/(x)inetd.conf 파일의 소유자가 root이고, 권한이 644이하인 경우<br>취약 - /etc/(x)inetd.conf 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. /etc/xinetd.conf 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/xinetd.conf</pre> <pre>-rw-----. 1 root root 1001 2013-10-07 10:34 /etc/xinetd.conf</pre> <p>[AIX, HP-UX]</p> <p>1. /etc/inetd.conf 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/inetd.conf</pre> <pre>-rw-----. 1 root root 1001 2013-10-07 10:40 /etc/inetd.conf</pre> <p>[Solaris]</p> <p>1. /etc/inet/inetd.conf 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/inet/inetd.conf</pre> <pre>-rw-----. 1 root root 1001 2013-10-07 10:40 /etc/inet/inetd.conf</pre>                                                                                                                                                                       |       |        |     |   |
| 조치 방법 | <p>[Linux]</p> <p>1. /etc/xinetd.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</p> <pre># chmod 644 /etc/xinetd.conf           // 파일 퍼미션 644 설정</pre> <pre># chown root /etc/xinetd.conf          // 파일 소유자 root 설정</pre> <p>※ "/etc/xinetd.d/" 하위 디렉터리에 취약한 파일도 위와 동일한 방법으로 조치</p> <p>[AIX, HP-UX]</p> <p>1. /etc/inetd.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</p> <pre># chmod 644 /etc/inetd.conf           // 파일 퍼미션 644 설정</pre> <pre># chown root /etc/inetd.conf          // 파일 소유자 root 설정</pre> <p>[Solaris]</p> <p>1. /etc/inet/inetd.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</p> <pre># chmod 644 /etc/inet/inetd.conf      // 파일 퍼미션 644 설정</pre> <pre># chown root /etc/inet/inetd.conf      // 파일 소유자 root 설정</pre> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |

### 1.2.6. /etc/(r)syslog.conf 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | US2-06 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 설명    | <p>기본적으로 시스템 운영 중 발생하는 Info 및 alert등에 대한 기록을 남기기 위한 "(r)syslog.conf" 파일의 보안 설정이 되었는지 점검한다.</p> <p>Syslog 데몬은 시스템의 로그를 기록하는 전용 데몬으로 원격 또는 로컬 시스템의 커널 메시지 및 시스템 로그를 감시하는 역할을 한다. 이 설정이 제대로 되어 있지 않을 경우 적절한 로그가 시스템 로그 파일에 남지 않아 침입자의 흔적이나 시스템 오류사항에 대해 분석을 할 수 없다.</p>                                                                                             |       |        |     |   |
| 진단 기준 | <p>양호 - /etc/(r)syslog.conf 파일의 소유자가 root이고, 권한이 644이하인 경우</p> <p>취약 - /etc/(r)syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우</p>                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. /etc/rsyslog.conf 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/rsyslog.conf</pre> <pre>-rw-r--r-. 1 root root 3239 2014-02-27 16:41 /etc/rsyslog.conf</pre> <p>[AIX, HP-UX, Solaris]</p> <p>1. /etc/syslog.conf 파일의 퍼미션과 소유자를 확인</p> <pre># ls -l /etc/syslog.conf</pre> <pre>-rw-r--r-. 1 root root 3239 2014-02-27 16:41 /etc/syslog.conf</pre> |       |        |     |   |
| 조치 방법 | <p>[Linux]</p> <p>1. /etc/rsyslog.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</p> <pre># chmod 644 /etc/rsyslog.conf</pre> <pre># chown root /etc/rsyslog.conf</pre> <p>[AIX, HP-UX, Solaris]</p> <p>1. /etc/syslog.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</p> <pre># chmod 644 /etc/syslog.conf</pre> <pre># chown root /etc/syslog.conf</pre>                                 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |

### 1.2.7. /etc/services 파일 소유자 및 권한 설정

| 분류    | 파일 및 디렉터리 관리                                                                                                                                               | 항목 코드 | US2-07 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                 |       |        |     |   |
| 설명    | Services 파일을 관리자가 아닌 일반 사용자들이 접근 및 변경 가능하면 이를 통해 정상적인 서비스를 제한하거나 허용되지 않은 서비스를 실행시켜 침해사고의 위험이 있으므로 제한하여야 한다.                                                |       |        |     |   |
| 진단 기준 | 양호 - /etc/services 파일의 소유자가 root이고, 권한이 644이하인 경우<br>취약 - /etc/services 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우                                             |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris]<br>1. /etc/services 파일의 퍼미션과 소유자를 확인<br># ls -l /etc/services<br>-rw-r--r-. 1 root root 641020 2013-10-02 02:06 /etc/services |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX, Solaris]<br>1. /etc/services 파일의 퍼미션을 644로, 소유자를 root로 변경<br># chmod 644 /etc/services<br># chown root /etc/services                   |       |        |     |   |
| 비고    |                                                                                                                                                            |       |        |     |   |



### 1.3. 서비스 관리

#### 1.3.1. root 계정의 telnet, ssh 접근 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | US3-01 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | <p>Root 계정으로 직접 로그인 하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 접속에 대한 관리가 필요하다.</p> <p>또한 일반 사용자 계정 접속 후 관리자 계정으로의 변경 시 로그가 남지만 관리자 계정으로 바로 접속하는 경우 어느 사용자가 접속했는지 알 수 없으므로 문제 발생시 책임 소재 파악이 용이하지 않다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | <p>양호 - root 계정의 telnet, ssh 접속이 제한되어 있는 경우</p> <p>취약 - root 계정의 telnet, ssh 접속이 제한되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | <p>■ root계정의 telnet 접속이 제한되어 있는지 확인</p> <p>[Linux]</p> <p>1. /etc/securetty 파일에 pts/0 ~ pts/x 관련 설정이 존재하는지 확인</p> <pre># cat /etc/securetty</pre> <p>※ tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함</p> <p>※ pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함</p> <p>[AIX]</p> <p>1. /etc/security/user 파일에서 root의 rlogin 값이 “false”로 설정되어 있는지 확인</p> <pre># cat /etc/security/user</pre> <pre>root :     rlogin = false</pre> <p>[HP-UX]</p> <p>1. /etc/securetty 파일에서 “console”이 정의되어 있는지 확인</p> <pre># cat /etc/securetty</pre> <pre>console</pre> <p>[Solaris]</p> <p>1. /etc/default/login 파일에서 “CONSOLE=/dev/console”이 정의되어 있는지 확인</p> <pre># cat /etc/default/login</pre> <pre>CONSOLE = /dev/console</pre> <p>■ root계정의 ssh 접속이 제한되어 있는지 확인</p> <p>[Linux, AIX, Solaris]</p> <p>1. /etc/ssh/sshd_config 파일에서 “PermitRootLogin no”로 설정되어 있는지 확인</p> <pre># cat /etc/ssh/sshd_config   grep PermitRootLogin</pre> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>[HP-UX]</p> <ol style="list-style-type: none"> <li>1. /opt/ssh/etc/sshd_config 파일에서 “PermitRootLogin no”로 설정되어 있는지 확인<br/># cat /opt/ssh/etc/sshd_config   grep PermitRootLogin</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 조치 방법 | <p>■ root계정의 telnet 접속 제한 설정</p> <p>[Linux]</p> <ol style="list-style-type: none"> <li>1. “/etc/securetty” 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리</li> </ol> <p>[AIX]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/security/user” 파일을 연 후<br/># /etc/security/user</li> <li>2. rlogin 설정을 아래와 같이 수정 또는, 신규 삽입 (root 설정에 해당되는 부분 수정)<br/>root :<br/>rlogin = false</li> </ol> <p>※ rlogin(remote-login): 자주 접속하는 호스트에 대해 자동으로 원격 접속을 할 수 있도록 사용하는 명령어</p> <p>[HP-UX]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/securetty” 파일을 연 후<br/># vi /etc/security</li> <li>2. 아래와 같이 주석 제거 또는, 신규 삽입<br/>console</li> </ol> <p>※ “/etc/securetty” 파일은 디폴트로 존재하지 않으므로 /etc 디렉터리 내에 “securetty” 파일이 존재하지 않는 경우 새로 생성한 후 적용함</p> <p>[Solaris]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/default/login” 파일을 연 후<br/># vi /etc/default/login</li> <li>2. 아래와 같이 주석 제거 또는, 신규 삽입<br/>CONSOLE=/dev/console</li> </ol> <p>■ root계정의 ssh 접속 제한 설정</p> <p>[Linux, AIX, Solaris]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후<br/># vi /etc/ssh/sshd_config</li> <li>2. 아래와 같이 설정 변경<br/>PermitRootLogin no</li> </ol> <p>[HP-UX]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 /opt/ssh/etc/sshd_config 파일을 연 후<br/># vi /opt/ssh/etc/sshd_config</li> <li>2. 아래와 같이 설정 변경<br/>PermitRootLogin no</li> </ol> |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### 1.3.2. Session Timeout 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | US3-02 | 중요도 | L |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | <p>로그인하여 계정을 모두 사용한 후 사용자의 부주의로 계정이 접속한 상태로 방치할 경우 악의적인 목적으로 사용될 수 있으며, 권한이 없는 사용자에 의한 사용이 이루어질 수 있다.</p> <p>그러므로 일정 시간 이후 어떠한 이벤트가 발생하지 않으면 연결을 강제로 종료하는 session timeout 설정이 필요하다.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 진단 기준 | <p>양호 - Session Timeout 이 설정되어 있는 경우</p> <p>취약 - Session Timeout 이 설정되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>해당 설정파일을 확인하여 Session Timeout 설정이 되어 있는지 확인</p> <p>[Linux, AIX, HP-UX]</p> <p>&lt;sh(born shell), ksh(korn shell), bash(born again shell)를 사용 하는 경우&gt;</p> <p>1. /etc/profile 파일에서 "TIMEOUT" 설정 확인</p> <pre># cat /etc/profile(.profile) TMOUT = 300 export TMOUT</pre> <p>&lt;csh을 사용 하는 경우&gt;</p> <p>1. /etc/csh.login 또는 /etc/csh.cshrc 파일에서 "set autologout" 설정 확인</p> <pre># cat /etc/csh.login 또는, # cat /etc/csh.cshrc set autologout=10</pre> <p>[Solaris]</p> <p>1. /etc/default/login 파일에서 "TIMEOUT" 설정 확인</p> <pre># cat /etc/default/login TIMEOUT=600 export TMOUT</pre> |       |        |     |   |
| 조치 방법 | <p>해당 설정파일에서 일정시간 동안 입력이 없을 경우 접속된 Session을 끊도록 설정</p> <p>[Linux, AIX, HP-UX]</p> <p>&lt;sh(born shell), ksh(korn shell), bash(born again shell)를 사용 하는 경우&gt;</p> <p>1. vi 편집기를 이용하여 "/etc/profile(.profile)" 파일을 연 후</p> <pre># vi /etc/profile(.profile)</pre> <p>2. 아래와 같이 수정 또는 추가</p> <pre>TIMEOUT=600 (단위: 초) export TMOUT</pre> <p>&lt;csh을 사용 하는 경우&gt;</p> <p>1. vi 편집기를 이용하여 "/etc/csh.login" 또는, "/etc/csh.cshrc" 파일을 연 후</p>                                                                                                                                                  |       |        |     |   |

|           |                                                                                                                                                                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <pre># vi /etc/csh.login</pre> <p>2. 아래와 같이 수정 또는 추가</p> <pre>set autologout=10 (단위: 분)</pre> <p>[Solaris]</p> <p>1. vi 편집기를 이용하여 “/etc/default/login” 파일을 연 후</p> <pre># vi /etc/default/login</pre> <p>2. 아래와 같이 수정 또는 추가</p> <pre>TIMEOUT=600 (단위: 초)</pre> <pre>export TMOUT</pre> |
| <b>비고</b> | <p>모니터링 용도로 사용할 경우 해당 계정의 환경변수 파일에만 예외적으로 600초 이상의 시간 입력</p> <p>(예) root 로 모니터링 할 경우 /.profile, /.bash_profile 등에 600초 이상 입력</p>                                                                                                                                                       |

### 1.3.3. 원격 접속 IP 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | US3-03 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고를 방지하기 위하여 TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 진단 기준 | 양호 - 서버로 접속하는 접속 IP를 설정했을 경우<br>취약 - 서버로 접속하는 접속 IP를 설정하지 않았을 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | TCP Wrapper 설치 여부 확인 후, 접속을 허용하는 hosts.allow와 제한하는 hosts.deny 파일의 설정값 확인<br><br>[Linux, AIX, Solaris]<br>1. All deny 적용 확인 및 접근 허용 IP 적절성 확인<br># cat /etc/hosts.deny<br># cat /etc/hosts.allow<br><br>[HP-UX]<br>1. All deny 적용 확인 및 서비스 접근 가능 IP 확인<br># cat /var/adm/inetd.sec                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 조치 방법 | /etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근 허용 IP 등록<br><br>[Linux, AIX, Solaris]<br>1. vi 편집기를 이용하여 “/etc/hosts.deny” 파일을 연 후<br># vi /etc/hosts.deny<br>2. 아래와 같이 수정 또는 추가 (ALL Deny 설정)<br>ALL:ALL<br>3. vi 편집기를 이용하여 “/etc/hosts.allow” 파일을 연 후<br># vi /etc/hosts.allow<br>4. 아래와 같이 접속 허용 서비스 및 IP 설정<br>sshd : 192.168.0.148, 192.168.0.6 (다른 서비스도 동일한 방식으로 설정)<br><br>※ TCP Wrapper 접근제어 가능 서비스<br>SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH<br><br>[HP-UX]<br>HP-UX 서버의 경우 “/var/adm/inetd.sec” 파일을 이용하여 서버 자체적으로 접근제어를 할 수 있으며, 해당 파일이 존재하지 않을 경우 “/usr/newconfig/var/adm/inetd.sec” 샘플 파일을 복사하여 사용함<br><br>1. vi 편집기를 이용하여 “/var/adm/inetd.sec” 파일을 연 후 |       |        |     |   |

|           |                                                                                                                                                                                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <pre># vi /var/adm/inetd.sec</pre> <p>2. 아래와 같이 수정 또는 추가</p> <ul style="list-style-type: none"> <li>- telnet 으로의 모든 접속 차단 =&gt; telnet deny *.*.*.*</li> <li>- telnet 접속을 허용할 IP 등록 =&gt; telnet allow [telnet 접속 허용 IP 등록]</li> </ul> <p>(다른 서비스들도 위와 동일한 방법으로 설정)</p> |
| <b>비고</b> | 허용되지 않은 IP는 접속 불가                                                                                                                                                                                                                                                       |

### 1.3.4. rhosts, hosts.equiv 사용 금지

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                             | 항목 코드 | US3-04 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 설명    | <p>*'r'command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있을 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 된다. 만약 사용이 불가피한 경우 /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root 또는, 해당 계정으로 설정한 뒤 권한을 600으로 설정하고 해당 파일 설정에 '+' 설정(모든 호스트 허용)이 포함되지 않도록 한다.</p> <p>*'r'command : 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음.</p> <p>*NET Backup : 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.</p>                     |       |        |     |   |
| 진단 기준 | <p>양호 - login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우</p> <ol style="list-style-type: none"> <li>1. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우</li> <li>2. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한이 600 이하인 경우</li> <li>3. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우</li> <li>4. /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우</li> </ol> <p>취약 - login, shell, exec 서비스를 사용하고, 위와 같은 설정이 적용되지 않은 경우</p> |       |        |     |   |
| 점검 방법 | <p>.rhosts, hosts.equiv 파일 존재 유무 및 내용 확인</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <ol style="list-style-type: none"> <li>1. 파일 소유자 및 권한 확인 <pre># ls -al /etc/hosts.equiv</pre> <pre># ls -al \$HOME/.rhosts</pre> </li> <li>2. 계정 별 '+' 부여 적절성 확인 <pre># cat /etc/hosts.equiv</pre> <pre># cat \$HOME/.rhosts</pre> </li> </ol> <p>- /etc/hosts.equiv : TRUSTED 시스템을 등록</p> <p>- \$HOME/.rhosts : 사용자 별로 'r'command를 통해 접근이 가능하도록 설정할 수 있음</p>     |       |        |     |   |
| 조치 방법 | <p>.rhosts, hosts.equiv 파일의 사용이 불필요 시에는 삭제한다.</p> <p>사용 시에는 파일의 소유자를 root로 퍼미션을 600으로 설정하고, 파일 내용 중에 "+" 가 포함되지 않도록 설정</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <p>■ .rhosts, hosts.equiv 파일 미사용 시</p> <ol style="list-style-type: none"> <li>1. .rhosts, hosts.equiv 파일 삭제 <pre># rm -f [삭제 할 파일 및 디렉터리 경로]</pre> </li> </ol>                                                                                                                      |       |        |     |   |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |     |                   |        |                     |        |                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------------------|--------|---------------------|--------|---------------------|
|        | <pre># rm -f \$HOME/.rhosts 또는 or /etc/ hosts.equiv</pre> <p>■ .rhosts, hosts.equiv 파일 사용 시</p> <ol style="list-style-type: none"> <li>1. “/etc/hosts.equiv” 및 “\$HOME/.rhosts” 파일의 소유자를 root 또는, 해당 계정으로 변경 <pre># chown root /etc/hosts.equiv</pre> <pre># chown [계정 명] \$HOME/.rhosts</pre> </li> <li>2. “/etc/hosts.equiv” 및 “\$HOME/.rhosts” 파일의 퍼미션을 600 이하로 변경 <pre># chmod 600 /etc/hosts.equiv</pre> <pre># chmod 600 \$HOME/.rhosts</pre> </li> <li>3. “/etc/hosts.equiv” 및 “\$HOME/.rhosts” 파일에서 “+”를 제거하고 허용 호스트 및 계정 등록 <pre># vi /etc/hosts.equiv (or \$HOME/.rhosts)</pre> <table border="1"> <tbody> <tr> <td>+ +</td><td>모든 호스트의 모든 계정을 신뢰</td></tr> <tr> <td>+ test</td><td>모든 호스트의 test 계정을 신뢰</td></tr> <tr> <td>Web1 +</td><td>Web1 호스트의 모든 계정을 신뢰</td></tr> </tbody> </table> </li> </ol> | + + | 모든 호스트의 모든 계정을 신뢰 | + test | 모든 호스트의 test 계정을 신뢰 | Web1 + | Web1 호스트의 모든 계정을 신뢰 |
| + +    | 모든 호스트의 모든 계정을 신뢰                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |     |                   |        |                     |        |                     |
| + test | 모든 호스트의 test 계정을 신뢰                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |     |                   |        |                     |        |                     |
| Web1 + | Web1 호스트의 모든 계정을 신뢰                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |     |                   |        |                     |        |                     |
| 비고     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |     |                   |        |                     |        |                     |



### 1.3.5. finger 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | US3-05 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 설명    | <p>*Finger(사용자정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있으므로, 사용하지 않는다면 해당 서비스를 중지하여야 한다.</p> <p>*Finger(사용자정보 확인 서비스): who 명령어가 현재 사용 중인 사용자들에 대한 간단한 정보만을 보여주는 데 반해 finger 명령은 옵션에 따른 시스템에 등록된 사용자 뿐만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌.</p>                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | <p>양호 - finger 서비스가 비활성화 되어 있는 경우</p> <p>취약 - finger 서비스가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. “/etc/xinetd.d/finger” 파일에서 서비스 비활성화 여부 확인</p> <pre># cat /etc/xinetd.d/finger   grep disable disable                = no</pre> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. /etc/inetd.conf” 파일에서 finger 서비스 라인 #처리(주석처리) 또는 삭제 되어 있는지 확인</p> <pre># cat /etc/inetd.conf   grep finger finger stream tcp nowait bin /usr/sbin/fingerd fingerd</pre> <p>[Solaris 5.10 이상]</p> <p>1. svcs 명령어를 통하여 finger 서비스 활성화 여부 확인</p> <pre># svcs   grep finger</pre> <p>2. inetadm 명령어를 통하여 finger 서비스 활성화 여부 확인</p> <pre># inetadm   grep finger</pre> |       |        |     |   |
| 조치 방법 | <p>설정파일에서 해당 서비스 비활성화</p> <p>[Linux]</p> <p>1. vi 편집기를 이용하여 “/etc/xinetd.d/finger” 파일을 연 후</p> <pre># vi /etc/xinetd.d/finger</pre> <p>2. 아래와 같이 설정 (Disable = yes 설정)</p> <pre>service finger {     socket_type      = stream     wait            = no</pre>                                                                                                                                                                                                                                                                                                   |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> user          = nobody server        = /usr/sbin/in.fingerd disable       = yes } </pre> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/inetd.conf” 파일을 연 후<br/># vi /etc/inetd.conf</li> <li>2. finger 서비스 라인 #처리(주석처리)<br/>#finger stream tcp nowait bin /usr/sbin/fingerd fingerd</li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcadm 명령어를 통하여 finger 서비스 비활성화<br/># svcadm disable svc:/network/finger:default</li> <li>2. inetadm 명령어를 통하여 finger 서비스 비활성화<br/># inetadm -d svc:/network/finger:default</li> </ol> |
| 비고 | <p>※ Utilities for facility control</p> <ul style="list-style-type: none"> <li>- svcs : (svc status)현재 서비스들(데몬서비스)의 상태를 보여줌</li> <li>- svcadm : svc 들을 제어한다. 재시작, 설정변경들이 가능함</li> <li>- inetadm : inetd.conf 를 대신하여 inet 관련 서비스들을 제어함. 데몬서비스중에 network 관련들만 제어가능</li> </ul> <p>※ 솔라리스에서는 kill -HUP 명령으로 데몬을 재시작해도 inetd.conf 수정사항이 적용되지 않음. 반드시 inetconv 명령을 사용해서 갱신해야 적용됨.</p>                                                                                                                                                                                                                                  |

### 1.3.6. r 계열 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | US3-06 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | <p>*'r' command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있는 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 위험이 있다.</p> <p>*'r'command : 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음.</p> <p>*NET Backup : 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.</p>                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - r 계열 서비스(rlogin, rsh, rexec)가 비활성화 되어 있는 경우</p> <p>취약 - r 계열 서비스(rlogin, rsh, rexec)가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인</p> <pre># cat /etc/xinetd.d/rsh</pre> <pre># cat /etc/xinetd.d/rlogin</pre> <pre># cat /etc/xinetd.d/rexec</pre> <p>※ 각 서비스 설정파일에서 “disable = yes”로 되어 있는지 확인</p> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인</p> <pre># cat /etc/inetd.conf   egrep “rsh rlogin rexec” (# 처리 되어 있으면 비활성화)</pre> <p>[Solaris 5.10 이상]</p> <p>1. svcs 명령어를 통하여 r계열 서비스 활성화 여부 확인</p> <pre># svcs   egrep “login rexec shell”</pre> <p>2. inetadm 명령어를 통하여 r계열 서비스 활성화 여부 확인</p> <pre># inetadm   egrep “login rexec shell”</pre> |       |        |     |   |
| 조치 방법 | <p>NET Backup등 특별한 용도로 사용하지 않는다면 해당 서비스 비활성화</p> <p>[Linux]</p> <p>1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 rlogin, rsh, rexec 파일을 연 후</p> <p>2. 아래와 같이 설정 (disable = yes 설정)</p> <ul style="list-style-type: none"> <li>- /etc/xinetd.d/rlogin 파일</li> <li>- /etc/xinetd.d/rsh 파일</li> <li>- /etc/xinetd.d/rexec 파일</li> </ul> <pre>service      rlogin</pre>                                                                                                                                                                                                                                                                                     |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre>{ ... disable          = yes }</pre> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. vi편집기를 이용해서 /etc/inetd.conf 파일을 연 후<br/># vi /etc/inetd.conf</li> <li>2. r계열 서비스 주석 처리<br/>#shellstream tcp nowait root /usr/sbin/in.rshd in.rshd<br/>#shellstream tcp6 nowait root /usr/sbin/in.rshd in.rshd<br/>#loginstream tcp6 nowait root /usr/sbin/in.rlogind in.rlogind<br/>#execstream tcp nowait root /usr/sbin/in.rexecd in.rexecd<br/>#execstream tcp6 nowait root /usr/sbin/in.rexecd in.rexecd</li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcadm 명령어를 통하여 r계열 서비스 비활성화<br/># svcadm disable svc:/network/login:rlogin<br/># svcadm disable svc:/network/rexec:default<br/># svcadm disable svc:/network/shell:default</li> <li>2. inetadm 명령어를 통하여 r계열 서비스 비활성화<br/># inetadm -d svc:/network/login:rlogin<br/># inetadm -d svc:/network/rexec:default<br/># inetadm -d svc:/network/shell:default</li> </ol> |
| 비고 | login, rshell, rexec 서비스는 backup 등의 용도로 종종 사용되며 /etc/hosts.equiv 또는, 각 홈 디렉터리 밑에 있는 .rhosts 파일에 설정 유무를 확인하여 해당 파일이 존재하지 않거나 해당 파일 내에 설정이 없다면 사용하지 않는 것으로 파악                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### 1.3.7. Dos 공격에 취약한 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | US3-07 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 설명    | <p>*Dos(서비스 거부 공격)에 취약한 echo, discard, daytime, chargen 서비스는 취약점이 많이 발표된 불필요한 서비스들로 해당 서비스 사용을 중지하여야 한다. 만약 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 Dos(서비스 거부 공격)의 대상이 될 수 있다.</p> <p>*Dos(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격임. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 진단 기준 | <p>양호 - Dos 공격에 취약한 서비스가 비활성화 되어 있는 경우</p> <p>취약 - Dos 공격에 취약한 서비스가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 점검 방법 | <p>Dos 공격에 취약한 서비스(echo, discard, daytime, chargen)가 활성화 되어 있는지 점검</p> <p>[Linux]</p> <p>1. "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 서비스 비활성화 여부 확인</p> <pre># cat /etc/xinetd.d/echo # cat /etc/xinetd.d/discard # cat /etc/xinetd.d/daytime # cat /etc/xinetd.d/chargen</pre> <p>※ 각 서비스 설정파일에서 “disable = yes”로 되어 있는지 확인</p> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. /etc/inetd.conf 파일에서 echo, discard, daytime, chargen 서비스 비활성화 여부 확인</p> <pre># cat /etc/inetd.conf   egrep "echo discard daytime chargen"</pre> <p>(# 처리 되어 있으면 비활성화)</p> <p>[Solaris 5.10 이상]</p> <p>1. svcs 명령어를 통하여 echo, discard, daytime, chargen 서비스 활성화 여부 확인</p> <pre># svcs   egrep "echo discrd daytime chargen"</pre> <p>2. inetadm 명령어를 통하여 echo, discard, daytime, chargen 서비스 활성화 여부 확인</p> <pre># inetadm   egrep "echo discrd daytime chargen"</pre> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>Dos 공격에 취약한 서비스(echo, discard, daytime, chargen)가 제공되지 않도록 해당 서비스 비활성화</p> <p>[Linux]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 echo, discard, daytime, chargen 파일을 연 후</li> <li>2. 아래와 같이 설정 (disable = yes 설정) <ul style="list-style-type: none"> <li>- /etc/xinetd.d/echo 파일</li> <li>- /etc/xinetd.d/discard 파일</li> <li>- /etc/xinetd.d/daytime 파일</li> <li>- /etc/xinetd.d/chargen 파일</li> </ul> <pre> service      echo { ... disable      = yes } </pre> </li> </ol> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. vi편집기를 이용해서 /etc/inetd.conf 파일을 연 후 <pre> # vi /etc/inetd.conf </pre> </li> <li>2. echo, discard, daytime, chargen 서비스 주석 처리 <pre> #echo      stream  tcp    nowait  root    internal #discard   stream  tcp    nowait  root    internal #chargen   stream  tcp    nowait  root    internal #daytime   stream  tcp    nowait  root    internal #echo      dgram   udp    wait    root    internal #discard   dgram   udp    wait    root    internal #chargen   dgram   udp    wait    root    internal #daytime   dgram   udp    wait    root    internal </pre> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcadm 명령어를 통하여 echo, discard, daytime, chargen 서비스 비활성화 <pre> # svcadm disable svc:/network/chargen:dgram # svcadm disable svc:/network/chargen:stream # svcadm disable svc:/network/daytime:dgram # svcadm disable svc:/network/daytime:stream # svcadm disable svc:/network/discard:dgram # svcadm disable svc:/network/discard:stream # svcadm disable svc:/network/echo:dgram # svcadm disable svc:/network/echo:stream </pre> </li> <li>2. inetadm 명령어를 통하여 echo, discard, daytime, chargen 서비스 비활성화 <pre> # inetadm -d svc:/network/chargen:dgram </pre> </li> </ol> |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                                                                                                                                                                                                                                  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre># inetadm -d svc:/network/chargen:stream # inetadm -d svc:/network/daytime:dgram # inetadm -d svc:/network/daytime:stream # inetadm -d svc:/network/discard:dgram # inetadm -d svc:/network/discard:stream # inetadm -d svc:/network/echo:dgram # inetadm -d svc:/network/echo:stream</pre> |
| 비고 |                                                                                                                                                                                                                                                                                                  |

### 1.3.8. RPC 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | US3-08 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 설명    | <p>*RPC (Remote Procedure Call) 서비스는 분산처리 환경에서 개발을 하는 데 있어 많은 이점을 제공하지만, 아래와 같은 서비스들은 버퍼 오버플로우(Buffer Overflow) 취약성이 다수 존재하여 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 한다.</p> <p>rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.yppupdated, rpc.rquotad, kcms_server, cachefs</p> <p>*RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.</p>                                                                                                                                                                                                         |       |        |     |   |
| 진단 기준 | <p>양호 - 불필요한 RPC 서비스가 비활성화 되어 있는 경우</p> <p>취약 - 불필요한 RPC 서비스가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. "/etc/xinetd.d/" 디렉터리 내 RPC서비스 파일에서 비활성화 여부 확인</p> <pre># cat /etc/xinetd.d/rstatd</pre> <p>... 이하 생략 ...</p> <p>※ 각 서비스 설정파일에서 “disable = yes”로 되어 있는지 확인</p> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. /etc/inetd.conf 파일에서 불필요한 RPC 서비스 비활성화 여부 확인</p> <pre># cat /etc/inetd.conf   grep rpc.cmsd</pre> <p>... 이하 생략 ...</p> <p>[Solaris 5.10 이상]</p> <p>1. svcs 명령어를 통하여 RPC 서비스 활성화여부 확인</p> <pre># svcs   egrep “cms ttbserver sadmin rusers wall...(생략)…”</pre> <p>2. inetadm 명령어를 통하여 echo, discard, daytime, chargen 서비스 활성화여부 확인</p> <pre># inetadm   egrep “cms ttbserver sadmin rusers wall...(생략)…”</pre> |       |        |     |   |
| 조치 방법 | <p>일반적으로 사용하지 않는 RPC 서비스들을 비활성화</p> <p>[Linux]</p> <p>1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내의 불필요한 RPC 서비스 파일을 연 후</p> <p>2. 아래와 같이 설정 (disable = yes 설정)</p> <pre>service finger {     disable          = yes     ... 이하 생략 ...</pre>                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |



|                 | <div data-bbox="379 232 395 255" style="text-align: right;">}</div> <div data-bbox="357 315 1390 1189"> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. vi 편집기를 이용하여 “/etc/inetd.conf” 파일을 연 후</li> <li>2. RPC 서비스 #처리(주석처리) <div data-bbox="379 443 1390 510"> <pre>#rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd ... 생략 ...</pre> </div> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcadm 명령어를 통하여 RPC서비스 비활성화 <div data-bbox="379 656 1098 891"> <pre># svcadm disable svc:/network/rpc/bootparams:default # svcadm disable svc:/network/rpc/spray:default # svcadm disable svc:/network/rpc/cde-ttdbserver:tcp # svcadm disable svc:/network/rpc/rusers:default # svcadm disable svc:/network/rpc/rstat:default ... 생략 ...</pre> </div> </li> <li>2. inetadm 명령어를 통하여 RPC서비스 비활성화 <div data-bbox="379 954 1034 1189"> <pre># inetadm -d svc:/network/rpc/bootparams:default # inetadm -d svc:/network/rpc/spray:default # inetadm -d svc:/network/rpc/cde-ttdbserver:tcp # inetadm -d svc:/network/rpc/rusers:default # inetadm -d svc:/network/rpc/rstat:default ... 생략 ...</pre> </div> </li> </ol> </div> <div data-bbox="373 1256 1442 2067"> <table> <tr> <th colspan="2">불필요한 RPC 서비스</th></tr> <tr> <td>rpc.cmsd</td><td>데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용</td></tr> <tr> <td>rusersd</td><td>rusers 명령의 조회에 응답</td></tr> <tr> <td>rstatd</td><td>커널에서 얻은 성능 통계 리턴</td></tr> <tr> <td>rpc.ttdbserverd</td><td>시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램 지원</td></tr> <tr> <td>kcms_server</td><td>kodak color management 관련된 api 와 라이브러리들은 데스크탑의 디지털 이미지들의 컬러 퍼포먼스를 컨트롤할 수 있는 Profile를 만들거나 관리하기 위해 사용</td></tr> <tr> <td>rpc.ttdbserverd</td><td>RPC 기반의 ToolTalk 데이터베이스 서버 프로그램</td></tr> <tr> <td>Walld</td><td>다른 사용자들에게 메시지 발송</td></tr> <tr> <td>rpc.nids</td><td>NIS+ server Daemon</td></tr> <tr> <td>rpc.yppupdated</td><td>Network Information Services(NIS) 맵 정보 갱신</td></tr> <tr> <td>cachefs</td><td>Cache 파일 시스템 데몬</td></tr> <tr> <td>sadmind</td><td>remote로부터의 시스템 관리</td></tr> </table> </div> | 불필요한 RPC 서비스 |  | rpc.cmsd | 데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용 | rusersd | rusers 명령의 조회에 응답 | rstatd | 커널에서 얻은 성능 통계 리턴 | rpc.ttdbserverd | 시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램 지원 | kcms_server | kodak color management 관련된 api 와 라이브러리들은 데스크탑의 디지털 이미지들의 컬러 퍼포먼스를 컨트롤할 수 있는 Profile를 만들거나 관리하기 위해 사용 | rpc.ttdbserverd | RPC 기반의 ToolTalk 데이터베이스 서버 프로그램 | Walld | 다른 사용자들에게 메시지 발송 | rpc.nids | NIS+ server Daemon | rpc.yppupdated | Network Information Services(NIS) 맵 정보 갱신 | cachefs | Cache 파일 시스템 데몬 | sadmind | remote로부터의 시스템 관리 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--|----------|--------------------------------------------------------------------------|---------|-------------------|--------|------------------|-----------------|---------------------------------------------|-------------|------------------------------------------------------------------------------------------------------|-----------------|---------------------------------|-------|------------------|----------|--------------------|----------------|-------------------------------------------|---------|-----------------|---------|-------------------|
| 불필요한 RPC 서비스    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rpc.cmsd        | 데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rusersd         | rusers 명령의 조회에 응답                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rstatd          | 커널에서 얻은 성능 통계 리턴                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rpc.ttdbserverd | 시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램 지원                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| kcms_server     | kodak color management 관련된 api 와 라이브러리들은 데스크탑의 디지털 이미지들의 컬러 퍼포먼스를 컨트롤할 수 있는 Profile를 만들거나 관리하기 위해 사용                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rpc.ttdbserverd | RPC 기반의 ToolTalk 데이터베이스 서버 프로그램                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| Walld           | 다른 사용자들에게 메시지 발송                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rpc.nids        | NIS+ server Daemon                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| rpc.yppupdated  | Network Information Services(NIS) 맵 정보 갱신                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| cachefs         | Cache 파일 시스템 데몬                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |
| sadmind         | remote로부터의 시스템 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |              |  |          |                                                                          |         |                   |        |                  |                 |                                             |             |                                                                                                      |                 |                                 |       |                  |          |                    |                |                                           |         |                 |         |                   |

|    |             |                                                                 |
|----|-------------|-----------------------------------------------------------------|
|    | sprayd      | 지정된 수의 패킷을 호스트에 전송하고 성능 통계를 보고하는 spray 명령에 의해 전송된 패킷 수신         |
|    | rpc.pcnfsd  | PC-NFS (개인용 컴퓨터 네트워크 파일 시스템) 클라이언트에서의 서비스 요청 처리                 |
|    | rex         | 원격 시스템용 프로그램 실행                                                 |
|    | rpc.rquotad | 리모트 머신에 NFS mount 되고 있는 파일 시스템에 대해 사용자에게 대한 로컬 머신에서의 할당 제한치를 반환 |
| 비고 |             |                                                                 |

### 1.3.9. tftp, talk 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | US3-09 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | 운영체제는 ftp, tftp, telnet, talk 등의 서비스를 포함하고 있으므로 시스템 운영에 필요하지 않는 불필요한 서비스를 제거하여 보안성을 높일 수 있고 해당 불필요한 서비스 취약점 발견으로 인한 피해를 최소화할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - tftp, talk 서비스가 비활성화 되어 있는 경우</p> <p>취약 - tftp, talk 서비스가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <p>1. "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk서비스 파일에서 비활성화 여부 확인</p> <pre># cat /etc/xinetd.d/tftp</pre> <p>... 이하 생략 ...</p> <p>※ 각 서비스 설정파일에서 “disable = yes”로 되어 있는지 확인</p> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. /etc/inetd.conf 파일에서 tftp, talk, ntalk 서비스 비활성화 여부 확인</p> <pre># cat /etc/inetd.conf   egrep "tftp talk "</pre> <pre>tftp  dgram udp6   SRC   nobody /usr/sbin/tftpd          tftpd -n talk  dgram  udp     wait  root   /usr/sbin/talkd           talkd ntalk dgram  udp     wait  root   /usr/sbin/talkd           talkd</pre> <p>[Solaris 5.10 이상]</p> <p>1. /etc/inet/inetd.conf 파일에서 tftp 서비스 비활성화 여부 확인</p> <pre># cat /etc/inet/inetd.conf   egrep "tftp talk"</pre> <pre>tftp  dgram udp6   wait  root   /usr/sbin/in.tftpdin.tftpd -s /tftpboot</pre> <p>2. svcadm 명령어를 통하여 RPC서비스 비활성화</p> <pre># svcadm disable svc:/network/talk:default # svcadm disable svc:/network/tftp/udp6:default</pre> <p>3. inetadm 명령어를 통하여 RPC서비스 비활성화</p> <pre># inetadm -d svc:/network/talk:default # inetadm -d svc:/network/tftp/udp6:default</pre> |       |        |     |   |
| 조치 방법 | <p>[Linux]</p> <p>1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 tftp, talk, ntalk 파일을 연 후</p> <p>2. 아래와 같이 설정 (disable = yes 설정)</p> <ul style="list-style-type: none"> <li>- /etc/xinetd.d/tftp 파일</li> <li>- /etc/xinetd.d/talk 파일</li> <li>- /etc/xinetd.d/ntalk 파일</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> service  tftp {     ... 생략 ...     disable = yes } </pre> <p>[AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>vi 편집기를 이용하여 “/etc/inetd.conf” 파일을 연 후</li> <li>tftp, talk, ntalk 서비스 #처리(주석처리) <pre> #tftp  dgram udp6    SRC    nobody /usr/sbin/tftpd      tftpd -n #talk  dgram  udp     wait   root  /usr/sbin/talkd      talkd #ntalk  dgram  udp     wait   root  /usr/sbin/talkd      talkd </pre> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>svcadm 명령어를 통하여 tftp, talk서비스 비활성화 <pre> # svcadm disable svc:/network/talk:default # svcadm disable svc:/network/tftp/udp6:default </pre> </li> <li>inetadm 명령어를 통하여 tftp, talk서비스 비활성화 <pre> # inetadm -d svc:/network/talk:default # inetadm -d svc:/network/tftp/udp6:default </pre> </li> </ol> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### 1.3.10. NFS 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | US3-10 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | <p>*NFS(Network File System) 서비스는 root 권한 획득을 가능하게 하는 등 침해사고 위험성이 높으므로 사용하지 않는 경우 중지시킨다.</p> <p>*NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | <p>양호 - NFS 서비스 관련 데몬이 비활성화 되어 있는 경우</p> <p>취약 - NFS 서비스 관련 데몬이 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 점검 방법 | <p>사용하지 않는다면 NFS 서비스 중지</p> <p>아래의 방법으로 NFS 서비스를 제거한 후 시스템 부팅 시, 스크립트 실행 방지 가능</p> <ol style="list-style-type: none"> <li>1. /etc/dfs/dfstab의 모든 공유 제거</li> <li>2. NFS 데몬(nfsd, statd, mountd) 중지</li> <li>3. 시동 스크립트 삭제 또는, 스크립트 이름 변경</li> </ol> <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. NFS 데몬 구동 여부 확인</li> </ol> <pre># ps -ef   grep nfsd</pre> <pre>root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd</pre> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcs 명령어를 통하여 NFS 데몬 구동 여부 확인</li> </ol> <pre># svcs -a   grep -i nfs</pre> <pre>disabled May_29 svc:/network/nfs/server:default</pre> |       |        |     |   |
| 조치 방법 | <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. NFS 데몬(nfsd)을 중지</li> </ol> <pre># ps -ef   grep nfsd</pre> <pre>root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd</pre> <pre># kill -9 3809</pre> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. svcadm 명령어를 통하여 NFS 데몬 중지</li> </ol> <pre># svcadm disable svc:/network/nfs/server:default</pre>                                                                                                                                                                                                                                                               |       |        |     |   |
| 비고    | <p>showmount, share, exportfs 등의 명령어를 사용하여 로컬 서버에 마운트 되어 있는 디렉터리 확인 및 NFS 설정파일에 공유디렉터리 설정 여부 확인 후 해당 디렉터리가 존재하지 않을 경우 서비스 중지 가능</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |

### 1.3.11. NFS 접근 통제

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | US3-11 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | NFS와 NIS(Network Information Service) 같은 패키지를 이용하면 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여, 마치 로컬 파일시스템처럼 사용할 수 있다. 따라서 NFS를 사용하지 않는다면 반드시 제거해야 하고, 사용한다면 접근 권한을 설정하여 통제해야 한다                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | 양호 - 공유 디렉터리 권한이 적절하게 설정된 경우<br>취약 - 공유 디렉터리 권한이 적절하게 설정되지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | 임의의 호스트 접근이 제한되어 있는지 확인<br><br>[Linux, AIX, HP-UX]<br>1. everyone으로 시스템이 마운트 되어 있는지 확인<br># showmount -e hostname<br>2. /etc/exports 파일에서 접근 통제 설정 여부 확인<br># cat /etc/exports<br>- 취약한 설정 예 : /var/www/img *(ro,all_squash)<br>- 양호한 설정 예 : /data 172.27.0.0/16(rw,no_root_squash)<br><br>[Solaris]<br>1. /etc/dfs/dfstab 파일에서 접근 통제 설정 여부 확인<br># cat /etc/dfs/dfstab<br>- 취약한 설정 예 : share -F nfs -o rw /export/home/test<br>- 양호한 설정 예 : share -F nfs -o rw=client1:client2 /export/home/test |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX]<br>1. everyone 마운트 제거<br># umount "파일시스템 이름"<br>2. /etc/exports 파일에서 접근 통제 설정<br># vi /etc/exports<br>(예) /data 172.27.0.0/16(rw,no_root_squash)<br><br>[Solaris]<br>1. /etc/dfs/dfstab 파일에서 접근 통제 설정<br># vi /etc/dfs/dfstab<br>(예) share -F nfs -o rw=client1:client2 /export/home/test                                                                                                                                                                                     |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |

### 1.3.12. automount 제거

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | US3-12 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | <p>*automountd 데몬에는 로컬 공격자가 데몬에 *RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하여 이를 통해 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있다.</p> <p>*automountd: 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능을 말함.</p> <p>*RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.</p>                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 진단 기준 | <p>양호 - automount 서비스가 비활성화 되어 있는 경우</p> <p>취약 - automount 서비스가 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. automountd 서비스 데몬 확인</p> <pre># ps -ef   grep auto</pre> <pre>root 186 1 0 9월 07 ? 0:00 /usr/lib/autofs/automountd</pre> <p>[Solaris 5.10 이상]</p> <p>1. automountd 서비스 데몬 확인</p> <pre># svcs -a   grep autofs</pre>                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 조치 방법 | <p>[Linux]</p> <p>1. automountd서비스 데몬 실행 중지</p> <pre># ps -ef   grep auto</pre> <pre>root 650 1 0 9월 07 ? 0:00 /usr/lib/autofs/automountd</pre> <pre># kill -9 650</pre> <p>2. 시스템 재시작시 automount 가 시작되지 않도록 설정</p> <p>&lt;방법1&gt; 부팅스크립트에서 automountd 제거</p> <pre># chkconfig --level 0123456 autofs off</pre> <p>&lt;방법2&gt; 아래와 같이 파일경로 확인 후 파일명 변경</p> <p>(예) # mv /etc/rc2.d/S28autofs /etc/rc2.d/S28autofs.orig</p> <p>[AIX]</p> <p>1. automountd 서비스 데몬 실행 중지</p> <pre># ps -ef   grep automount</pre> <pre>root 650 1 0 3월 30 ? 0:30 /usr/lib/netsvc/fs/automount/automount -f /etc/auto_master</pre> <pre># kill -9 650</pre> <p>2. 시스템 재시작시 automount 가 시작되지 않도록 설정</p> |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre># mv /etc/rc2.d/S74autofs /etc/rc2.d/S74autofs.orig</pre> <p>[HP-UX]</p> <ol style="list-style-type: none"> <li>1. automountd 서비스 데몬 실행 중지 <pre># ps -ef   grep automount</pre> <pre>root 650 1 0 3월 30 ? 0:30 /usr/lib/netsvc/fs/automount/automount -f /etc/auto_master</pre> <pre># kill -9 650</pre> </li> <li>2. 시스템 재시작시 automount 가 시작되지 않도록 설정 <pre># vi /etc/rc.config.d/nfsconf</pre> <p>(수정 전) AUTOFS=1<br/>(수정 후) AUTOFS=0</p> </li> </ol> <p>[Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>1. automountd 서비스 데몬 실행 중지 <pre># ps -ef   grep auto</pre> <pre>root 650 1 0 9월 07 ? 0:00 /usr/lib/autofs/automountd</pre> <pre># kill -9 650</pre> </li> <li>2. 시스템 재시작시 automount 가 시작되지 않도록 아래의 파일들 삭제 또는 파일명 변경 <pre>- /etc/rc2.d/S74autofs</pre> <pre>- /etc/auto_master</pre> <pre>- /etc/auto_home</pre> <p>(예) # mv /etc/rc2.d/S74autofs /etc/rc2.d/S74autofs.orig</p> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>1. automountd 서비스 데몬 실행 중지 <pre># svcadm disable svc:/system/filesystem/autofs:default</pre> </li> <li>2. 시스템 재시작시 automount 가 시작되지 않도록 아래의 파일들 삭제 또는 파일명 변경 <pre>- /etc/rc2.d/S74autofs</pre> <pre>- /etc/auto_master</pre> <pre>- /etc/auto_home</pre> <p>(예) # mv /etc/rc2.d/S74autofs /etc/rc2.d/S74autofs.orig</p> </li> </ol> |
| 비고 | <p>NFS 및 *삼바(Samba) 서비스에서 사용 시 automountd 사용 여부 확인이 필요하며, 적용시 CDROM의 자동 마운트는 이뤄지지 않음 (/etc/auto.*, /etc/auto_* 파일을 확인하여 필요 여부 확인)</p> <p>*삼바(Samba): 서로 다른 운영체제(OS) 간의 자원 공유를 위해 이용하는 서버로 같은 네트워크 내 연결된 PC는 서로 운영체제가 달라도 네트워크로 파일을 주고받을 수 있고 자원을 공유할 수 있음</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



### 1.3.13. Sendmail 버전 점검

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | US3-13 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | Sendmail은 널리 쓰이는 만큼 많은 취약점이 알려져 있어 공격에 목표가 되기 쉬우므로 서버에서 Sendmail을 사용하는 목적을 검토하여 사용할 필요가 없는 경우 서비스를 제거하는 것이 바람직하다. 만일 운영할 필요가 있다면 취약점이 없는 Sendmail 버전을 유지하고 취약점에 대한 패치가 발표되었을 시 빠른 시기에 이를 적용하도록 해야한다. 그렇지 않을 경우 버퍼 오버플로우(Buffer Overflow)의 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 진단 기준 | 양호 - Sendmail 버전을 정기적으로 점검하고, 최신 버전 패치를 했을 경우<br>취약 - Sendmail 버전을 점검하지 않고, 취약한 버전을 사용할 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>Sendmail 프로세스 확인                             <pre># ps -ef   grep sendmail</pre> <p>root 536638 163960 0 Jul 03 - 2:34 sendmail: accepting connections</p> </li> <li>Sendmail 버전 확인                             <pre># cat /etc/mail/sendmail.cf   grep DZ</pre> <p>DZ8.11.0</p> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>Sendmail 프로세스 확인                             <pre># svcs -a   grep sendmail</pre> <p>online 13:17:45 svc:/network/smtp:sendmail</p> </li> <li>Sendmail 버전 확인                             <pre># cat /etc/mail/sendmail.cf   grep DZ</pre> <p>DZ8.13.8</p> </li> </ol> |       |        |     |   |
| 조치 방법 | <p>■ Sendmail을 사용할 경우</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <p>Sendmail의 버전을 확인하고, <a href="http://www.sendmail.org/">http://www.sendmail.org/</a> 또는 각 OS Vender 에서 제공하는 보안 패치를 설치</p> <p>■ Sendmail을 사용하지 않을 경우</p> <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>필요하지 않을 경우 Sendmail 데몬 중지                             <pre># ps -ef   grep sendmail</pre> <p>root 536638 163960 0 Jul 03 - 2:34 sendmail: accepting connections</p> <pre># kill -9 536638</pre> </li> </ol>                                                                                                                                                                                                |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre># stopsrc -s sendmail // AIX에서 Sendmail 중지 명령어</pre> <p>2. 시스템 재시작시 Sendmail이 구동되지 않도록 OS별로 아래와 같이 설정<br/>[Linux, Solaris 5.9 이하]</p> <p>&lt;방법1&gt; 부팅스크립트에서 Sendmail 제거</p> <pre># chkconfig sendmail off //모든 런레벨에서 Sendmail 서비스 중지 # chkconfig --level 2345 sendmail off //런레벨 2~5에서 Sendmail 서비스 중지</pre> <p>&lt;방법2&gt; Sendmail 구동 스크립트 파일명 변경</p> <pre># ls -al /etc/rc*.d/*   grep sendmail //파일 위치 검색 #mv /etc/rc2.d/S88sendmail /etc/rc2.d/S88sendmail.orig //파일명 변경</pre> <p>[AIX]</p> <p>(1) Sendmail 구동 스크립트 파일 위치 검색</p> <pre># ls -al /etc/rc.d/rc*.d/*   grep sendmail</pre> <p>(2) Sendmail 구동 스크립트 파일명 변경</p> <pre># mv /etc/rc2.d/S88sendmail /etc/rc2.d/S88sendmail.orig</pre> <p>(3) /etc/rc.tcpip 파일에서 아래 내용 #처리(주석 처리)</p> <p>(수정 전) start /usr/lib/sendmail "\$src_running" "-bd -q\${qpi}"</p> <p>(수정 후) #start /usr/lib/sendmail "\$src_running" "-bd -q\${qpi}"</p> <p>[HP-UX]</p> <p>(1) Sendmail 구동 스크립트 파일 위치 검색</p> <pre># ls -al /sbin/rc*.d/*   grep sendmail</pre> <p>(2) Sendmail 구동 스크립트 파일명 변경</p> <pre># mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/S540sendmail.orig</pre> <p>(3) /etc/rc.config.d/mailservs 파일에서 SENDMAIL_SERVER 값을 "0"으로 변경<br/>(9.x 이하: /etc/netbsdsrc)</p> <pre>SENDMAIL_SERVER=0</pre> <p>[Solaris 5.10 이상]</p> <p>1. Sendmail 데몬 중지</p> <pre># svcadm disable svc:/network/smtp:sendmail</pre> |
| 비고 | Sendmail 최신 버전 : 8.14.8 (2014년 3월 기준)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### 1.3.14. 인증받지 않은 사용자의 Sendmail q 옵션 사용

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                              | 항목 코드 | US3-14 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | SMTP 서비스 사용시 일반 사용자의 q 옵션을 사용한 Sendmail 실행을 방지하여 메일 큐 내용과 sendmail 설정을 보거나, 메일큐를 강제로 drop 시킬 수 있는 기능을 막아야 한다. 그렇지 않을 경우 비인가자에 의한 SMTP 서비스 오류 발생이 가능하다.                                                                                                                              |       |        |     |   |
| 진단 기준 | 양호 - SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우<br>취약 - 일반 사용자의 Sendmail 실행 방지가 설정되어 있지 않은 경우                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris]<br>1. sendmail.cf 파일에서 restrictqrun 옵션 설정 여부 확인<br># cat /etc/mail/sendmail.cf   grep PrivacyOptions<br>O PrivacyOptions=authwarnings<br><br>※ Restrictqrun 옵션 : sendmail -q 사용을 제한 (root 및 queue 소유자만 접근가능)                                           |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX, Solaris]<br>1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후<br># vi /etc/mail/sendmail.cf<br>2. O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가<br>(수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn<br>(수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                     |       |        |     |   |

### 1.3.15. Sendmail expn, vrfy 명령어 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                             | 항목 코드 | US3-15 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 설명    | <p>SMTP(Simple Mail Transfer Protocol)는 많은 취약성을 갖고 있어 잠재적인 위험이 존재한다. 서버에서 SMTP를 사용하는 목적을 검토하여 사용할 필요가 없는 경우 서비스를 제거해야 하며, SMTP 서비스 운영 시 Sendmail Abuse를 방지하기 위해 Sendmail의 기본적인 서비스인 *VRFY, *EXPN을 막아야 한다.</p> <p>*VRFY: SMTP 클라이언트가 SMTP 서버에 특정 아이디에 대한 메일이 있는지 검증하기 위해 보내는 명령어</p> <p>*EXPN(메일링 리스트 확장): 메일 전송 시 포워딩하기 위한 명령어</p> |       |        |     |   |
| 진단 기준 | <p>양호 - Sendmail 미사용 또는, noexpn, novrfy 옵션이 설정되어 있는 경우</p> <p>취약 - Sendmail을 사용하면서 noexpn, novrfy 옵션이 설정되어 있지 않은 경우</p>                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>1. sendmail.cf 파일에서 expn, vrfy 명령어 제한 여부 확인</p> <pre># cat /etc/mail/sendmail.cf   grep "PrivacyOptions"</pre> <p>O PrivacyOptions=authwarnings,novrfy,noexpn</p>                                                                                                                           |       |        |     |   |
| 조치 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>1. vi 편집기를 이용하여 “/etc/mail/sendmail.cf” 파일을 연 후</p> <pre># vi /etc/mail/sendmail.cf</pre> <p>2. noexpn, novrfy 옵션 추가</p> <p>(수정 전) O PrivacyOptions=authwarnings</p> <p>(수정 후) O PrivacyOptions=authwarnings, noexpn, novrfy</p>                                                            |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |

### 1.3.16. DNS 버전 점검

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | US3-16                       | 중요도 | H            |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|------------------------------|-----|--------------|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                   |       |                              |     |              |
| 설명    | DNS 보안에 관하여 소홀하여 패치를 하지 않는다면 DNS 취약점을 활용한 공격에 노출될 수 있다. 공격자는 조작된 DNS 쿼리를 다량으로 전달하여 DNS 캐시서버의 내용을 임의로 변경할 수 있고, 악성코드가 설치된 임의의 주소 등으로 변경이 가능하기 때문에 DNS 보안에 많은 신경을 써야 한다.                                                                                                                                                                                                                                                       |       |                              |     |              |
| 진단 기준 | 양호 - DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우<br>취약 - DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우                                                                                                                                                                                                                                                                                                                                    |       |                              |     |              |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris 5.9 이하]<br>1. DNS 서비스 사용 및 BIND 버전 확인<br># ps -ef   grep named<br># named -v<br><br>[Solaris 5.10 이상]<br>1. DNS 서비스 구동 여부 확인<br># svcs -a   grep dns                                                                                                                                                                                                                                             |       |                              |     |              |
| 조치 방법 | <p>■ DNS 서비스를 사용할 경우</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <p>“DNS” 서비스 사용 시 BIND 버전 확인 후 최신 버전으로 업데이트</p> <p>■ DNS 서비스를 사용하지 않는 경우</p> <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. 서비스 중지</p> <pre># ps -ef   grep named root 27977      1   0   May 08 ?        0:27 /usr/sbin/in.named # kill -9 27977</pre> <p>[Solaris 5.10 이상]</p> <p>1. 서비스 중지</p> <pre># svcadm disable svc:/network/dns/server:default</pre> |       |                              |     |              |
| 비고    | - 패치를 적용할 경우 시스템 및 서비스의 영향도를 충분히 고려해야 함.<br>- BIND 버전 현황 (2014년 3월 기준)                                                                                                                                                                                                                                                                                                                                                       |       |                              |     |              |
|       | BIND VERSION                                                                                                                                                                                                                                                                                                                                                                                                                 |       | STATUS                       |     | RELEASE DATE |
|       | 9.10.0b2                                                                                                                                                                                                                                                                                                                                                                                                                     |       | Development                  |     | Mar 2014     |
|       | 9.9.5-W1                                                                                                                                                                                                                                                                                                                                                                                                                     |       | Current-Stable, ESV, Windows |     | Feb 2014     |
|       | 9.9.5                                                                                                                                                                                                                                                                                                                                                                                                                        |       | Current-Stable, ESV          |     | Jan 2014     |
|       | 9.8.7-W1                                                                                                                                                                                                                                                                                                                                                                                                                     |       | Windows, Approaching EOL     |     | Feb 2014     |

|  |                                                                                |                                  |          |
|--|--------------------------------------------------------------------------------|----------------------------------|----------|
|  | 9.8.7                                                                          | Approaching EOL                  | Jan 2014 |
|  | 9.6.x – 9.6-ESV-R11-W1                                                         | End-of-Life (EOL) as of Feb 2014 |          |
|  | 9.7.x – 9.7.7                                                                  | Deprecated as of Nov 2012        |          |
|  | ※ <a href="http://www.isc.org/downloads/">http://www.isc.org/downloads/</a> 참조 |                                  |          |

### 1.3.17. DNS recursion 제한 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | US3-17 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | <p>recursion이란 자신의 PC에 설정하여 사용하는 DNS에서, 도메인에 대한 질의를 받아 응답을 찾아가는 과정으로, 도메인에 접속하기 위해 어떤 과정을 거쳐 답을 찾아 오는지에 대한 정보를 설명한다.</p> <p>이러한 recursion이 허용되어 있는 DNS 서버는 DNS cache poisoning 공격에 취약하며, 일종의 증폭기 또는 좀비로 악용되어 특정 시스템 또는 네트워크에 공격할 가능성이 있다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 진단 기준 | <p>양호 - DNS recursion이 제한되어 있는 경우</p> <p>취약 - DNS recursion이 허용되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>&lt;방법1&gt; 설정 파일에서 recursion 설정 여부 확인</p> <p>1. bind 9.2 버전 이하</p> <pre># cat /etc/named.conf   grep recursion</pre> <p>recursion yes;</p> <p>2. bind 9.3 버전 이상</p> <pre># cat /etc/named.caching-nameserver.conf</pre> <p>recursion yes;</p> <p>&lt;방법2&gt; nslookup 명령어를 이용하여, recursion 설정 여부 확인</p> <pre># nslookup www.yahoo.co.kr nis.dacom.co.kr</pre> <p>Server: nis.dacom.co.kr</p> <p>Address: 164.124.101.31#53</p> <p>Non-authoritative answer:</p> <p>*** Can't find www.yahoo.co.kr: No answer</p> <p>위의 질의는 nis.dacom.co.kr DNS 서버에 www.yahoo.co.kr에 대한 정보를 질의한 것으로, 위임권한이 있는 도메인이 아니기 때문에 nis.dacom.co.kr에서 클라이언트가 요구한 응답을 하지 않음</p> <p>&lt;방법3&gt; 아래 사이트에서 DNS서버 IP를 입력하여 DNS서버가 recursion이 허용되어 있는지 여부를 간단히 확인할 수 있음</p> <p><a href="http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl">http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl</a></p> |       |        |     |   |
| 조치 방법 | <p>DNS 설정 파일의 내용을 수정하여 조치.</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <p>&lt;방법1&gt; 설정 파일에서 recursion 제한 설정</p> <p>1. bind 9.2 버전 이하</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre># vi /etc/named.conf   grep recursion recursion no; 2. bind 9.3 버전 이상 # vi /etc/named.caching-nameserver.conf recursion no;</pre> <p>&lt;방법2&gt; 설정 파일에서 특정 IP 대역에 대해서만 recursion을 허용</p> <ul style="list-style-type: none"> <li>- bind 9.2 버전 이하 : /etc/named.conf</li> <li>- bind 9.3 버전 이상 : /etc/named.caching-nameserver.conf</li> </ul> <pre>Options {     allow-recursion {127.0.0.1; 192.168.2.0/24; }; };</pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                               |



### 1.3.18. DNS Zone Transfer 제한 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | US3-18 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 설명    | DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않으므로 적절한 보안 설정을 통하여 도메인 정보 전송을 제한하여야 한다. 만약, DNS 도메인 정보가 외부로 노출될 경우 악의적인 사용자가 해당 정보를 이용하여 홈페이지 및 하위 URL 정보를 입수하여 웹 애플리케이션 구조를 예측할 수 있다.                                                                                                                                                                                                                                                       |       |        |     |   |
| 진단 기준 | 양호 - DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우<br>취약 - DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris]<br>1. 설정 파일에서 zone transfer 설정 확인<br># cat /etc/named.conf<br>Options {<br>allow-transfer{10.10.10.10;};<br>};                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 조치 방법 | DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용한다면 DNS설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정<br><br>[Linux, AIX, HP-UX, Solaris]<br>1. 특정 서버의 Zone Transfer 지정<br># vi /etc/named.conf<br>Options {<br>allow-transfer{10.10.10.111; 10.10.10.112;};<br>};<br>2. 특정 도메인의 Zone에 대해서 제한할 경우에는 다음과 같이 설정<br># vi /etc/named.conf<br>zone "xxx.co.kr" {<br>Type master ;<br>File "db.xxx.co.kr";<br>allow-transfer{10.10.10.111; 10.10.10.112;};<br>} |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |

### 1.3.19. ftp 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | US3-19 | 중요도 | L |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | 기본적인 FTP서비스는 계정과 패스워드가 암호화 되지 않은 채로 전송되며, 간단한 Sniffer 에 의해서도 스니핑이 가능하므로 FTP를 사용 하지 않는 것이 좋다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 진단 기준 | 양호 - ftp 서비스가 비활성화 되어 있는 경우<br>취약 - ftp 서비스가 활성화 되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <ol style="list-style-type: none"> <li>Default ftp 서비스 비활성화 여부 확인<br/> <pre># cat /etc/inetd.conf   grep ftp</pre> <pre>ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a</pre> </li> <li>proftpd 서비스 데몬 확인<br/> <pre># ps -ef   grep proftpd</pre> </li> <li>vsftpd 서비스 데몬 확인<br/> <pre># ps -ef   grep vsftpd</pre> <pre>root      3809      3721      0      08:44:40  ?          0:00</pre> <pre>/usr/sbin/vsftpd/etc/vsftpd/vsftpd.conf</pre> </li> </ol> <p>[Solaris 5.10 이상]</p> <ol style="list-style-type: none"> <li>FTP 서비스 구동 확인<br/> <pre># svcs -a   grep dns</pre> </li> </ol>                                                                                                                                                                                                                         |       |        |     |   |
| 조치 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>■ Default FTP 서비스 중지</p> <ol style="list-style-type: none"> <li>“/etc/inetd.conf” 파일에서 ftp 서비스 라인 #처리(주석처리)<br/>                     (수정 전) <pre>ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a</pre><br/>                     (수정 후) <pre>#ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a</pre> </li> <li>inetd 서비스 재시작<br/> <pre>#ps -ef   grep inetd</pre> <pre>root      141      1      0 15:03:22 ?          0:01 /usr/sbin/inetd -s</pre> <pre>#kill -HUP [PID]</pre> <br/> <pre># refresh -s inetd //AIX에서 inetd 재시작 명령어</pre> <pre># /usr/sbin/inetd -c //HP-UX에서 inetd 재시작 명령어</pre> <pre># inetconv -i /etc/inet/inetd.conf //솔라리스에서 inetd 재시작 명령어</pre> </li> </ol> <p>■ ProFTP 서비스 중지</p> <ol style="list-style-type: none"> <li>proftpd 서비스 데몬 중지<br/> <pre># kill -9 [PID]</pre> </li> </ol> |       |        |     |   |

|    |                                                                                                                                                                                              |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>■ vsFTP 서비스 중지</p> <p>1. vsftpd 서비스 데몬 중지</p> <pre># kill -9 [PID]</pre> <p>[Solaris 5.10]</p> <p>1. svcadm 명령어를 통해 FTP 서비스 비활성화</p> <pre># svcadm disable svc:/network/ftp:default</pre> |
| 비고 |                                                                                                                                                                                              |

### 1.3.20. Anonymous FTP 접근 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | US3-20 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 설명    | Anonymous FTP(익명 FTP)를 사용할 경우 악의적인 사용자가 시스템에 관한 정보를 획득할 수 있으며 디렉터리에 쓰기 권한이 설정되어 있을 경우 local exploit을 사용하여 다양한 공격이 가능하게 되므로 반드시 필요한 사용자만 접속할 수 있도록 설정하여 권한 없는 사용자의 FTP 사용을 제한하여야 한다.                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 진단 기준 | 양호 - Anonymous FTP (익명 ftp) 접속을 차단한 경우<br>취약 - Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris]<br><b>■ Default FTP를 사용하는 경우</b><br>1. /etc/passwd 파일에 ftp 계정 존재 여부 확인<br># cat /etc/passwd   grep ftp<br><br><b>■ ProFTP 를 사용하는 경우</b><br>1. proftpd.conf 파일에서 <Anonymous ~ ftp> 부분 확인<br>※ UserAlias 항목이 주석처리 되어있거나, 없으면 양호<br># cat etc/proftpd/proftpd.conf<br>UserAlias                 anonymous ftp<br><br><b>■ vsFTP를 사용하는 경우</b><br>1. vsftpd.conf 파일에서 anonymous_enable 값이 No로 설정되어 있는지 확인<br># cat etc/vsftpd/vsftpd.conf<br>anonymous_enable = Yes (익명 FTP 허용) |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX, Solaris]<br><b>■ Default FTP를 사용하는 경우</b><br>1. ftp 계정 삭제<br># userdel ftp //Linux, HP-UX, Solaris에서 ftp 계정 삭제<br># rmuser ftp //AIX에서 ftp 계정 삭제<br><br><b>■ proftpd 를 사용하는 경우</b><br>1. proftpd.conf 파일에서 <Anonymous ~ ftp> 부분의 UserAlias 항목 주석("#") 처리<br># cat etc/proftpd/proftpd.conf<br>#UserAlias                 anonymous ftp<br><br><b>■ vsftpd 를 사용하는 경우</b><br>1. vsftpd.conf 파일에서 anonymous_enable 값을 No 로 설정<br># vi etc/vsftpd/vsftpd.conf<br>anonymous_enable = No  |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |

### 1.3.21. root 및 불필요한 계정의 ftp 접근 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | US3-21 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | FTP 서비스는 아이디 및 비밀번호가 암호화되지 않은 채로 전송되어 간단한 스니퍼에 의해서도 아이디 및 비밀번호가 노출될 수 있으므로 반드시 필요한 경우를 제외하고는 FTP 서비스 사용을 제한하여야 한다. 불가피하게 FTP 서비스를 사용하여야 하는 경우 root 계정의 직접 접속을 제한하여 root 계정의 비밀번호 정보가 노출되지 않도록 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 진단 기준 | <p>양호 - FTP 서비스가 비활성화 되어 있거나, 활성화 시 root 및 불필요한 계정 접속을 차단한 경우</p> <p>취약 - FTP 서비스가 활성화 되어 있고, root 및 불필요한 계정 접속을 허용한 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>■ Default FTP를 사용하는 경우</p> <p>1. 아래와 같이 ftp에 대한 root 계정으로의 접속 제한 설정 확인</p> <pre># cat /etc/ftpusers (또는 /etc/ftpd/ftpusers)</pre> <p>root</p> <p>■ ProFTP 를 사용하는 경우</p> <p>1. 설정파일에서 root계정 접속 제한 설정 확인</p> <pre># cat /etc/proftpd.conf</pre> <p>RootLogin off 또는 해당 설정 없음</p> <p>■ vsFTP를 사용하는 경우</p> <p>1. 아래와 같이 ftp에 대한 root 계정으로의 접속 제한 설정 확인</p> <pre># cat /etc/vsftp/ftpusers (또는 /etc/vsftpd.ftpusers)</pre> <pre># cat vsftpd.userlist</pre> <p>root</p> <p>※ vsFTP를 사용할 경우 FTP 접근제어 파일</p> <p>(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist<br/>(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)</p> <p>(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers<br/>(ftpusers 파일에 등록된 계정들만 접속이 차단됨)</p> |       |        |     |   |
| 조치 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>■ Default FTP를 사용하는 경우</p> <p>1. vi 편집기를 이용하여 ftpusers 파일을 연 후<br/>("/etc/ftpusers" 또는, "/etc/ftpd/ftpusers")<br/>#vi /etc/ftpusers 또는, /etc/ftpd/ftpusers</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>2. root 계정 추가 또는, 주석제거<br/>(수정 전) #root 또는, root 계정 미등록<br/>(수정 후) root</p> <p>■ ProFTP 를 사용하는 경우</p> <p>1. vi 편집기를 이용하여 proftpd 설정파일("/etc/proftpd.conf")을 연 후<br/>#vi /etc/proftpd.conf</p> <p>2. RootLogin off 설정 또는 RootLogin 라인 삭제<br/>RootLogin off</p> <p>■ vsFTP를 사용하는 경우</p> <p>1. vi 편집기를 이용하여 ftpusers 파일을 연 후<br/># vi /etc/vsftp/ftpusers (또는 /etc/vsftpd.ftpusers)<br/># vi vsftpd.userlist</p> <p>2. root 계정 추가 또는, 주석제거<br/>root</p> <p>※ vsFTP를 사용할 경우 FTP 접근제어 파일</p> <p>(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist<br/>(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)</p> <p>(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers<br/>(ftpusers 파일에 등록된 계정들만 접속이 차단됨)</p> |
| 비고 | 애플리케이션에서 root로 바로 접속하여 ftp를 사용하고 있을 경우 확인 필요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### 1.3.22. SNMP 서비스 비활성화

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | US3-22 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 설명    | <p>*SNMP(Simple Network Management Protocol)서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스 이다. SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발생할 수 있으므로 SNMP 서비스를 사용하지 않을 경우 중지시킨다.</p> <p>*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.</p>                                                                                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - SNMP 서비스를 사용하지 않는 경우<br/>취약 - SNMP 서비스를 사용하는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris 5.9 이하]</p> <p>1. SNMP 서비스가 구동 여부 확인</p> <pre># ps -ef   grep snmp root 229412 163960 0 Jul 03 - 4:11 /usr/sbin/snmpd</pre> <p>[Solaris 5.10 이상]</p> <p>1. SNMP 서비스가 구동 여부 확인</p> <pre># svcs -a   grep snmp online 13:27:56 svc:/application/management/snmpdx:default</pre>                                                                                                                                     |       |        |     |   |
| 조치 방법 | <p>[Linux]</p> <p>1. SNMP 서비스 중지</p> <pre># ps -ef   grep snmp root 247 1 0 Oct 01 ? 0:00 /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf # kill -9 247</pre> <p>2. 프로세스 시작 스크립트 변경</p> <p>※ ls -al /etc/rc*.d/*   grep snmp 로 검색하여 위치 확인 후 이름 변경</p> <pre># mv /etc/rc3.d /S76snmpdx /etc/rc3.d /S76snmpdx.orig</pre> <p>[AIX]</p> <p>1. SNMP 서비스 중지</p> <pre># stopsrc -s dpid2 # stopsrc -s snmpmibd # stopsrc -s hostmibd # stopsrc -s snmpd</pre> |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>또는</p> <pre># /usr/sbin/snmpd stop</pre> <p>2. 시스템 재시작시 자동 실행 방지를 위해 아래와 같은 라인 #처리(주석처리)</p> <pre># vi /etc/rc.tcpip #start /usr/sbin/snmpd "\$src_running" #start /usr/sbin/hostmibd "\$src_running" #start /usr/sbin/snmpmibd "\$src_running" #start /usr/sbin/dpid2 "\$src_running"</pre> <p>[HP-UX]</p> <p>1. SNMP 서비스 중지</p> <pre># /sbin/init.d/SnmpMaster stop</pre> <p>2. 다음 파일에서 SNMP 관련 값을 0으로 변경</p> <pre>/etc/rc.config.d/SnmpHpunix → SNMP_HPUNIX_START=0 /etc/rc.config.d/SnmpMaster → SNMP_MASTER_START=0 /etc/rc.config.d/SnmpMib2 → SNMP_MIB2_START=0 /etc/rc.config.d/SnmpTrpDst → SNMP_TRAPDEST_START=0</pre> <p>[Solaris 5.9 이하]</p> <p>1. SNMP 서비스 중지</p> <pre># /etc/init.d/init.dmi stop # /etc/init.d/init.sma stop # /etc/init.d/init.snmpdx stop</pre> <p>2. 프로세스 시작 스크립트 파일 실행권한 제거</p> <pre># chmod a-x /etc/init.d/init.dmi # chmod a-x /etc/init.d/init.sma # chmod a-x /etc/init.d/init.snmpdx</pre> <p>3. /etc/rc3.d 디렉터리에 존재하는 심볼릭 링크파일 제거</p> <pre># cd /etc/rc3.d # rm S76snmpdx # rm S77dmi # rm S82initsma</pre> <p>[Solaris 5.10 이상]</p> <p>1. svcadm 명령어를 통해 SNMP 서비스 중지</p> <pre># svcadm disable svc:/application/management/snmpdx</pre> |
| 비고 | <p>NMS 에서 서버를 모니터링 하는 경우 SNMP 를 사용하며 기타 SNMP를 사용할 경우 Community String 변경 시 통신하고자 하는 Server/Client에 모두 같은 Community String 을 사용해야 함.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



### 1.3.23. SNMP Default Community String 변경

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | US3-23 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | <p>*SNMP(Simple Network Management Protocol) 서비스는 시스템 상태를 실시간으로 파악하는 *NMS(Network Management System)를 위하여 UNIX 시스템에서 기본적으로 제공하는 서비스이며 정보를 받기 위해 일종의 패스워드인 Community String을 사용한다. *Community String은 Default로 public, private으로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 시스템의 주요 정보 및 설정을 파악할 수 있다.</p> <p>*SNMP(Simple Network Management Protocol):TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.</p> <p>*NMS(Network Management System): 네트워크상의 모든 장비의 중앙 감시 체제를 구축하여 모니터링, 플래닝, 분석을 시행하고 관련 데이터를 보관하여 필요 즉시 활용 가능하게 하는 관리 시스템을 말함.</p> <p>*Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비밀번호인 'Community String'을 사용함.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - SNMP Community 이름이 public, private 이 아닌 경우<br/> 취약 - SNMP Community 이름이 public, private 인 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | <p>[Linux, AIX, HP-UX, Solaris]</p> <p>1. snmpd.conf 파일에서 Default Community String 값 사용 여부 확인</p> <pre># cat /etc/snmp/conf/snmpd.conf read-community public</pre> <p>※ snmpd.conf 기본 파일 위치</p> <ul style="list-style-type: none"> <li>- Linux : /etc/snmp/snmpd.conf</li> <li>- AIX : /etc/snmpd.conf</li> <li>- HP-UX : /etc/SnmpAgent.d/snmpd.conf</li> <li>- Solaris : /etc/snmp/conf/snmpd.conf</li> </ul>                                                                                                                                                                                                                                                   |       |        |     |   |
| 조치 방법 | <p>SNMP 설정 파일에서 community name을 기본값인 public이 아닌 추측 불가능한 다른 이름으로 변경</p> <p>[Linux, AIX, HP-UX, Solaris]</p> <pre># vi /etc/snmp/conf/snmpd.conf read-community &lt;추측하기 어려운 값&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |

### 1.3.24. 서비스 배너설정 및 불필요한 OS 정보 제거

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | US3-24 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | 서비스 접속 시에 나오는 Default banner는 시스템 OS버전 및 각 서비스 데몬의 버전 등 불필요한 정보를 제공한다. 이러한 불필요한 정보는 가능한 제공하지 말아야 하며, 불법접근을 경고하는 메시지를 제공하여 악의적인 공격 의도를 사전에 경고하는 것이 좋다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 진단 기준 | 양호 - 배너에 O/S 및 버전 정보가 제거되어 있는 경우<br>취약 - 배너에 O/S 및 버전 정보가 제거되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | <p>[Linux]</p> <ol style="list-style-type: none"> <li>1. /etc/issue(또는 /etc/issue.net) 파일 설정 확인<br/>                         # cat /etc/issue (또는 /etc/issue.net)<br/>                         BANNER="배너 내용"</li> <li>2. /etc/motd 파일 설정 확인<br/>                         # cat /etc/motd<br/>                         "배너 내용"</li> <li>3. FTP 배너 설정 확인<br/>                         # cat /etc/vsftpd/vsftpd.conf<br/>                         ftpd_banner= "배너 내용"</li> <li>4. Sendmail 배너 설정 확인<br/>                         # cat /etc/mail/sendmail.cf<br/>                         O SmtgGreetingMessage= \$j Sendmail \$v/\$Z; \$b (Default 값)</li> </ol> <p>[AIX]</p> <ol style="list-style-type: none"> <li>1. /etc/issue(또는 /etc/issue.net) 파일 설정 확인<br/>                         # cat /etc/issue (또는 /etc/issue.net)<br/>                         BANNER="배너 내용"</li> <li>2. /etc/motd 파일 설정 확인<br/>                         # cat /etc/motd<br/>                         "배너 내용"</li> <li>3. telnet 배너 설정 확인<br/>                         # cat /etc/security/login.cf<br/>                         Default :<br/>                         herald="배너 내용"</li> <li>4. FTP 배너 설정 확인<br/>                         ※ FTP는 기존 시스템에 설치된 환경에 따라 ftpd.cat 파일의 위치가 다를 수 있으니, Find를 통해 먼저 ftpd.cat 파일을 검색하여 찾은 후 버전정보를 표시하는 %s 문구를 확인<br/>                         # find /usr -name "ftpd.cat"<br/>                         # cat ftpd.cat</li> </ol> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>"(%s) FTP server (%s) ready."</p> <p>5. Sendmail 배너 설정 확인</p> <pre># cat /etc/mail/sendmail.cf</pre> <p>O SmtgGreetingMessage= \$j Sendmail \$v/\$Z: \$b (Default 값)</p> <p>[HP-UX]</p> <p>1. /etc/issue(또는 /etc/issue.net 파일 설정 확인</p> <pre># cat /etc/issue (또는 /etc/issue.net)</pre> <p>BANNER="배너 내용"</p> <p>2. /etc/motd 파일 설정 확인</p> <pre># cat /etc/motd</pre> <p>"배너 내용"</p> <p>3. FTP 배너 설정 확인</p> <p>&lt;wu-ftpd v2.4 미만&gt;</p> <pre># cat /etc/ftpd/ftpaccess</pre> <p>suppresshostname yes</p> <p>suppressversion yes</p> <p>banner /etc/ftpd/ftp_banner</p> <p>&lt;wu-ftpd v2.4 이상&gt;</p> <pre># cat /etc/ftpd/ftpaccess</pre> <p>greeting terse</p> <p>4. Sendmail 배너 설정 확인</p> <pre># cat /etc/mail/sendmail.cf</pre> <p>O SmtgGreetingMessage= \$j Sendmail \$v/\$Z: \$b (Default 값)</p> <p>[Solaris]</p> <p>1. /etc/issue(또는 /etc/issue.net 파일 설정 확인</p> <pre># cat /etc/issue (또는 /etc/issue.net)</pre> <p>BANNER="배너 내용"</p> <p>2. /etc/motd 파일 설정 확인</p> <pre># cat /etc/motd</pre> <p>"배너 내용"</p> <p>3. telnet 배너 설정 확인</p> <pre># cat /etc/default/telnetd</pre> <p>BANNER="배너 내용"</p> <p>4. FTP 배너 설정 확인</p> <pre># cat /etc/default/ftpd</pre> <p>BANNER="배너 내용"</p> <p>5. Sendmail 배너 설정 확인</p> <pre># cat /etc/mail/sendmail.cf</pre> <p>O SmtgGreetingMessage= \$j Sendmail \$v/\$Z: \$b (Default 값)</p> |
| 조치 방법 | 각 서비스 banner에 불필요한 정보가 포함되지 않도록 설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>[Linux]</p> <ol style="list-style-type: none"> <li>1. /etc/issue(또는 /etc/issue.net) 파일 설정<br/> # vi /etc/issue (또는 /etc/issue.net)<br/> BANNER="Authorized users only. All activity may be monitored and reported."</li> <li>2. /etc/motd 파일 설정<br/> # vi /etc/motd<br/> "Authorized users only. All activity may be monitored and reported."</li> <li>3. FTP 배너 설정 확인<br/> # vi /etc/vsftpd/vsftpd.conf<br/> ftpd_banner= "Authorized users only. All activity may be monitored and reported."</li> <li>4. Sendmail 배너 설정<br/> # vi /etc/mail/sendmail.cf<br/> (수정 전) O SmtgGreetingMessage=\$j Sendmail \$v/\$Z: \$b<br/> (수정 후) O SmtgGreetingMessage=WARNING:Authorized use only</li> </ol> <p>[AIX]</p> <ol style="list-style-type: none"> <li>1. /etc/issue(또는 /etc/issue.net) 파일 설정<br/> # vi /etc/issue (또는 /etc/issue.net)<br/> BANNER="Authorized users only. All activity may be monitored and reported."</li> <li>2. /etc/motd 파일 설정<br/> # vi /etc/motd<br/> "Authorized users only. All activity may be monitored and reported."</li> <li>3. telnet 배너 설정<br/> ※ /etc/security/login.cf 파일의 default: 라인 끝에 herald = "Wn Authorized users only. Wn login: " 추가<br/> # vi /etc/security/login.cf<br/> default:<br/> ... 생략 ...<br/> herald = "Wn Authorized users only. Wn login: "</li> <li>4. FTP 배너 설정<br/> #dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat &gt; /tmp/ftpd.msg<br/> // cat파일은 수정 할 수 없기 때문에 임시 msg 파일로 변경<br/> #vi /tmp/tfpd.msg // 9번째 줄을 아래와 같이 수정(%s 제거)<br/> (수정 전) "(%s) FTP server (%s) ready. "<br/> (수정 후) FTP Server (Unauthorized Access Prohibited.) ready<br/> #gencat /tmp/ftpd.cat /tmp/ftpd.msg<br/> #cp -p /tmp/ftpd.cat /usr/lib/nls/msg/en_US/ftpd.cat</li> <li>5. Sendmail 배너 설정<br/> # vi /etc/mail/sendmail.cf<br/> (수정 전) O SmtgGreetingMessage=\$j Sendmail \$v/\$Z: \$b<br/> (수정 후) O SmtgGreetingMessage=WARNING:Authorized use only</li> </ol> <p>[HP-UX]</p> |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>1. /etc/issue(또는 /etc/issue.net) 파일 설정<br/> # vi /etc/issue (또는 /etc/issue.net)<br/> BANNER="Authorized users only. All activity may be monitored and reported."</p> <p>2. /etc/motd 파일 설정<br/> # vi /etc/motd<br/> "Authorized users only. All activity may be monitored and reported."</p> <p>3. FTP 배너 설정<br/> # vi /etc/inetd.conf에 다음 내용 추가<br/> ftp stream tcp nowait root /usr/sbin/ftpd ftpd -a<br/> /etc/ftpd/ftppaccess<br/> (-a : 뒤에 따라오는 설정파일을 사용하겠다는 옵션)<br/> &lt;wu-ftpd v2.4 미만&gt;<br/> # vi /etc/ftpd/ftppaccess<br/> suppresshostname yes // hostname 숨김<br/> suppressversion yes // version 정보 숨김<br/> banner /etc/ftpd/ftp_banner // FTP 배너가 작성된 파일<br/> &lt;wu-ftpd v2.4 이상&gt;<br/> # vi /etc/ftpd/ftppaccess<br/> greeting terse // hostname 및 version 정보숨김</p> <p>4. Sendmail 배너 설정<br/> # vi /etc/mail/sendmail.cf<br/> (수정 전) O SmtgGreetingMessage=\$j Sendmail \$v/\$Z: \$b<br/> (수정 후) O SmtgGreetingMessage=WARNING:Authorized use only</p> <p>[Solaris]</p> <p>1. /etc/issue(또는 /etc/issue.net) 파일 설정<br/> # vi /etc/issue (또는 /etc/issue.net)<br/> BANNER="Authorized users only. All activity may be monitored and reported."</p> <p>2. /etc/motd 파일 설정<br/> # vi /etc/motd<br/> "Authorized users only. All activity may be monitored and reported."</p> <p>3. telnet 배너 설정<br/> # vi /etc/default/telnetd<br/> BANNER="Authorized users only .All activity may be monitored and reported."</p> <p>4. FTP 배너 설정 확인<br/> # vi /etc/default/ftpd<br/> BANNER="Authorized users only .All activity may be monitored and reported."</p> <p>5. Sendmail 배너 설정<br/> # vi /etc/mail/sendmail.cf<br/> (수정 전) O SmtgGreetingMessage=\$j Sendmail \$v/\$Z: \$b<br/> (수정 후) O SmtgGreetingMessage=WARNING:Authorized use only</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 1.4. 로그 및 패치관리

### 1.4.1. 최신 보안패치 및 벤더 권고사항 적용

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                               | 항목 코드 | US4-01 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                              |       |        |     |   |
| 설명    | 주기적인 패치 적용을 통하여 보안성 및 시스템 안전성을 확보하는 것이 시스템 운용의 중요한 요소이다. 서비스 중인 시스템의 경우 패치 적용에 따르는 문제점(현재 운용 중인 응용프로그램의 예기치 않은 중지, 패치 자체의 버그 등)과 재부팅의 어려움 등으로 많은 패치를 적용하는 것이 매우 어렵기 때문에 패치 적용시 많은 부분을 고려하여야 한다.                                         |       |        |     |   |
| 진단 기준 | 양호 - 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우<br>취약 - 패치 적용 정책을 수립하지 않고 주기적으로 패치관리를 하지 않는 경우                                                                                                                                                 |       |        |     |   |
| 점검 방법 | [Linux, AIX, HP-UX, Solaris]<br>인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인                                                                                                                                                                            |       |        |     |   |
| 조치 방법 | [Linux, AIX, HP-UX, Solaris]<br>※ 설정 기준 권고 (또는 정책기준)<br>1. 보안 취약점이 발표되면 시스템 영향도를 평가하고, 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응하는 것이 좋다.<br>2. 패치를 수행할 시 시스템의 영향도에 따라 패치를 차등 수행하도록 한다.<br>3. 시스템 운영에 영향을 주지 않는 범위 내에서 주기적으로 패치를 수행할 것을 권고함. |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                         |       |        |     |   |

## 1.4.2. 로그 기록 설정

| 분류     | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드                          | US4-02 | 중요도 | H |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------|-----|---|--------|--|-----|----|------|----------------------------|----------|------------------------------|------|-----------------------|--------|--------------------------------|------|-------------|-----|-----------------------|------|------------------|------|-------------------------|--------|-------------------------|------|-----------------|------|--------------|--------|-------------|----------|--|-----|----|-------|--------------------|------|-------------------------------|--------|------------------------|-------|-----------|
| 대상     | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| 설명     | 시스템의 가용성 및 무결성 등을 침해하는 사건이 발생할 경우, 일반적으로 super user 권한으로 사건이 진행되기 때문에 su의 로그기록이 필요하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| 진단 기준  | 양호 - 로그 기록 정책이 정책에 따라 설정되어 수립되어 있는 경우<br>취약 - 로그 기록 정책 미수립, 또는 정책에 따라 설정되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| 점검 방법  | [Linux, AIX, HP-UX, Solaris]<br>/etc/(r)syslog.conf 파일에 info 및 alert 등에 대해 적절히 기록하도록 설정되어 있는지 점검                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| 조치 방법  | [Linux, AIX, HP-UX, Solaris]<br>1. /etc/(r)syslog.conf 에서 다음과 같이 설정한다.<br>(설정 예)<br><div>mail.debug        /var/log/maillog<br/>*.info            /var/log/messages<br/>*.alert           /var/log/messages<br/>*.alert           /dev/console<br/>*.alert           root<br/>*.emerg           *</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | <table><tr><th colspan="2">메시지 종류</th></tr><tr><th>메시지</th><th>설명</th></tr><tr><td>auth</td><td>로그인 등의 인증 프로그램 유형이 발생한 메시지</td></tr><tr><td>authpriv</td><td>개인 인증을 요구하는 프로그램 유형이 발생한 메시지</td></tr><tr><td>cron</td><td>cron, at 데몬에서 발생한 메시지</td></tr><tr><td>daemon</td><td>telnet, ftpd 등과 같은 데몬이 발생한 메시지</td></tr><tr><td>kern</td><td>커널이 발생한 메시지</td></tr><tr><td>lpr</td><td>프린터 유형의 프로그램이 발생한 메시지</td></tr><tr><td>mail</td><td>메일 시스템에서 발생한 메시지</td></tr><tr><td>news</td><td>유즈넷 뉴스 프로그램 유형이 발생한 메시지</td></tr><tr><td>syslog</td><td>syslog 프로그램 유형이 발생한 메시지</td></tr><tr><td>user</td><td>사용자 프로세스 관련 메시지</td></tr><tr><td>uucp</td><td>시스템이 발생한 메시지</td></tr><tr><td>local0</td><td>여분으로 남겨둔 유형</td></tr></table> <table><tr><th colspan="2">메시지 우선순위</th></tr><tr><th>메시지</th><th>설명</th></tr><tr><td>alert</td><td>즉각적으로 조치를 취해야 할 상황</td></tr><tr><td>crit</td><td>급한 상황은 아니지만, 치명적인 시스템 문제 발생 시</td></tr><tr><td>deberg</td><td>프로그램 실행 시 발생하는 오류 발생 시</td></tr><tr><td>emerg</td><td>매우 위험한 상황</td></tr></table> |                                |        |     |   | 메시지 종류 |  | 메시지 | 설명 | auth | 로그인 등의 인증 프로그램 유형이 발생한 메시지 | authpriv | 개인 인증을 요구하는 프로그램 유형이 발생한 메시지 | cron | cron, at 데몬에서 발생한 메시지 | daemon | telnet, ftpd 등과 같은 데몬이 발생한 메시지 | kern | 커널이 발생한 메시지 | lpr | 프린터 유형의 프로그램이 발생한 메시지 | mail | 메일 시스템에서 발생한 메시지 | news | 유즈넷 뉴스 프로그램 유형이 발생한 메시지 | syslog | syslog 프로그램 유형이 발생한 메시지 | user | 사용자 프로세스 관련 메시지 | uucp | 시스템이 발생한 메시지 | local0 | 여분으로 남겨둔 유형 | 메시지 우선순위 |  | 메시지 | 설명 | alert | 즉각적으로 조치를 취해야 할 상황 | crit | 급한 상황은 아니지만, 치명적인 시스템 문제 발생 시 | deberg | 프로그램 실행 시 발생하는 오류 발생 시 | emerg | 매우 위험한 상황 |
|        | 메시지 종류                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | 메시지                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 설명                             |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | auth                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 로그인 등의 인증 프로그램 유형이 발생한 메시지     |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | authpriv                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 개인 인증을 요구하는 프로그램 유형이 발생한 메시지   |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | cron                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | cron, at 데몬에서 발생한 메시지          |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | daemon                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | telnet, ftpd 등과 같은 데몬이 발생한 메시지 |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | kern                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 커널이 발생한 메시지                    |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | lpr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 프린터 유형의 프로그램이 발생한 메시지          |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | mail                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 메일 시스템에서 발생한 메시지               |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | news                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 유즈넷 뉴스 프로그램 유형이 발생한 메시지        |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | syslog                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | syslog 프로그램 유형이 발생한 메시지        |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | user                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 사용자 프로세스 관련 메시지                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | uucp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 시스템이 발생한 메시지                   |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | local0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 여분으로 남겨둔 유형                    |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | 메시지 우선순위                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | 메시지                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 설명                             |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | alert                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 즉각적으로 조치를 취해야 할 상황             |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
|        | crit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 급한 상황은 아니지만, 치명적인 시스템 문제 발생 시  |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| deberg | 프로그램 실행 시 발생하는 오류 발생 시                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |
| emerg  | 매우 위험한 상황                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                |        |     |   |        |  |     |    |      |                            |          |                              |      |                       |        |                                |      |             |     |                       |      |                  |      |                         |        |                         |      |                 |      |              |        |             |          |  |     |    |       |                    |      |                               |        |                        |       |           |

|    |                                                                                          |                     |
|----|------------------------------------------------------------------------------------------|---------------------|
|    | err                                                                                      | 에러 발생 시             |
|    | info                                                                                     | 단순한 프로그램에 대한 정보 메시지 |
|    | notice                                                                                   | 에러가 아닌 알림에 관한 메시지   |
|    | warning                                                                                  | 주의를 요하는 메시지         |
| 비고 | 위에 제시한 모든 로그설정을 강제화할 경우, 시스템 퍼포먼스로 로그 저장에 따른 서버 용량 문제가 발생할 수 있으므로 시스템 운영 환경과 특성을 고려하여 적용 |                     |



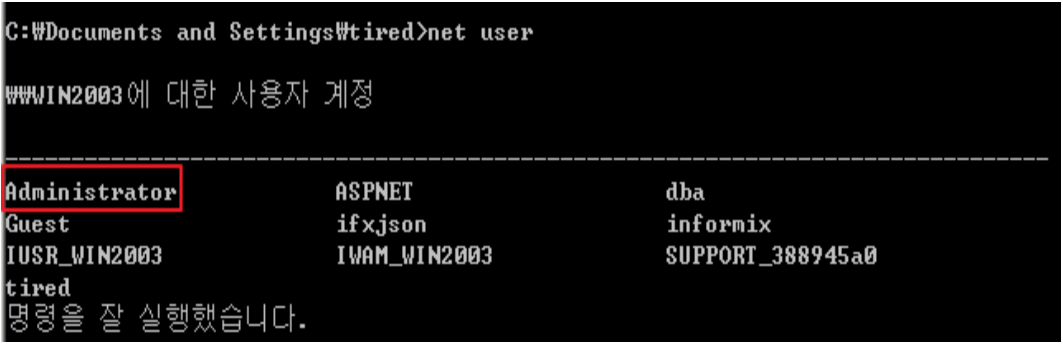
### 1.4.3. 로그의 정기적 검토 및 보고

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | US4-03 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Linux, AIX, HP-UX, Solaris                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | 로그 정보는 침해사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 정기적인 로그 분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있다.                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | <p>양호 - 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지고 있는 경우</p> <p>취약 - 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우</p>                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | 인터뷰를 통해 정기적인 로그 분석에 대한 결과물 확인                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 조치 방법 | <p>※ 로그파일에는 해킹의 흔적들이 남겨져 있을 수 있으므로, 다음과 같이 로그 파일의 백업에 대한 검토를 해야 함.</p> <ol style="list-style-type: none"> <li>1. su 시도에 관한 로그</li> <li>2. 반복적인 로그인 실패에 관한 로그</li> <li>3. 로그인 거부 메시지에 관한 로그</li> <li>4. 기본적 log 파일의 위치는 /var/adm, /var/log</li> </ol> <p>※ 커널과 시스템에 관련된 로그 메시지들은 syslogd와 klogd 두개의 데몬에 의해서 /var/log/messages에 기록하게 됨. 이 파일을 분석함으로써 시스템을 항상 점검 관리해야 함.</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |

## 2. Windows 시스템 취약성 점검항목 및 가이드

### 2.1. 계정 관리

#### 2.1.1. Administrator 계정 이름 바꾸기

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | WS1-01 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 설명    | <p>관리자 계정으로 설정 되어 있는 "Administrator" 계정을 다른 이름으로 바꾸고 "Administrator" 라는 가짜 계정을 만들어 아무런 권한도 주지 않는 방법을 사용할 수 있는데, 이러한 방법은 "모호함을 통한 보안(Security through obscurity)"의 한 예이다. 즉, Bogus 계정을 만드는 것이다.</p> <p>Administrator 계정은 로그인 시 몇 번이고 실패해도 절대 접속을 차단하지 않기 때문에 시스템을 공격하려는 사람들은 이 계정의 패스워드 유추를 계속 시도할 수 있다. 따라서 관리자 계정의 이름을 바꿈으로써 공격자는 패스워드뿐만 아니라 계정이름도 유추하여야 하는 어려움을 줄 수 있다. 또 하나의 방법은 보안정책 설정에서 로그인 실패 횟수에 따른 계정 잠금을 설정하여 brute force 공격이나 사전공격에 대응할 수 있다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - Administrators 그룹에 관리자 계정이 하나만 존재 할 경우</p> <p>취약 - 두 개 이상 존재할 경우</p>                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 점검 방법 | <p>Administrator 계정명 존재 유무 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net user 명령어 실행 후 Administrator 계정명 존재 유무 확인</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; "계정: Administrator 계정 이름 바꾸기" 의 값을 확인</p>                                                                   |       |        |     |   |
| 조치 방법 | <p>불필요한 Administrators 그룹에 포함된 계정을 Administrators 그룹에서 제거하고 다른 그룹에 넣어준다.</p> <p>Administrator 계정을 관리자 계정이 아닌 일반 계정으로 사용하거나, 또는 Administrator가 아닌 다른 이름의 관리자 계정을 생성해 사용하도록 해야 하며, Administrator 권한을 가지는 유저는 최소한의 숫자로 제한 되어야 한다. 또한 Password는 최소 8자리 이상으로 숫자와 영어, 특수문자를 혼합하여 설정한다.</p>                                                                                                                                                                         |       |        |     |   |

[Win2003, Win2008]

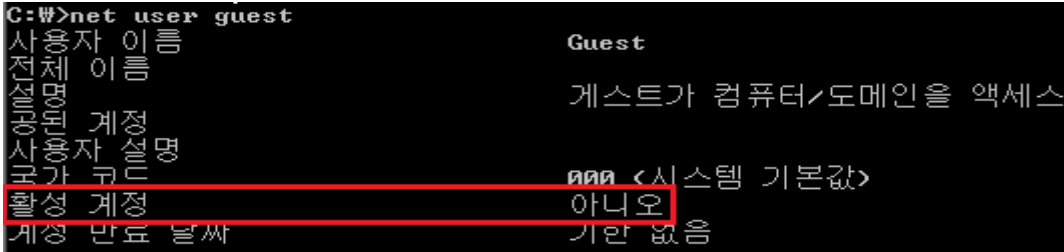
■ 로컬 보안 정책에서 변경

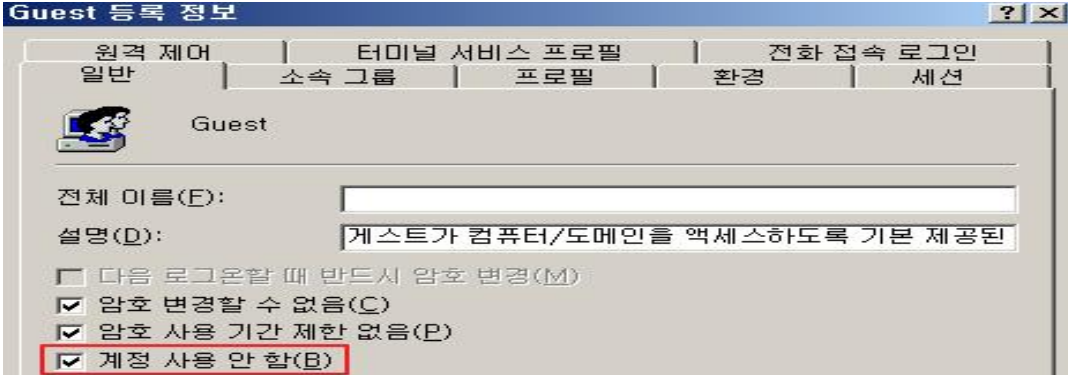
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > 계정:  
Administrator 계정 이름 바꾸기 에서 계정 이름 변경



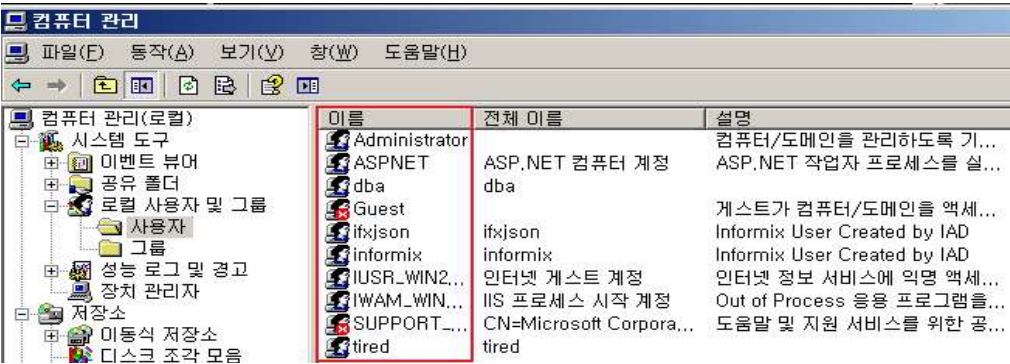
비고

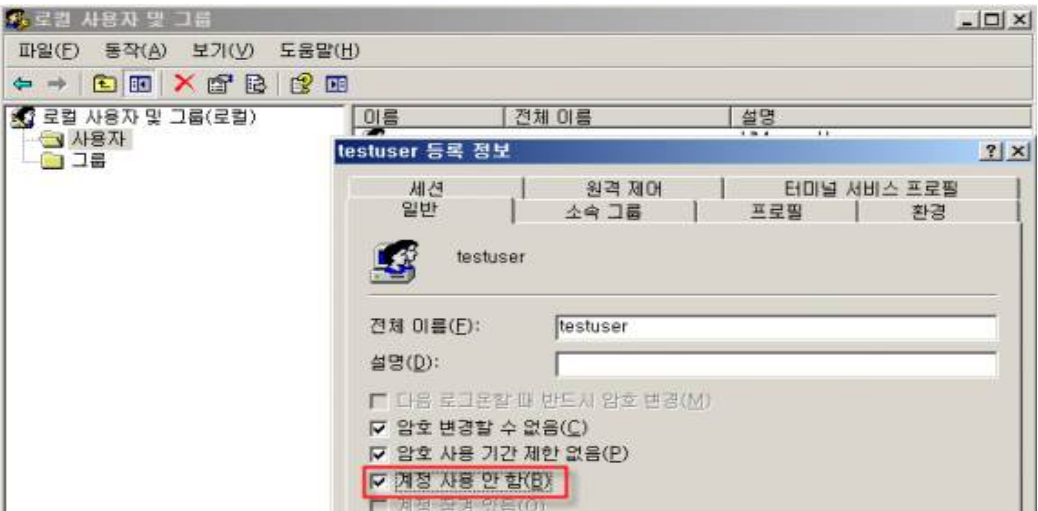
## 2.1.2. Guest 계정 상태

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | WS1-02 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | <p>대부분의 시스템은 Guest 계정의 사용을 필요치 않으며 앞으로도 계속 Guest 계정의 사용을 제한해야 한다.</p> <p>만약 불특정 다수의 접근이 필요할 경우 Guest가 아닌 일반 사용자 계정을 생성해 사용 하도록 한다.</p>                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | <p>양호 - Guest 계정이 비활성화 되어 있는 경우</p> <p>취약 - Guest 계정이 활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 점검 방법 | <p>Guest 계정 활성화 상태를 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net user guest 명령어 실행 후 Guest 계정 활성 상태 확인</p>  <p>■ 로컬 사용자 및 그룹에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; Guest 속성 &gt; "계정 사용 안함" 체크 유무 확인</p>  |       |        |     |   |

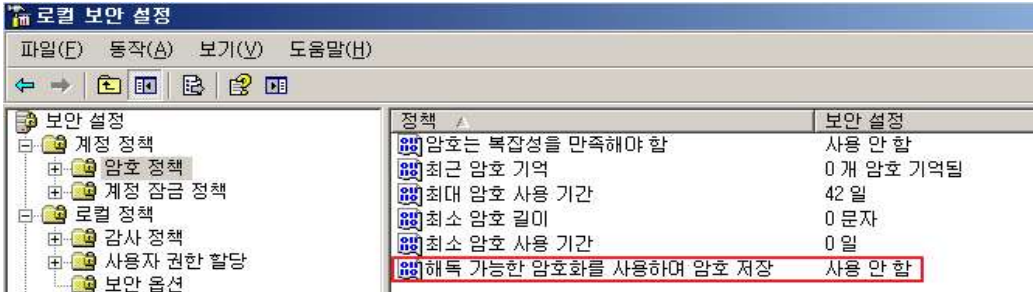
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>Guest 계정을 비활성화 시킨다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 변경<br/>시작 &gt; 실행 &gt; cmd &gt; net user guest /active:no 명령어 실행<br/>※ cmd를 관리자 권한으로 실행</p> <pre>C:\&gt;net user guest /active:no 명령을 잘 실행했습니다.</pre> <p>■ 로컬 사용자 및 그룹에서 확인<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; Guest 속성 &gt; "계정 사용 안함" 체크</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### 2.1.3. 불필요한 계정 제거

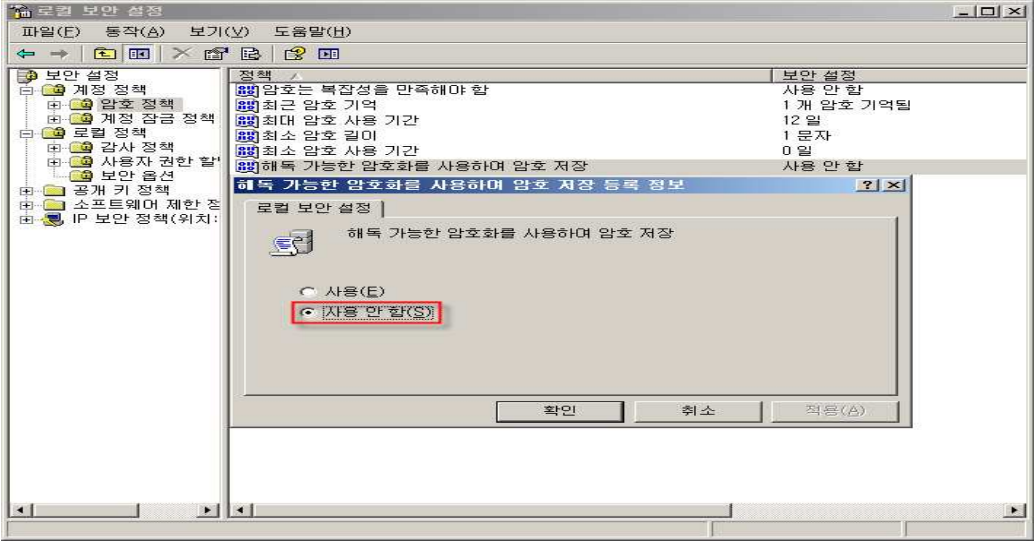
| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | WS1-03 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 설명    | <p>로그인이 가능한 사용자 계정들은 로그인을 통해서 시스템에 접근이 가능하기 때문에 로그인 계정의 패스워드 부재로 인한 패스워드 유출이나 패스워드 추측 공격으로 패스워드 유출가능성이 있다.</p> <p>오랫동안 로그인 하지 않은 계정은 계정만 만들어지고 관리가 되지 않는 계정일 가능성이 높으며, 이런 경우 계정을 악의적인 사용자가 불법적으로 사용해도 알 수 없고, 패스워드 변경이 없으므로 패스워드 유출가능성이 존재한다. 또한 반복된 로그인 실패 기록이 남아있는 계정은 패스워드 추측에 의한 불법적인 로그인 시도 가능성도 있다. 그러므로 사용 목적이 만료된 관리자, Guest, 테스트 계정, 무자격 사용자(ex. 퇴직자) 등 시스템에 불필요한 계정을 주기적으로 삭제 조치해야 한다.</p>                                          |       |        |     |   |
| 진단 기준 | <p>양호 - 불필요한 계정이 존재하지 않을 경우</p> <p>취약 - 불필요한 계정이 존재할 경우</p>                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | <p>불필요한 계정이 존재하는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net user 명령어 실행 후 사용자 계정 점검</p>  <p>■ 로컬 사용자 및 그룹에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; 속성 &gt; "계정 사용 안함" 체크 유무 확인</p>  |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>불필요한 계정은 비활성화 시키거나, 삭제한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 변경</p> <p>시작 &gt; 실행 &gt; cmd &gt; net user "제거할 계정명" /delete를 입력하여 삭제</p> <pre>C:\W&gt;net user test /delete 명령을 잘 실행했습니다.</pre> <p>■ 로컬 사용자 및 그룹에서 변경</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; 속성 &gt; "계정 사용 안 함" 체크하거나 계정 삭제</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                    |

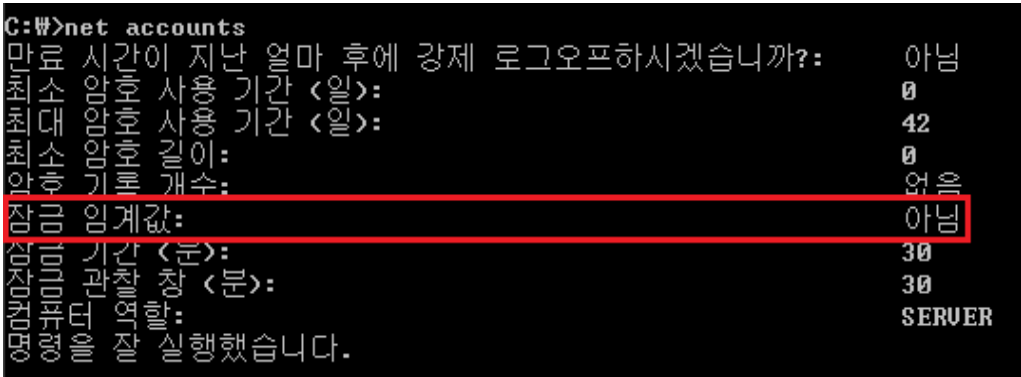
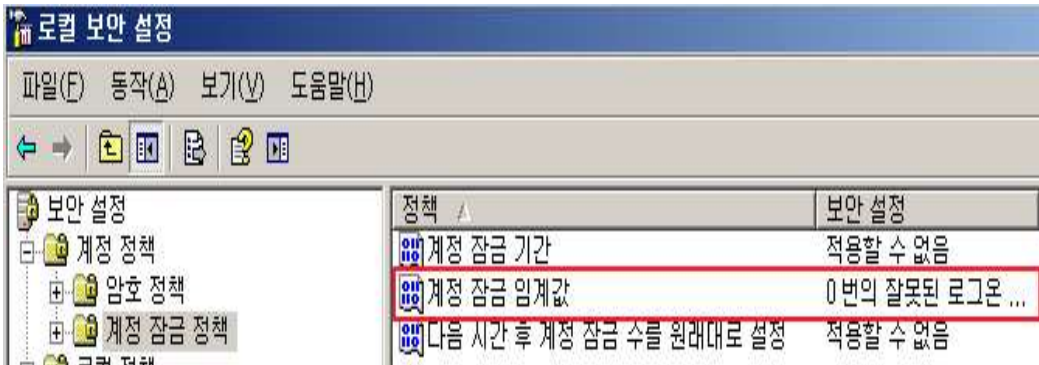
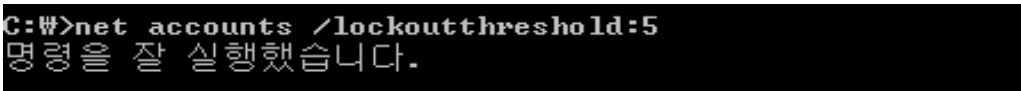
## 2.1.4. 해독 가능한 암호화를 사용하여 암호 저장

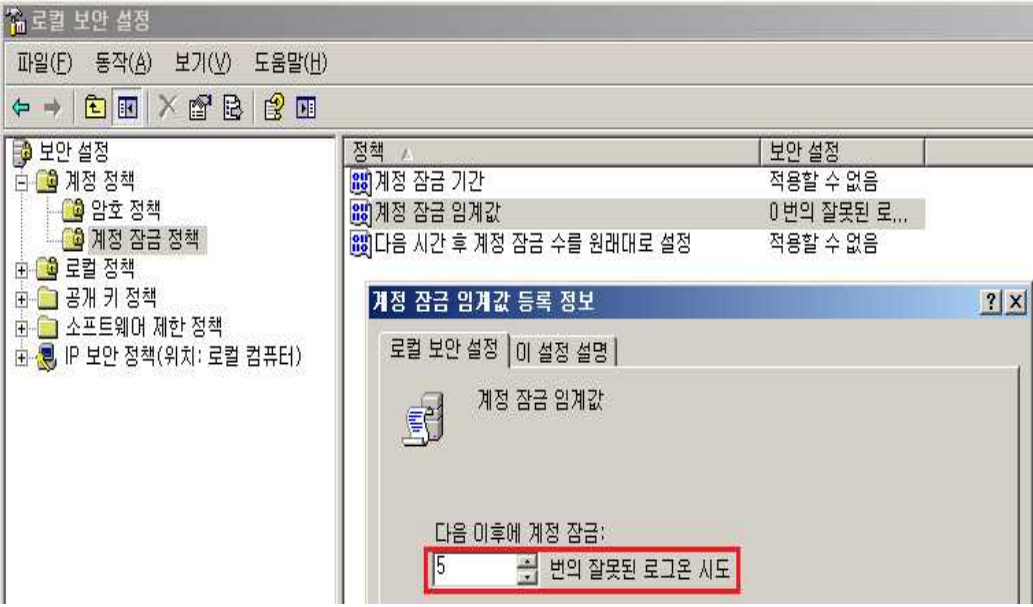
| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | WS1-04 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 설명    | 이 정책을 사용하면 인증을 위해 사용자 암호를 알아야 하는 응용 프로그램 프로토콜이 지원되지만 해독 가능한 방식으로 저장되는 암호는 해독할 수 있기 때문에 이 암호화를 공격할 수 있는 공격자가 노출된 계정을 사용하여 네트워크 리소스에 로그인 할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 진단 기준 | <p>양호 - "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용 안 함" 으로 설정되어 있을 경우</p> <p>취약 - "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용" 으로 설정되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 점검 방법 | <p>"해독 가능한 암호화를 사용하여 암호 저장" 정책의 설정 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트를 이용하여 설정 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; secedit /export /cfg c:\Wcfg.txt 명령어 실행</p> <p>탐색기 &gt; cfg.txt 파일을 열어서 ClearTextPassword 설정 값이 1로 되어 있는지 확인 (0일 경우 양호, 1일 경우 취약)</p> <pre>[Unicode] Unicode=yes [System Access] MinimumPasswordAge = 0 MaximumPasswordAge = 42 MinimumPasswordLength = 0 PasswordComplexity = 0 PasswordHistorySize = 0 LockoutBadCount = 0 RequireLogonToChangePassword = 0 ForceLogoffWhenHourExpire = 0 NewAdministratorName = "Admin" NewGuestName = "Guest" ClearTextPassword = 0 LSAAnonymousNameLookup = 0</pre> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "해독 가능한 암호화를 사용하여 암호 저장" 설정 확인</p>  |       |        |     |   |
| 조치 방법 | <p>"해독 가능한 암호화를 사용하여 암호 저장" 정책을 "사용 안 함" 으로 설정<br/>[Win2003, Win2008]</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함" 으로 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |



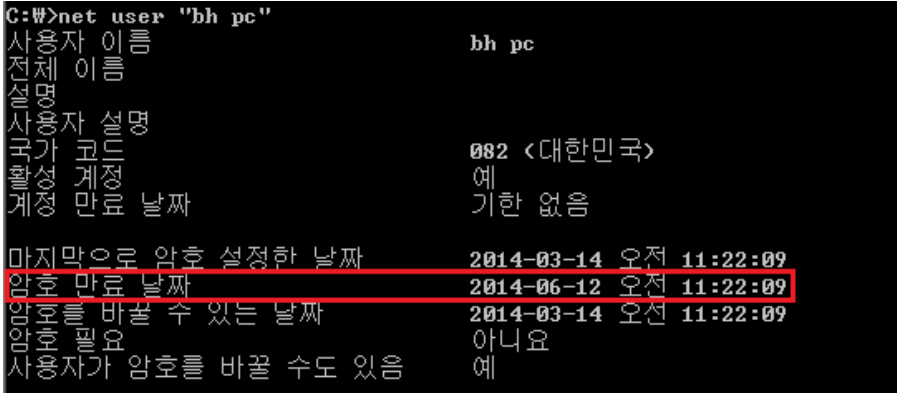
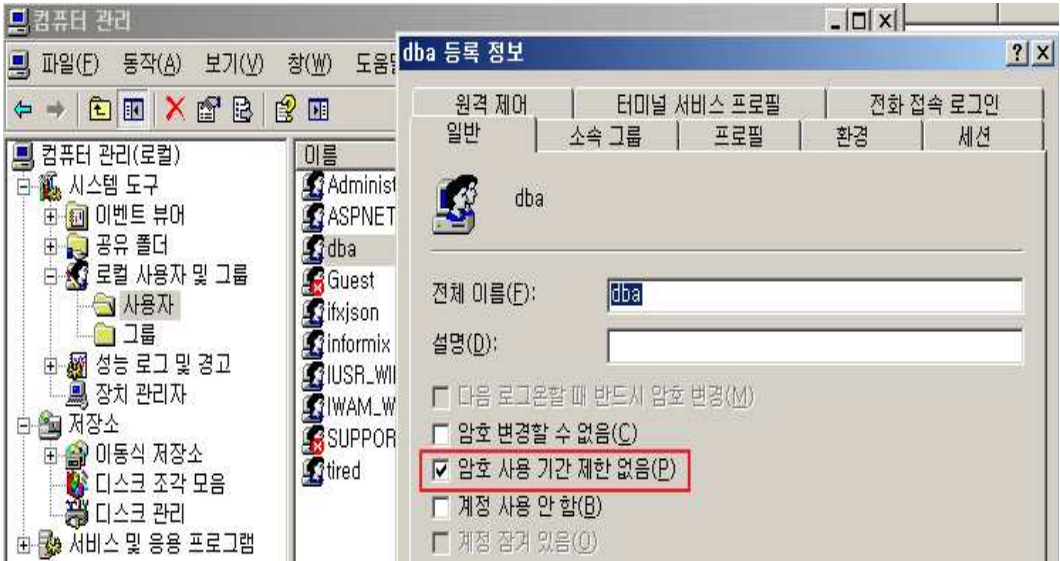
|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                    |

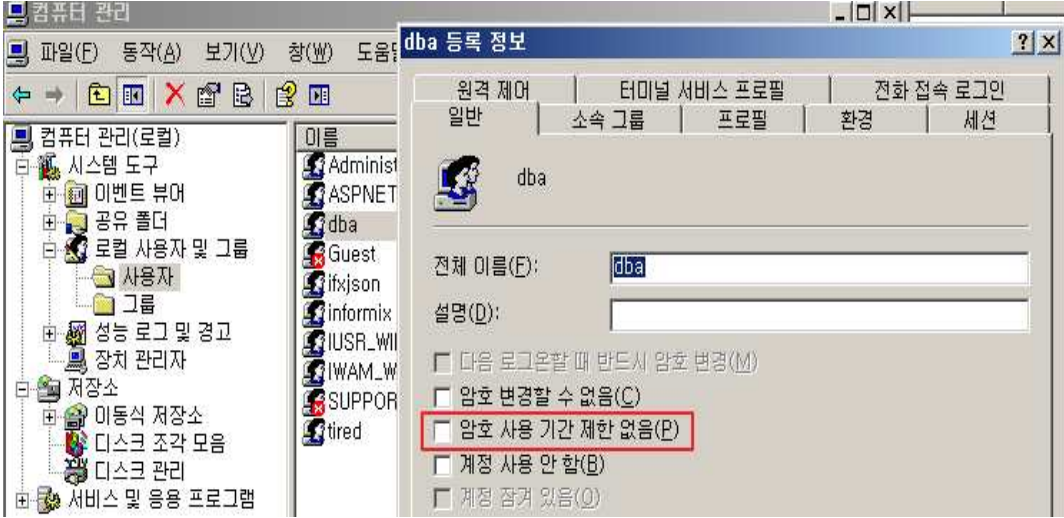
## 2.1.5. 계정 잠금 임계값 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | WS1-05 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | 암호 공격에서는 자동화된 방법을 통해 모든 사용자 계정에 대해 수천 또는 수백만 개의 암호 조합을 시도하기 때문에 가능한 로그인 실패 수를 제한하여야 한다.                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | 암호 - 계정 잠금 임계값이 5번으로 설정되어 있는 경우<br>취약 - 계정 잠금 임계값이 5번으로 설정되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 점검 방법 | <p>계정 잠금 임계값이 5번으로 설정되어 있는지 확인한다.<br/>                     [Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net accounts 명령어 실행 후 계정 잠금 임계값 설정 확인</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 계정 잠금 정책 &gt; "계정 잠금 임계값" 설정 확인</p>  |       |        |     |   |
| 조치 방법 | <p>계정 잠금 임계값을 5번으로 설정한다.</p> <p>■ 명령 프롬프트에서 설정</p> <p>시작 &gt; 실행 &gt; cmd &gt; net accounts /lockoutthreshold:5 명령어 실행</p> <p>※ cmd를 관리자 권한으로 실행</p>                                                                                                                                                                                                                                  |       |        |     |   |

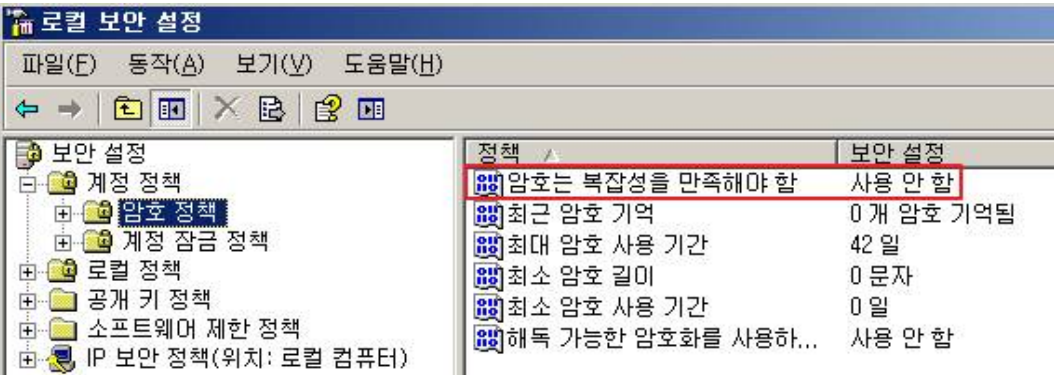
|    |                                                                                                                                                                                                           |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 계정 잠금 정책 &gt; "계정 잠금 임계값"을 5번으로 설정</p>  |
| 비고 |                                                                                                                                                                                                           |

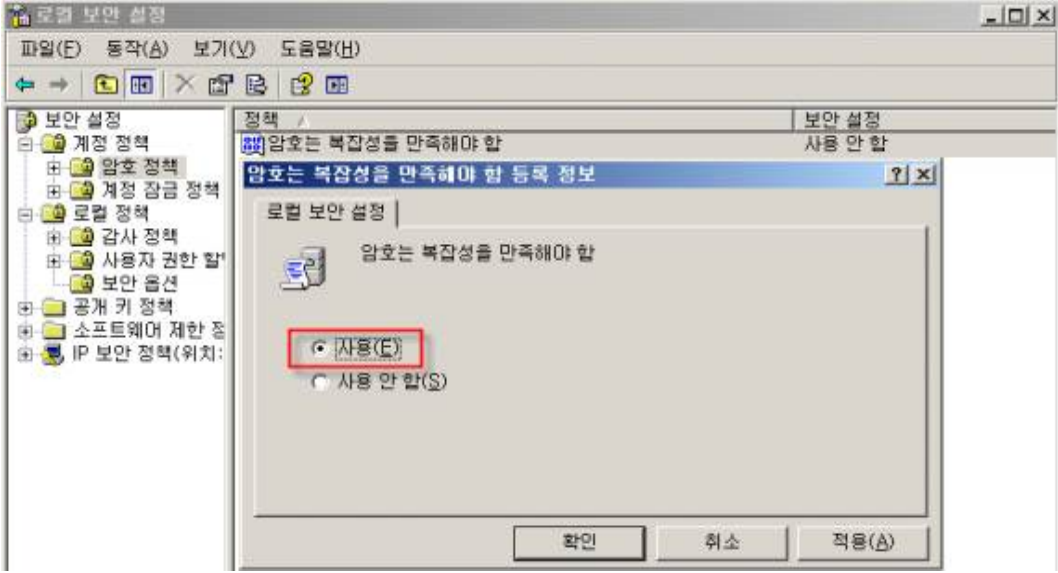
## 2.1.6. 패스워드 사용 만기 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | WS1-06 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 설명    | 패스워드 최대 사용 기간을 설정하더라도, 패스워드 만료 기간 설정을 활성화 시켜 주지 않으면 기능이 제대로 작동되지 않는다. 즉, 패스워드를 사용할 수 있는 기간에 대해 정책을 설정하면, 그 정책이 적용될 수 있도록 활성화 시켜주어야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 진단 기준 | <p>양호 - 패스워드 사용 만기 정책이 설정되어 있는 경우</p> <p>취약 - 패스워드 사용 만기 정책이 설정되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>패스워드 사용 만기 정책이 설정 되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net user "계정명" 명령어를 입력하여 "암호 만료 날짜" 설정 확인</p>  <p>마지막으로 암호 설정한 날짜 2014-03-14 오전 11:22:09<br/> <b>암호 만료 날짜 2014-06-12 오전 11:22:09</b><br/>         암호를 바꿀 수 있는 날짜 2014-03-14 오전 11:22:09<br/>         암호 필요 아니요<br/>         사용자가 암호를 바꿀 수도 있음 예</p> <p>■ 컴퓨터 관리에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; 설정할 계정 선택 &gt; 속성 에서 "암호 사용 기간 제한 없음" 이 해제되어 있는지 확인</p>  |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>패스워드 사용 만료 정책을 활성화 시킨다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 설정</p> <p>시작 &gt; 실행 &gt; cmd &gt; wmic useraccount where name="계정명" set passwordexpires=true</p> <p>명령어 입력</p> <pre>C:\W&gt;wmic useraccount where name="bh pc" set passwordexpires=true Updating property(s) of 'WWWIN-6LAH01QKUGQ\ROOT\WIMU2:Win32_UserAccount.Domain="WIN-6LAH01QKUGQ",Name="bh pc"' Property(s) update successful.</pre> <p>■ 컴퓨터 관리에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 로컬 사용자 및 그룹 &gt; 사용자 &gt; 설정할 계정 선택 &gt; 속성에서 "암호 사용 기간 제한 없음" 해제</p>  |
|       | 비고                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

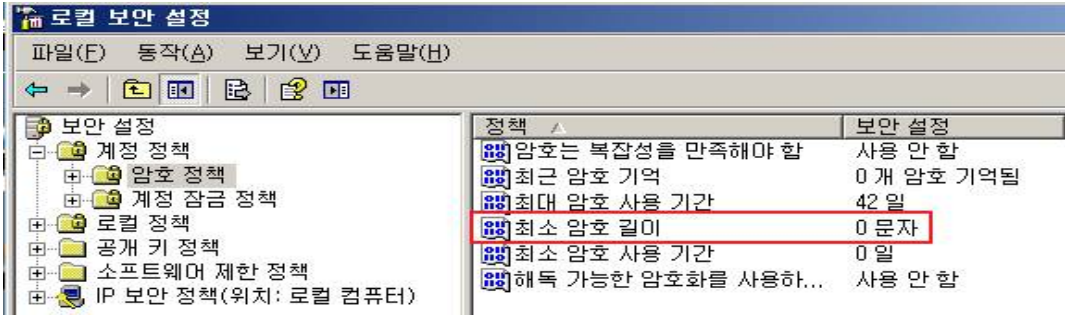
## 2.1.7. 패스워드 복잡성 설정

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | WS1-07 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | <p>영어, 숫자만으로 이루어진 암호는 공개되어 있는 유틸리티를 사용하여 아주 쉽게 공격할 수 있기 때문에 암호가 공격 당하는 것을 방지하려면 암호를 여러 종류의 문자를 이용하여 설정해야 한다.</p> <p>또한 최소 암호 길이를 8로 지정하여 이 정책 설정과 함께 사용하면 하나의 암호를 만들 수 있는 경우의수가 매우 많아져 무작위 공격을 성공하는 것이 어려워진다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | <p>양호 - "암호는 복잡성을 만족해야 함" 정책이 "사용" 으로 되어 있을 경우</p> <p>취약 - "암호는 복잡성을 만족해야 함" 정책이 "사용 안 함" 으로 되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 점검 방법 | <p>패스워드 복잡성 설정이 "사용" 으로 설정되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <ol style="list-style-type: none"> <li>1. 시작 &gt; 실행 &gt; cmd &gt; secdit /export /cfg /c:Wcfg.txt 명령어 실행</li> <li>2. 탐색기 &gt; c:Wcfg.txt 파일을 열어서 PasswordComplexity 설정 값이 1로 되어 있는지 확인 (설정 값이 1일 경우 양호, 0일 경우 취약)</li> </ol> <pre> 1 [Unicode] 2 Unicode=yes 3 [System Access] 4 MinimumPasswordAge = 0 5 MaximumPasswordAge = 42 6 MinimumPasswordLength = 0 7 PasswordComplexity = 0 8 PasswordHistorySize = 0 9 LockoutBadCount = 0 </pre> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "암호는 복잡성을 만족해야 함" 의 설정 확인</p>  |       |        |     |   |

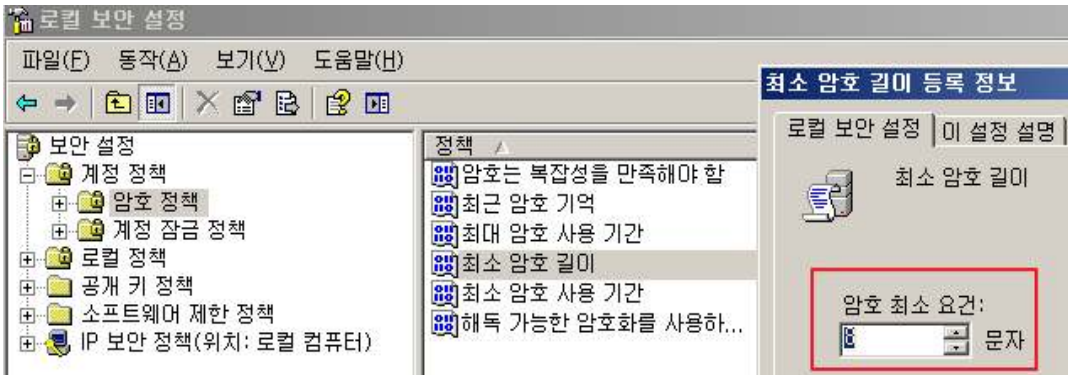
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>패스워드 암호 복잡성 정책을 사용하도록 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "암호는 복잡성을 만족해야 함" 정책을 "사용" 으로 설정</p>  <p>The screenshot shows the 'Local Security Policy' window. In the left-hand tree, 'Account Policies' is expanded, and 'Password Policy' is selected. The right pane shows the policy '암호는 복잡성을 만족해야 함' (Passwords must meet complexity requirements). The '사용(E)' (Use) radio button is selected and highlighted with a red rectangle, while the '사용 안 함(S)' (Do not use) button is unselected. The '확인' (OK) button is visible at the bottom right.</p> |
| 비고    | <p>이 정책 설정은 암호를 변경하거나 새 암호를 만드는 경우 암호가 강력한 암호로 간주되는 데 필요한 일련의 규정을 만족시키는지를 결정한다.</p> <ul style="list-style-type: none"> <li>• 암호는 적어도 6자 이상이어야 함</li> <li>• 사용자 계정 이름이나 표시 이름의 문자를 3개 이상 연속하여 포함하지 않아야 함.</li> <li>• 암호에는 다음 네 가지 중 세 가지 범주의 문자가 포함되어야 함. <ul style="list-style-type: none"> <li>- 대문자(A, B, C, ...)</li> <li>- 소문자(a, b, c, ...)</li> <li>- 숫자(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)</li> <li>- 영어, 숫자이외의 문자와 유니코드 문자(( ) ` ~ ! @ # \$ % ^ &amp; * - + =   W { } [ ] : ;</li> </ul> </li> </ul> <p>" ' &lt; &gt; , . ? / € Γ ' λ 및 공백)</p>                                                                                                                                                                                     |



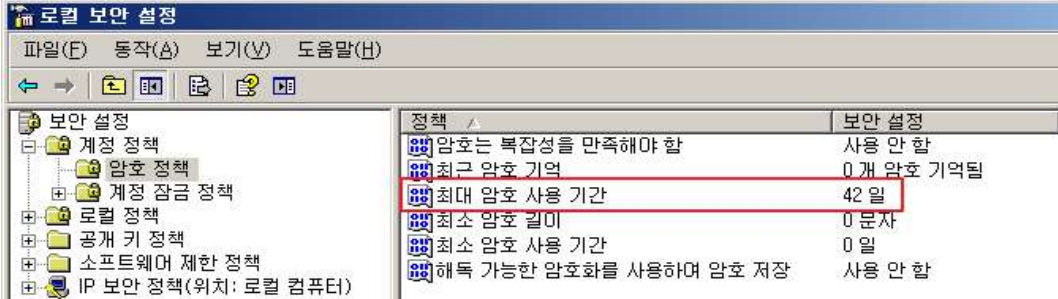
## 2.1.8. 패스워드 최소 암호 길이

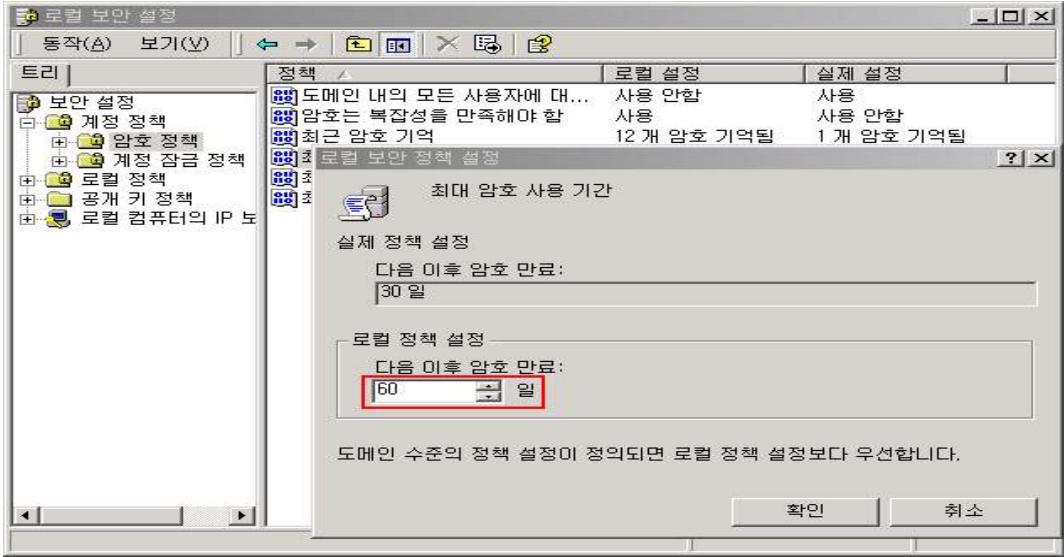
| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | WS1-08 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | <p>특정 사용자 계정의 암호를 알아내기 위해 수행할 수 있는 암호 공격의 유형은 일반적인 단어와 구사어를 시도하는 사전 공격과 가능한 모든 문자의 조합을 시도하는 무작위 공격이 있다.</p> <p>대부분의 환경에서 8자리의 암호를 사용하면 적절한 보안이 제공될 뿐만 아니라 사용자가 쉽게 기억할 수 있으며 무작위 공격을 적절히 방어할 수 있다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 진단 기준 | <p>양호 - 패스워드 최소 암호 길이가 8문자(이상) 일 경우</p> <p>취약 - 패스워드 최소 암호 길이가 8문자(미만) 일 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>패스워드 최소 암호 길이의 설정 값이 8문자(이상) 인지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 프롬프트에서 확인</p> <ol style="list-style-type: none"> <li>1. 시작 &gt; 실행 &gt; cmd &gt; secdit /export /cfg /c:Wcfg.txt 명령어 실행</li> <li>2. 탐색기 &gt; c:Wcfg.txt 파일을 열어서 MinimumPasswordLength 설정 값이 8문자 이상으로 설정되어 있는지 확인</li> </ol> <pre> 1 [Unicode] 2 Unicode=yes 3 [System Access] 4 MinimumPasswordAge = 0 5 MaximumPasswordAge = 42 6 MinimumPasswordLength = 0     </pre> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최소 암호 길이" 정책이 8문자 이상으로 설정되어 있는지 확인</p>  |       |        |     |   |
| 조치 방법 | <p>패스워드 최소 암호 길이를 8자리 이상으로 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최소 암호 길이" 정책을 8문자(이상)로 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |



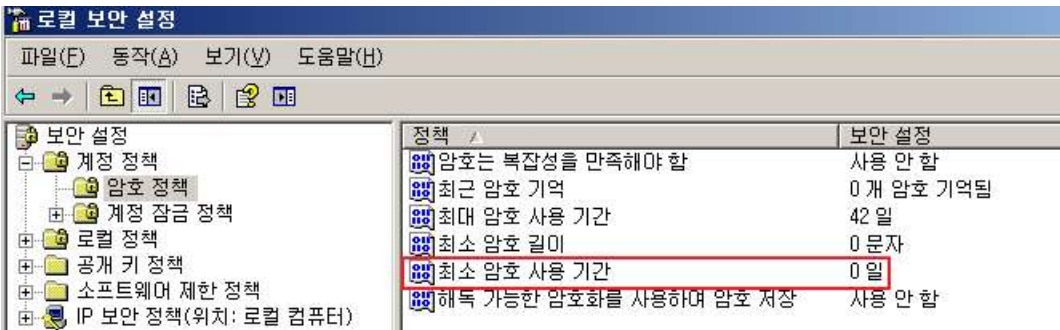
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the 'Local Security Policy' window. In the left pane, 'Security Settings' is expanded, and 'Password Policy' is selected. The right pane shows the 'Password Policy' settings. The 'Minimum password length' is set to 8. The 'Password must meet the following criteria' section is highlighted with a red box, showing a list of requirements: 'Password must be at least 8 characters long', 'Password must contain at least one uppercase letter', 'Password must contain at least one lowercase letter', 'Password must contain at least one number', and 'Password must contain at least one special character'.</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

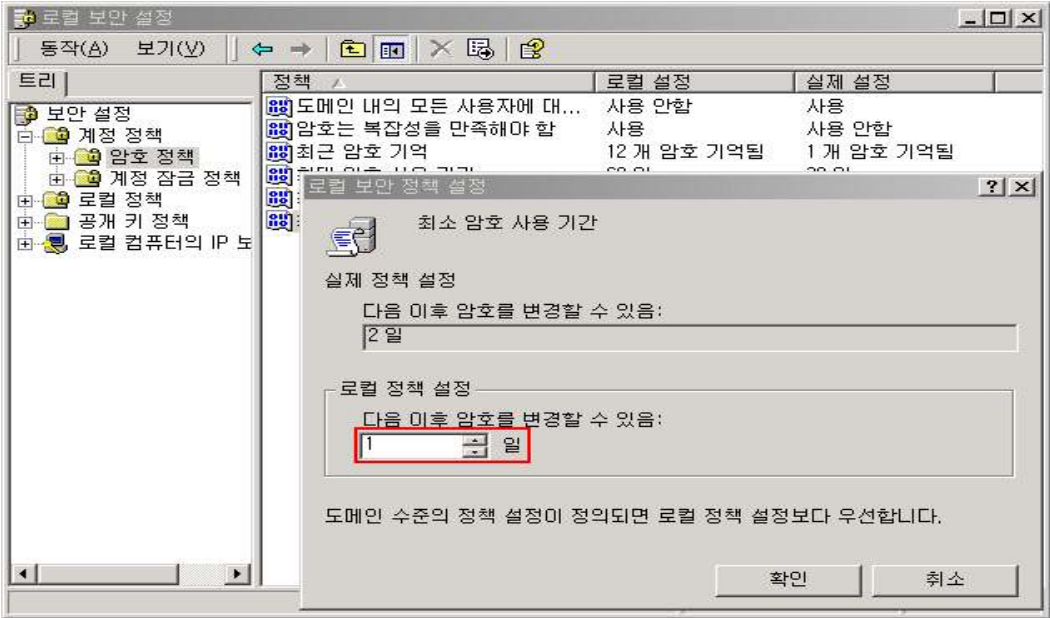
## 2.1.9. 패스워드 최대 사용 기간

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | WS1-09 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | 시간과 컴퓨터 처리 능력이 충분한 공격자는 가장 복잡한 암호를 포함하여 모든 암호를 추측하거나 공격 할 수 있다. 사용자가 암호를 자주 바꾸도록 하면 유효한 암호가 공격 당하는 위험을 줄일 뿐 아니라 누군가가 불법으로 획득한 암호를 사용하여 무단 로그인하는 위험을 줄일 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 진단 기준 | 암호 - 최대 암호 사용 기간이 90일 이하일 경우<br>취약 - 최대 암호 사용 기간이 90일 초과일 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | <p>패스워드 최대 암호 사용 기간의 설정 값이 90일(이하)로 설정되어 있는지 확인한다.<br/>                     [Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; cmd &gt; secdit /export /cfg /c:Wcfg.txt 명령어 실행</li> <li>탐색기 &gt; c:Wcfg.txt 파일을 열어서 MaximumPasswordAge 설정 값이 90일 이하로 설정되어 있는지 확인</li> </ol> <pre> 1 [Unicode] 2 Unicode=yes 3 [System Access] 4 MinimumPasswordAge = 0 5 MaximumPasswordAge = 42 6 MinimumPasswordLength = 0 7 PasswordComplexity = 0 8 PasswordHistorySize = 0 9 LockoutBadCount = 0                     </pre> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최대 암호 사용 기간" 정책이 90일 이하로 설정되어 있는지 확인</p>  <p>The screenshot shows the 'Local Security Policy' window. In the left pane, 'Account Policies' is expanded, and 'Password Policy' is selected. The right pane shows a list of password policies. 'Maximum Password Age' is highlighted with a red box, showing a value of '42 days'.</p> |       |        |     |   |
| 조치 방법 | <p>패스워드 최대 암호 사용 기간을 90일 이하로 설정한다.<br/>                     [Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최대 암호 사용 기간" 을 90일 이하로 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |

|    |                                                                                                         |
|----|---------------------------------------------------------------------------------------------------------|
|    |                       |
| 비고 | <p>패스워드 최대 사용 기간을 설정해도 1.6 패스워드 사용 만기 정책이 설정되어 있지 않으면 적용되지 않으므로, 1.6 패스워드 사용 만기 정책 항목을 활성화 시켜줘야 한다.</p> |

## 2.1.10. 패스워드 최소 사용 기간

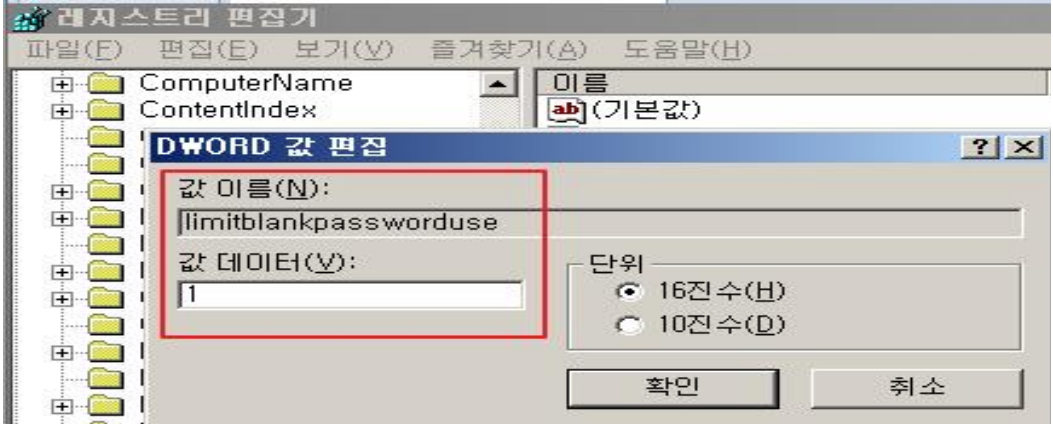
| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드 | WS1-10 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 설명    | <p>사용자가 암호를 계속 바꿔서 이전에 즐겨 쓰던 암호를 다시 사용할 수 있다면 암호를 정기적으로 바꾸도록 요구하는 것은 효과가 없으며, 정책 설정을 최근 암호 기억 설정과 함께 사용하면 이전 암호를 다시 사용하는 것을 막을 수 있다.</p> <p>최근 암호 기억 설정을 유효하게 하려면 최소 암호 사용 기간 정책 설정을 0보다 큰 값으로 구성해야 한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - 최소 암호 사용 기간이 1일(이상) 으로 설정되어 있는 경우</p> <p>취약 - 최소 암호 사용 기간이 설정되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 점검 방법 | <p>패스워드 최소 사용 기간이 1일(이상) 으로 설정되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; cmd &gt; secdit /export /cfg /c:Wcfg.txt 명령어 실행</li> <li>탐색기 &gt; c:Wcfg.txt 파일을 열어서 MinimumPasswordAge 설정 값이 1일(이상) 으로 설정되어 있는지 확인</li> </ol> <pre> 1  [Unicode] 2  Unicode=yes 3  [System Access] 4  MinimumPasswordAge = 0 5  MaximumPasswordAge = 42 6  MinimumPasswordLength = 0 7  PasswordComplexity = 0 8  PasswordHistorySize = 0 </pre> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최소 암호 사용 기간" 정책이 1일(이상) 으로 설정되어 있는지 확인</p>  |       |        |     |   |
| 조치 방법 | <p>패스워드 최소 사용 기간이 1일(이상)으로 설정한다.</p> <p>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 계정 정책 &gt; 암호 정책 &gt; "최소 암호 사용 기간" 을 1일(이상) 으로 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |

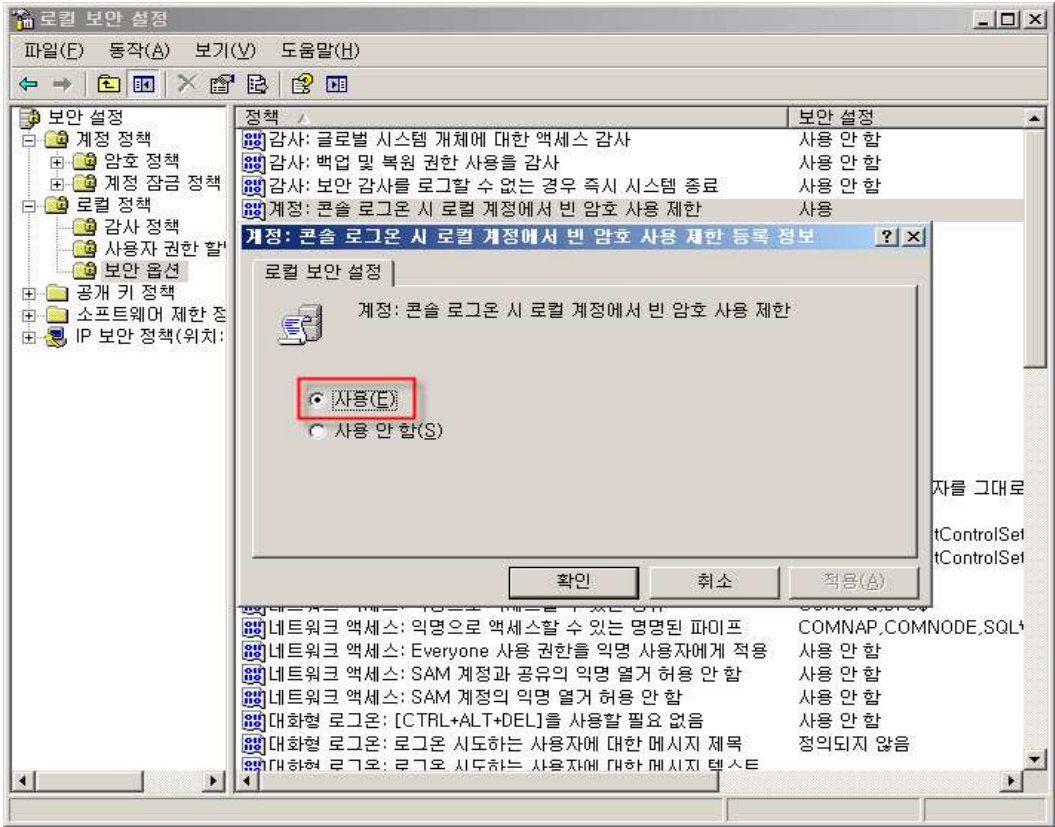
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the Windows Security Policy configuration interface. On the left, a tree view shows the hierarchy: Security Settings &gt; Account Policies &gt; Password Policy. The main pane displays a comparison between 'Local Policy' and 'Domain Policy' for password requirements. The 'Local Policy' section is active, showing 'Minimum password age' set to 1 day. A red rectangle highlights the '1' in the '1 day' field. The 'Domain Policy' section shows '2 days'. At the bottom, there are '확인' (OK) and '취소' (Cancel) buttons.</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

### 2.1.11. 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한

| 분류    | 계정 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | WS1-11 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | 이 정책 설정은 빈 암호를 사용하는 로컬 계정에 터미널 서비스, Telnet 및 FTP와 같은 네트워크 서비스의 원격 대화형 로그인을 허용할지 여부를 결정한다. 이 정책 설정은 콘솔에서 실제로 수행하는 대화형 로그인이나 도메인 계정을 사용하는 로그인에는 영향을 주지 않는다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 진단 기준 | <p>양호 - "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용" 으로 되어 있을 경우</p> <p>취약 - "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용 안 함" 으로 되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 점검 방법 | <p>"콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용" 으로 설정되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>1. 시작 &gt; 실행 &gt; cmd &gt; secdit /export /cfg /c:Wcfg.txt 명령어 실행</p> <p>2. 탐색기 &gt; c:Wcfg.txt 파일을 열어서 MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse 값이 4,1 로 설정되어 있는지 확인 (값이 4,1일 경우 양호)</p> <pre> 54 MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,0 55 MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0 56 MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled=4,0 57 MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0 58 MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0 59 MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1 60 MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,536870912 61 MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,536870912 </pre> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa 에서 limitblankpassworduse 의 값이 1로 되어 있는지 확인 (값이 1일 경우 양호)</p>  <p>■ 로컬 보안 정책에서 확인</p> |       |        |     |   |



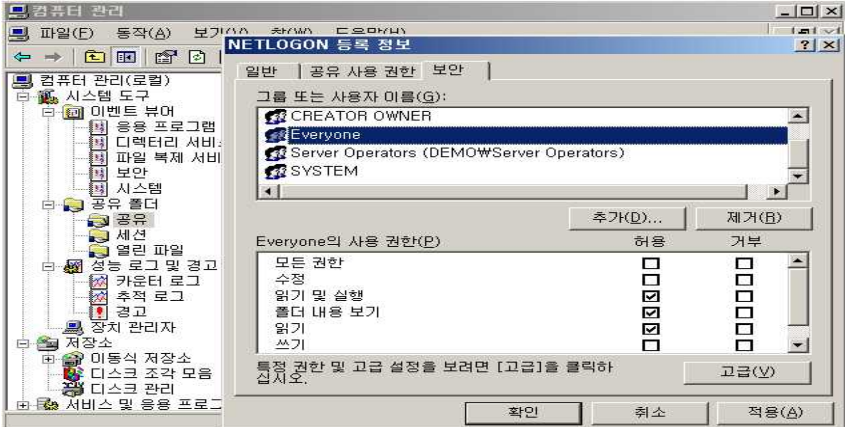
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; “계정 : 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책이 “사용” 으로 되어 있는지 확인 (설정이 “사용” 으로 되어 있는 경우 양호)</p>                                                                                                                                                                                                                                  |
| 조치 방법 | <p>“콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책을 “사용” 으로 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 레지스트리에서 설정 변경</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 에서 limitblankpassworduse 의 값을 1로 변경</p>  <p>■ 로컬 보안 정책에서 설정 변경</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; “계정 : 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책을 “사용” 으로 설정</p> |

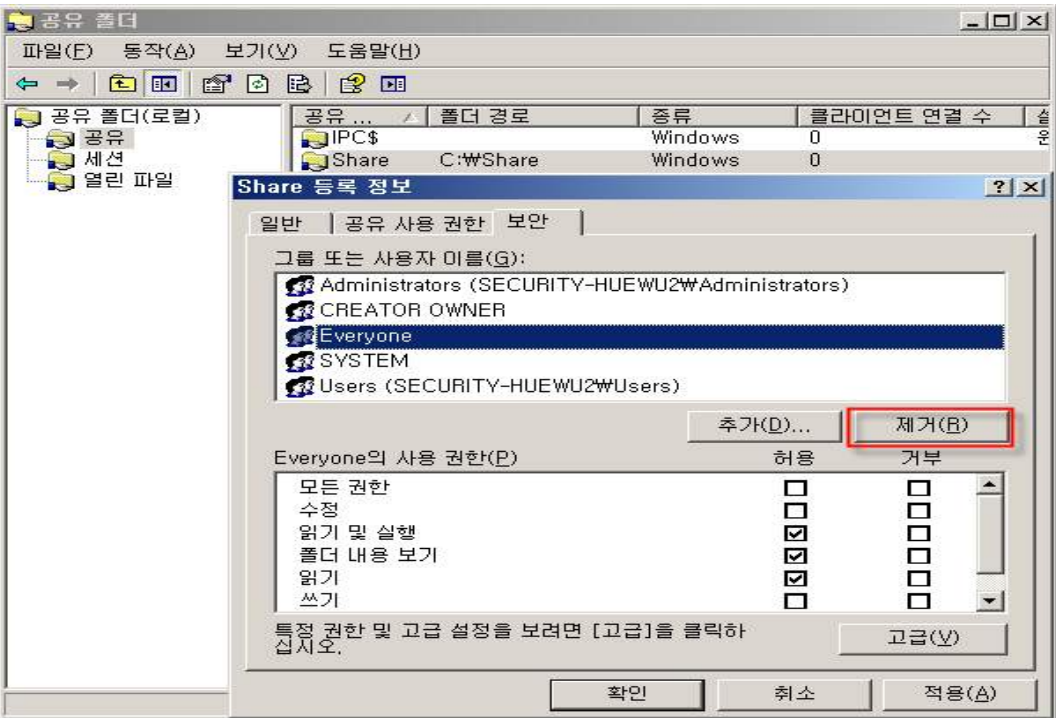
|    |                                                                                     |
|----|-------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                     |



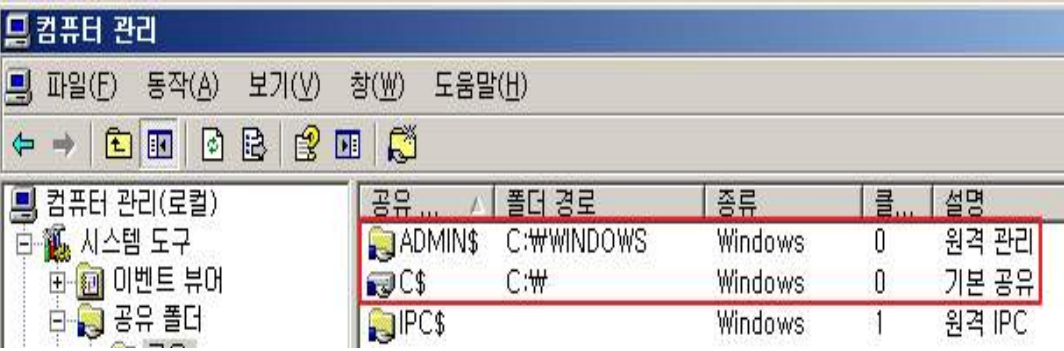
## 2.2. 서비스 관리

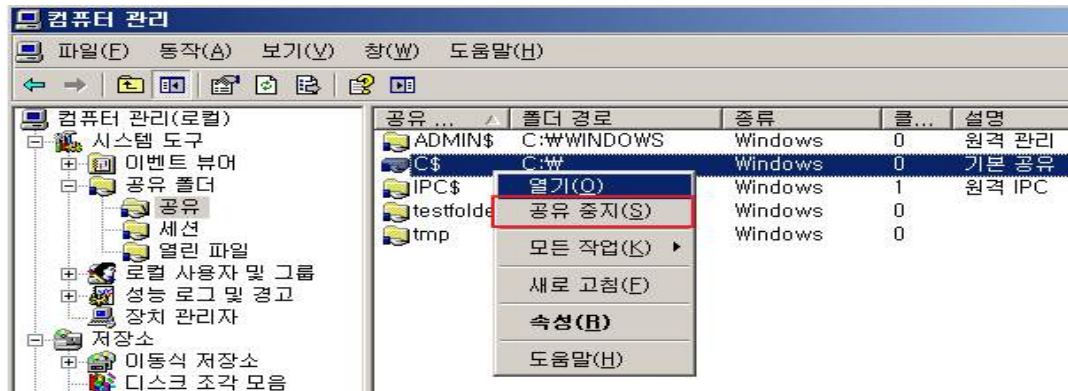
### 2.2.1. 공유 권한 및 사용자 그룹 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | WS2-01 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 설명    | <p>디폴트 공유인 C\$, D\$, Admin\$, IPC\$ 등을 제외한 공유폴더를 everyone 그룹으로 공유가 금지되었는지 여부를 점검한다.</p> <p>Everyone이 공유계정에 포함 되어 있을 경우 익명 사용자의 접근이 가능하므로 접근을 확인하여 제어하면 익명사용자에 의한 접근을 차단 할 수 있다.</p>                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 진단 기준 | <p>양호 - 일반 공유 디렉터리가 없거나 공유 디렉터리 접근 권한에 Everyone없을 경우</p> <p>취약 - 일반 공유 디렉터리의 접근 권한에 Everyone이 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>일반 공유폴더가 존재하는지 확인하고, 있을 경우 접근 권한에 Everyone으로 되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 컴퓨터 관리에서 확인</p> <p>1. 시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유 에서 일반 공유폴더가 존재하는지 확인 (C\$, D\$, Admin\$, IPC\$ 등을 제외한 일반 공유폴더가 존재하지 않으면 양호)</p>  <p>2. 위 1번 항목에서 C\$, D\$, Admin\$, IPC\$ 등을 제외한 일반 공유폴더가 존재하는 경우. 일반 공유폴더 &gt; 속성 &gt; 보안 탭에서 Everyone 으로 된 공유가 존재하는지 확인 (Everyone 공유가 존재하지 않으면 양호)</p>  |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                     |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>일반 공유폴더의 Everyone 접근 권한을 제거한다.<br/>[Win2003, Win2008]</p> <p>■ 컴퓨터 관리에서 설정 변경</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유 &gt; 일반 공유폴더 선택 &gt; 속성 &gt; 보안 탭에서 Everyone으로 된 공유를 제거하고, 접근이 필요한 계정의 권한만 추가</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                     |

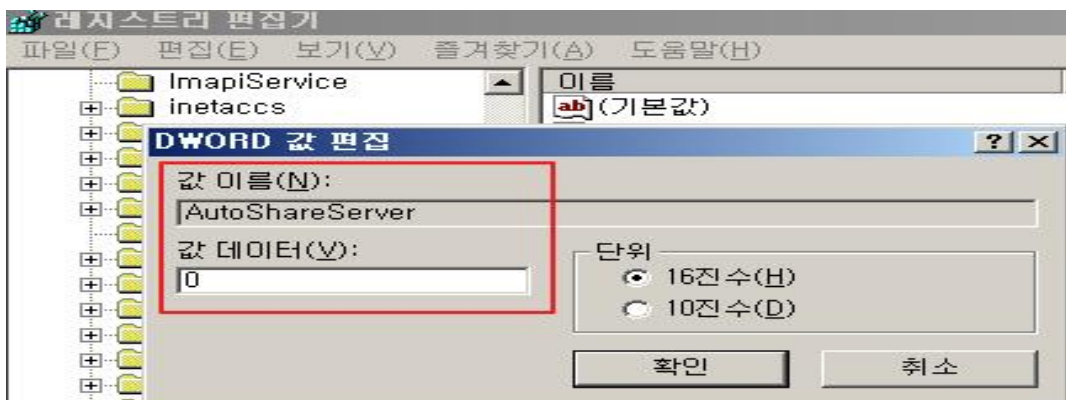
## 2.2.2. 하드디스크 기본 공유 제거

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | WS2-02 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | 시스템의 기본공유 항목이 제거되지 않게 되면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있다. 예전에 발생한 Nimda 바이러스도 여러 가지 방법 중에서 이러한 공유기능을 침투의 한 경로로 이용한 것으로 기본 공유를 제거해야 한다.                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | 양호 - AutoShareServer가 0 이며 기본 공유가 존재하지 않을 경우<br>취약 - AutoShareServer가 1이거나 기본 공유가 존재하는 경우                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>시스템에서 기본 공유가 존재하는지 확인한다.<br/>                     [Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net share 명령어 실행 후 기본 공유가 존재하는지 확인</p>  <p>■ 컴퓨터 관리에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유에서 기본 공유 확인</p>  |       |        |     |   |
| 조치 방법 | <p>불필요한 기본 공유(C\$, D\$, Admin\$, IPC\$) 를 중지한다.<br/>                     [Win2003, Win2008]</p> <p>■ 컴퓨터 관리에서 설정 변경</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유 에서 불필요한 기본 공유에 대해 "공유 중지" 설정</p>                                                                                                                                                                                                                          |       |        |     |   |



■ 레지스트리에서 설정 변경

시작 > 실행 > regedit >  
 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 에서 AutoShareServer 의 값을 0으로 수정  
 (AutoShareServer가 없을 경우 DWORD로 새로 생성)

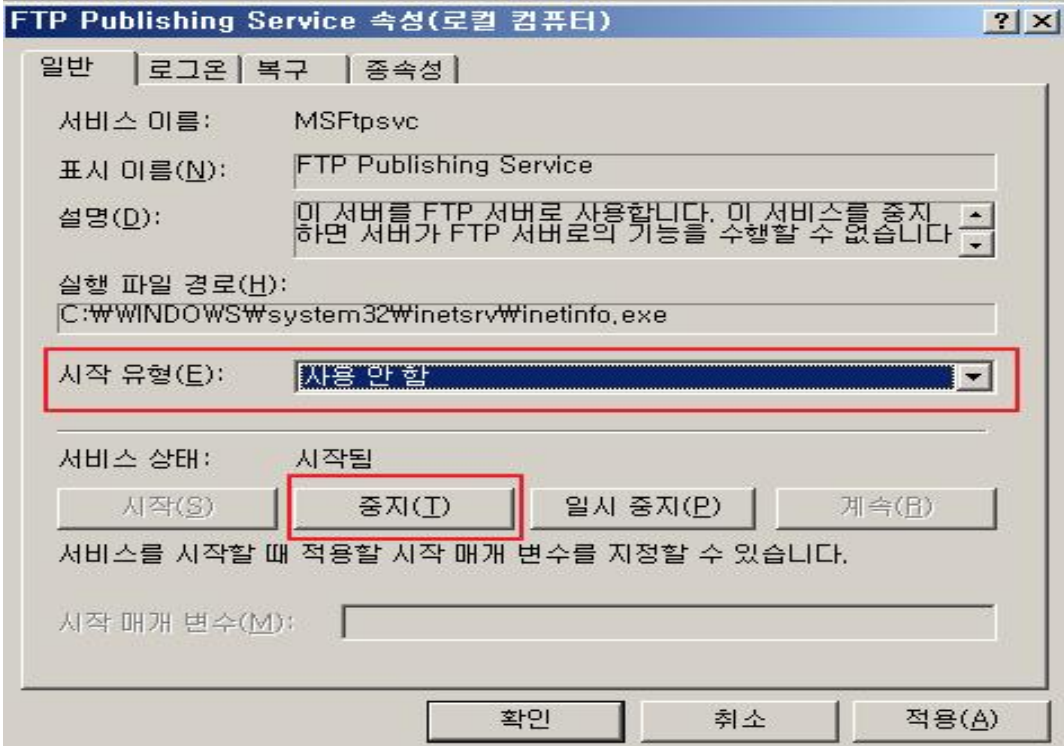


비고

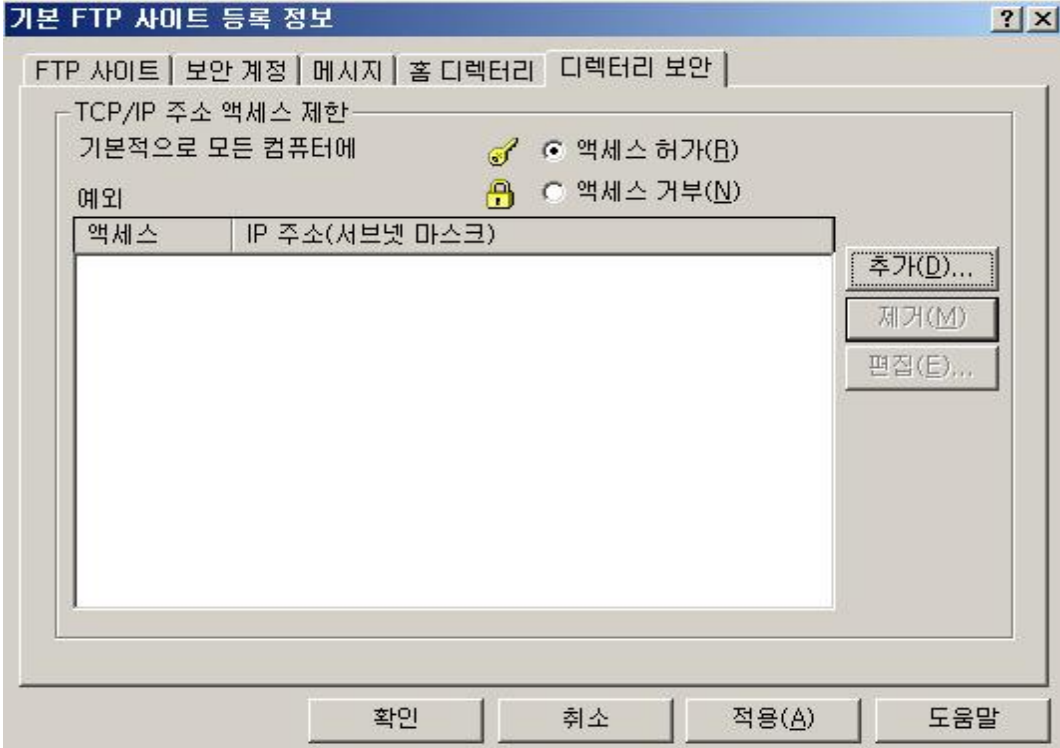
기본 공유 중지 시, 레지스트리 수정을 해야 영구 적용된다.

### 2.2.3. FTP 서비스 구동 점검

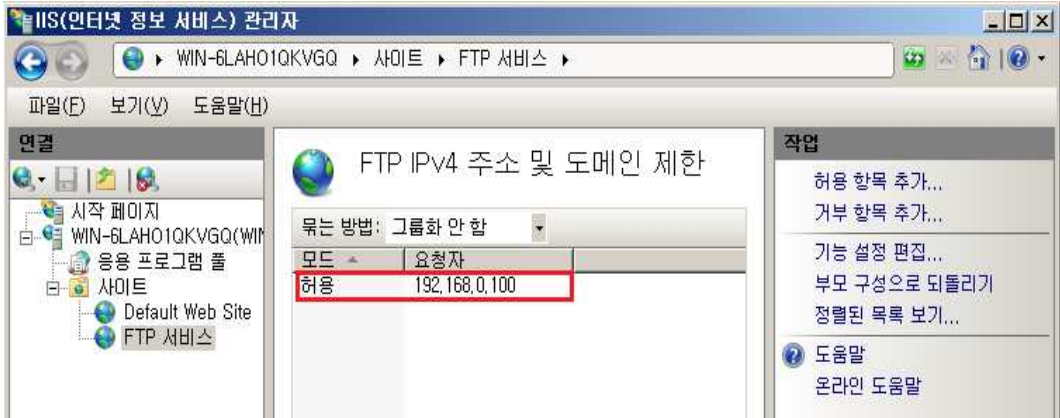
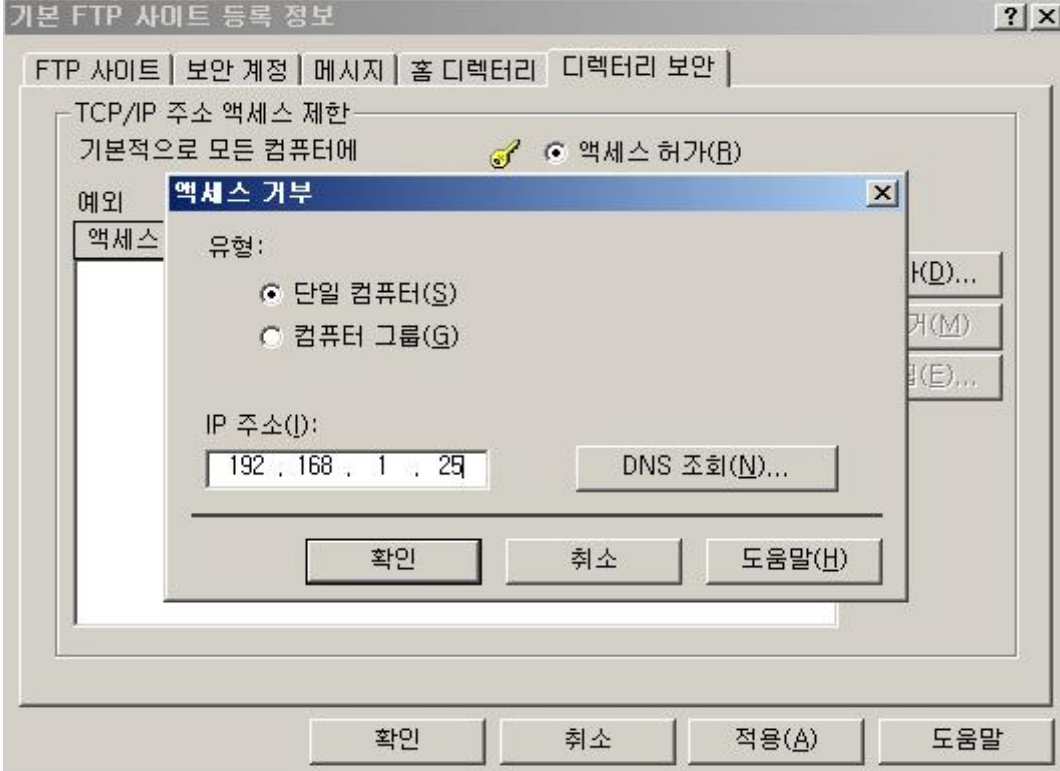
| 분류                                  | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | WS2-03 | 중요도 | H |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|------|----|----|-------|-------------------------------------|-------|-----|----|------------|-------|-----|----|-------------------------|-------|-----|----|-----------|-------|-----|----|------------------|-------|--|----|------------------------|-------|-----|----|------------------|-------|-----|----|
| 대상                                  | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| 설명                                  | 기본적인 FTP 서비스는 계정과 패스워드가 암호화 되지 않은 채로 전송 되므로 간단한 Sniffer 에 의해서도 스니핑이 가능하다. 따라서 FTP 서비스를 사용하지 않을 것을 권고 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| 진단 기준                               | 양호 - FTP 서비스를 사용하지 않는 경우<br>취약 - FTP 서비스를 사용하고 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| 점검 방법                               | <p>FTP 서비스가 구동 중인지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net start 명령어를 통해 FTP 서비스 구동 확인</p> <div><pre>C:\Documents and Settings\Administrator&gt;net start 다음과 같은 Windows 서비스가 시작되었습니다.  Application Experience Lookup Service Application Layer Gateway Service Automatic Updates Error Reporting Service Event Log FTP Publishing Service Help and Support HTTP SSL</pre></div> <p>■ 서비스에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 에서 FTP 서비스 구동 확인</p> <table><thead><tr><th>이름 ▲</th><th>설명</th><th>상태</th><th>시작 유형</th></tr></thead><tbody><tr><td> Distributed Transaction Coordinator</td><td>데이...</td><td>시작됨</td><td>자동</td></tr><tr><td> DNS Client</td><td>이 ...</td><td>시작됨</td><td>자동</td></tr><tr><td> Error Reporting Service</td><td>예상...</td><td>시작됨</td><td>자동</td></tr><tr><td> Event Log</td><td>이벤...</td><td>시작됨</td><td>자동</td></tr><tr><td> File Replication</td><td>여러...</td><td></td><td>수동</td></tr><tr><td> FTP Publishing Service</td><td>이 ...</td><td>시작됨</td><td>자동</td></tr><tr><td> Help and Support</td><td>이 ...</td><td>시작됨</td><td>자동</td></tr></tbody></table> |       |        |     |   | 이름 ▲ | 설명 | 상태 | 시작 유형 | Distributed Transaction Coordinator | 데이... | 시작됨 | 자동 | DNS Client | 이 ... | 시작됨 | 자동 | Error Reporting Service | 예상... | 시작됨 | 자동 | Event Log | 이벤... | 시작됨 | 자동 | File Replication | 여러... |  | 수동 | FTP Publishing Service | 이 ... | 시작됨 | 자동 | Help and Support | 이 ... | 시작됨 | 자동 |
| 이름 ▲                                | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 상태    | 시작 유형  |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| Distributed Transaction Coordinator | 데이...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| DNS Client                          | 이 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| Error Reporting Service             | 예상...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| Event Log                           | 이벤...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| File Replication                    | 여러...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       | 수동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| FTP Publishing Service              | 이 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| Help and Support                    | 이 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 시작됨   | 자동     |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |
| 조치 방법                               | <p>구동 중인 FTP 서비스를 중지시킨다.<br/>[Win2003, Win2008]</p> <p>■ 서비스에서 FTP 중지</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 에서 FTP Publishinb Service 를 중지하고, 시작 유형을 "사용 안 함" 으로 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |      |    |    |       |                                     |       |     |    |            |       |     |    |                         |       |     |    |           |       |     |    |                  |       |  |    |                        |       |     |    |                  |       |     |    |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>FTP Publishing Service 속성(로컬 컴퓨터)</p> <p>일반   로그인   복구   종속성</p> <p>서비스 이름: MSFtpsvc</p> <p>표시 이름(N): FTP Publishing Service</p> <p>설명(D): 이 서버를 FTP 서버로 사용합니다. 이 서비스를 중지하면 서버가 FTP 서버로의 기능을 수행할 수 없습니다.</p> <p>실행 파일 경로(H): C:\WINDOWS\system32\Winetsrv\inetinfo.exe</p> <p>시작 유형(E): 자동 안 함</p> <p>서비스 상태: 시작됨</p> <p>시작(S) 중지(I) 일시 중지(P) 계속(R)</p> <p>서비스를 시작할 때 적용할 시작 매개 변수를 지정할 수 있습니다.</p> <p>시작 매개 변수(M):</p> <p>확인 취소 적용(A)</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

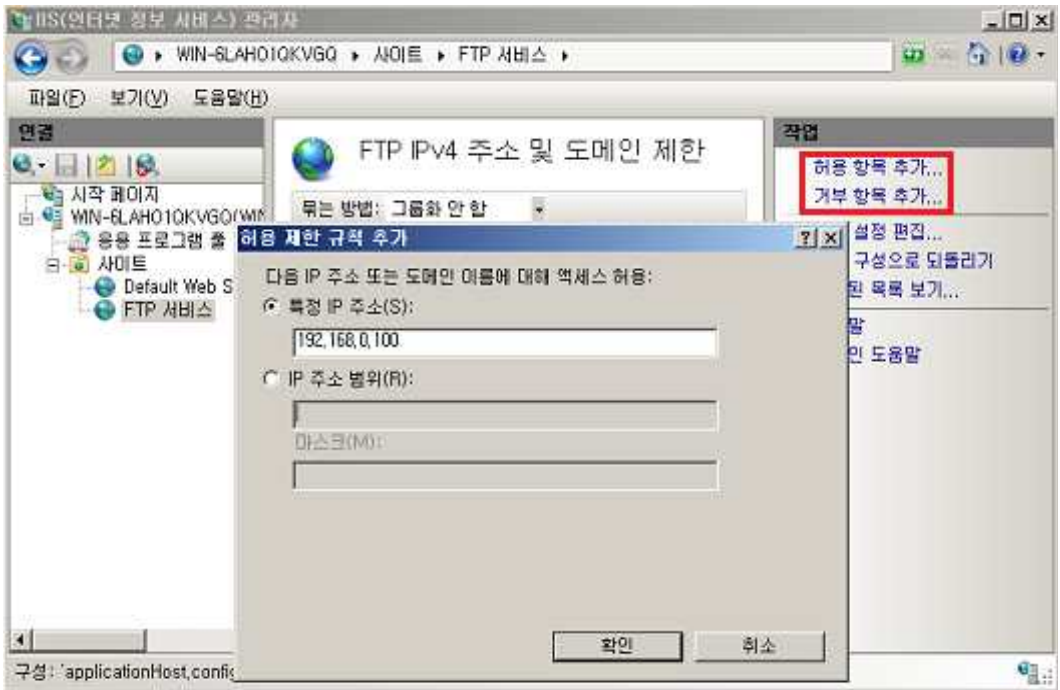
## 2.2.4. FTP 접근 통제 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | WS2-04 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | FTP 서비스를 사용할 경우 허가되지 않은 네트워크에 대해 FTP 접속을 차단하는 접근 통제를 설정해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 진단 기준 | 양호 - FTP 서비스에 접근 가능한 IP 제한 설정을 적용한 경우<br>취약 - FTP 서비스에 접근 가능한 IP 제한 설정을 적용하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | <p>FTP 서비스에 접근할 수 있는 IP가 설정되어 있는지 확인한다.</p> <p>[Win2003]</p> <p>■ 인터넷 정보 서비스(IIS) 관리에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 인터넷 정보 서비스(IIS) 관리 &gt; FTP 사이트 &gt; 사용중인 FTP 사이트 &gt; 속성 &gt; 디렉터리 보안에서 액세스 허가 또는 거부 IP가 등록되어 있는지 확인</p>  <p>[Win2008]</p> <p>■ IIS(인터넷 정보 서비스) 관리자에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; IIS(인터넷 정보 서비스) 관리자 &gt; 사용중인 FTP 사이트 &gt; FTP IPv4 주소 및 도메인 제한 에서 허용 및 거부 IP 설정 확인</p> |       |        |     |   |

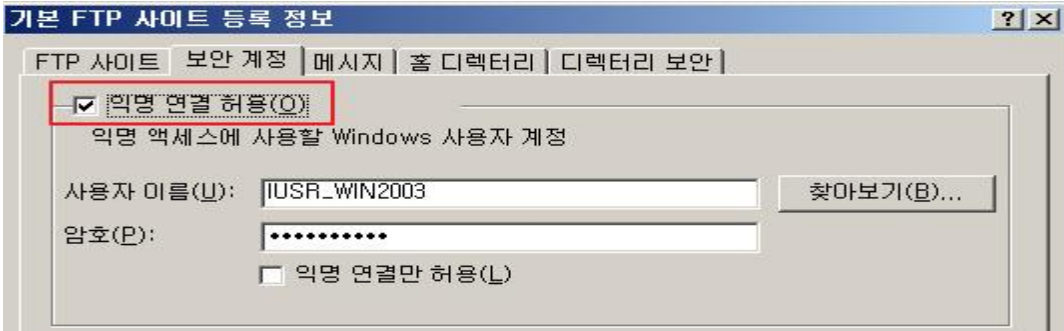


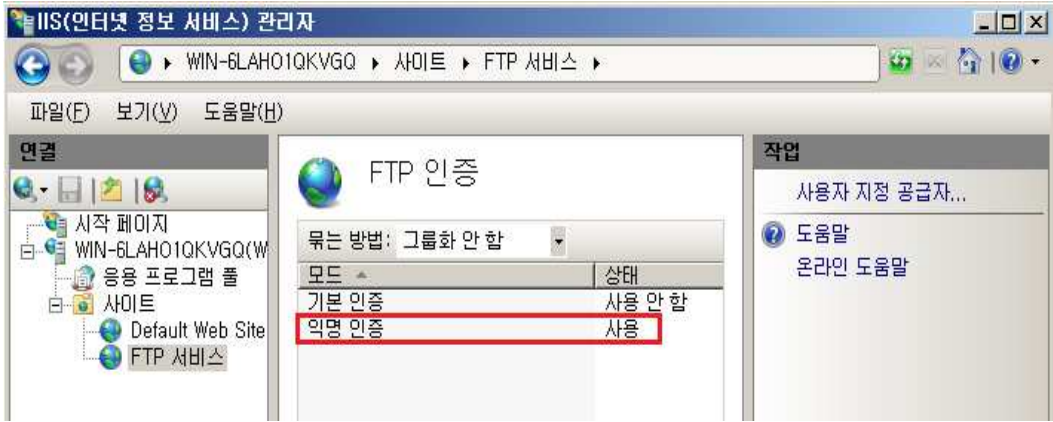
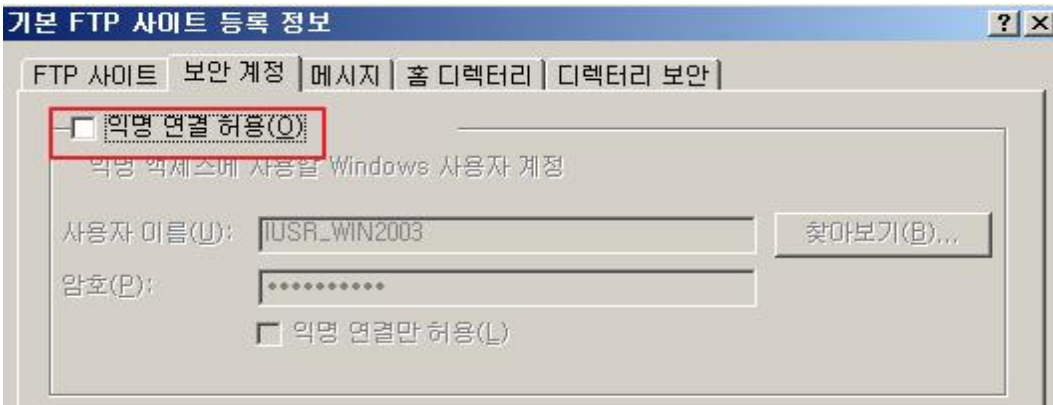
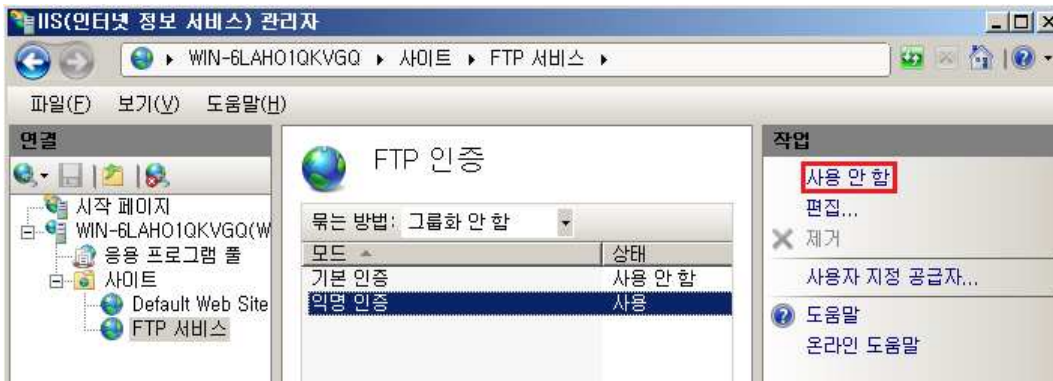
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                                                                                                                                                               |
| 조치 방법 | <p>FTP서비스에 접근을 허용하거나 거부하는 IP를 추가하여 설정한다.<br/>[Win2003]</p> <p>■ 인터넷 정보 서비스(IIS) 관리에서 설정<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 인터넷 정보 서비스(IIS) 관리 &gt; FTP 사이트 &gt; 사용중인 FTP 사이트 &gt; 속성 &gt; 디렉터리 보안에서 액세스를 허가하거나 거부하는 IP를 추가하여 설정</p>  <p>[Win2008]</p> <p>■ IIS(인터넷 정보 서비스) 관리자에서 설정<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; IIS(인터넷 정보 서비스) 관리자 &gt; 사용중인 FTP 서비스 &gt; FTP IPv4 주소 및 도메인 제한 에서 허용 및 거부 IP를 추가하여 설정</p> |



|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                    |

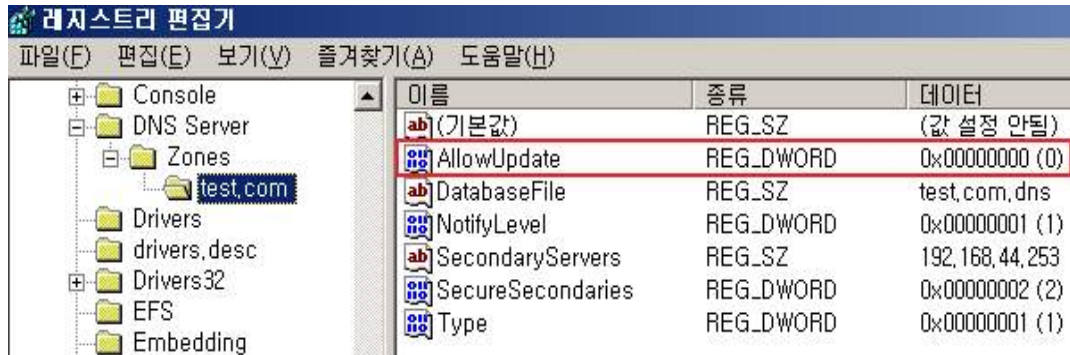
## 2.2.5. Anonymous FTP 접속 제한

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | WS2-05 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 설명    | <p>FTP 서비스를 이용해야 하는 경우 Default 설정으로 되어 있는 익명연결 허용을 금지하고, FTP 를 위한 계정을 따로 만들어서 사용해야 한다.</p> <p>또한 Password는 복잡도를 높이고 권한은 해당 디렉터리에 대한 읽기 권한만 부여한다. Home Directory는 Default로 설정하지 말고, 임의의 폴더를 생성하여 설정하는 것이 바람직하다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 진단 기준 | <p>양호 - FTP를 사용하지 않거나 "익명 연결 허용" 이 체크되어 있지 않은 경우</p> <p>취약 - FTP를 사용하거나 "익명 연결 허용" 이 체크되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>FTP 서비스의 "익명 연결 허용" 설정 여부를 확인한다.</p> <p>[Win2003]</p> <p>■ 명령 프롬프트에서 확인</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; cmd 에서 cd c:\WinetpubWAdminScripts 명령어 실행 후,</li> <li>cscript adsutil.vbs get MSFTPSVC/AllowAnonymous   find /v "Microsoft" 명령어를 실행하여 AllowAnonymous 값이 False인지 확인 (값이 False 일 경우 양호)</li> </ol> <pre>C:\WinetpubWAdminScripts&gt;cscript adsutil.vbs get MSFTPSVC/AllowAnonymous Microsoft (R) Windows Script Host 버전 5.6 Copyright (C) Microsoft Corporation 1996-2001. All rights reserved. AllowAnonymous                : &lt;BOOLEAN&gt; True</pre> <p>■ 인터넷 정보 서비스(IIS)에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 인터넷 정보 서비스(IIS) 관리 &gt; FTP 사이트 &gt; 사용중인 FTP 사이트 &gt; 속성 &gt; 보안계정 에서 "익명 연결 허용" 이 제한되어 있는지 확인 ("익명 연결 허용" 체크가 되어 있지 않으면 양호)</p>  <p>[Win2008]</p> <p>■ IIS(인터넷 정보 서비스) 관리자에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; IIS(인터넷 정보 서비스) 관리자 &gt; 사용중인 FTP 서비스 &gt; FTP 인증 에서 "익명 인증" 이 "사용 안 함" 으로 되어 있는지 확인한다. (익명 인증이 "사용 안 함" 으로 되어 있으면 양호)</p> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 조치 방법 | <p>FTP 서비스에 대하여 익명 연결을 허용하지 않도록 설정한다.<br/>[Win2003]</p> <p>■ 인터넷 정보 서비스에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 인터넷 정보 서비스(IIS) 관리 &gt; FTP 사이트 &gt; 사용중인 FTP 사이트 &gt; 속성 &gt; 보안계정 에서 "익명 연결 허용" 체크 해제</p>  <p>[Win2003]</p> <p>■ IIS(인터넷 정보 서비스) 관리자에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; IIS(인터넷 정보 서비스) 관리자 &gt; 사용중인 FTP 서비스 &gt; FTP 인증 에서 "익명 인증" 을 "사용 안 함" 으로 설정</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## 2.2.6. DNS 서비스 구동 점검

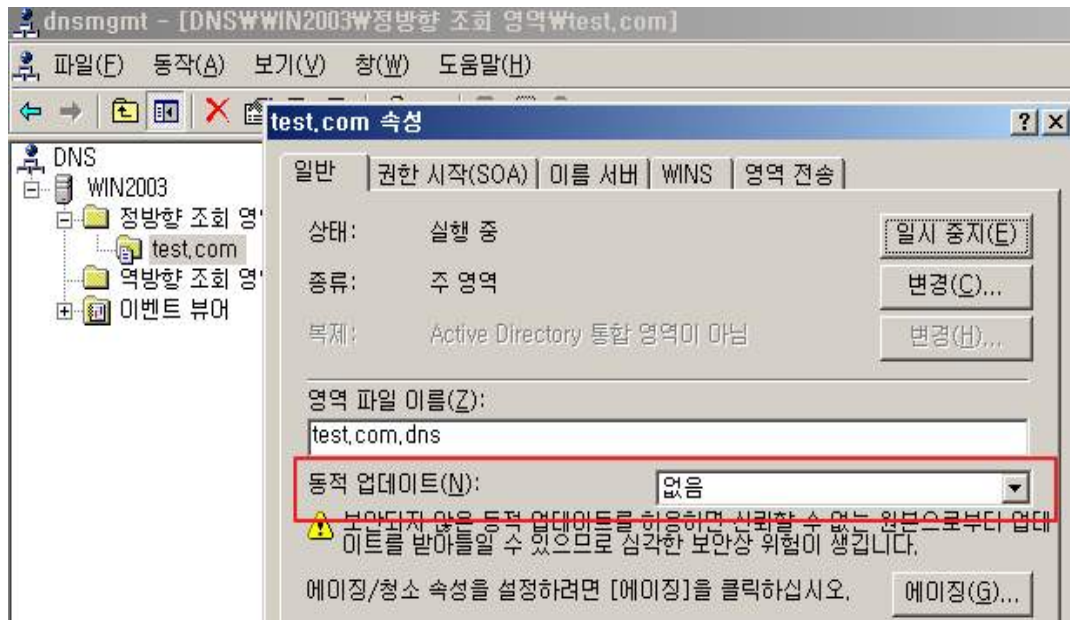
| 분류                         | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | WS2-06 | 중요도 | M |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|----|----|----|-------|----------------------------|-------|-----|----|------------|-------|-----|----|-------------------|--------|-----|----|-------------------------|-------|-----|----|
| 대상                         | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| 설명                         | <p>동적 업데이트는 변경 사항이 있을 때마다 DNS 클라이언트 컴퓨터가 자신의 리소스 레코드를 DNS서버에 등록하고 동적으로 업데이트할 수 있게 하며, 이 기능을 사용하면 특히 위치를 자주 이동하거나 변경하고 DHCP를 통해 IP 주소를 얻는 클라이언트의 영역 레코드 수동 관리 작업을 줄일 수 있다.</p> <p>하지만 동적 업데이트를 사용할 경우 악의적인 사용자에 의해 신뢰할 수 없는 데이터가 받아들여 질 수 있기 때문에 동적 업데이트를 사용하지 않아야 하며, DNS 서버를 사용하지 않을 경우 중지시켜야 한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| 진단 기준                      | <p>양호 - DNS 서비스를 사용하지 않거나 동적 업데이트가 "없음" 으로 설정되어 있는 경우</p> <p>취약 - DNS 서비스를 사용하며 동적 업데이트가 설정되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| 점검 방법                      | <p>DNS 서비스가 구동 중인지 확인하고, 구동 시 동적 업데이트 설정 여부를 점검한다.<br/>[Win2003, Win2008]</p> <p>1. DNS구동 여부 확인</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net start 명령어를 이용하여 DNS 서비스 구동 확인</p> <div><pre>C:\Documents and Settings\Administrator&gt;net start 다음과 같은 Windows 서비스가 시작되었습니다.  Application Experience Lookup Service Application Layer Gateway Service <b>DNS Server</b> Group Policy Client</pre></div> <p>■ 서비스에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 에서 DNS Server가 중지되어 있는지 확인</p> <table><thead><tr><th>이름</th><th>설명</th><th>상태</th><th>시작 유형</th></tr></thead><tbody><tr><td> Distributed Transaction...</td><td>데이...</td><td>시작됨</td><td>자동</td></tr><tr><td> DNS Client</td><td>미 ...</td><td>시작됨</td><td>자동</td></tr><tr><td> <b>DNS Server</b></td><td>DNS...</td><td>시작됨</td><td>자동</td></tr><tr><td> Error Reporting Service</td><td>예상...</td><td>시작됨</td><td>자동</td></tr></tbody></table> <p>2. DNS 구동 시, 동적 업데이트 설정 여부</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\DNS Server\Zones\운영중인 DNS 영역 에서 AllowUpdated의 값이 0 으로 되어 있는지 확인 (값이 0일 경우 양호)</p> |       |        |     |   | 이름 | 설명 | 상태 | 시작 유형 | Distributed Transaction... | 데이... | 시작됨 | 자동 | DNS Client | 미 ... | 시작됨 | 자동 | <b>DNS Server</b> | DNS... | 시작됨 | 자동 | Error Reporting Service | 예상... | 시작됨 | 자동 |
| 이름                         | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 상태    | 시작 유형  |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| Distributed Transaction... | 데이...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 시작됨   | 자동     |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| DNS Client                 | 미 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 시작됨   | 자동     |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| <b>DNS Server</b>          | DNS...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 시작됨   | 자동     |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |
| Error Reporting Service    | 예상...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 시작됨   | 자동     |     |   |    |    |    |       |                            |       |     |    |            |       |     |    |                   |        |     |    |                         |       |     |    |



- AllowUpdate = 0 : 동적 업데이트 사용 안함
- AllowUpdate = 1 : 동적 업데이트 사용

■ DNS 관리자에서 확인

시작 > 프로그램 > 관리도구 > DNS > 정방향 조회 영역 > 사용중인 DNS > 속성 > 일반 탭에서 "동적 업데이트" 가 "없음" 으로 되어 있는지 확인 (없음 일 경우 양호)



조치 방법

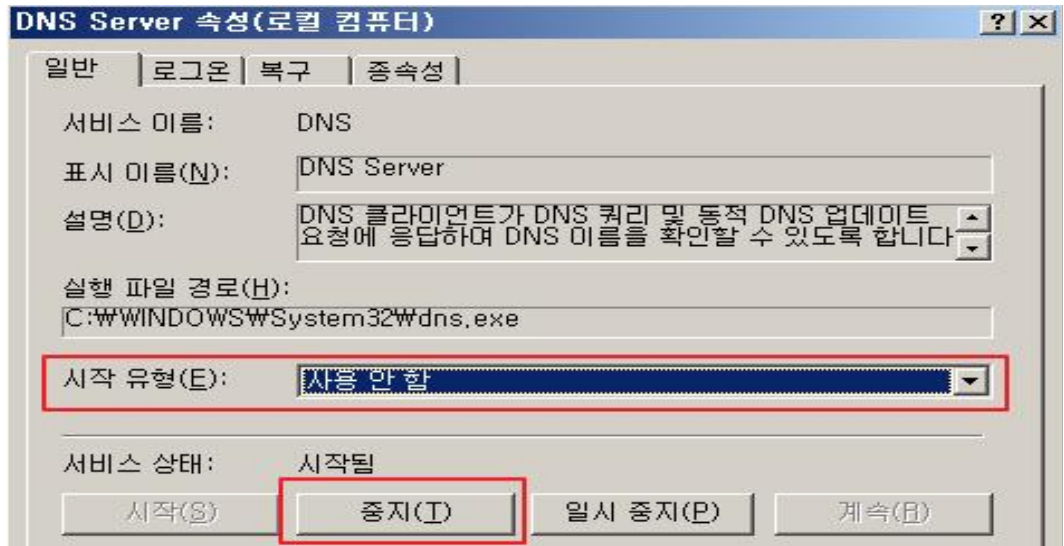
DNS 서비스 불필요 시 서비스를 중지/사용 안 함 설정하고, 사용할 경우 동적 업데이트를 "없음" 설정한다.

[Win2003, Win2008]

1. DNS 서비스 불필요 시 서비스 제거

■ DNS 관리자를 통한 설정

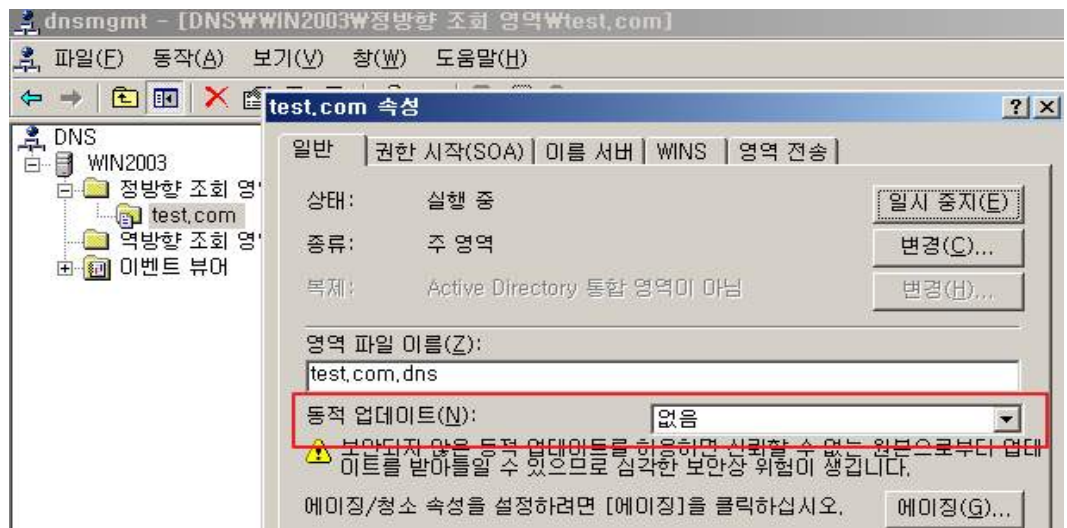
시작 > 프로그램 > 관리도구 > 서비스 > DNS Server > 속성 에서 시작 유형을 "사용 안 함" 으로 설정 후, DNS 서비스를 중지



## 2. DNS 서비스 사용 시 동적 업데이트 제거

### ■ DNS 관리자를 통한 설정

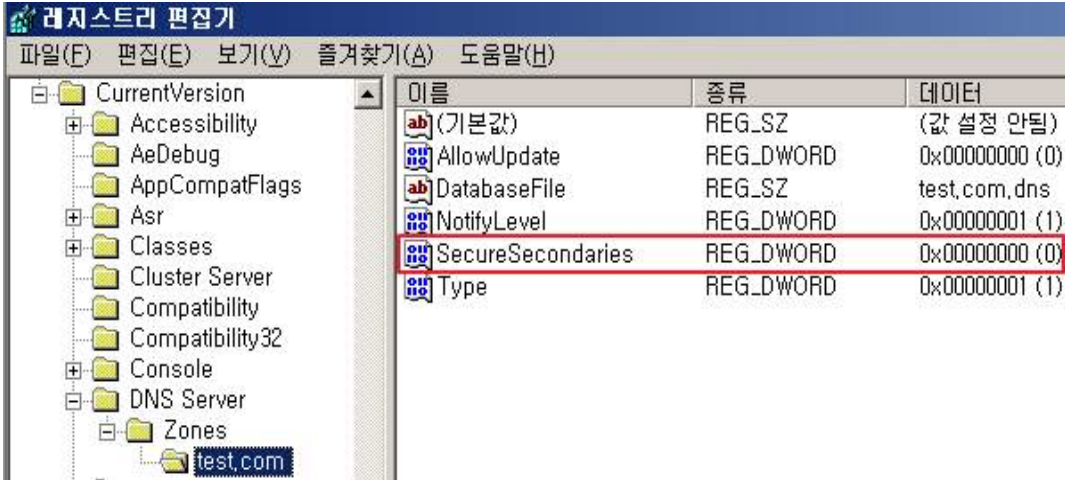
시작 > 프로그램 > 관리도구 > DNS > 정방향 조회 영역 > 사용중인 DNS > 속성  
에서 "동적 업데이트" 를 "없음" 으로 설정

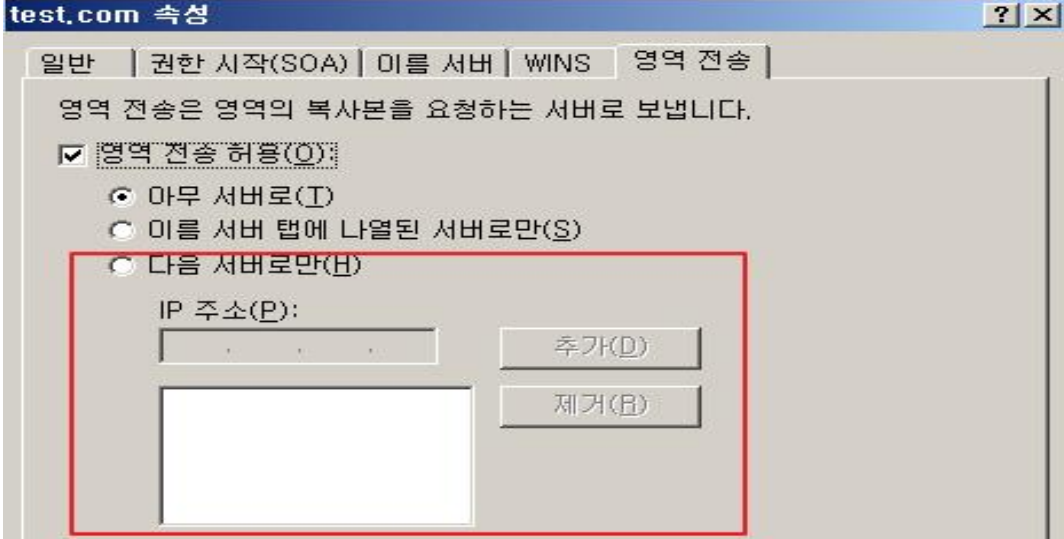
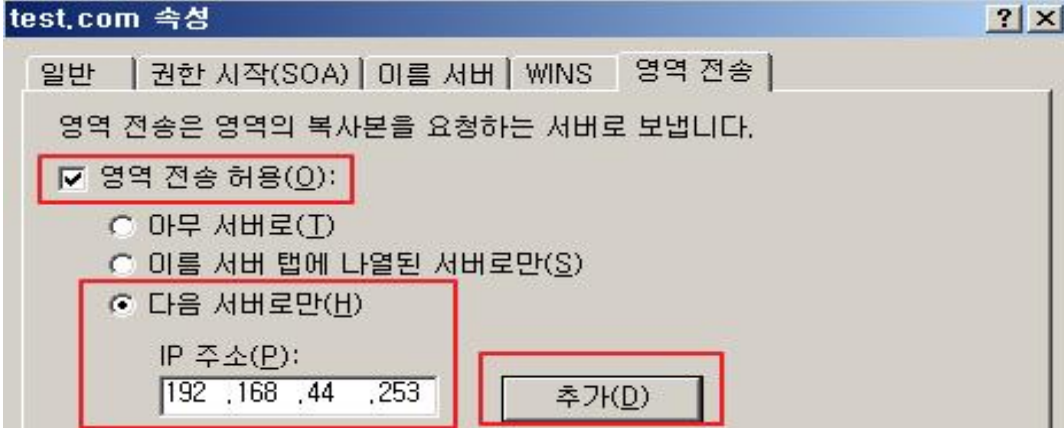


비고



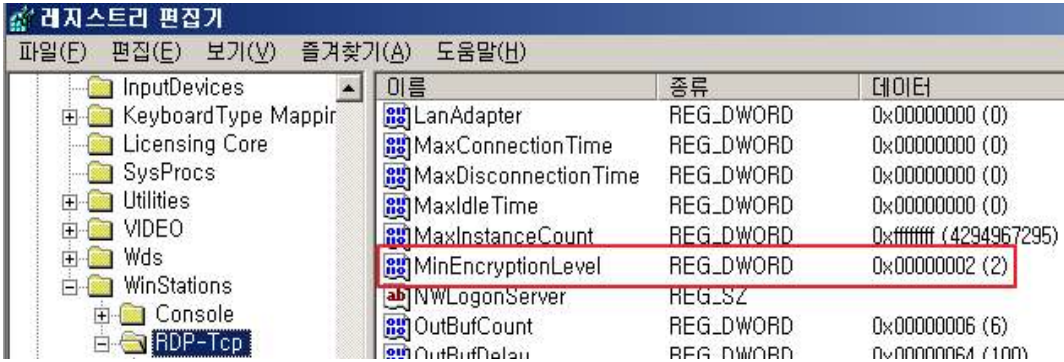
## 2.2.7. DNS Zone Transfer 설정

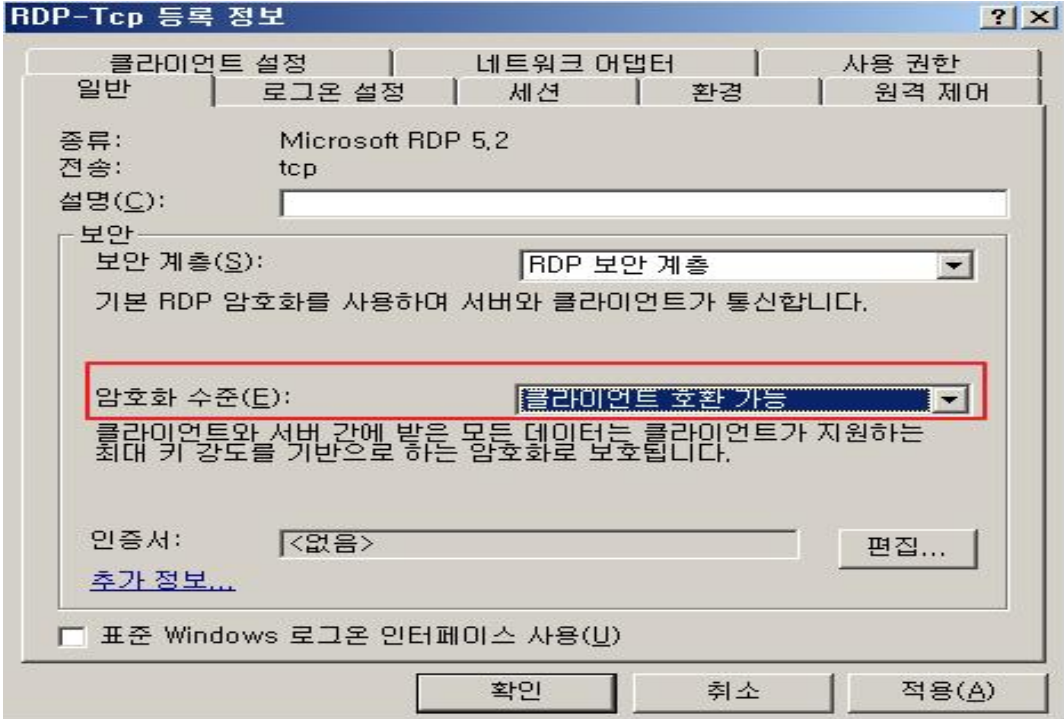
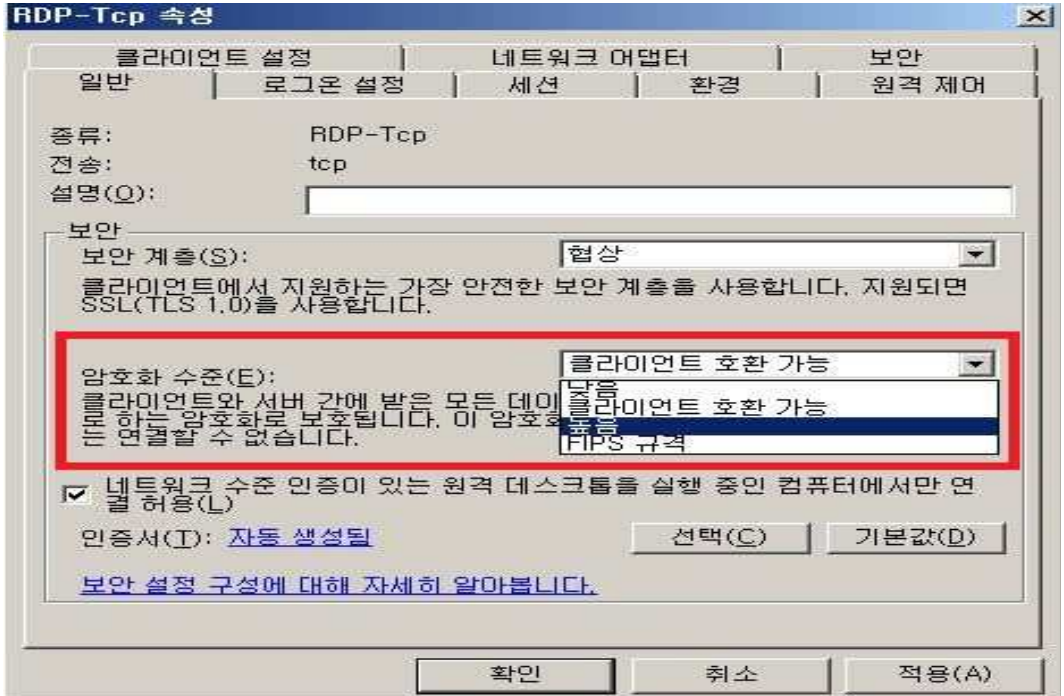
| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | WS2-07 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않으며, 적절한 설정을 통하여 이러한 정보의 전송을 제한할 수 있다. 또한 DNS 서버를 사용하지 않을 경우 서비스를 중지해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | <p>양호 - Zone Transfer(영역 전송) 허용을 하지 않거나, 특정 서버로만 허용되어 있는 경우</p> <p>취약 - Zone Transfer(영역 전송)이 특정 서버 이외에 허용되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | <p>DNS 영역 전송의 설정을 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\DNS Server\Zones\운영중인 DNS 영역 에서 SecureSecondaries 값이 2로 설정되어 있는지 확인 (해당 값이 2일 경우 양호)</p>  <p>                     - SecureSecondaries = 0 : 아무 서버로 영역 전송<br/>                     - SecureSecondaries = 1 : 이름 서버 탭에 나열된 서버로만 영역 전송<br/>                     - SecureSecondaries = 2 : 다음 서버로만 영역 전송                 </p> <p>■ DNS 관리자에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; DNS &gt; 정방향 조회 영역 &gt; 사용중인 DNS &gt; 속성 &gt; 영역 전송 에서 특정 서버로만 영역 전송이 이루어지도록 되어있는지 확인</p> <p>("영역 전송 허용" 설정이 제한되어 있거나, 허용 시, "다음 서버로만" 으로 설정되어 있을 경우 양호)</p> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                            |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                          |
| 조치 방법 | <p>영역 전송을 특정 서버로만 이루어질 수 있도록 IP를 등록한다.<br/>[Win2003, Win2008]</p> <p>■ DNS 관리자에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; DNS &gt; 정방향 조회 영역 &gt; 사용중인 DNS &gt; 속성 &gt; 영역 전송 에서 "영역 전송 허용"을 제한하거나, 사용 시 특정 서버로만 영역 전송이 이루어지도록 IP 등록</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                            |

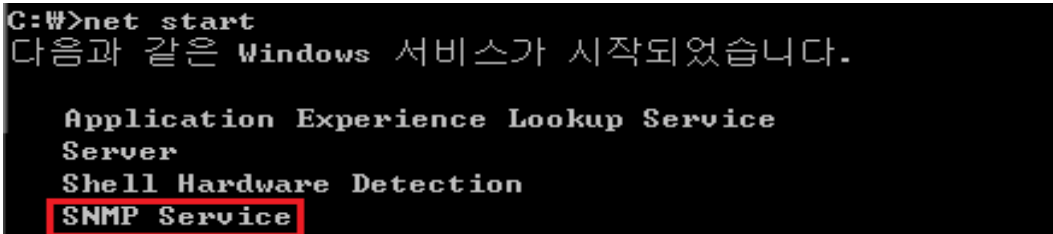


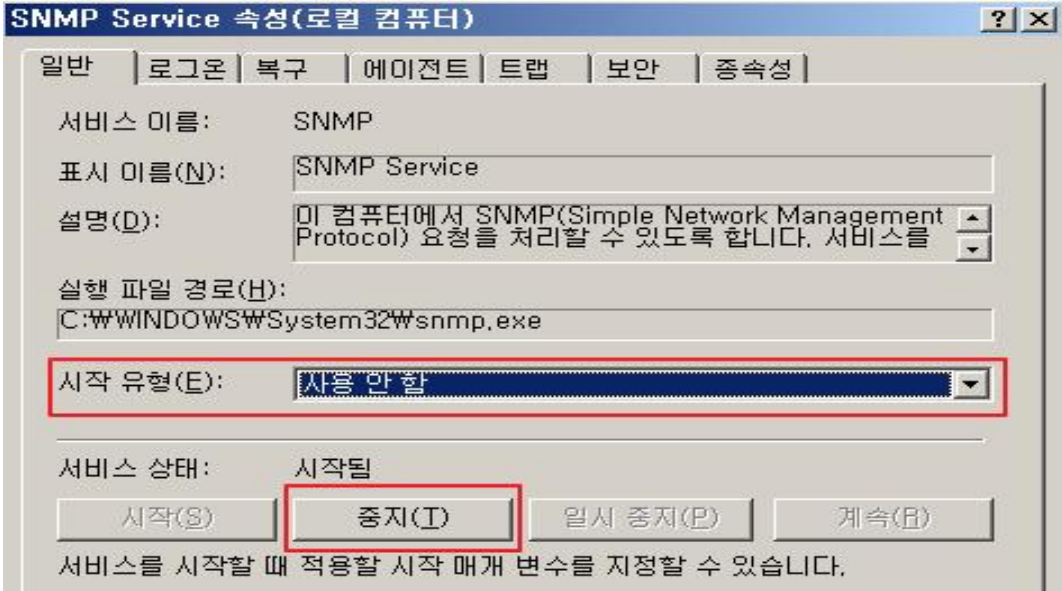
## 2.2.8. 터미널 서비스 암호화 수준 설정

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | WS2-08 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | 터미널 서비스는 원격지에 있는 서버를 관리하기 위한 유용한 도구이나 취약한 패스워드를 사용하거나 접근제어가 적절치 못할 경우 해킹의 도구로 악용될 수 있다. 따라서 불필요하게 터미널 서비스가 사용되고 있는지 점검해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 진단 기준 | <p>양호 - 터미널 서비스를 사용하지 않거나, 사용 시 암호화 수준을 "클라이언트와 호환 가능(중간)" 이상으로 설정한 경우</p> <p>취약 - 터미널 서비스를 사용하고 암호화 수준이 "낮음" 으로 설정한 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>터미널 서비스가 구동 중인지 확인하고, 구동 시 암호화 수준 값을 점검한다.<br/>[Win2003, Win2008]</p> <p>1. 터미널 서비스 구동 여부 확인</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net start 명령어를 실행하여 터미널 서비스 구동 여부 확인</p>  <p>2. 터미널 서비스 구동 시 암호화 수준 확인</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; regedit &gt; HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp에서 MinEncryptionLevel의 값이 2 이상으로 되어 있는지 확인 (해당 값이 2이상 일 경우 양호)</p>  <p>■ 서비스에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 터미널 서비스 구성 &gt; 연결 &gt; RDP-Tcp &gt; 속성에서 암호화 수준이 "낮음" 이외의 값으로 설정되어 있는지 확인 (해당 값이 "낮음" 이외의 값으로 설정되어 있을 시 양호)</p> |       |        |     |   |

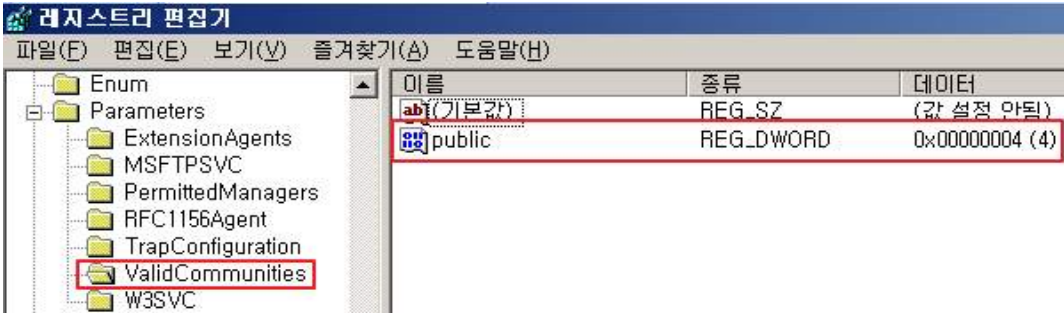
|       |                                                                                                                                                                                                                                                                                                                            |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                         |
| 조치 방법 | <p>터미널 서비스 불필요 시 서비스를 중지/사용 안 함 설정하고, 사용 시 암호화 수준을 "클라이언트와 호환 가능(중간)" 이상으로 설정한다.</p> <p>[Win2003, Win2008]</p> <p>■ 서비스에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 터미널 서비스 구성 &gt; 연결 &gt; RDP-Tcp &gt; 속성에서 암호화 수준을 "낮음" 이외의 값으로 설정</p>  |
| 비고    |                                                                                                                                                                                                                                                                                                                            |

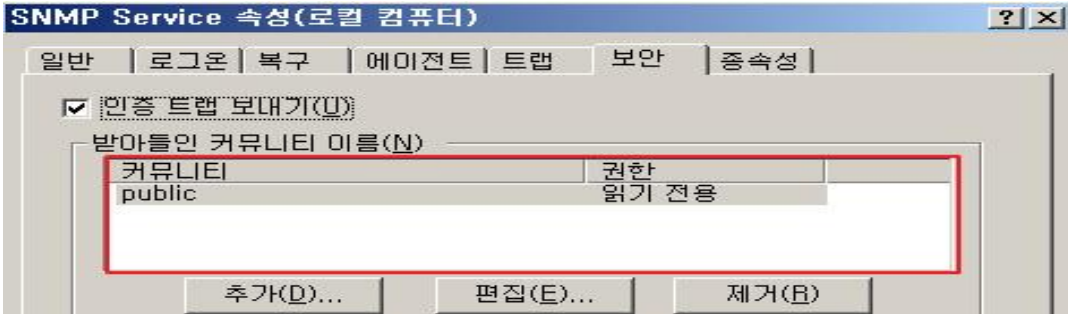
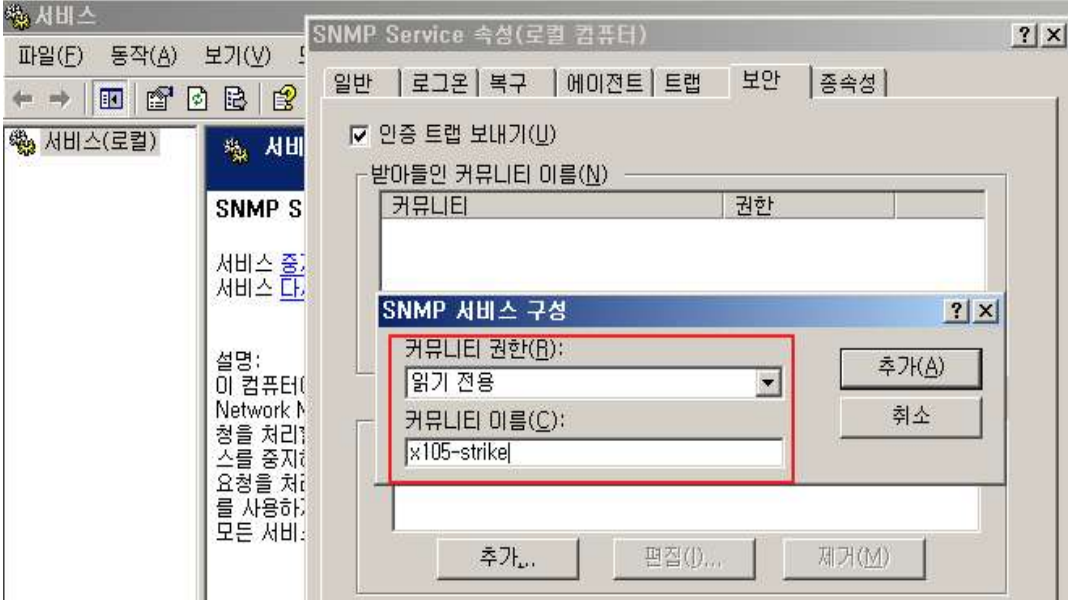
## 2.2.9. SNMP 서비스 구동 점검

| 분류                                                                                                           | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드      | WS2-09 | 중요도           | M |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------|---------------|---|------|----|----|-------|-------------|-----------------------------------------------------------------------------------------------------|-------|-----|----|--------------|-------------------------------------------------------------------------------------------------------------|-------|-----|----|--------------|--------------------------------------------------------------------------------------------|-------|-----|----|--------------|--------------------------------------------------------------------------------------------------------------|-------|-----|----|--------------|------------------------------------------------------------------------------------------------------------|-------|-----|----|--------------|------------------------------------------------------------------------------------------------|-------|--|----|---------------|---------------------------------------------------------------------------------------------------------|-------|------------|----|--------------|-------------------------------------------------------------------------------------------------------|-------|-----|----|---------------|
| 대상                                                                                                           | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |        |               |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
| 설명                                                                                                           | SNMP 서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스로 SNMP 서비스를 사용하지 않을 경우 중지시켜야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |        |               |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
| 진단 기준                                                                                                        | 양호 - SNMP 서비스를 사용하지 않을 경우<br>취약 - SNMP 서비스를 사용하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |        |               |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
| 점검 방법                                                                                                        | <p>SNMP 서비스가 구동되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인<br/>시작 &gt; 실행 &gt; cmd &gt; net start 명령어를 이용하여 SNMP 서비스 구동 여부 확인</p> <div></div> <p>■ 서비스에서 확인<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 에서 SNMP Service가 시작되어 있는지 확인</p> <table><tr><th>이름 ▲</th><th>설명</th><th>상태</th><th>시작 유형</th><th>다음 사용자로 로그인</th></tr><tr><td> Secondary Logon</td><td>다른...</td><td>시작됨</td><td>자동</td><td>Local System</td></tr><tr><td> Security Accounts Ma...</td><td>서비...</td><td>시작됨</td><td>자동</td><td>Local System</td></tr><tr><td> Server</td><td>이 ...</td><td>시작됨</td><td>자동</td><td>Local System</td></tr><tr><td> Shell Hardware Detect...</td><td>자동...</td><td>시작됨</td><td>자동</td><td>Local System</td></tr><tr><td> Simple TCP/IP Services</td><td>다음...</td><td>시작됨</td><td>자동</td><td>Local System</td></tr><tr><td> Smart Card</td><td>컴퓨...</td><td></td><td>수동</td><td>Local Service</td></tr><tr><td> <b>SNMP Service</b></td><td>이 ...</td><td><b>시작됨</b></td><td>자동</td><td>Local System</td></tr><tr><td> SNMP Trap Service</td><td>로컬...</td><td>시작됨</td><td>수동</td><td>Local Service</td></tr></table> |            |        |               |   | 이름 ▲ | 설명 | 상태 | 시작 유형 | 다음 사용자로 로그인 |  Secondary Logon | 다른... | 시작됨 | 자동 | Local System |  Security Accounts Ma... | 서비... | 시작됨 | 자동 | Local System |  Server | 이 ... | 시작됨 | 자동 | Local System |  Shell Hardware Detect... | 자동... | 시작됨 | 자동 | Local System |  Simple TCP/IP Services | 다음... | 시작됨 | 자동 | Local System |  Smart Card | 컴퓨... |  | 수동 | Local Service |  <b>SNMP Service</b> | 이 ... | <b>시작됨</b> | 자동 | Local System |  SNMP Trap Service | 로컬... | 시작됨 | 수동 | Local Service |
| 이름 ▲                                                                                                         | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 상태         | 시작 유형  | 다음 사용자로 로그인   |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Secondary Logon          | 다른...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Security Accounts Ma...  | 서비...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Server                   | 이 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Shell Hardware Detect... | 자동...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Simple TCP/IP Services   | 다음...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  Smart Card               | 컴퓨...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            | 수동     | Local Service |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  <b>SNMP Service</b>      | 이 ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>시작됨</b> | 자동     | Local System  |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
|  SNMP Trap Service        | 로컬...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 시작됨        | 수동     | Local Service |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |
| 조치 방법                                                                                                        | <p>불필요한 SNMP 서비스를 중지시킨다.<br/>[Win2003, Win2008]</p> <p>■ 서비스에서 설정<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 &gt; SNMP Service &gt; 속성에서 시작 유형을 "사용 안 함" 으로 적용 후, SNMP 서비스를 중지</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |        |               |   |      |    |    |       |             |                                                                                                     |       |     |    |              |                                                                                                             |       |     |    |              |                                                                                            |       |     |    |              |                                                                                                              |       |     |    |              |                                                                                                            |       |     |    |              |                                                                                                |       |  |    |               |                                                                                                         |       |            |    |              |                                                                                                       |       |     |    |               |

|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                    |

## 2.2.10. SNMP Default Community String 변경

| 분류    | 서비스 관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | WS2-10 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | SNMP 서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스이다. 그러나 이 정보를 받기 위한 일종의 패스워드인 Community String이 Default로 public, private로 설정되어 있는 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 비인가 사용자가 시스템의 주요 정보 및 설정 상황을 파악 할 수 있는 취약성이 존재한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | <p>양호 - SNMP Community 이름이 public, private이 아니고, 권한이 읽기 전용인 경우</p> <p>취약 - SNMP Community 이름이 public, private이거나 쓰기 권한이 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 점검 방법 | <p>SNMP Community 값의 public, private 설정 여부와 읽기 권한으로 되어있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities 에서 이름이 Public, Private이 아니고, 데이터 값이 4로 되어 있는지 확인 (이름이 Public, Private으로 되어 있지 않고, 데이터 값이 4로 되어있으면 양호)</p>  <ul style="list-style-type: none"> <li>- ValidCommunities = 1 (속성 없음)</li> <li>- ValidCommunities = 2 (알림 속성)</li> <li>- ValidCommunities = 4 (읽기 전용속성)</li> <li>- ValidCommunities = 8 (읽기,쓰기속성)</li> <li>- ValidCommunities = 16 (읽기,만들기속성)</li> </ul> <p>■ 서비스에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 &gt; SNMP Service &gt; 속성 &gt; 보안 탭에서 커뮤니티 이름이 Public, Private 이외의 값으로 되어 있고, 읽기 전용으로 되어 있는지 확인</p> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                 |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                               |
| 조치 방법 | <p>SNMP 서비스 불필요 시 서비스를 중지시키고, 사용 시 커뮤니티 이름을 Public, Privacy 이외의 값으로 추가하고, 권한은 읽기 전용으로 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 서비스에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 서비스 &gt; SNMP Service &gt; 속성 &gt; 보안 탭에서 커뮤니티 이름을 Public, Privacy 이외의 값으로 추가하고, 권한은 읽기 전용으로 설정</p>  |
| 비고    | <p>NMS 에서 서버를 모니터링 하는 경우 SNMP 를 사용하며 기타 SNMP 를 사용할 경우 Community 이름 변경시 통신하고자 하는 Server/Client에 모두 같은 Community 이름을 사용해야 한다.</p>                                                                                                                                                                                                                                 |

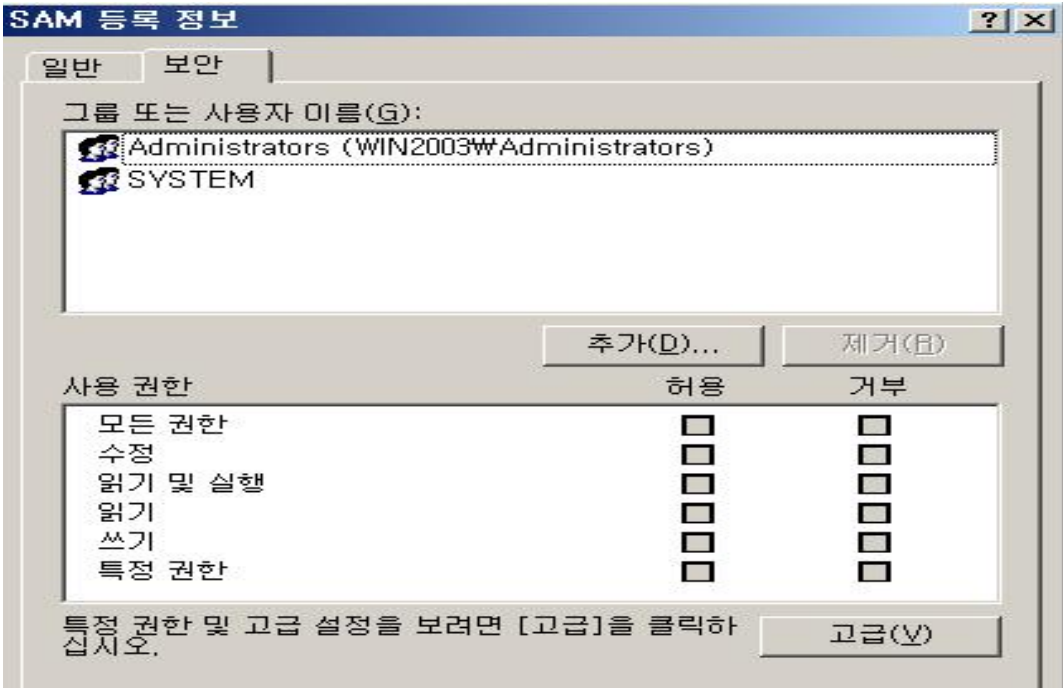
## 2.3. 기타 보안설정

### 2.3.1. 백신 프로그램 설치

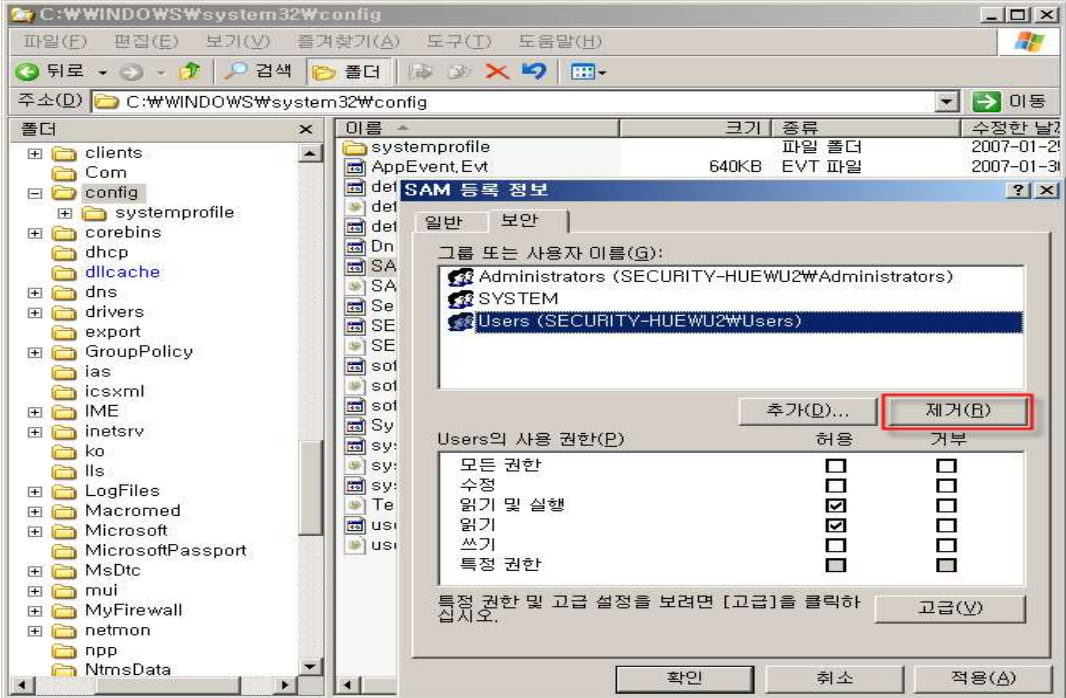
| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | WS3-01 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 설명    | <p>웜, 트로이목마 등의 악성 바이러스로 인한 피해규모가 커지고 있으며 이에 대한 피해를 최소화 하기 위해 반드시 바이러스 백신 프로그램을 설치해야 한다.</p> <p>바이러스 백신 프로그램은 바이러스 감염 여부 진단 및 치료, 파일의 보호를 할 수 있으며 예방도 가능하다.</p>                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | <p>양호 - 바이러스 백신 프로그램이 설치되어 있는 경우</p> <p>취약 - 바이러스 백신 프로그램이 설치되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>다음 항목들을 수동으로 점검한다.</p> <ul style="list-style-type: none"> <li>- 바이러스 백신 프로그램 설치 여부</li> <li>- 실시간 감시 기능 설정 여부</li> <li>- 최신 Update 여부</li> </ul>                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 조치 방법 | <p>담당자를 통하여 바이러스 백신을 설치하도록 권고하며, 최신 보안패치를 확인하고, 실시간 감시를 설정해야 한다.</p> <ul style="list-style-type: none"> <li>- 안철수 연구소 : <a href="http://www.ahnlab.com">http://www.ahnlab.com</a></li> <li>- 하우리 : <a href="http://www.hauri.co.kr">http://www.hauri.co.kr</a></li> <li>- 시만텍코리아 : <a href="http://www.symantec.co.kr">http://www.symantec.co.kr</a></li> <li>- 한국트렌드마이크로: <a href="http://www.trendmicro.co.kr/">http://www.trendmicro.co.kr/</a></li> </ul> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |



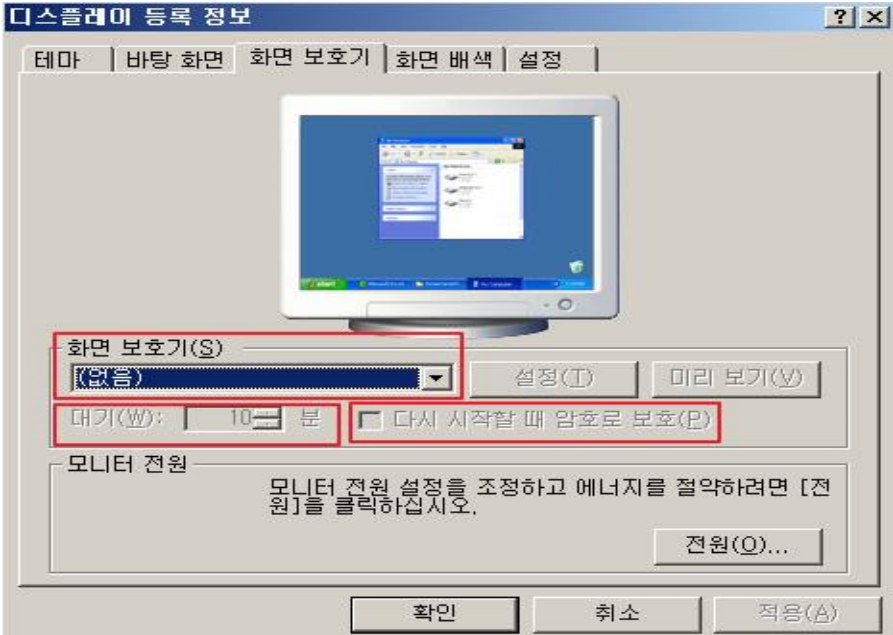
### 2.3.2. SAM 파일 접근 통제 설정

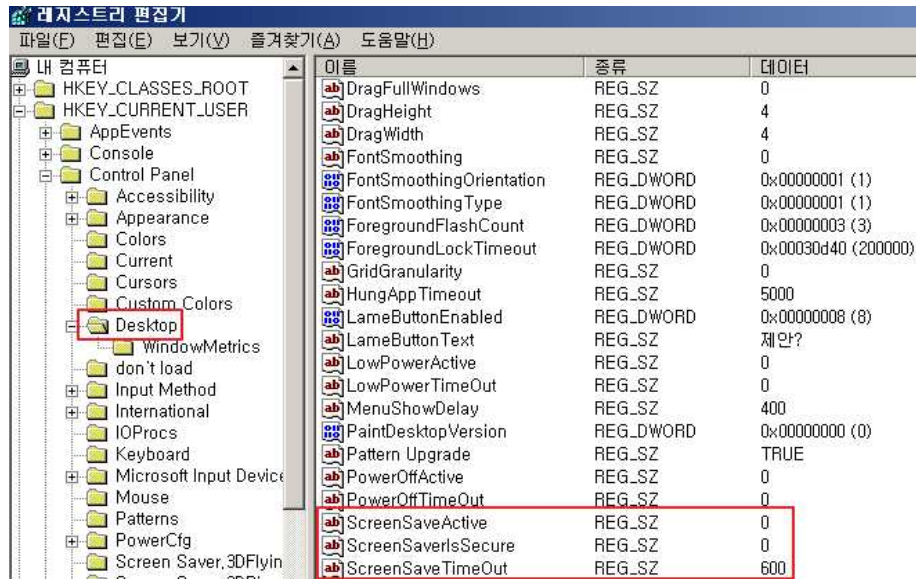
| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | WS3-02 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | <p>Security Account Manager (SAM) 파일은 사용자와 그룹 계정들을 다루고, LSA를 위한 인증을 제공한다.</p> <p>패스워드 공격 시도에 의한 Password Database가 노출 될 수 있으므로, Administrator 및 Sytem 그룹 외에는 SAM 파일에 대한 접근이 제한되어야 한다.</p>                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 진단 기준 | <p>양호 - SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 등록되어 있는 경우</p> <p>취약 - SAM 파일에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>SAM 파일의 접근 권한이 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 탐색기에서 확인</p> <p>탐색기 &gt; C:WWindowsWsystem32WconfigWSAM &gt; 속성 &gt; 보안 탭에서 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인</p>  <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; cacs %systemroot%Wsystem32WconfigWSAM 명령어를 통해 SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인</p> <p>※ 명령 프롬프트를 관리자 권한으로 실행</p> |       |        |     |   |



|              |                                                                                                                                                                                                                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <pre>C:\&gt;cacls %systemroot%\system32\config\SAM C:\WINDOWS\system32\config\SAM BUILTIN\Administrators:F NT AUTHORITY\SYSTEM:F</pre>                                                                                                                                                                            |
| <p>조치 방법</p> | <p>SAM 파일의 접근권한을 Administrator, System 그룹만 모든 권한을 허용하도록 설정한다.</p> <p>[Win2003, Win2008]</p> <p>■ 탐색기에서 설정</p> <p>탐색기 &gt; C:\WINDOWS\system32\config\SAM &gt; 속성 &gt; 보안 탭에서 Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거</p>  |
| <p>비고</p>    |                                                                                                                                                                                                                                                                                                                   |

### 2.3.3. 화면보호기 설정

| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | WS3-03 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 설명    | 사용자들은 시스템에서 잠시 떨어져 있을 경우에는 로그오프 하거나 워크스테이션 잠금 설정이 되어있는지 확인해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | <p>양호 - 화면보호기를 설정하고 암호를 사용하며 대기 시간이 5분 일 경우</p> <p>취약 - 화면보호기가 설정되어 있지 않거나 암호를 사용하지 않거나 대기시간이 5분 초과 일 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | <p>시스템의 화면보호기 설정이 되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 디스플레이에서 확인</p> <p>시작 &gt; 제어판 &gt; 디스플레이 &gt; 화면보호기 탭에서 아래 항목의 설정 여부 확인</p> <ol style="list-style-type: none"> <li>1. 화면 보호기 : 없음 이외의 값으로 설정되어 있을 경우 양호</li> <li>2. 대기 시간 : 5분</li> <li>3. 다시 시작할 때 암호로 보호 기능 사용 체크 여부</li> </ol>  <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_CURRENT_USER\Control Panel\Desktop 에서 아래와 같이 설정되어 있는지 확인</p> <ul style="list-style-type: none"> <li>- ScreenSaveActive = 1 (화면 보호기 활성화 : 1일 경우 양호)</li> <li>- ScreenSaverIsSecure = 1 (다시 시작할 때 암호로 보호 : 1일 경우 양호)</li> <li>- ScreenSaveTimeOut = 300 (대기 시간 설정 초 단위)</li> </ul> |       |        |     |   |



조치 방법시스템에 화면보호기 설정을 한다.

[Win2003, Win2008]

■ 디스플레이에서 설정

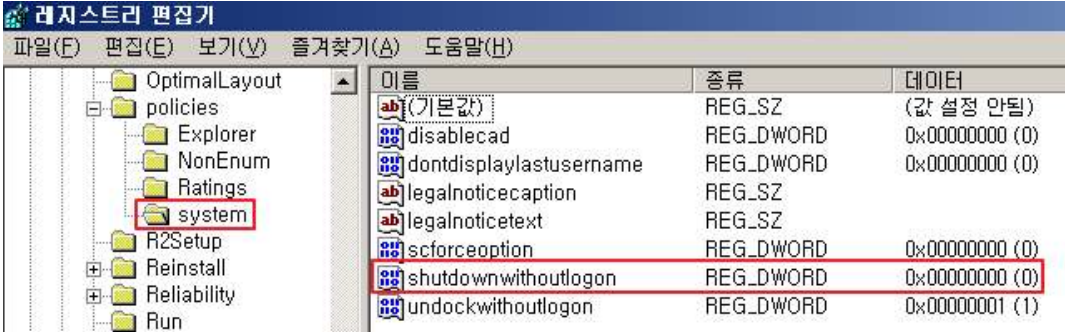
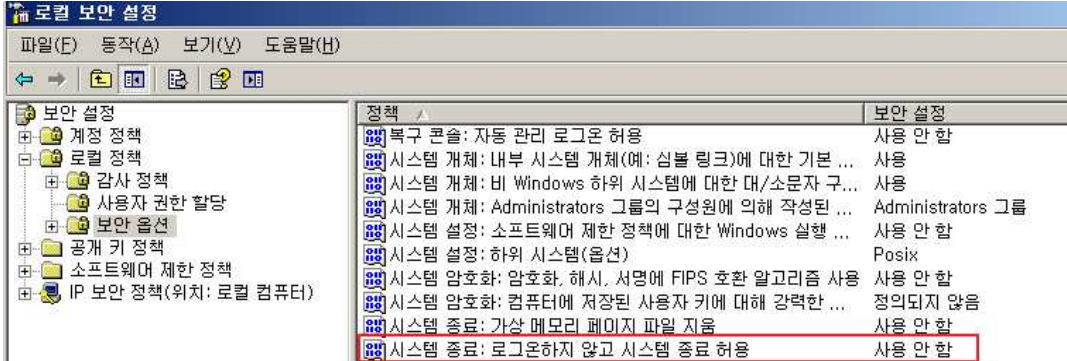
시작 > 제어판 > 디스플레이 > 화면보호기 탭에서 아래와 같이 설정

1. 화면 보호기 : 없음 이외의 값
2. 대기 시간 : 5분
3. 다시 시작할 때 암호로 보호 기능 체크

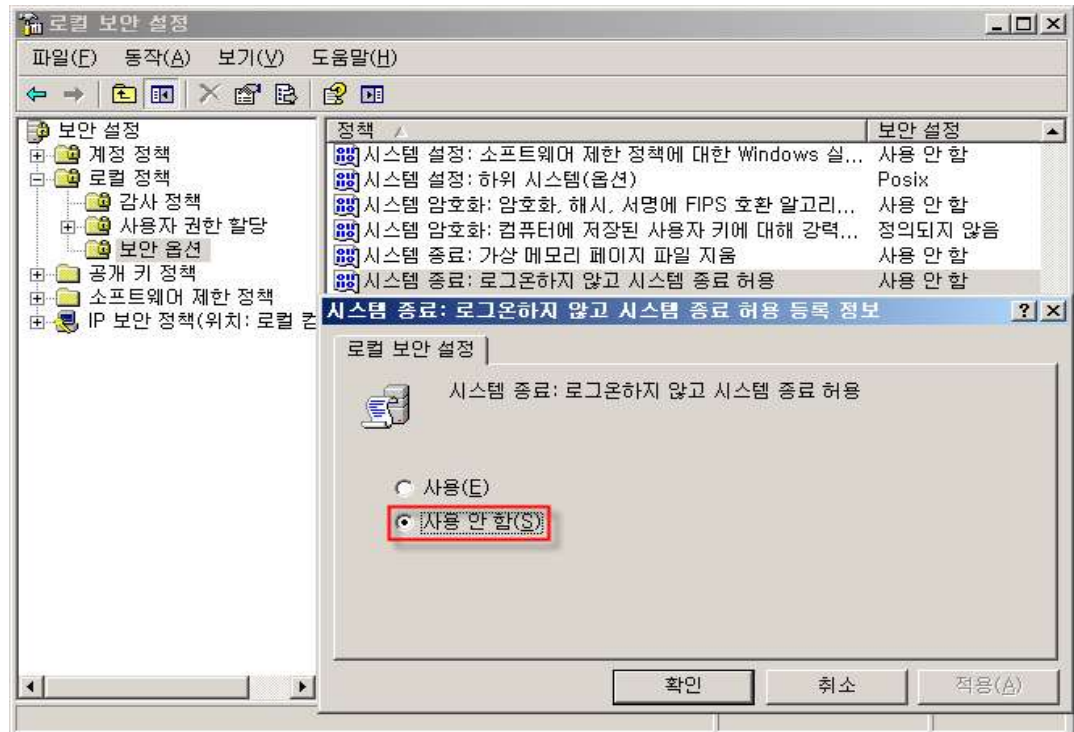


비고

### 2.3.4. 로그인 하지 않고 시스템 종료 허용

| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | WS3-04 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | 로그인 창에 "시스템 종료" 버튼이 활성화 되면, 비인가된 사용자 또는 인가된 사용자의 비의도적인 실수 등으로 로그인을 하지 않고도 시스템의 불법적인 시스템 다운을 가능하게 하여, 정상적인 서비스에 장애를 발생시킬 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 진단 기준 | <p>양호 - "로그온 하지 않고 시스템 종료 허용"이 "사용 안 함" 으로 설정되어 있을 경우</p> <p>취약 - "로그온 하지 않고 시스템 종료 허용"이 "사용" 으로 설정되어 있을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 점검 방법 | <p>"로그온 하지 않고 시스템 종료 허용"이 "사용 안 함" 으로 설정되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 에서 ShutdownWithoutLogon 값이 "0" (사용안함) 으로 설정되어 있는지 확인 (값이 0 으로 설정되어 있는 경우 양호)</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; "시스템 종료 : 로그인하지 않고 시스템 종료 허용" 정책이 "사용 안 함" 으로 되어 있는지 확인</p>  |       |        |     |   |
| 조치 방법 | <p>"로그온 하지 않고 시스템 종료 허용"이 "사용 안 함" 으로 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |

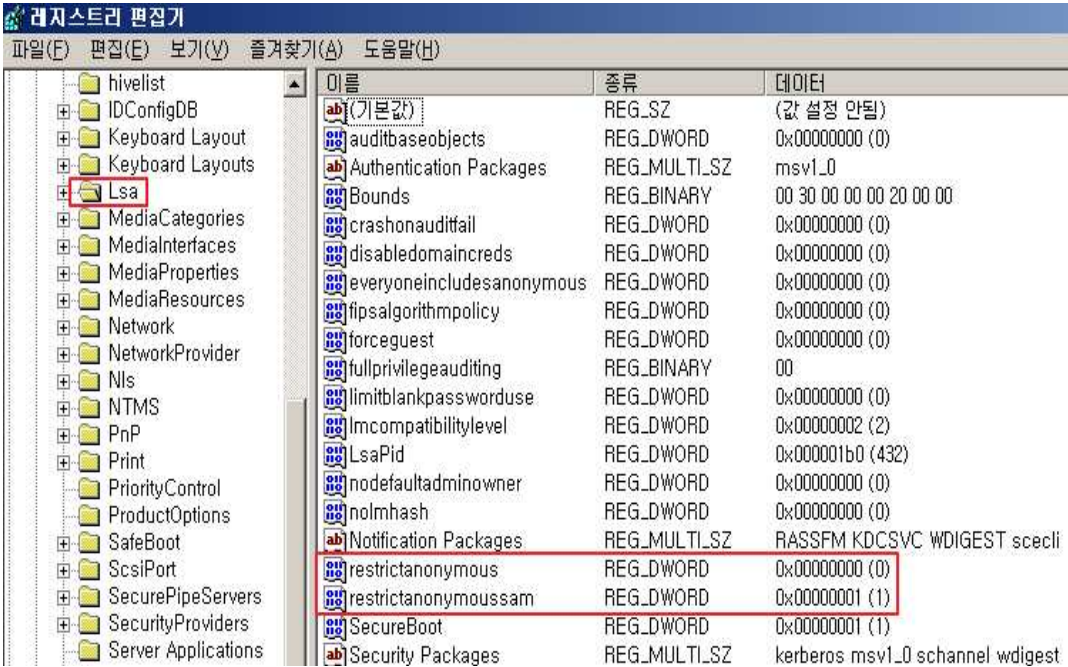
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 보안 옵션 > " 시스템 종료: 로그온하지 않고 시스템 종료 허용" 정책을 "사용 안 함" 으로 설정

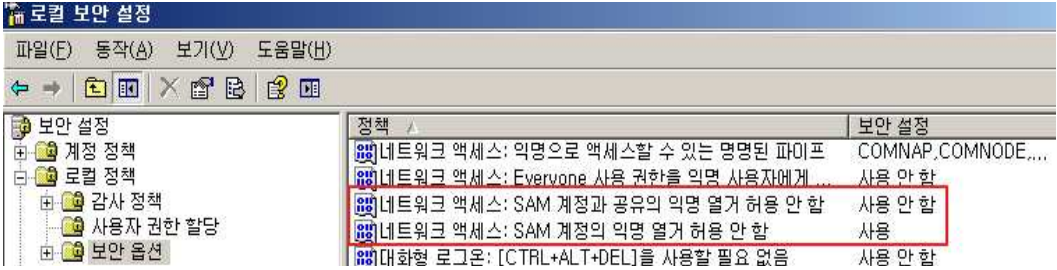
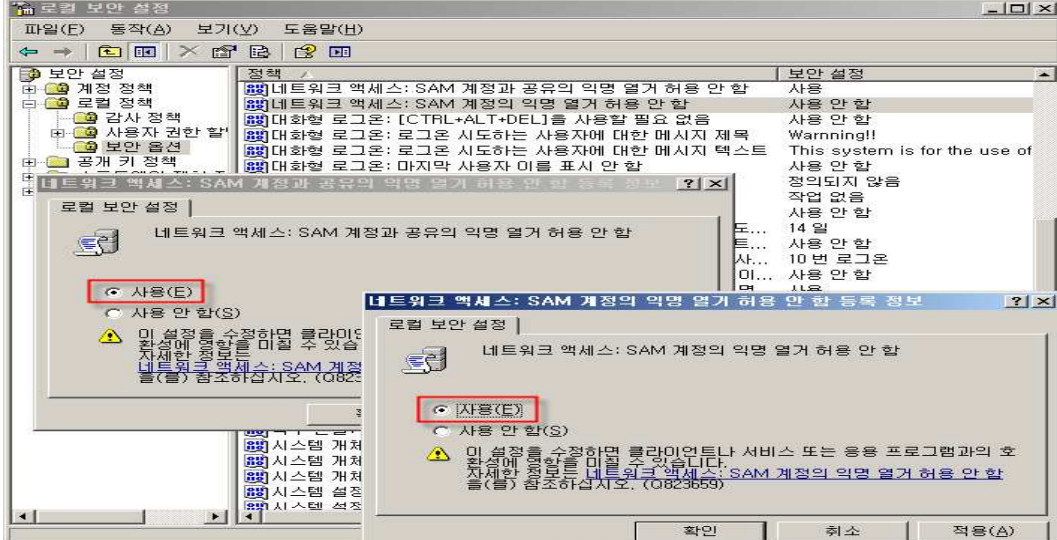


비고

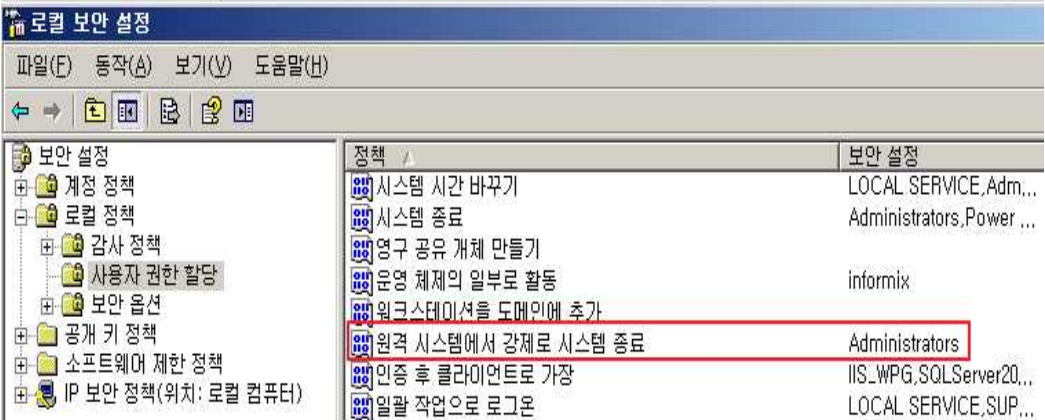


### 2.3.5. Null Session 접근 점검

| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 항목 코드 | WS3-05 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | 비인가된 사용자가 Null Session을 통해 사용자 인증을 거치지 않고 서버에 접근할 수 있으며, 또한 시스템 내부로의 접근이 가능하여 임의의 명령어 실행, 임의의 파일 수정, 시스템 관리자 권한 획득과 같은 공격 가능성이 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 진단 기준 | <p>양호 - 아래의 보안옵션을 모두 사용하고 있는 경우</p> <p>취약 - 아래의 보안옵션 중 하나라도 사용하고 있지 않은 경우</p> <ul style="list-style-type: none"> <li>- 네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함</li> <li>- 네트워크 액세스: SAM 계정의 익명 열거 허용 안 함</li> </ul>                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 점검 방법 | <p>Null Session 접근에 대한 보안옵션이 설정되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt;</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WLSa 에서 restrictanonymous과 restrictanonymoussam의 값이 1로 되어 있는지 확인</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 에서 “네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함” 정책과 “네트워크 액세스: SAM 계정의 익명 열거 허용 안 함” 정책이 모두 “사용” 으로 되어 있는지 확인 (사용으로 설정되어 있을 경우 양호)</p> |       |        |     |   |

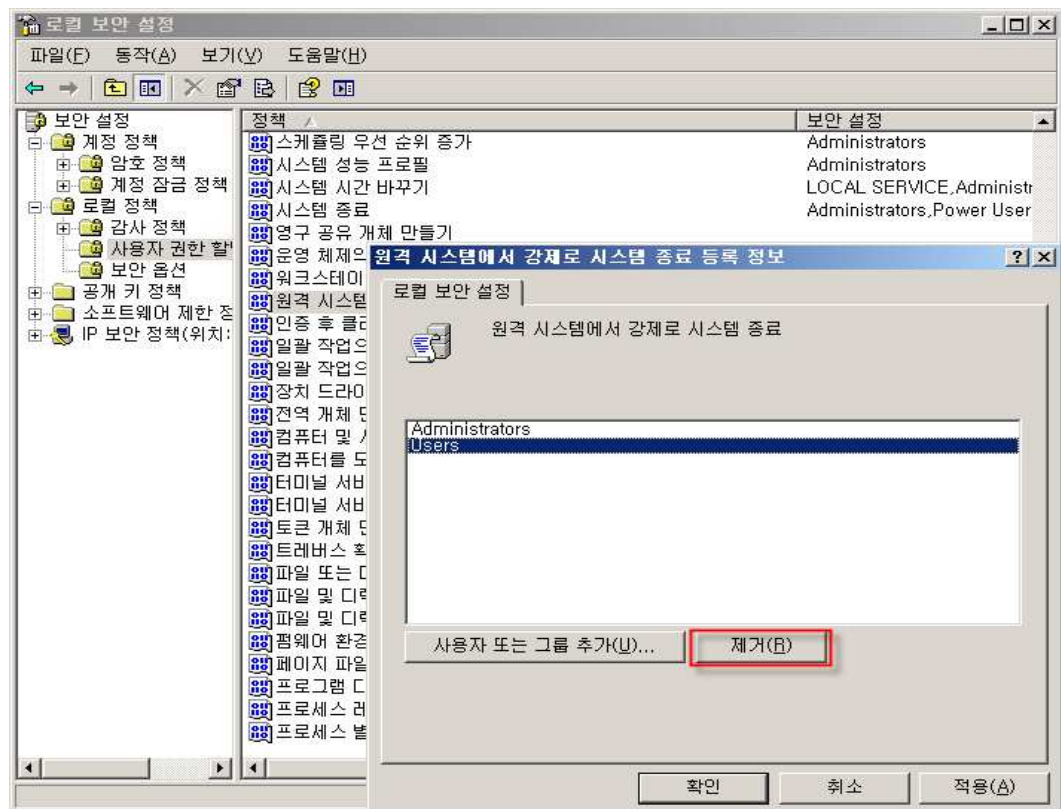
|              |                                                                                                                                                                                                                                                                                                                                 |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |                                                                                                                                                                                                                                               |
| <p>조치 방법</p> | <p>Null Session 접근에 대한 보안옵션을 설정한다..<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 옵션 에서 “네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함” 정책과 “네트워크 액세스: SAM 계정의 익명 열거 허용 안 함” 정책을 모두 “사용” 으로 설정</p>  |
| <p>비고</p>    |                                                                                                                                                                                                                                                                                                                                 |

### 2.3.6. 원격 시스템에서 강제로 시스템 종료

| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | WS3-06 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 이 보안 설정은 원격에서 네트워크를 사용하여 운영체제를 종료할 수 있는 사용자 및 그룹을 결정하며, 해당 권한부여가 부적절 할 경우 서비스 거부 공격에 이용 될 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 진단 기준 | <p>양호 - "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 만 존재할 경우</p> <p>취약 - "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 외 다른 계정 및 그룹이 존재할 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>"원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 만 존재하는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 명령 프롬프트에서 확인</p> <p>1. 시작 &gt; 실행 &gt; cmd.exe &gt; secedit /export /cfg c:\Wcfg.txt 명령어 실행</p> <p>2. 탐색기 &gt; c:\Wcfg.txt 파일을 열어서 SeRemoteShutdownPrivilege 설정 값에 S-1-5-32-544만 적용되어 있는지 확인</p> <pre> 94 SeDebugPrivilege = *S-1-5-32-544 95 SeRemoteShutdownPrivilege = *S-1-5-32-544 </pre> <p>- 잘 알려진 보안 식별자</p> <p>Administrators(S-1-5-32-544), Power Users(S-1-5-32-547), Backup operators(S-1-5-32-551), Users(S-1-5-32-545)</p> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 사용자 권한 할당 &gt; "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 그룹만 존재하는지 확인</p>  |       |        |     |   |
| 조치 방법 | <p>"원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 만 존재하도록 설정한다.</p> <p>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |



시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 사용자 권한 할당 > “원격 시스템에서 강제로 시스템 종료” 정책에 “Administrators” 그룹만 존재하도록 다른 사용자 및 그룹 제거



비고

### 2.3.7. Autologon 사용 제한

| 분류                   | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드          | WS3-07 | 중요도 | H |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------|-----|---|----|----|-----|----------------------|--------|---------|--------------------|--------|---------------|----------|--------|--|----------------|--------|---|------------------|-----------|----------------|-------------------|--------|----|--------------------|--------|----|-------------------|--------|---------|-----------------|--------|----------|-----------------|--------|---------------|------------------|-----------|----------------|--------------------|--------|--|-----------------|--------|--|
| 대상                   | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| 설명                   | Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에서 로그인 계정 및 암호를 확인할 수 있으므로 Autologon 기능을 사용하지 말아야 한다.<br>사용 시 비인가자가 시스템이 물리적으로 접근할 수 있으며, 시스템 정보 유출 및 손상 될 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| 진단 기준                | 양호 - AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우<br>취약 - AutoAdminLogon 값이 1로 설정되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| 점검 방법                | <p>AutoAdminLogon 값이 0으로 설정되어 있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon 에서 AutoAdminLogon 가 존재하지 않거나 "0" 으로 설정되어 있는지 확인<br/>(AutoAdminLogon가 존재하지 않거나, 0으로 설정되어 있을 경우 양호)</p> <div><p><b>레지스트리 편집기</b></p><p>파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)</p><table><thead><tr><th>이름</th><th>종류</th><th>데이터</th></tr></thead><tbody><tr><td>AltDefaultDomainName</td><td>REG_SZ</td><td>WIN2003</td></tr><tr><td>AltDefaultUserName</td><td>REG_SZ</td><td>Administrator</td></tr><tr><td>AppSetup</td><td>REG_SZ</td><td></td></tr><tr><td>AutoAdminLogon</td><td>REG_SZ</td><td>1</td></tr><tr><td>AutoRestartShell</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>cachedlogonscount</td><td>REG_SZ</td><td>10</td></tr><tr><td>DebugServerCommand</td><td>REG_SZ</td><td>no</td></tr><tr><td>DefaultDomainName</td><td>REG_SZ</td><td>WIN2003</td></tr><tr><td>DefaultPassword</td><td>REG_SZ</td><td>cyberone</td></tr><tr><td>DefaultUserName</td><td>REG_SZ</td><td>Administrator</td></tr><tr><td>forceunlocklogon</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>LegalNoticeCaption</td><td>REG_SZ</td><td></td></tr><tr><td>LegalNoticeText</td><td>REG_SZ</td><td></td></tr></tbody></table></div> |                |        |     |   | 이름 | 종류 | 데이터 | AltDefaultDomainName | REG_SZ | WIN2003 | AltDefaultUserName | REG_SZ | Administrator | AppSetup | REG_SZ |  | AutoAdminLogon | REG_SZ | 1 | AutoRestartShell | REG_DWORD | 0x00000001 (1) | cachedlogonscount | REG_SZ | 10 | DebugServerCommand | REG_SZ | no | DefaultDomainName | REG_SZ | WIN2003 | DefaultPassword | REG_SZ | cyberone | DefaultUserName | REG_SZ | Administrator | forceunlocklogon | REG_DWORD | 0x00000000 (0) | LegalNoticeCaption | REG_SZ |  | LegalNoticeText | REG_SZ |  |
| 이름                   | 종류                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 데이터            |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| AltDefaultDomainName | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | WIN2003        |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| AltDefaultUserName   | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Administrator  |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| AppSetup             | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| AutoAdminLogon       | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 1              |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| AutoRestartShell     | REG_DWORD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0x00000001 (1) |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| cachedlogonscount    | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 10             |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| DebugServerCommand   | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | no             |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| DefaultDomainName    | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | WIN2003        |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| DefaultPassword      | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | cyberone       |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| DefaultUserName      | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Administrator  |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| forceunlocklogon     | REG_DWORD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0x00000000 (0) |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| LegalNoticeCaption   | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| LegalNoticeText      | REG_SZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |
| 조치 방법                | <p>AutoAdminLogon 값을 0으로 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 레지스트리에서 설정</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon에서 AutoAdminLogon 값을 0 으로 설정<br/>※ DefaultPassword 가 존재하면 삭제</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |        |     |   |    |    |     |                      |        |         |                    |        |               |          |        |  |                |        |   |                  |           |                |                   |        |    |                    |        |    |                   |        |         |                 |        |          |                 |        |               |                  |           |                |                    |        |  |                 |        |  |

The screenshot shows the Windows Registry Editor with the following structure:

- Left pane: Tree view showing the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.
- Right pane: List of registry values:
 

| 이름                     | 종류        | 데이터             |
|------------------------|-----------|-----------------|
| AutoRestartShell       | REG_DWORD | 0x00000001 (1)  |
| cachedlogonscount      | REG_SZ    | 10              |
| DebugServerCommand     | REG_SZ    | no              |
| DefaultDomainName      | REG_SZ    | SECURITY-HUE    |
| DefaultUserName        | REG_SZ    | Administrator   |
| forceunlocklogon       | REG_DWORD | 0x00000000 (0)  |
| LegalNoticeCaption     | REG_SZ    |                 |
| LegalNoticeText        | REG_SZ    |                 |
| passwordexpirywarning  | REG_DWORD | 0x0000000e (14) |
| PowerdownAfterShutdown | REG_SZ    | 0               |
| PreloadFontFile        | REG_SZ    | gulim           |
| ReportBootOk           | REG_SZ    | 1               |

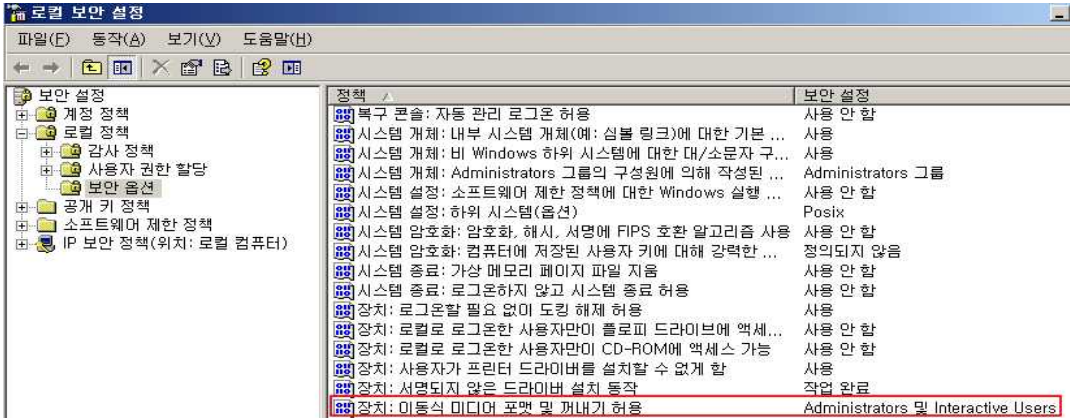
The 'DWORD 값 편집' dialog box is open with the following details:

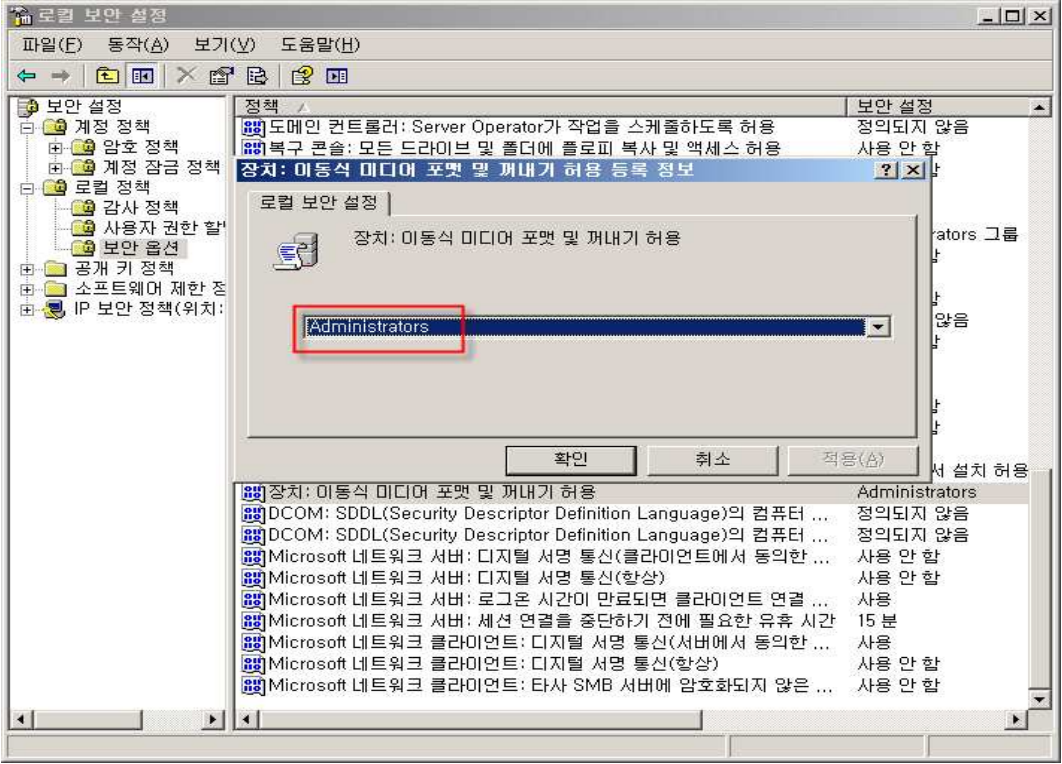
- 값 이름(N): AutoAdminLogon
- 값 데이터(V): 0 (highlighted with a red rectangle)
- 단위: ☒ 16진수(H) ☐ 10진수(D)
- Buttons: 확인, 취소

Bottom status bar: 내 컴퓨터\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

비고

### 2.3.8. 이동식 미디어 포맷 및 꺼내기 허용

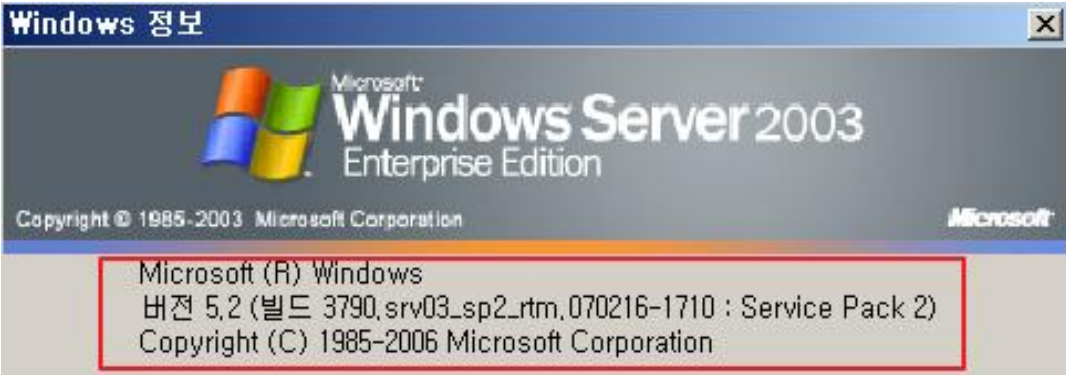
| 분류    | 기타 보안설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드 | WS3-08 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | 이 정책 설정은 이동식 NTFS 미디어 포맷 및 꺼내기가 허용되는 사용자를 결정한다. 사용자가 관리권한을 가진 다른 컴퓨터로 이동식 디스크의 데이터를 이동하여 파일에 대한 소유권을 얻고 자신에게 모든 권한을 부여하여 파일을 보거나 수정할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 진단 기준 | <p>양호 - "이동식미디어 포맷 및 꺼내기 허용" 정책이 "Administrators" 으로 되어있는 경우</p> <p>취약 - "이동식미디어 포맷 및 꺼내기 허용" 정책이 "Administrators" 으로 되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 점검 방법 | <p>"이동식미디어 포맷 및 꺼내기 허용" 정책이 "Administrators" 으로 설정되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt; HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 에서 allocatedasd 값이 "0" 으로 되어 있는지 확인</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어 있는지 확인</p>  |       |        |     |   |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>조치 방법</p> | <p>"이동식미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 으로 설정한다..<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션 &gt; "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 으로 설정</p>  <p>The screenshot shows the 'Local Security Policy' window. In the left-hand tree, 'Local Policies' is expanded, and 'Security Options' is selected. The main pane displays the policy '장치: 이동식 미디어 포맷 및 꺼내기 허용' (Device: Removable Storage). The policy is currently set to 'Administrators', which is highlighted with a red rectangle. Below the main pane, a list of other security policies is visible, including '이동식 미디어 포맷 및 꺼내기 허용' (Removable Storage) and various network-related policies.</p> |
| <p>비고</p>    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



## 2.4. 로그 및 패치관리

### 2.4.1. 최신 서비스 팩 적용

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                             | 항목 코드 | WS4-01 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | 서비스 팩은 Windows와 관련된 응용프로그램, 서비스, 실행파일 등 여러 수정 파일들을 모아 놓은 프로그램으로 최신 서비스 팩을 설치해야 한다..                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | 양호 - 최신 서비스 팩이 설치되어 있는 경우<br>취약 - 최신 서비스 팩이 설치되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 점검 방법 | <p>최신 서비스 팩이 설치되어 있는지 확인한다.<br/>                     [Win2003, Win2008]<br/>                     ■ 명령어를 통한 확인<br/>                     시작 &gt; 실행 &gt; winver 명령어를 실행하여 버전 확인<br/>                     [Win2003 서비스 팩 버전확인]</p>  <p>[Win2008 서비스 팩 버전확인]</p>  |       |        |     |   |
| 조치 방법 | 서비스 팩 버전 확인 후, 최신 버전이 아닐 경우 아래 사이트에서 다운로드하여 설치<br>Service Pack 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장한다. 이유는 현재 많은 인터넷 웜(Worm)이 Windows 의 취약점을 이용하여 공격을 하기 때문에                                                                                                                                                                                                                                                                              |       |        |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>O/S를 설치한 후 곧바로 네트워크에 연결하는 것은 곧바로 서버에 피해를 입을 수 있기 때문이다.</p> <p>[Win2003]<br/> Microsoft® 2003 보안 패치 사이트(Windows 2003 SP2, 14년 3월 현재)<br/> <a href="http://www.microsoft.com/ko-kr/download/details.aspx?id=41">http://www.microsoft.com/ko-kr/download/details.aspx?id=41</a></p> <p>[Win2008]<br/> Microsoft® 2008 보안 패치 사이트(Windows 2008 SP2, 14년 3월 현재)<br/> <a href="http://www.microsoft.com/ko-kr/download/details.aspx?id=15278">http://www.microsoft.com/ko-kr/download/details.aspx?id=15278</a></p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## 2.4.2. 최신 HOT FIX 적용

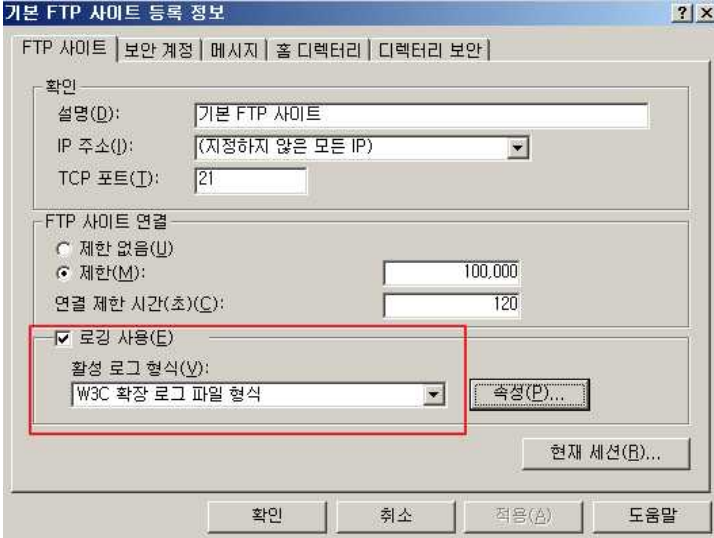
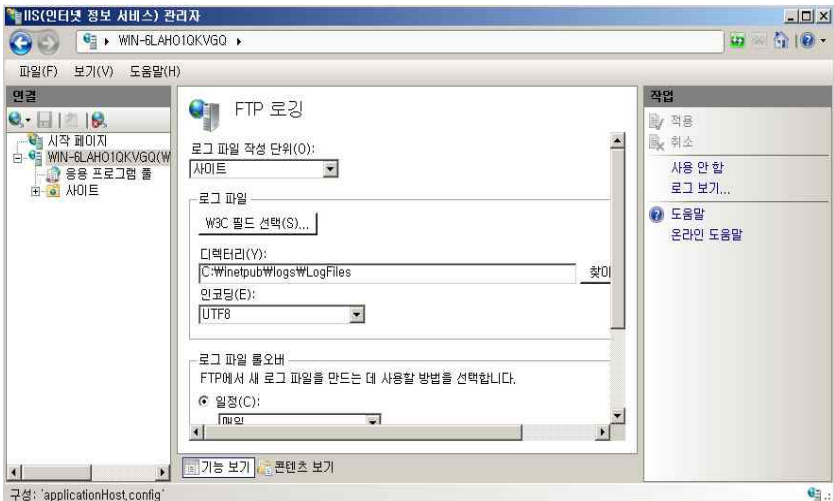
| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | WS4-02 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | Hot Fix는 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램이다. Hot Fix는 각각의 Service Pack 이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표되며, Hot Fix 보다 취약성을 이용한 공격도구가 먼저 나올 수 있으므로 Hot Fix는 배포 후 가능한 빨리 설치 할 것을 권장한다.                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 진단 기준 | 양호 - 최신 Hot Fix가 설치되어 있을 경우<br>취약 - 최신 Hot Fix가 설치되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 점검 방법 | 보안 패치 업데이트가 주기적으로 이루어지고 있는지 확인한다.<br>[Win2003, Win2008]<br>■ 프로그램 추가/제거에서 확인<br>시작 > 설정 > 제어판 > 프로그램 추가/제거 > 업데이트 표시 > 보안 패치 업데이트 날짜 확인<br>※ Windows 정기 보안 업데이트 릴리즈 날짜는 매월 둘째 주 수요일(한국시간)                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 조치 방법 | 최신 Hot Fix를 설치한다<br>[Win2003, Win2008]<br>■ Hot Fix 수동 설치<br>아래의 패치 리스트를 조회하여, 서버에 필요한 패치 선별 후, 수동으로 설치<br><a href="http://technet.microsoft.com/ko-kr/security/">http://technet.microsoft.com/ko-kr/security/</a><br><br>■ Windows 자동 업데이트를 통한 설치<br>Internet Explorer > 상단의 도구 메뉴 > Windows Update 를 클릭하면 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 설치를 쉽게 할 수 있다.<br><br>■ PMS(Patch Management System) Agent를 통한 설치<br>PMS Agent를 통한 보안 패치 및 Hot Fix의 경우는 적용 후 시스템 재시작을 요하는 경우가 대부분이므로, 관리자는 서비스에 지장이 없는 시간대에 적용을 하는 것을 권장한다. |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |



### 2.4.3. 백신 프로그램 업데이트

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                         | 항목 코드 | WS4-03 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | 계속되는 신종 바이러스의 출현으로 인해 백신 프로그램의 설치만으로는 그 효과를 볼 수 없으므로 바이러스 정보에 대한 주기적인 업데이트를 통해 최신의 바이러스까지 치료할 수 있는 기능이 필요하다.                                                                                                                                                      |       |        |     |   |
| 진단 기준 | 양호 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있을 경우<br>취약 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우                                                                                                                                                                         |       |        |     |   |
| 점검 방법 | 바이러스 백신 프로그램의 최신 엔진 업데이트 설치 유무를 수동으로 확인한다                                                                                                                                                                                                                         |       |        |     |   |
| 조치 방법 | <p>담당자를 통해 바이러스 백신 설치 후 엔진 업데이트를 설정하도록 한다.</p> <p>백신회사 마다 다소 차이는 있으나 매주 업데이트가 이뤄지고, 긴급한 경우 수시로 업데이트를 하기도 한다. 따라서 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신회사에서 발표하는 경보를 주시해야 한다.</p> <p>또한, 백신 프로그램의 자동 업데이트 기능을 이용하면 인터넷에 연결되어 있을 때 변동 사항을 자동으로 업데이트 되도록 설정해야 한다.</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                   |       |        |     |   |

## 2.4.4. FTP 로깅 설정

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | WS4-04 | 중요도 | L |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 설명    | FTP 서비스 사용 내역에 대한 로그를 남기지 않는 경우 공격에 대한 감사추적이 불가능하므로, FTP 서비스 사용에 따른 로그를 남기도록 설정해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 진단 기준 | <p>양호 - FTP 서비스 사용에 대한 로그를 남기는 경우</p> <p>취약 - FTP 서비스 사용에 대한 로그를 남기지 않는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>FTP 서비스 사용 시 로깅 사용이 설정되어 있는지 확인한다.</p> <p>[Win2003]</p> <p>■ 인터넷 정보 서비스(IIS)에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 인터넷 정보 서비스(IIS) 관리 &gt; 사용중인 FTP 사이트 &gt; 속성 &gt; FTP 사이트 &gt; 로깅 사용에 체크되어 있는지 확인</p>  <p>[Win2008]</p> <p>■ IIS(인터넷 정보 서비스) 관리자에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; IIS(인터넷 정보 서비스) 관리자 &gt; 사용중인 FTP 서비스 &gt; FTP 로깅 서비스가 실행되고 있는지 확인</p>  |       |        |     |   |

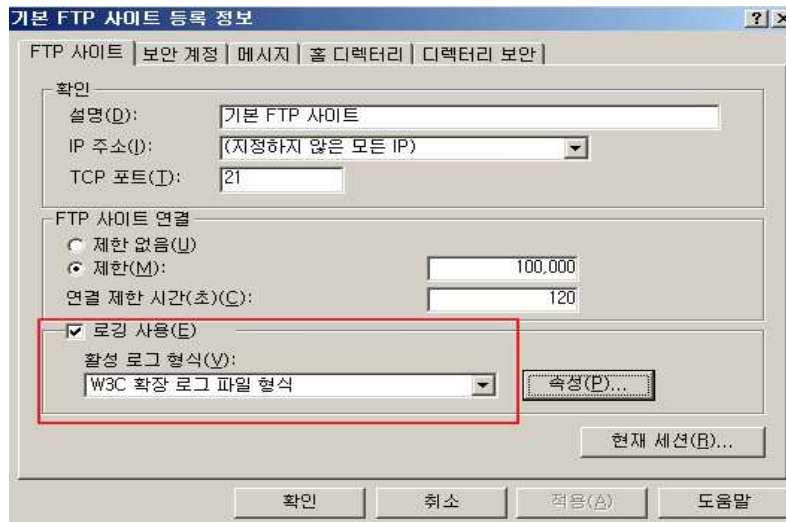
FTP 사용 시 로깅 사용을 활성화 시키고, 운영 환경에 따라 로그 주기를 결정한다.

[Win2003]

■ 인터넷 정보 서비스(IIS)에서 설정

1. FTP 로깅 사용 활성화

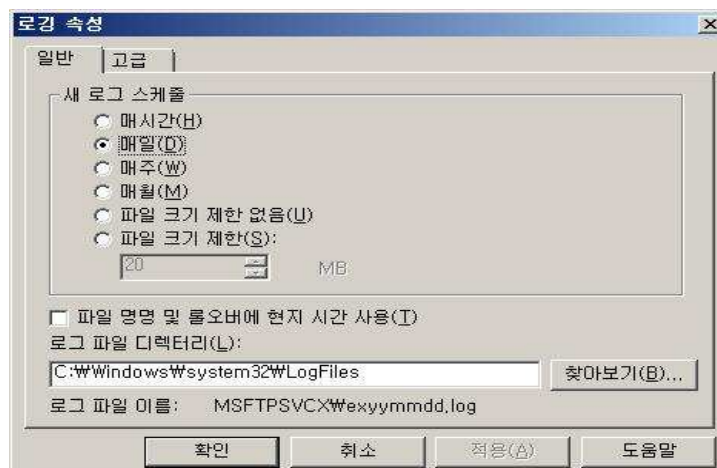
시작 > 프로그램 > 관리도구 > 인터넷 정보 서비스(IIS) 관리 > 사용중인 FTP 사이트 > 속성 > FTP 사이트 > 로깅 사용 에 체크



## 조치 방법

2. 로그 주기 설정 (1번 설정에 이어서)

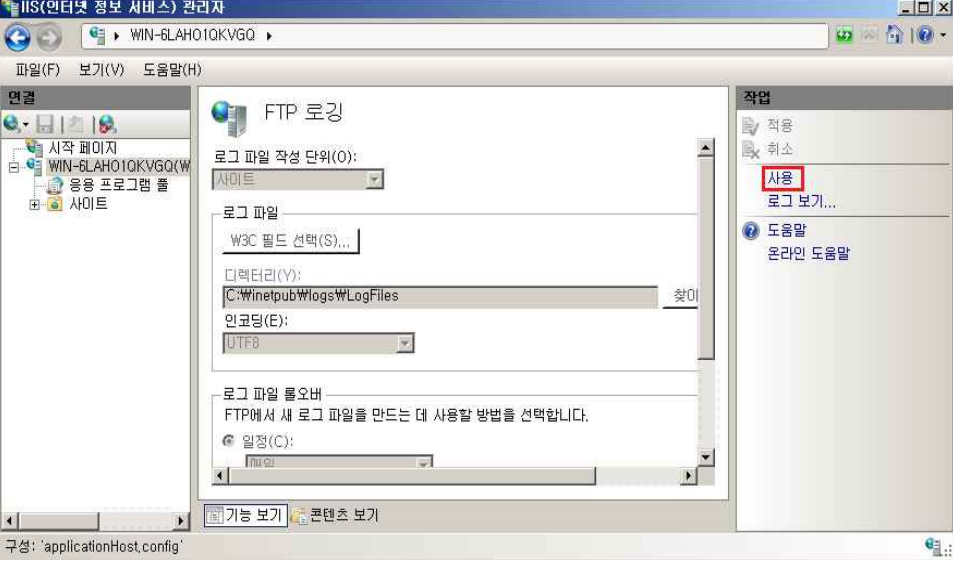
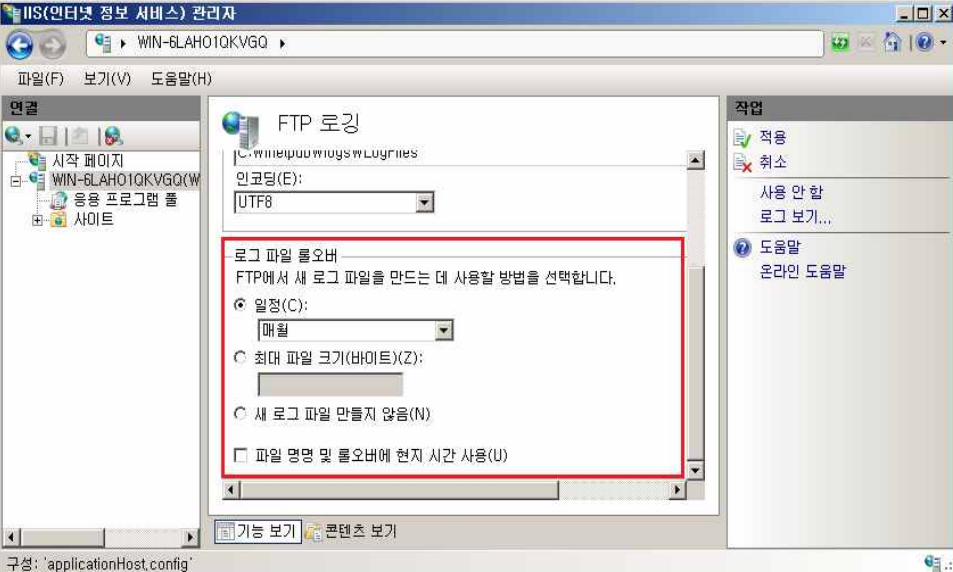
로깅 사용 체크란 안에 있는 속성을 클릭하여 운영 환경에 맞도록 로그 주기를 결정



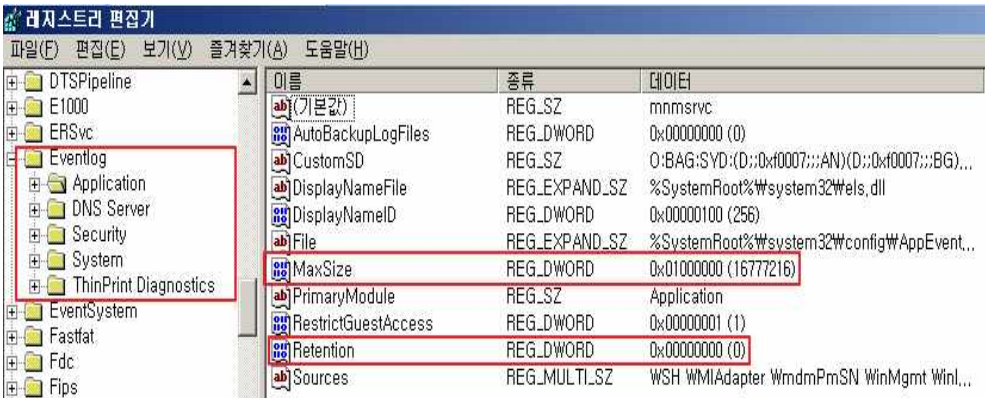
[Win2008]

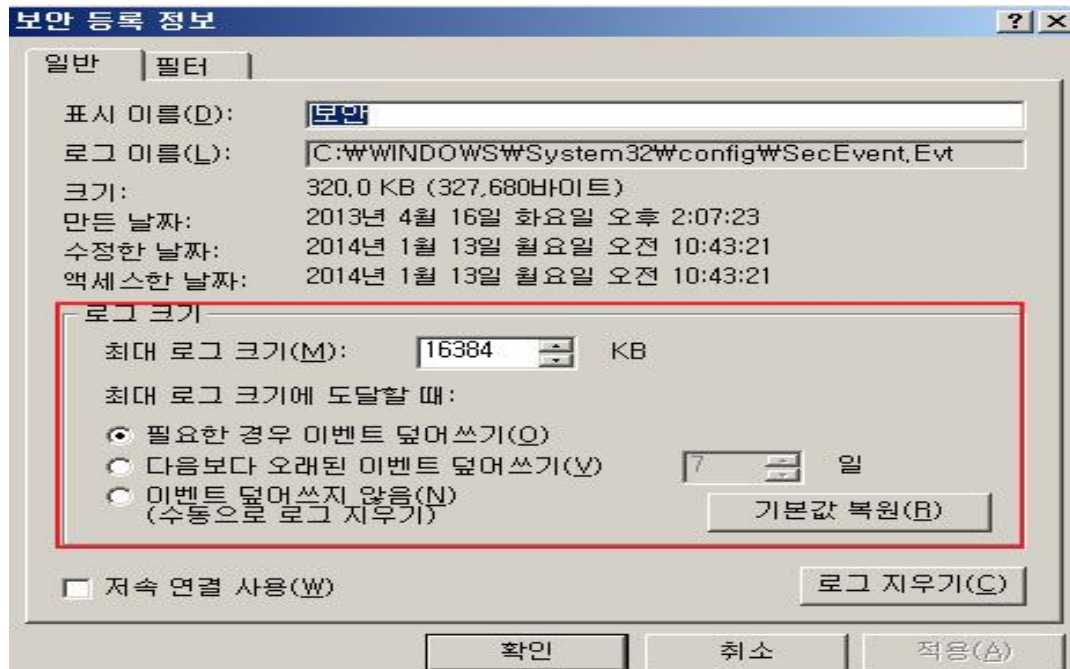
■ IIS(인터넷 정보 서비스) 관리자에서 설정

1. 시작 > 프로그램 > 관리도구 > IIS(인터넷 정보 서비스) 관리자 > 사용중인 FTP 서비스 > FTP 로깅 에서 "사용" 클릭하여 FTP 로깅 실행

|    |                                                                                                                                                                                                                                             |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>2. 로그 주기 설정 (1번 설정에 이어서)<br/>로그 파일 롤오버 안에서 로그 주기, 크기 등의 환경 설정</p>  |
| 비고 |                                                                                                                                                                                                                                             |

## 2.4.5. 이벤트 로그 관리 설정

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | WS4-05 | 중요도 | L |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 설명    | <p>컴퓨터에 관한 작업은 로그라는 정보로 저장하며, 로그는 컴퓨터 관련 범죄가 발생했을 시 해킹의 흔적을 찾기 위해 로그를 분석한다.</p> <p>단순히 해킹의 흔적을 찾기 위한 수단만이 아니라 로그분석을 통해 공격기법을 발견하여 시스템 취약점을 제거 할 수 있고, 공격에 대한 근원을 찾을 수 있다면 자산의 손실을 공격자에게 법적인 책임을 물을 수가 있으므로 로그에 대한 관리와 분석이 중요하다.</p>                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 진단 기준 | <p>양호 - 로그기록에 대해 정기적 검토, 분석, 그에 대한 리포트 작성 및 보고 등의 조치가 되어있을 경우</p> <p>취약 - 로그기록에 대해 미 검사, 미 검토 되었을 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>시스템 사용에 대한 로그기록의 정기적 검토, 분석, 보고 등의 설정이 되어 있는지 확인한다.</p> <p>[Win2003, Win2008]</p> <p>■ 레지스트리에서 확인</p> <p>시작 &gt; 실행 &gt; regedit &gt;</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog 의 하위폴더들의 MaxSize 값이 적절하게 설정되어 있는지 확인하고, Retention값이 7776000 (90일)로 되어 있는지 확인</p>  <p>- Retention = 0 : 필요한 경우 이벤트 덮어 쓰기</p> <p>- Retention = 4294967295 : 이벤트 덮어쓰지 않음</p> <p>※ 그 이외의 Retention 데이터 값은 1초 단위로 설정됨</p> <p>■ 이벤트 뷰어에서 확인</p> <p>[Win2003]</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 이벤트 뷰어 &gt; 각 항목의 속성 에서 각 로그의 사이즈와 덮어 쓰기 설정 확인</p> |       |        |     |   |



[Win2008]

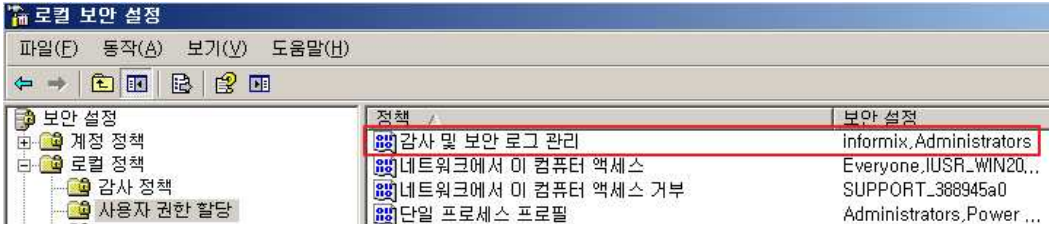
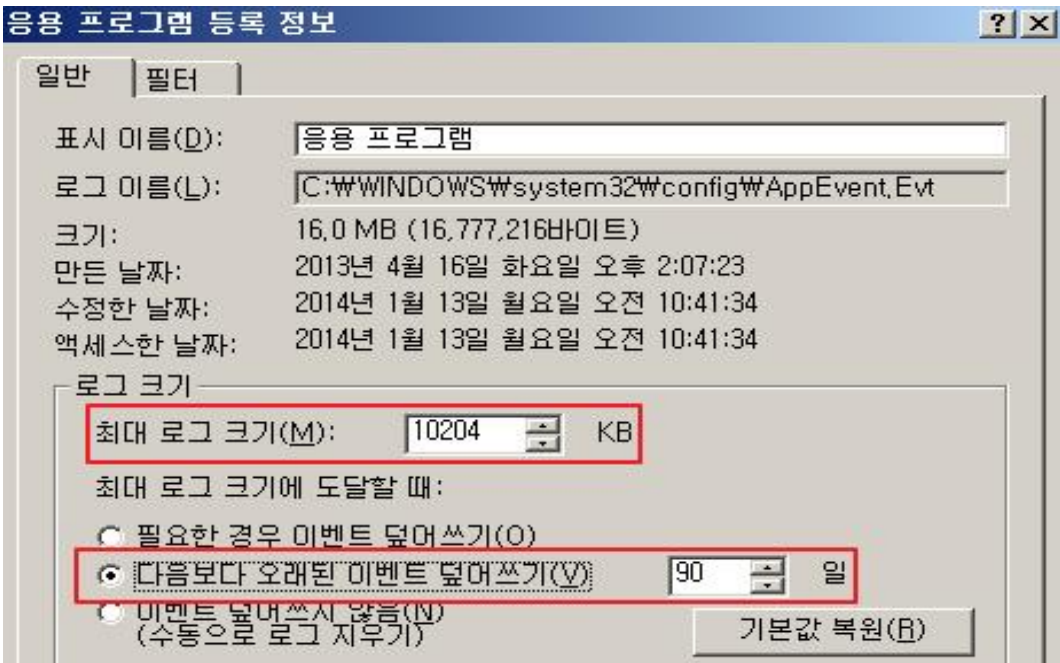
시작 > 프로그램 > 관리도구 > 이벤트 뷰어 > Windows 로그 > 각 항목의 속성 에서  
각 로그 사이즈와 덮어쓰기 설정 확인



■ 명령 프롬프트에서 확인

1. 시작 > 실행 > cmd > secedit /export /cfg c:\Wcfg.txt 명령어 실행
2. 탐색기 > c:\Wcfg.txt 파일을 열어서 SeSecurityPrivilege 설정에 불필요한 계정 또는 그룹이 존재하고 있는지 확인



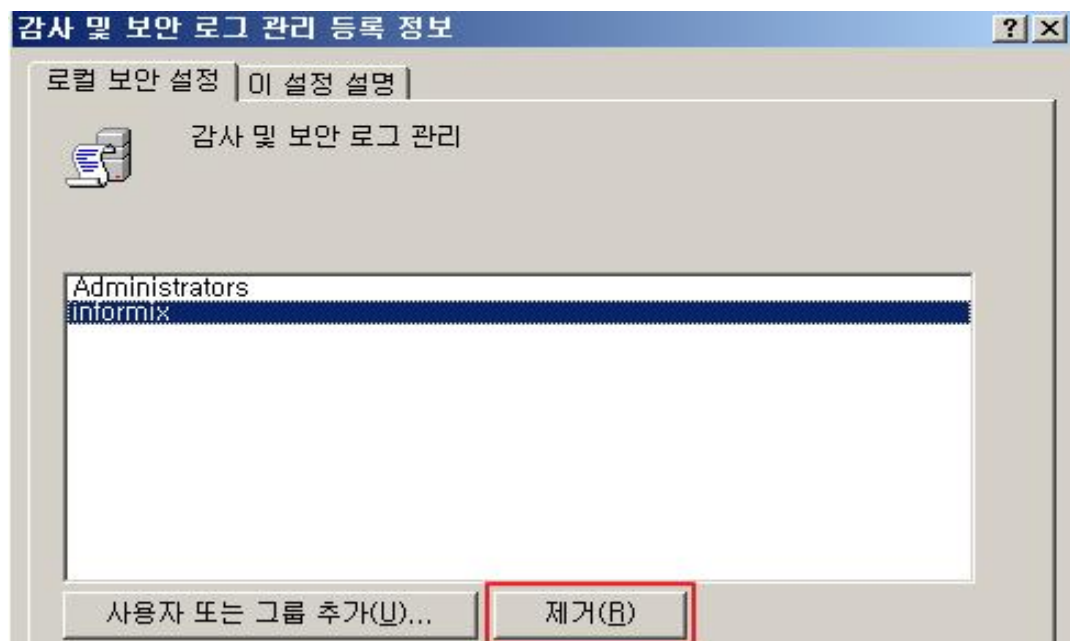
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <pre> 99 SeLoadDriverPrivilege = *S-1-5-32-544 100 SeBatchLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-559 101 SeServiceLogonRight = UpdatusUser,BUILTIN,*S-1-5-80-0 102 SeInteractiveLogonRight = vmware ,Guest,*S-1-5-32-544,*S-1-5-32-545,*S-1-5-32-551 103 SeSecurityPrivilege = informix,*S-1-5-32-544           </pre> <p>※ 잘 알려진 보안 식별자<br/>Administrators(S-1-5-32-544), Power Users(S-1-5-32-547), Backup operators(S-1-5-32-551), Users(S-1-5-32-545)</p> <p>■ 로컬 보안 정책에서 확인<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 사용자 권한 할당 &gt; “감사 및 보안 로그 관리” 정책에서 불필요한 계정 또는 그룹이 존재하는지 확인</p>  |
| 조치 방법 | <p>시스템 사용에 대한 로그기록의 정기적 검토, 분석, 보고 등을 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 이벤트 뷰어에서 설정<br/>[Win2003]<br/>시작 &gt; 프로그램 &gt; 관리도구 &gt; 이벤트 뷰어 &gt; 각 항목의 속성 에서<br/>최대 로그 크기 10204KB 이상, “90일 이후 이벤트 덮어쓰기” 으로 설정</p>  <p>[Win2008]</p>                                                                                                                                                                                                                                                                                                                                                                                 |

시작 > 프로그램 > 관리도구 > 이벤트 뷰어 > 각 항목의 속성 에서 "최대 로그 크기" 를 10204KB 이상으로 설정



■ 로컬 보안 정책에서 설정

시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 사용자 권한 할당 > “감사 및 보안 로그 관리” 정책에서 불필요한 계정 또는 그룹 제거

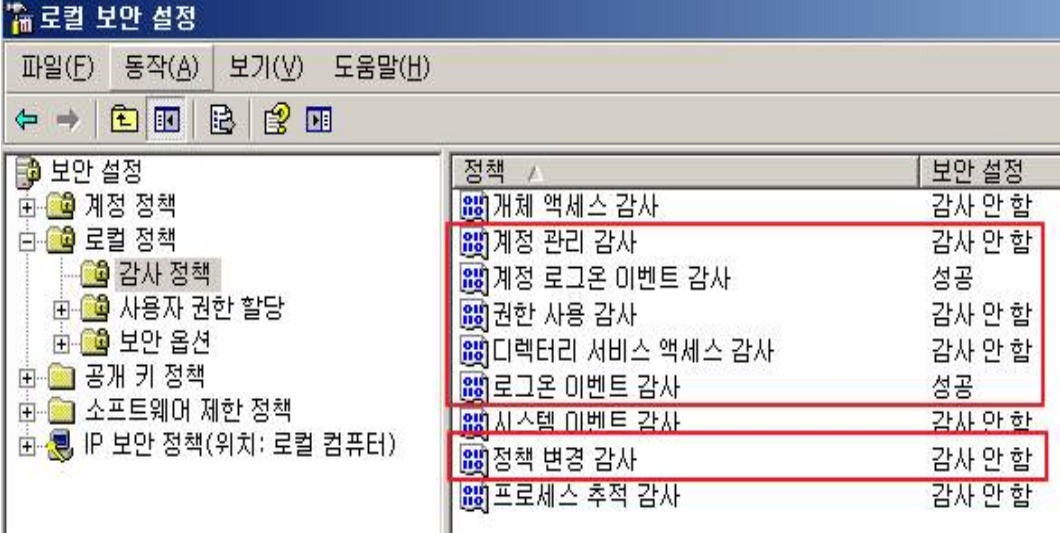


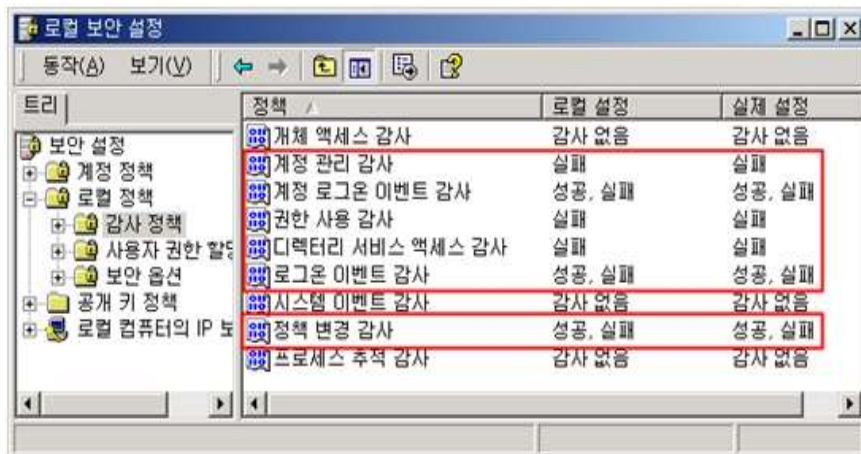
※ 로컬보안정책을 이용하여 감사 정책을 구성하기 위해서는 Administrators 그룹 구성원 또는 적절한 권한이 부여된 사용자이어야 한다.

비고



## 2.4.6. 감사 정책 설정

| 분류    | 로그 및 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | WS4-06 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 2003, Windows 2008                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 설명    | <p>감사 설정이 구성되어 있지 않거나 감사 설정 수준이 너무 낮으면 보안 관련 문제 발생 시 원인을 파악하기 어려우며 법적 대응을 위한 충분한 증거로 사용될 수도 없다.</p> <p>그러나 감사 설정이 너무 높으면 보안 로그에 불필요한 항목이 많이 기록되므로 매우 중요한 항목과 혼동할 수 있으며, 컴퓨터 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요구 사항과 조직의 정책에 따라 필요한 로그를 남기도록 설정해야 한다.</p>                                                                                                                                                                               |       |        |     |   |
| 진단 기준 | <p>양호 - 아래와 같은 이벤트에 대한 감사 설정이 되어 있는 경우.</p> <p>취약 - 아래와 같은 이벤트에 대한 감사 설정이 되어 있지 않은 경우</p> <ul style="list-style-type: none"> <li>- 로그인 이벤트, 계정 로그인 이벤트, 정책 변경 : 성공/실패 감사</li> <li>- 계정 관리, 디렉터리 서비스 액세스, 권한 사용 : 실패 감사</li> </ul>                                                                                                                                                                                                |       |        |     |   |
| 점검 방법 | <p>이벤트에 대한 감사 설정이 진단 기준에서 명시된 것과 같이 되어있는지 확인한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 확인</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 감사정책 에서 아래와 같이 이벤트 감사 정책이 설정되어 있는지 확인</p> <ul style="list-style-type: none"> <li>- 로그인 이벤트, 계정 로그인 이벤트, 정책 변경 : 성공/실패 감사</li> <li>- 계정 관리, 디렉터리 서비스 액세스, 권한 사용 : 실패 감사</li> </ul>  |       |        |     |   |
| 조치 방법 | <p>이벤트에 대한 감사 설정을 점검 방법에 명시되어 있는 기준과 같이 설정한다.<br/>[Win2003, Win2008]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>시작 &gt; 프로그램 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 로컬 정책 &gt; 감사 정책 에서 아래와 같이 이벤트 감사 정책 설정</p>                                                                                                                                                                                                                                         |       |        |     |   |



※ 각 감사정책에 대한 설명

- 로그인 이벤트

사용자가 컴퓨터에 로그인하거나 로그오프 할 때마다 로그인 이 시도된 컴퓨터의 보안 로그에 이벤트 생성

- 계정 로그인 이벤트

사용자가 도메인에 로그인하면 도메인 컨트롤러에 로그인 시도 기록

- 계정 관리

사용자나 그룹이 작성, 변경 또는 삭제된 시간을 판단하는데 사용

- 개체 액세스

시스템 액세스 컨트롤 목록(SACL)이 있는 Windows 2000 기반 네트워크의 모든 개체에 대해 감사를 활성화

보안 로그에 이벤트를 표시하려면 먼저 개체 액세스 감사를 활성화한 후 감사할 각 개체에 대해 SACL을 정의

- 디렉터리 서비스 액세스

Active Directory 개체의 SACL에 나열된 사용자가 해당 개체에 액세스를 시도할 때 감사 항목이 생성

- 권한 사용

권한 사용의 성공 및 실패를 감사할 경우 사용자 권한을 이용하려고 할 때마다 이벤트가 생성

- 프로세스 추적

실행되는 프로세스에 대한 자세한 추적 정보를 감사하는 경우 이벤트 로그에 프로세스를 작성하고 종료하려고 한 시도가 나타남

- 시스템 이벤트

사용자나 프로세스가 컴퓨터 환경을 변경하면 시스템 이벤트가 생성

시스템 이벤트를 감사할 경우 보안 로그가 삭제된 시간도 감사

- 정책 변경

감사 정책 변경의 성공 및 실패를 감사

비고

### 3. 네트워크 취약성 점검항목 및 가이드

#### 3.1. 계정관리

##### 3.1.1. 패스워드 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | NW-01 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Passport, Juniper, Pionlink                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 설명    | 네트워크 장비의 초기 설정 패스워드를 변경하지 않고 사용하는 경우 비인가자의 불법적인 접근이 가능하며, 기본 패스워드는 인터넷상에서 검색을 통해 노출되어 있어 비인가자의 관리자 권한획득이 가능함. 네트워크 장비의 초기 설정 패스워드는 반드시 변경 설정하여야 한다.                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 진단 기준 | 양호 - 장비 접속 패스워드를 변경, 설정하여 사용하는 경우<br>취약 - 장비 접속 패스워드가 설정되어 있지 않거나, 초기 설정 패스워드를 사용하는 경우                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Enable 패스워드 설정 확인, Line Access에서 각 라인별(VTY, CON, AUX) 패스워드 설정 확인</p> <p>&lt;Alteon, Passport&gt;<br/>콘솔 및 Telnet으로 접근 시 각각 계정에 따라 설정 되어 있는 기본 패스워드 확인<br/>예) Alteon Switch : admin/admin, admin/null</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 패스워드 설정 확인</p> <p>&lt; Piolink &gt;<br/>(configuration)# 에서 password 명령어를 통해 패스워드 설정 확인</p> |       |       |     |   |
| 조치 방법 | <p>&lt; CISCO &gt;<br/>1. Enable 패스워드<br/>Router# config terminal (단축 명령은 config t)<br/>Enter configuration commands, one per line. End with CNTL/Z.<br/>Router(config)# enable password &lt;패스워드&gt;<br/>Router(config)# ^Z (Ctrl + z)<br/>Router#</p> <p>2. Virtual Terminal Password 설정<br/>Router# config terminal<br/>Router(config)# line vty ?<br/>&lt;0-4&gt; First Line number<br/>Router(config)# line vty 0 4<br/>Router(config-line)# login</p>           |       |       |     |   |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <pre>Router(config-line)# password &lt;패스워드&gt;</pre> <p>3. 콘솔 패스워드 설정</p> <pre>Router# config terminal Router(config)# line console ? &lt;0-0&gt; First Line number Router(config)# line console 0 Router(config-line)# login Router(config-line)# password &lt;패스워드&gt;</pre> <p>4. 보조포트(AUX) 패스워드 설정</p> <pre>Router# config terminal Router(config)# line aux ? &lt;0-0&gt; First Line number Router(config)# line aux 0 Router(config-line)# login Router(config-line)# password &lt;패스워드&gt;</pre> <p>&lt; Alteon &gt;</p> <ol style="list-style-type: none"> <li>1. # cfg/sys/access/user/admpw (administrator 패스워드 변경 시)</li> <li>2. # apply</li> <li>3. # save</li> </ol> <p>&lt; Passport &gt;</p> <p>[CLI]</p> <ol style="list-style-type: none"> <li>1. switch 로 접속</li> <li>2. 다음 중 해당하는 계정에 따라 명령어 실행</li> </ol> <pre># config cli password ro &lt;username&gt; # config cli password l1 &lt;username&gt; # config cli password l2 &lt;username&gt; # config cli password l3 &lt;username&gt; # config cli password rw &lt;username&gt; # config cli password rwa &lt;username&gt; # config cli password slboper &lt;username&gt; # config cli password l4oper &lt;username&gt; # config cli password oper &lt;username&gt; # config cli password slbadmin &lt;username&gt; # config cli password l4admin &lt;username&gt; # config cli password ssladmin &lt;username&gt;</pre> <p>&lt; Juniper &gt;</p> <pre>user@juniper&gt; configure [edit] user@juniper# set system root-authentication plain-text-passwd New password : 패스워드 &lt;- 새로운 패스워드 입력</pre> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>retype new password: : 패스워드 &lt;- 입력했던 패스워드 확인</p> <p>&lt; Piolink &gt;</p> <ol style="list-style-type: none"> <li>1. Switch로 접속</li> <li>2. root 계정으로 로그인</li> <li>3. (configuration)# 에서 password 명령어 사용</li> <li>4. new password: 입력</li> <li>5. retype password: 입력</li> </ol> |
| 비고 |                                                                                                                                                                                                                                                                                       |

### 3.1.2. 패스워드 복잡성 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | NW-02 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | 공통                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 설명    | <p>단순하거나 추측하기 쉬운 패스워드를 사용할 경우 악의적인 사용자가 쉽게 장비에 접속할 수 있으므로 암호 복잡성을 적용하여야 함. 패스워드 복잡성을 적용하지 않은 경우 공격자는 *무작위 대입 공격(Brute Force Attack)을 통하여 패스워드를 쉽게 획득할 수 있다.</p> <p>※무작위 대입 공격(Brute Force Attack) : 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.</p>                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 진단 기준 | <p>양호 - 패스워드 정책이 수립되어 있으며, 보안 정책을 반영하여 설정되어 있는 경우</p> <p>취약 - 초기 설정 패스워드를 사용하거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 점검 방법 | 장비별 담당자의 패스워드 복잡성 설정 적용 여부 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 조치 방법 | <p>인증 과정을 통해서 비인가자의 접속을 제한한다.</p> <p>&lt; 공통 &gt;</p> <p>패스워드 설정 시 아래와 같은 패스워드 정책을 적용해야 함</p> <ol style="list-style-type: none"> <li>1. 암호는 최소 8 자 이상이어야 함 (Passport 9 자 이상)</li> <li>2. 사용자 계정 이름이나 이름의 문자를 3 개 이상 연속하여 포함하지 않아야 함</li> <li>3. 암호에는 다음 네 가지 중 세 가지 범주의 문자가 포함되어야 함</li> </ol> <p>가. 대문자(26 개))</p> <p>나. 소문자(26 개)</p> <p>다. 숫자(10 개)</p> <p>가. 특수문자(32개)</p> <p>※ 개인정보의 안전성 확보조치 기준 고시 및 해설서</p> <ul style="list-style-type: none"> <li>• 최소 10자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 2종류 이상으로 구성한 경우</li> <li>• 최소 8자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 3종류 이상으로 구성한 경우</li> </ul> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |

### 3.1.3. 암호화된 패스워드 사용

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | NW-03 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Passport, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 설명    | 네트워크 장비의 패스워드는 디폴트로 평문 텍스트 형태로 저장되기 때문에 설정파일 유출 시 패스워드도 함께 노출됨. 평문으로 저장 되어 있을시 해독될 가능성이 쉬워 정보에 대한 유출 위험이 있으므로 모든 패스워드를 암호화하여 저장하도록 설정을 변경해야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | 양호 - 패스워드 암호화 설정이 적용된 경우<br>취약 - 패스워드 암호화 설정이 적용되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running-config<br/>1. Enable Secret 사용 확인<br/>2. Password-Encryption 서비스 동작 확인</p> <p>&lt;Passport&gt;<br/>Configuration file에서 Enable Secret 패스워드를 제외한 모든 패스워드 암호화 설정 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt;configure<br/>[edit]<br/>user@juniper#show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 패스워드 암호화 설정 확인</p>                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 조치 방법 | <p>&lt; CISCO &gt;<br/>Enable secret 패스워드는 암호화 되어 표시됨<br/>Enable secret 패스워드는 Enable password 보다 강력하고 우선적으로 사용함<br/>※ Enable 패스워드와 Enable secret 패스워드는 서로 다르게 입력<br/>Router# config terminal<br/>Enter configuration commands, one per line. End with CNTL/Z.<br/>Router(config)# enable secret &lt;패스워드&gt;<br/>Router(config)# service password-encryption<br/>Router(config)# ^Z<br/>Router# show running<br/>enable secret 5 \$1\$mERr\$9WCswBwUv6WeC6M8kNSs8<br/>enable password 7 0822455D0A1648121C0A0E082F</p> <p>&lt; Passport &gt;<br/>설정파일(Configuration file)에서 패스워드를 암호화함으로써 인증되지 않은 사용자가 설정 파일의 패스워드를 획득할 수 있는 가능성을 방지함</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]</p> |       |       |     |   |

|    |                                                                                                                                                              |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> user@juniper#      set      system      root-authentication      encrypted-password #1\$14c5.%4Bopasddfs0" user@juniper# ^Z                     </pre> |
| 비고 |                                                                                                                                                              |



## 3.2. 접근관리

### 3.2.1. VTY 접근(ACL) 설정

| 분류    | 접근관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | NW-04 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Passport,Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 설명    | <p>VTY(Virtual Teletype) 사용 시 Telnet이나 SSH로 원격 접속이 가능함. 원격 접속 시 평문으로 정보가 전송되는 Telnet은 패스워드 추측 공격(Password Guessing) 및 *스니핑 공격에 취약하므로 보안상 SSH 사용을 권고함. 인가된 사용자만의 안전한 접근 관리를 위해 접속할 수 있는 IP를 제한하여 비인가자의 접근을 차단하여야 한다.</p> <p>*스니핑(sniffing): 네트워크상의 데이터를 도청하는 행위</p>                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | <p>양호 - VTY 접근 시 접근 통제(ACL) 설정이 되어있는 경우</p> <p>취약 - VTY 접근 시 접근 통제(ACL) 설정이 되어있지 않는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 점검 방법 | <p>&lt; Cisco &gt;</p> <p>Router# show running-config</p> <p>1. Access-List 설정 확인</p> <p>2. 각 Line Vty에 access-class 설정 확인</p> <p>&lt;Alteon, Passport&gt;</p> <p>장비로 접속하여 Telnet 또는 SSH 사용자의 접속 IP 설정 확인(Access Policies)</p> <p>&lt; Juniper &gt;</p> <p>user@juniper# configure</p> <p>[edit]</p> <p>user@juniper# show</p> <p>root authentication 설정을 이용하여 [edit system] 레벨에서 ACL 설정 확인</p>                                                                                                                                                                                                                                                                 |       |       |     |   |
| 조치 방법 | <p>&lt; CISCO &gt;</p> <p>1. VTY 접근 허용 IP 설정</p> <p>Router# config terminal</p> <p>Router(config)# access-list [1-99] {permit deny} [Source Network] [WildcardMask]</p> <p>Router(config)# access-list [1-99] permit any -&gt; 기본 deny 방지</p> <p>Router(config)# line vty 0 4</p> <p>Router(config)# access-class [1-99] in</p> <p>ex) 192.168.2.1 에서만 vty 접근 가능</p> <p>Router(config)# access-list 1 permit 192.168.2.1</p> <p>2. SSH 사용할 경우</p> <p>Global configuration mode 로 접속</p> <p>(config)# access-list &lt;access_list_num&gt; permit &lt;source_ip mask&gt;</p> <p>(config)#ssh access-group &lt;num&gt;</p> <p>(config)#write memory</p> <p>또는,</p> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Global configuration mode 로 접속<br/>(config)# ip ssh client &lt;IP_address&gt;<br/>또는,<br/>Global configuration mode 로 접속<br/>(config)# ip ssh client &lt;IP_address&gt; &lt;mac_address&gt;</p> <p>&lt; Alteon &gt;<br/>1. switch 로 접속<br/>2. # cfg<br/>3. # sys<br/>4. # access<br/>5. # mgmt<br/>6. # add &lt;mgmt network address&gt; &lt;mgmt network mask&gt; &lt;management access protocol&gt;<br/>7. # apply<br/>8. # save</p> <p>&lt; Passport &gt;<br/>1. switch 로 접속<br/>2. # config sys access-policy<br/>3. config/sys/access-policy# enable true<br/>4. config/sys/access-policy# policy &lt;pid&gt; create<br/>5. config/sys/access-policy# policy &lt;pid&gt;<br/>6. config/sys/access-policy/policy/&lt;pid&gt;# enable true<br/>7. config/sys/access-policy/policy/&lt;pid&gt;# accesslevel rwa<br/>8. config/sys/access-policy/policy/&lt;pid&gt;# host &lt;ip-addr&gt;<br/>9. config/sys/access-policy/policy/&lt;pid&gt;# service snmp enable<br/>10. config/sys/access-policy/policy/&lt;pid&gt;# service telnet enable</p> <p>&lt; Juniper &gt;<br/>ACL 로깅 설정<br/>Access-list를 생성하면 기본 Deny가 되므로 네트워크 담당자를 통해 설정<br/>user@juniper&gt;configure<br/>[edit]<br/>user@juniper# source-address 127.0.0.0/24;<br/>user@juniper# source-address 224.0.0.0/4;<br/>user@juniper# source-address 0.0.0.0/0;</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### 3.2.2. Session Timeout 설정

| 분류    | 접근관리                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | NW-05 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper, Piolink                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 설명    | 관리자가 네트워크 장비에 로그인 후 세션을 종료하지 않고 자리를 비우는 동안 악의적인 사용자가 접속된 터미널을 이용하여 불법적인 행위를 시도할 수 있다. 원격 접속 시 일정 시간 동안 키 입력이 없는 경우 연결된 접속을 자동 종료시키는 설정이 필요하다.                                                                                                                                                                                                                                      |       |       |     |   |
| 진단 기준 | 양호 - Session Timeout 시간을 설정한 경우<br>취약 - Session Timeout 시간을 설정하지 않은 경우                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 점검 방법 | <p>&lt;Cisco&gt;<br/>Router# show running-config<br/>각 Line Access의 exec-timeout 설정 확인</p> <p>&lt; Alteon &gt;<br/>idle timeout in minutes 설정 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt;configure<br/>[edit]<br/>user@juniper#show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 Session Timeout 설정 확인</p> <p>&lt; Piolink &gt;<br/>terminal timeout 설정 확인</p>         |       |       |     |   |
| 조치 방법 | <p>&lt; CISCO &gt;<br/>1. Console<br/>Router# config terminal<br/>Router(config)# line con 0<br/>Router(config-line)# exec-timeout 5 0</p> <p>2. VTY<br/>Router# config terminal<br/>Router(config)# line vty 0 4<br/>Router(config-line)# exec-timeout 5 0</p> <p>3. AUX<br/>Router# config terminal<br/>Router(config)# line aux 0<br/>Router(config-line)# exec-timeout 5 0</p> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>&lt; Alteon &gt;</p> <ol style="list-style-type: none"> <li>1. # cfg</li> <li>2. # sys</li> <li>3. # idle &lt;idle timeout in minutes, affects both console and telnet&gt;</li> <li>4. # apply</li> <li>5. # save</li> </ol> <p>※ 디폴트 : 5 분 설정</p> <p>&lt; Juniper &gt;</p> <pre>user@juniper&gt; configure [edit] user@juniper# set admin auth timeout 360 ——unknown keyword timeout</pre> <p>&lt; Piolink &gt;</p> <ol style="list-style-type: none"> <li>1. 관리자 모드로 접속</li> <li>2. configure</li> <li>3. terminal timeout &lt;interval&gt;</li> </ol> <p>※ 1분에서 60분 사이의 시간을 설정이 가능함</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### 3.2.3. VTY 접속 시 안전한 프로토콜 사용

| 분류    | 접근관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | NW-06 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |
| 설명    | VTY 접속 시 Telnet 프로토콜을 많이 사용하지만, Telnet은 패킷을 암호화하지 않은 텍스트 형태로 전송하므로 스니핑 공격에 의해 패스워드가 쉽게 노출되는 취약점이 존재함. 따라서 패킷 자체를 암호화하여 전송하는 SSH 프로토콜 사용을 권장한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 진단 기준 | 양호 - VTY 접속 시 SSH를 사용하는 경우<br>취약 - VTY 접속 시 Telnet을 사용하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <pre> &lt; CISCO &gt; Router# show ip ssh SSH Enabled - version 1.5 Authentication timeout: 120 secs; Authentication retries: 3 (활성화) %SSH has not been enabled (비 활성화) SSH 활성화 확인  &lt; Alteon &gt; /sys/sshd에서 SSH 활성화 확인  &lt; Juniper &gt; user@juniper# set ssh  SSH 버전 확인                     </pre>                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 조치 방법 | Telnet사용 제한, SSH사용 설정 변경한다. <pre> &lt; CISCO &gt; SSH 설정 방법 사전 작업 : 라우터명, 도메인명 설정 Router# config terminal Router(config)# hostname &lt;호스트명&gt; Router(config)# ip domain-name &lt;도메인명&gt; Router(config)# username &lt;ID&gt; password &lt;PASS&gt; Router(config)# crypto key generate rsa ! How many bits in the modulus [512]: 1024 &lt;- 입력 ! Router(config)# ip ssh time-out [초] &lt;- timeout 시간(단위: second) Router(config)# ip ssh authentication-retries [횟수] &lt;- 재시도 횟수 Router(config)# line vty 0 4 Router(config-line)# login local Router(config-line)# transport input ssh SSH 접속                     </pre> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>1. ssh 접속 프로그램 사용</p> <p>2. # ssh -c rsa -l &lt;ID&gt; &lt;라우터 IP&gt;</p> <p>&lt; Alteon &gt;</p> <p>SSH 설정 방법</p> <p>1. switch 로 접속</p> <p>2. # cfg</p> <p>3. # /sys/sshd ena</p> <p>4. # /sys/sshd on</p> <p>5. # apply</p> <p>6. # save</p> <p>&lt; Juniper &gt;</p> <p>1. SSH 버전 확인</p> <p>user@juniper# set ssh</p> <p>2. services로 검색하여 ssh를 사용하지 않을 경우 접속 가능 IP를 제한하여야 함</p> <p>user@juniper&gt; configure</p> <p>[edit]</p> <p>user@juniper# set ssh enable</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### 3.2.4. 불필요한 보조 입·출력 포트 사용 금지

| 분류    | 접근관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | NW-07 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 설명    | 불필요한 보조 입·출력 포트가 활성화되어 있으면 비인가자가 불법적인 접속을 시도 할 수 있으므로 라우터나 스위치의 불필요한 포트를 차단하여 외부 접속으로 인한 내부 네트워크의 장애 발생과 데이터 손실을 예방하여야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | 양호 - 불필요한 보조 입·출력 포트 사용을 제한한 경우<br>취약 - 불필요한 보조 입·출력 포트 사용을 제한하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running<br/>불필요한 보조 입출력 포트의 오른쪽 끝부분에 Up (활성화)<br/>불필요한 보조 입출력 포트의 오른쪽 끝부분에 Down (비활성화)</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt;configure<br/>[edit]<br/>user@juniper#show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 interface 차단 설정 확인</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 조치 방법 | <p>포트 차단 및 허용 설정을 확인한다.</p> <p>&lt; CISCO &gt;<br/>1. AUX 포트 접속 차단<br/>Router# config terminal<br/>Router(config)# line aux 0<br/>Router(config-line)# no password (어떤 사용자도 접속 금지)<br/>Router(config-line)# transport input none (어떤 입력도 받지 않음)<br/>Router(config-line)# no exec (어떤 명령도 실행 안 됨)<br/>Router(config-line)# exec-timeout 0 1 (1 초 지나면 자동 타임아웃)</p> <p>2. 해당 인터페이스 차단<br/>Router# config terminal<br/>Router(config)# int f0/1 (해당 포트 선택)<br/>Router(config-line)# shutdown</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# editinterface so-1/0/3<br/>[edit interfaces so-1/0/3]<br/>user@juniper# setunit0familyinetaddress10.0.20.1/24<br/>user@juniper# commit</p> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |

### 3.3. 패치관리

#### 3.3.1. 최신 보안 패치 및 벤더 권고사항 적용

| 분류    | 로그 관리 관련 진단                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | NW-08 | 중요도 | L |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | 공통                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 설명    | 네트워크 장비의 보안 수준을 높이고 성능 및 기능 향상을 위해서는 버전 업그레이드 및 보안 패치 작업을 수행하여 취약점을 보완하는 작업이 필요하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 진단 기준 | 양호 - 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우<br>취약 - 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 점검 방법 | < CISCO ><br>Router# show version<br>버전정보 확인<br><br>< Juniper ><br>user@juniper> configure<br>[edit]<br>user@juniper# show version<br>root authentication 설정을 이용하여 [edit system] 레벨에서 패치 정보 확인                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 조치 방법 | 장비 별 제공하는 최신 취약점 정보를 파악 후 최신 패치 및 업그레이드를 수행하여야 한다.<br><br>< 공통 ><br>• 네트워크 장비는 지속해서 취약점이 발견되고 있으며, 이에 대한 패치도 계속 제공되고 있음<br>• 테스트와 수정을 통하여 검증 받은 패치를 사용하여야 하며, 이외 버전은 꼭 필요한 기능이 있는 경우만 사용함<br>• 최신 패치를 적용 하지 않을 경우 IP Option, TCP, IPv6, Header 패킷을 발송할 경우 서비스 거부 등의 피해가 발생할 수 있음<br><br>1. CISCO 버전별 정보<br><a href="http://www.cisco.com/web/about/security/intelligence/ios-ref.html">http://www.cisco.com/web/about/security/intelligence/ios-ref.html</a><br><br>2. Juniper 버전별 정보<br><a href="http://www.juniper.net/us/en/products-services/routing/">http://www.juniper.net/us/en/products-services/routing/</a> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |



### 3.4. 기능관리

#### 3.4.1. SNMP 서비스 확인

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | NW-09 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Passport, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 설명    | <p>*SNMP는 *UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 *DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능저하, 크래쉬, 리로드 등의 위험이 존재함. 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 *Community String을 유추할 수 없게 설정하여야 한다.</p> <p>*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.</p> <p>*UDP: 사용자 데이터그램 프로토콜(User Datagram Protocol)의 줄임말로 인터넷상에서 서로 정보를 주고받을 때 정보를 보낸다는 신호나 받는다는 신호 절차를 거치지 않고, 보내는 쪽에서 일방적으로 데이터를 전달하는 통신 프로토콜을 말함.</p> <p>*Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비밀번호인 'Community String'을 사용함.</p> <p>*Dos(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격임. 특정 서버에게 수많은 접속 시도를 만 들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 받아내는 등의 공격이 이 범위에 포함됨.</p> |       |       |     |   |
| 진단 기준 | <p>양호 - SNMP 서비스를 불필요하게 사용하지 않는 경우</p> <p>취약 - SNMP 서비스를 불필요하게 사용하는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;</p> <pre>Router# show running-config Router# show snmp</pre> <p>1. SNMP 설정 확인<br/>2. SNMP 서비스 동작 확인</p> <p>※ SNMP 서비스 비활성화 시 아래 문구 출력</p> <pre>! %SNMP agent not enabled !</pre> <p>&lt; Juniper &gt;</p> <pre>user@juniper&gt; configure [edit] user@juniper# show snmp</pre> <p>root authentication 설정을 이용하여 [edit system] 레벨에서 snmp 서비스 설정 확인</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |

|       |                                                                                                                                                                                                                                                                                                                             |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>SNMP 서비스가 불필요할 경우 중지하여야 한다.</p> <p>&lt; CISCO &gt;<br/> Router# config terminal<br/> Router(config)# no snmp-server<br/> Router(config)# ^Z</p> <p>&lt; Alteon / Passport &gt;<br/> SNMP 서비스가 불필요하다면 서비스 중지</p> <p>&lt; Juniper &gt;<br/> user@juniper&gt; configure<br/> user@juniper# no set snmp community public</p> |
| 비고    |                                                                                                                                                                                                                                                                                                                             |

### 3.4.2. SNMP community string 복잡성 설정

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | NW-10 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Passport, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | NMP의 Public, Private과 같은 디폴트 community String을 변경하지 않고 사용할 경우, 악의적인 사용자가 장비 설정을 쉽게 변경하여 중요 시스템 정보가 노출될 수 있으므로 추측하기 어려운 Community String으로 변경하는 설정이 필요하다.                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | <p>양호 - SNMP 서비스를 사용하지 않거나, 유추하기 어려운 Community String을 설정한 경우</p> <p>취약 - 디폴트 Community String을 변경하지 않거나, 유추하기 쉬운 Community String으로 설정한 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running-config</p> <p>SNMP 설정 확인</p> <p>&lt; Alteon, Passport &gt;<br/>#snmp 설정에서 Community String 설정 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 community string 확인</p>                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 조치 방법 | <p>Public, Private 외 다른 Community String을 설정하여야 한다.</p> <p>&lt; CISCO &gt;<br/>Community String 문자열 변경<br/>Router# config terminal<br/>Router(config)# snmp-server Community &lt;커뮤니티명&gt;</p> <p>&lt; Alteon &gt;<br/>네트워크 장비는 SNMP 로의 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열,<br/>영문자 혼합으로 변경 권고함</p> <ol style="list-style-type: none"> <li>1. switch 로 접속</li> <li>2. # cfg/sys/ssnmp</li> <li>3. 다음 중에 해당하는 경우 선택</li> </ol> <p># rcomm - SNMP read community string 을 설정(최대 32 자, Default String - public)</p> <p># wcomm - SNMP write community string 을 설정(최대 32 자, Default String - private)</p> |       |       |     |   |

|    |                                                                                                                                         |
|----|-----------------------------------------------------------------------------------------------------------------------------------------|
|    | 4. # apply<br>5. # save<br><br>< Passport ><br>1. switch 로 접속<br>2. # config snmp-v3 community commname <Comm Idx> new-commname <value> |
| 비고 |                                                                                                                                         |

### 3.4.3. TFTP 서비스 차단

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                | 항목 코드 | NW-11 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                              |       |       |     |   |
| 설명    | TFTP 서비스는 인증 절차를 요구하지 않으므로 평문으로 통신하므로 보안상 취약하다. 이 서비스를 사용하지 않는다면 비활성화해야 하지만 사용이 필요하다면 접근 제한(ACL) 설정을 통해 비인가자의 접근을 차단하여야 한다.                                                                                                                                                                         |       |       |     |   |
| 진단 기준 | 양호 - TFTP 서비스를 사용하지 않거나, ACL을 적용하여 사용하는 경우<br>취약 - TFTP 서비스를 사용하고 ACL을 설정하지 않은 경우                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running-config</p> <p>TFTP 설정 정보 확인</p> <p>&lt; Alteon &gt;<br/>/cfg/slb/filt에서 tftp 서비스 설정 제거 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 TFTP 서비스 확인</p> |       |       |     |   |
| 조치 방법 | <p>불필요한 TFTP 서비스 사용 시 제거하여야 한다.</p> <p>&lt; CISCO &gt;<br/>외부망에서 사용할 필요가 없는 TFTP 서비스 포트 차단<br/>Router# config terminal<br/>Router(config)# no service tftp</p> <p>&lt; Alteon &gt;<br/># /cfg/slb/filt &lt;filter number&gt;/sport 69 (tftp 서비스 제거)</p>                                             |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                     |       |       |     |   |

### 3.4.4. Spoofing 방지 필터링 적용

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | NW-12 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 설명    | Source IP 주소가 broadcast, multicast, loopback인 것은 전혀 사용될 필요가 없으나 종종 악의적인 목적(DoS 공격 시)으로 사용될 수도 있으므로, ACL를 설정하여 변조된 불법 패킷을 차단하도록 설정하여야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 진단 기준 | 양호 - 악의적인 공격에 대비하여 Source IP에 ACL을 적용한 경우<br>취약 - 악의적인 공격에 대비하여 Source IP에 ACL을 적용하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running</p> <p>IP spoofing 방지 설정 확인</p> <p>&lt; Alteon &gt;<br/>/slb/filt에서 IP spoofing 방지를 위한 ACL 설정 확인</p> <p>&lt; Juniper &gt;<br/>Configure Firewall Filters와 Apply Firewall Filters 설정 확인</p>                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 조치 방법 | <p>Source IP에 ACL 적용한다.</p> <p>&lt; CISCO &gt;<br/>1. Global configuration mode 로 접속<br/>2. access-list number deny ip 127.0.0.0 0.255.255.255 any<br/>3. access-list number deny ip 224.0.0.0 31.255.255.255 any<br/>4. access-list number deny ip host 0.0.0.0 any<br/>5. access-list number permit ip any any</p> <p>&lt; Alteon &gt;<br/>1. switch로 접속함.<br/>2. # cfg<br/>3. # /slb/filt &lt;filter number&gt;<br/>4. # sip 127.0.0.0</p> <p>&lt; Juniper &gt;<br/>1. Configure Firewall Filters<br/>[edit firewall]<br/>firewall {<br/>filter filter-name {<br/>term term-name {<br/>accounting-profile name;<br/>from {<br/>source-address 127.0.0.0/24;</p> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> source-address 224.0.0.0/4; source-address 0.0.0.0/0; } then { discard; } } } } } </pre> <p>2. Apply Firewall Filters</p> <pre> [edit interfaces interface-name unit logical-unit-number family inet] interfaces { interface-name { unit logical-unit-number { family inet { filter { input filter-name; output filter-name; } } } } } </pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                     |

### 3.4.5. 사용하지 않는 인터페이스의 shutdown 설정

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | NW-13 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 설명    | 사용하지 않는 포트에 연결된 인터페이스를 shutdown 하지 않을 경우 물리적인 접근을 통해 비인가자의 불법적인 접근이 가능함. 네트워크 정보 유출 및 내부 네트워크 손상 위험 방지를 위해 사용하지 않는 인터페이스를 shutdown 시키는 설정이 필요하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 진단 기준 | 양호 - 사용하지 않는 인터페이스가 차단된 경우<br>취약 - 사용하지 않는 인터페이스가 차단되지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 점검 방법 | <p>&lt; Cisco &gt;<br/>                     Router# show running-config<br/>                     Router# show interface status<br/>                     Router# show ip interface brief</p> <p>1. 각 Interface 설정 확인<br/>                     2. Interface 상태 확인<br/>                     (해당포트가 down/up 이 되어 있는지 확인할 수 있음)</p> <p>&lt; Juniper &gt;<br/>                     user@juniper&gt; configure<br/>                     user@juniper# show ip</p> <p>불필요한 포트 차단 확인</p>                                                                                                                                                                                                                                                                      |       |       |     |   |
| 조치 방법 | <p>사용하지 않은 인터페이스 차단하여야 한다.</p> <p>&lt; CISCO &gt;<br/>                     Router# config terminal<br/>                     Router(config)# interface fastethernet 0/1<br/>                     Router(config-line)# shutdown<br/>                     사용할 포트는 no shutdown 으로 포트 상태를 up 시켜줌</p> <p>&lt; Alteon &gt;<br/>                     사용하지 않은 인터페이스 차단<br/>                     # config terminal<br/>                     # interface fastethernet 0/1<br/>                     # shutdown<br/>                     사용할 포트는 no shutdown으로 포트 상태를 up 시켜줌</p> <p>&lt; Juniper &gt;<br/>                     기본적인 인터페이스 비활성<br/>                     [edit interface interface-name] &lt;- 해당 인터페이스 이름 삽입<br/>                     disable;</p> |       |       |     |   |



|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> 예제&gt; user@juniper# configure user@juniper# edit interfaces [edit interfaces] user@juniper# set so-1/1/0 disable user@juniper# ^z user@juniper# edit interface [edit interfaces] user@juniper# show so-1/1/0 so-1/1/0 {   disable;   mtu 8000;   clocking internal;   encapsulation aaa;   sonet-options {     fcs 16;   }   unit 0 {     family inet {       address 1.1.1.1/32 {         destination 1.1.1.2;       }     }   } } </pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### 3.4.6. Finger 서비스 차단

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | NW-14 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 설명    | Finger 서비스를 사용할 경우 기본적인 장비의 접속 상태가 노출될 수 있고, 특별히 NMS 등에서 사용하지 않으면 VTY(Virtual Teletype)의 사용 현황을 원격에서 파악하는 것이 가능하므로 Finger 서비스 제한 설정이 필요하다.                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | 양호 - Finger 서비스를 차단하고 있는 경우<br>취약 - Finger 서비스를 차단하고 있지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 점검 방법 | <pre> &lt; CISCO &gt; Router# show running-config  Finger 서비스 설정 확인  &lt; Juniper &gt; user@juniper&gt; configure [edit] user@juniper# show root authentication 설정을 이용하여 [edit system] 레벨에서 Finger 서비스 설정 확인                     </pre>                                                                                                                                                                                                                  |       |       |     |   |
| 조치 방법 | <p>사용하지 않을 경우 각 장비별 Finger 서비스의 사용을 제한하여야 한다.</p> <pre> &lt; CISCO &gt;  최근 출시되는 IOS는 no service finger 명령 대신 no ip finger 명령을 사용하기도 함 Router# config terminal Router(config)# no service finger (이전) Router(config)# no ip finger  &lt; Juniper &gt; user@juniper&gt; configure [edit] user@juniper# edit system services [edit system services] no finger {   &lt;connection-limit limit&gt;;   &lt;rate-limit limit&gt;; }                     </pre> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |

### 3.4.7. 웹 서비스 차단

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | NW-15 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | 네트워크 장비에서 제공하는 관리용 웹(HTTP) 사이트는 기존에 알려진 웹 취약점이나 패스워드 추측 공격 등에 취약할 수 있으므로 불필요한 경우에는 HTTP 사용을 제한하여야 함. HTTP 서버를 사용해야 한다면 HTTP 서버에 접속할 수 있는 관리자 IP를 제한해야 한다.                                                                                                                                                                                                                                                                      |       |       |     |   |
| 진단 기준 | 양호 - 웹 서비스를 차단한 경우<br>취약 - 웹 서비스를 차단하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | < CISCO ><br>Router# show running-config<br><br>웹 서비스 설정 확인                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 조치 방법 | HTTP 서비스 차단 또는 HTTP 서버를 관리하는 관리자 접속 IP를 설정하여야 한다.<br><br>< CISCO ><br>Router# config terminal<br>Router(config)# no ip http server<br>Router(config)# ^Z<br>※ IOS 상의 HTTP 서버를 사용해야만 한다면, HTTP WEB_EXEC 서비스를 비활성화 함으로써 위험을 우회할 수 있음<br>Router# config terminal<br>Router(config)# ip http active-session-modules exclude_webexec<br>Router(config)# ip http secure-active-session-modules exclude_webexec<br>Router(config)# ^Z |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |

### 3.4.8. TCP/UDP Small 서비스 차단

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | NW-16 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO                                                                                                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 설명    | Cisco 제품의 경우 DoS 공격의 대상이 될 수 있는 서비스(echo, discard, daytime, chargen)를 기본적으로 제공하므로 보안상 위험이 존재한다. 이러한 서비스는 일반적으로 거의 사용하지 않으므로 서비스가 불필요하게 열려있다면 제거하여 DoS 공격을 예방할 수 있다.                                                                                                                                                                                                                                                    |       |       |     |   |
| 진단 기준 | 양호 - TCP/UDP Small 서비스가 제한되어 있는 경우<br>취약 - TCP/UDP Small 서비스가 제한되어 있지 않는 경우                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 점검 방법 | < CISCO ><br>Router# show running-config<br><br>1. tcp-small-servers 설정 확인<br>2. udp-small-servers 설정 확인                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 조치 방법 | TCP/UDP Small Service 제한 설정<br><br>< CISCO ><br>서비스 거부 공격을 완전히 차단하지는 못하지만, 알려진 서비스 거부 공격 포트 설정 권고<br>TCP/UDP 관련 Small 서버들의 기능은 Disable 설정함<br><br>Router# config terminal<br>Router(config)# no service tcp-small-servers<br>Router(config)# no service udp-small-servers<br>Router(config)# ^Z<br>※ TCP/UDP Small 서비스는 IOS 11.3 이상에서는 기본적으로 서비스가 제거된 상태이므로 Small 서버들이 Default로 Disable되어 있지만 낮은 버전의 경우는 직접 설정해 주어야 함. |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |

### 3.4.9. IP BOOTP 서비스 제한

| 분류    | 보안기능 설정관련 진단                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | NW-17 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | BOOTP는 네트워크 사용자가 자동으로 IP 주소를 받게 구성되고 사용자의 간여 없이도 부트되는 운영체계를 가지고 있게 해주는 프로토콜이다. 그러나 사용하지 않는 불필요한 서비스는 시스템 또는 네트워크 공격자의 공격루트로 활용될 수 있다. 따라서 사용하지 않는 Bootp Server를 비활성화 시켜 시스템 또는 네트워크 공격자의 공격루트를 사전에 차단할 것을 권고한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 진단 기준 | 양호 - 사용하지 않는 Bootp Server가 비활성화 일 경우<br>취약 - 사용하지 않는 Bootp Server가 활성화 일 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 점검 방법 | <p>&lt; Cisco &gt;<br/>                     Router# show running-config</p> <p>ip bootp server 설정 확인</p> <p>&lt; Alteon &gt;<br/>                     #bootp disable 설정 확인</p> <p>&lt; Juniper &gt;<br/>                     user@switch&gt;show configuration &amp; show interfaces detail</p> <p>bootp 서비스 설정 확인</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 조치 방법 | <p>&lt; CISCO &gt;<br/>                     기준이 되는 IOS 버전은 기본적으로 설정이 되어 있다. 따라서 다음과 같은 절차에 따라서 작업을 할 필요가 있다.<br/>                     1. Global configuration mode로 들어간다.<br/>                     2. no ip bootp server</p> <p>각 IOS 버전 별로 서비스의 기본 상태는 다음과 같다.<br/>                     Ver 11.1, Ver 11.2, Ver 11.3, Ver 12.0, Ver 12.1, Ver 12.2, Ver 12.3 는 enabled 상태이다.</p> <p>&lt;Alteon&gt;<br/>                     1. 스위치로 접속한다.<br/>                     2. # cfg<br/>                     3. # sys<br/>                     4. # bootp disable enable<br/>                     5. # apply<br/>                     6. # save</p> <p>&lt; Juniper &gt;<br/>                     DHCP 서버 IP 주소와 서버가 연결되어있는 스위치에 대한 인터페이스 지정 옵션 제거</p> |       |       |     |   |

|    |                                                                                                                                                                                                |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> user@switch&gt; configure [edit] user@switchr# edit forwarding-options helpers bootp [edit forwarding-options helpers bootp] user@switch# no set interface (인터페이스 포트) server (주소) </pre> |
| 비고 | 단기적용                                                                                                                                                                                           |

### 3.4.10. Source 라우팅 차단

| 분류    | 기능관리                                                                                                                                                                                                              | 항목 코드 | NW-18 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Juniper                                                                                                                                                                                                    |       |       |     |   |
| 설명    | 라우터에서 패킷의 목적지에 따라 패킷을 라우팅하는 것이 기본이지만, 때에 따라 송신 측에서 라우팅 경로 정보를 송신 데이터에 포함해 라우팅시키는 방법을 사용하는 경우가 있다. 거의 사용하지 않는 방법이지만 내부의 라우팅 경로를 파악하여 라우팅이 되지 않는 중요 서버로 접근할 수 있으므로 소스 라우팅을 기본적으로 단하여야 한다.                           |       |       |     |   |
| 진단 기준 | 양호 - IP Source Routing이 제한되어 있는 경우<br>취약 - IP Source Routing이 제한되어 있지 않은 경우                                                                                                                                       |       |       |     |   |
| 점검 방법 | 장치별로 IP Source Routing 제한 설정<br><br>< Cisco ><br>Router# show running-config<br><br>ip source route 설정 확인<br><br>< Juniper ><br>user@juniper# show route<br><br>ip source route 설정 확인                             |       |       |     |   |
| 조치 방법 | < CISCO ><br>IP Source Routing 차단<br>Router# config terminal<br>Router(config)# no ip source-route<br>Router(config)# ^Z<br><br>< Juniper ><br>user@juniper> configure<br>[edit]<br>user@juniper# no-source-route |       |       |     |   |
| 비고    |                                                                                                                                                                                                                   |       |       |     |   |

### 3.4.11. arp proxy 제거

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | NW-19 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 설명    | arp proxy는 IP와 MAC address의 캐쉬 기능을 제공한다. 악의적인 사용자가 잘못된 IP와 MAC 정보를 보내올 경우 arp proxy는 잘못된 정보를 보관하게 된다. 이것은 잘못된 IP와 MAC이 관련된 호스트에 대한 정상적인 통신을 방해하거나 가로채기를 할 수 있게 한다. Arp proxy를 제한함으로써 통신방해나 가로채기 등과 같은 악의적인 목적으로 사용되지 못하게 한다.                                                                                                                                                                                          |       |       |     |   |
| 진단 기준 | 양호 - arp proxy를 제한하는 경우<br>취약 - arp proxy를 제한하지 않을 경우                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running-config</p> <p>각 인터페이스 정보에서 Proxy ARP 설정 확인</p> <p>&lt; Alteon &gt;<br/>proxy diable 설정 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper# show<br/>proxy {<br/>inet-address inet-address;<br/>}</p> <p>proxy로 검색하여 특정 MAC과 IP로 제한하거나 off되어 있는지 확인</p>                                                                                                                          |       |       |     |   |
| 조치 방법 | <p>사용하지 않을 경우 각 장비별 ARP Proxy 서비스를 제한하여야 한다.</p> <p>&lt; CISCO &gt;<br/>Proxy ARP를 차단하기 위해서는 no ip proxy-arp 명령 사용<br/>이더넷 인터페이스에 대한 적용 예<br/>Router# config terminal<br/>Router(config)# interface fastethernet 0/1<br/>Router(config-line)# no ip proxy-arp<br/>Router(config)# ^Z</p> <p>&lt; Alteon &gt;<br/>1. switch 접속<br/>2. # cfg<br/>3. # /slb/real<br/>4. # proxy disable<br/>5. # apply<br/>6. # save</p> |       |       |     |   |



|    |                                                                                                                                                       |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre>&lt; Juniper &gt; user@juniper&gt; configure [edit] user@juniper# delete interfaces (interface-name) unit logical - unit -member proxy-arp</pre> |
| 비고 |                                                                                                                                                       |

### 3.4.12. ICMP unreachable, Redirect 차단

| 분류    | 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드 | NW-20 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 설명    | ICMP unreachable 메시지에는 특정 호스트 및 게이트웨이에 패킷을 보냈을 때 어떠한 이유로 전달될 수 없는지 나타내는 코드들을 포함하고 있으므로 스캔을 통해 해당 정보가 공격자에게 유출될 수 있다. ICMP Redirect는 라우터가 송신 측 호스트에 적합하지 않은 경로로 설정되어 있으면 해당 호스트에 대한 최적 경로를 다시 지정해주는 용도로 사용되지만 불필요하게 설정되어 있다면 특정 목적지로 가기 위해 고의적으로 변경하여 패킷을 가로채는 방법으로 악용될 수 있으므로 서비스를 중지하여야 한다.                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 진단 기준 | 양호 - ICMP unreachable, ICMP Redirect가 차단되어 있는 경우<br>취약 - ICMP unreachable, ICMP Redirect가 차단되어 있지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 점검 방법 | <pre> &lt; CISCO &gt; Router&gt; enable Router# show running                     </pre> 각 인터페이스별 정보에 적용된 것을 확인 <pre> &lt; Juniper &gt; user@juniper# show                     </pre> ICMP Unreachables , ICMP redirects 적용 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 조치 방법 | 장비의 Configuration 설정에서 ICMP Unreachables, ICMP Redirects 차단하여야 한다. <pre> &lt; CISCO &gt; 인터페이스에 no ip unreachable 를 실행하여 차단하면 스캔 시 소요되는 시간도 길어져 스캔 공격을 지연·차단 가능 Router# config terminal Router(config)# interface FastEthernet0/1 (인터페이스 선택) Router(config-if)# no ip unreachable RIP, OSPF 등의 프로토콜을 사용함으로써 ICMP Redirect 제거 가능 Router# config terminal Router(config)# interface FastEthernet0/1 (인터페이스 선택) Router(config-if)# no ip redirects                     </pre> <pre> &lt; Juniper &gt; ICMP 트래픽을 추적하여 옵션 지정 가능 [edit protocols router-options]를 통하여 특정 ICMP 옵션 값 변환 가능 &lt;&gt; 표시 한곳에는 해당 옵션 값을 넣어주어야 함  [edit protocols router-discovery] traceoptions {                     </pre> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> file name &lt;replace&gt; &lt;size size&gt; &lt;files number&gt; &lt;no-stamp&gt; &lt;(world-readable   no-world-readable)&gt;; flag flag &lt;flag-modifier&gt; &lt;disable&gt;; }  ICMP 프로토콜의 트래픽을 추적하기 위한 명령어 [edit] routing-options {   traceoptions {     file routing-log;   } }  protocols {   router-discovery {     traceoptions {       file icmp-log;       flag state;     }   } } </pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                            |

### 3.5. 로그관리

#### 3.5.1. 로깅 버퍼 크기 설정

| 분류    | 로그관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | NW-21 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 설명    | <p>기본적으로 로그는 파일이 아닌 *버퍼 메모리에 저장되는데 메모리의 양을 초과하여 그가 저장될 경우 로그 정보를 잃게 되어 침해사고 발생 시 침입 흔적을 알 수 없는 상황이 발생할 수 있다. 그러므로 저장되는 로그 데이터 용량을 고려하여 버퍼 크기를 정하여야 한다.</p> <p>*버퍼 메모리: 일반적으로 주기억 장치와 중앙 처리 장치 사이에 명령이나 데이터를 일시 유지하는데 사용되는 고속의 기억 장치. 버퍼 메모리는 주기억 장치보다 메모리 용량은 적지만 고속의 기억 소자를 사용함으로써 주기억 장치와 중앙 처리 사이의 정보의 흐름을 원활하게 함.</p> <p>버퍼 메모리를 달리 로컬 메모리 혹은 캐시(cache)라고도 함.</p>                                                                                                                 |       |       |     |   |
| 진단 기준 | <p>양호 - 저장되는 로그 데이터보다 버퍼 용량이 큰 경우</p> <p>취약 - 저장되는 로그 데이터보다 버퍼 용량이 작은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;</p> <p>Router&gt; enable</p> <p>Router# show logging 로그에 대한 정보를 확인</p> <p>메모리(RAM)에 저장된 로그는 'show logging'으로 확인할 수 있고, 'clear logging'을 실행하거나 RAM에 저장된 로그는 재부팅하면 사라지게 됨.</p>                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 조치 방법 | <p>로그에 대한 정보를 확인하여 적절한 버퍼 크기 설정하여야 한다.</p> <p>&lt; CISCO &gt;</p> <p>최대 버퍼 크기는 65,500Kbyte 이며 버퍼 용량을 높게 설정하면 패킷 전달이 안 되는 경우가 발생하며, 일반적으로 16Kbyte 에서 32Kbyte 의 크기가 적당하며, 최대 용량이 16Kbyte 에 못 미치는 장비의 경우 장비 성능을 고려하여 최대 용량에 가깝게 설정하는 것을 권고함</p> <p>Router# config terminal</p> <p>Router(config)# logging on (로그를 메모리에 백업)</p> <p>Router(config)# logging buffered 16000 (16KByte 할당)</p> <p>Router(config)# logging buffered information (severity 레벨 설정)</p> <p>Router(config)# ^Z</p> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |

### 3.5.2. 정책에 따른 로깅 설정

| 분류    | 로그관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | NW-22 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Juniper                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 설명    | 관리자는 로그 정보를 통해 장비의 상태와 서비스 정상 여부를 파악할 수 있으며 네트워크에 어떤 종류의 공격이나 침입이 진행되고 있는지 알 수 있다. 정책에 따른 로깅 설정을 통해 로그를 정기적으로 검사하고 정상적인 운영 상태 및 공격 유형을 식별하여 네트워크 동향을 파악하여야 한다.                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 진단 기준 | 양호 - 로그 기록 정책에 따라 로깅 설정이 되어있는 경우<br>취약 - 로그 기록 정책 미 수립 또는, 로깅 설정이 미흡한 경우                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router&gt; enable<br/>Router# show logging</p> <p>로그에 대한 정보 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# show log messages</p> <p>로그에 대한 정보 확인.</p>                                                                                                                                                                                                                                                      |       |       |     |   |
| 조치 방법 | <p>로그 기록 정책을 수립하고 정책에 따른 로깅 설정하여야 한다.</p> <p>&lt; Cisco, Juniper &gt;<br/>라우터에 기본적으로 설정된 로그 파일 설정을 변경하지 않으면 로깅을 효율적으로 사용할 수 없으므로 크게 6가지로 이루어진 아래의 방법을 활용하여야 함</p> <p>1. 콘솔 로깅<br/>콘솔 로그 메시지는 오직 콘솔 포트에서만 보이므로 이 로그를 보기 위해서는 반드시 콘솔 포트에 연결하여야 함</p> <p>2. Buffered 로깅<br/>Buffered 로깅은 로그를 라우터의 RAM에 저장하는데 이 버퍼가 가득 차게 되면 오래된 로그는 자동으로 새로운 로그에 의해 대체됨</p> <p>3. Terminal 로깅<br/>Terminal monitor 명령을 사용하여 로깅을 설정하면 라우터에서 발생하는 로그 메시지를 VTY terminal에 보냄</p> <p>4. Syslog</p> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>시스코 라우터는 라우터의 로그 메시지가 외부의 syslog 서버에 저장되도록 설정할 수 있음</p> <p>5. SNMP traps<br/>SNMP trap이 설정되면 SNMP는 특별한 상황을 외부의 SNMP 서버에 전송하도록 설정할 수 있음</p> <p>6. ACL 침입 로깅<br/>표준 또는, 확장된 액세스 리스트를 설정할 때 특정한 룰에 매칭하였을 경우 해당 패킷 정보를 로그에 남기도록 설정할 수 있는데, 이는 액세스 리스트 룰의 끝에 로그나 로그 인풋을 추가하면 됨<br/>로그 인풋은 로그와는 달리 인터페이스 정보도 함께 남기게 되므로 어떤 인터페이스를 통해 로그가 남았는지를 알 수 있음</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                        |

### 3.5.3. NTP 서버 연동

| 분류    | 로그관리                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드 | NW-23 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | CISCO, Alteon, Juniper                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 설명    | <p>NTP(Network Time Protocol)는 로그의 통합 보관 시 시간의 동기화 등 정확하고 일관된 시간 관리를 위한 필수적인 조건이라 할 수 있음. 하지만 NTP가 사용하는 프로토콜은 보안 위협에 취약하므로 별도의 내부 NTP 서버나 신뢰할 수 있는 서버로 정해서 사용하여야 함.</p> <p>※ IOS 12.2 이전 버전을 사용하는 장비에는 접근 통제(ACL) 설정이 되어 있어야 양호</p>                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | <p>양호 - NTP 서비스가 서버로 설정된 경우</p> <p>취약 - NTP 서비스를 사용하지 않거나, 서버와 연동되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 점검 방법 | <p>&lt; CISCO &gt;<br/>Router# show running-config</p> <p>NTP 서버 설정 확인</p> <p>&lt; Alteon &gt;<br/>/sys/ntp에서 NTP 서버 설정 확인</p> <p>&lt; Juniper &gt;<br/>user@juniper&gt; configure<br/>[edit]<br/>user@juniper# show<br/>root authentication 설정을 이용하여 [edit system] 레벨에서 NTP 서비스 설정 확인</p>                                                                                                                        |       |       |     |   |
| 조치 방법 | <p>NTP 사용 시 신뢰할 수 있는 서버로 설정</p> <p>&lt; CISCO &gt;<br/>NTP 서버 연동 설정<br/>Router# config terminal<br/>Router(config)# ntp server 129.237.32.2 (NTP 서버 IP)<br/>Router(config)# ^Z</p> <p>■ Alteon</p> <ol style="list-style-type: none"> <li>1. switch로 접속함.</li> <li>2. # cfg</li> <li>3. # /sys/ntp</li> <li>4. # on</li> <li>5. # prsrvr [NTP 서버 IP]</li> <li>6. # intrval [동기화 주기]</li> </ol> <p>tzone +9:00</p> |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre> 7. # apply 8. # save  &lt; Juniper &gt; Juniper 라우터에서 NTP를 설정하기 위해 Boot 서버 설정 필요 user@juniper&gt; configure [edit] user@juniper# edit system ntp [edit system ntp] user@juniper# set boot-server 1.1.1.1 &lt;- (NTP 서버주소) • 클라이언트 모드 user@juniper# set server (NTP 서버주소) • 브로드캐스트 모드 user@juniper# set broadcast (NTP 서버주소) • Symmetric active 모드 user@juniper# set peer (NTP 서버주소) prefer user@juniper# set peer (NTP 서버주소) </pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                           |



## 4. 정보보호시스템 취약성 점검항목 및 가이드

### 4.1. 장비 SW/HW 관련 진단

#### 4.1.1. 최신 패치 적용 여부

| 분류                  | 장비 SW/HW 관련 진단                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | NF1-01 | 중요도 | H |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|-------|--|-------|---------------------------|--------|------------------------------------------------|--------------------|-------------------------------------|---------------------|-------------------------------------|
| 대상                  | 방화벽, IPS, IDS                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 설명                  | 보안장비는 지속적으로 취약점이 알려지고 있으며 이에 대한 패치도 지속해서 제공되고 있으므로 보안장비의 보안수준을 높이고 성능 및 기능 향상을 위해서는 버전 업그레이드 및 보안 패치 작업을 수행하여 최신 취약점을 보완하는 작업이 필요하다.                                                                                                                                                                                                                                                           |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 진단 기준               | 양호 - 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우<br>취약 - 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우                                                                                                                                                                                                                                                                                                        |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 점검 방법               | 자동 업데이트 기능 설정 또는 벤더사에 문의하여 업데이트 수행                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 조치 방법               | <div>벤더사에 문의하여 자동 업데이트 기능 설정</div> <table><tr><th colspan="2">장비 정보</th></tr><tr><td>호스트 명</td><td>Fortigate-200 <b>[변경]</b></td></tr><tr><td>펌웨어 버전</td><td>Fortigate-200 2.80,build489,051027 <b>[갱신]</b></td></tr><tr><td>FortiGuard - AV 파일</td><td>6.123(10/26/2005 14:55) <b>[갱신]</b></td></tr><tr><td>FortiGuard - IPS 파일</td><td>2.240(10/20/2005 17:01) <b>[갱신]</b></td></tr></table> |       |        |     |   | 장비 정보 |  | 호스트 명 | Fortigate-200 <b>[변경]</b> | 펌웨어 버전 | Fortigate-200 2.80,build489,051027 <b>[갱신]</b> | FortiGuard - AV 파일 | 6.123(10/26/2005 14:55) <b>[갱신]</b> | FortiGuard - IPS 파일 | 2.240(10/20/2005 17:01) <b>[갱신]</b> |
| 장비 정보               |                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 호스트 명               | Fortigate-200 <b>[변경]</b>                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 펌웨어 버전              | Fortigate-200 2.80,build489,051027 <b>[갱신]</b>                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| FortiGuard - AV 파일  | 6.123(10/26/2005 14:55) <b>[갱신]</b>                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| FortiGuard - IPS 파일 | 2.240(10/20/2005 17:01) <b>[갱신]</b>                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |
| 비고                  | 서비스의 영향을 고려하여 벤더사와 협의 후 적용                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |       |  |       |                           |        |                                                |                    |                                     |                     |                                     |

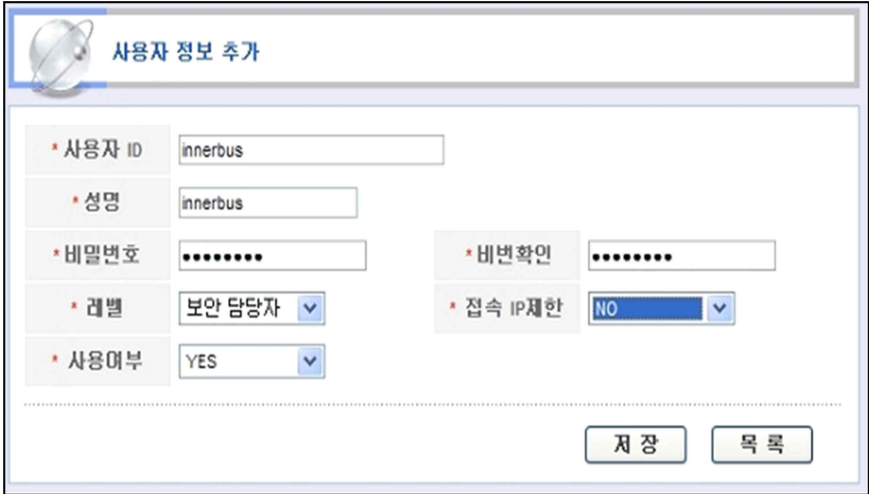
## 4.2. 계정 관리

### 4.2.1. 보안장비 Default 패스워드 변경

| 분류    | 계정 관리                                                                                                                                                                               | 항목 코드 | NF2-01 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽, IPS, IDS                                                                                                                                                                       |       |        |     |   |
| 설명    | 관리자 권한의 패스워드를 강력하게 설정하지 않을 경우 비 인가자가 관리자의 권한을 가질 수 있으며, 유출 시 장비 접근에 대한 패스워드 노출의 위험성이 존재한다                                                                                           |       |        |     |   |
| 진단 기준 | 양호 - 초기 패스워드를 변경하여 적절한 패스워드를 사용하고 있는 경우<br>취약 - 초기 패스워드를 사용하고 있는 경우                                                                                                                 |       |        |     |   |
| 점검 방법 | 설정된 패스워드가 영문 대문자, 소문자, 숫자, 특수문자 등이 포함된 8자리 이상으로 되어 있는지 확인한다.<br>- 패스워드 관리대장확인<br>- 패스워드 설정확인<br> |       |        |     |   |
| 조치 방법 | 초기 패스워드를 변경한다.<br>- 대문자, 소문자, 숫자, 특수문자 등이 포함된 8자리 이상의 암호 사용<br>- 진단 대상시스템과 관련되어 유추하기 쉬운 암호 사용 금지                                                                                    |       |        |     |   |
| 비고    |                                                                                                                                                                                     |       |        |     |   |

### 4.3. 네트워크 원격 관리

#### 4.3.1. 보안장비 원격관리 접근통제

| 분류    | 네트워크 원격 관리                                                                                                                                                                | 항목 코드 | NF3-01 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽, IPS, IDS                                                                                                                                                             |       |        |     |   |
| 설명    | 대부분 보안장비는 원격에서 관리하기 위한 관리자 접근방법을 제공하고 있어 이에 대한 통제가 필요하다. 일반적으로 IP 단위로 접근제한을 하여 보안장비에 대한 관리자 접근을 통제하며, 보안장비에서 제공하는 관리자 접근제한 기능을 통해 관리자 단말기 또는 콘솔 장비의 IP를 등록하고 접근을 제한할 수 있다 |       |        |     |   |
| 진단 기준 | 양호 - 원격 관리 시 관리자 IP만 접근 가능하도록 설정한 경우<br>취약 - 원격 관리 시 관리자 IP만 접근 가능하도록 설정하지 않은 경우                                                                                          |       |        |     |   |
| 점검 방법 | 보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인                                                                                                                                       |       |        |     |   |
| 조치 방법 | <p>원격 관리 시 관리자 및 특정 IP만 접근 가능하도록 설정함</p>                                               |       |        |     |   |
| 비고    |                                                                                                                                                                           |       |        |     |   |

#### 4.3.2. SNMP community string 복잡성 설정

| 분류    | 네트워크 원격 관리                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | NF3-02 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | SNMP에서 community string은 SNMP(데몬)와 클라이언트가 데이터를 교환하기 전에 인증하는 일종의 패스워드로서 초기값으로 설정되어 있는 Public, Private와 같은 SNMP default community string을 이용할 시에 해당 장비의 중요한 정보를 외부로 노출시킬 가능성이나 네트워크 장비 설정 등을 변경(RW)시킬 수 있는 위험성이 존재한다. 이를 그대로 사용하는 것은 패스워드를 사용하지 않는 계정을 사용하는 것 이상 위험함에도 불구하고 대부분의 시스템, 네트워크 관리자들이 기본적인 문자열인 public을 그대로 사용하거나 다른 문자열로 변경을 해도 상호나 monitor, router, mrtg 등 사회 공학적으로 추측할 수 있는 문자열을 사용하고 있어 문제가 되고 있다 |       |        |     |   |
| 진단 기준 | 양호 - SNMP Community 이름이 public, private 이 아닌 경우<br>취약 - SNMP Community 이름이 public, private 인 경우                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 점검 방법 | 정보보호시스템의 보안장비의 SNMP 설정 메뉴에서 커뮤니티스트링 값을 확인함<br>어플라이언스 제품을 제외한 소프트웨어 방식의 시스템인 경우 자체 OS 취약점 점검이 이루어지고 있는지 확인함                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 조치 방법 | 보안 장비는 SNMP로의 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경을 권고함<br>(SNMP 버전은 v1, v2, v3 가 존재하는데 v1, v2 는 암호화가 되어 있지 않고 텍스트 열로 전송되지만 v3 가 암호화가 설정되어 있고 해쉬 값으로 전송함.)비고                                                                                                                                                                                                                                        |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |

#### 4.4. 정책 관리 관련 진단

##### 4.4.1. Any(src) to Any(dst), Any 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                    | 항목 코드 | 코드NF4-01 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                            |       |          |     |   |
| 설명    | 입차단시스템이 물리적으로 존재하나 논리적인 접근제어가 이루어지고 있지 않기 때문에 인터넷을 포함한 모든 시스템에서 내부네트워크/시스템/서비스포트로 접근 가능한 보안 정책을 분석한다.                                                                                                                                                          |       |          |     |   |
| 진단 기준 | 양호 - Any(src) to Any(dst), Any 서비스 정책을 제한하고 있는 경우<br>취약 - Any(src) to Any(dst), Any 서비스 정책을 사용하고 있는 경우                                                                                                                                                         |       |          |     |   |
| 점검 방법 | 내부네트워크/시스템/서비스포트의 접근 가능한 보안 정책을 적용하고 있는지 확인한다.<br>아래와 같이 접근제어를 하지 않고, 모든 IP 및 포트를 허용하고 있으면 취약하다.<br><br>< 출발지 IP > Any,<br>< 목적지 IP > Any(내부 네트워크) < 목적지 Port > Any                                                                                            |       |          |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |          |     |   |
| 비고    |                                                                                                                                                                                                                                                                |       |          |     |   |

#### 4.4.2. Any(src) to Group(dst), Any 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                    | 항목 코드 | NF4-02 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | 목적지가 특정 IP Address 또는 C-Class이상으로 grouping되어 있으나 출발지 및 서비스포트가 Any로 정의되어 있기 때문에 불특정 다수의 시스템에서 내부망에 위치한 시스템의 Any 서비스 포트로 접근 가능한 보안 정책을 분석한다.                                                                                                                     |       |        |     |   |
| 진단 기준 | 양호 - Any(src) to Group(dst), Any 서비스 정책을 제한하고 있는 경우<br>취약 - Any(src) to Group(dst), Any 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                                  |       |        |     |   |
| 점검 방법 | 목적지가 특정 IP로 정의되어 있는 경우 출발지 및 서비스 포트가 Any로 설정되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우에 취약하다.<br>< 출발지 IP > Any(외부네트워크)<br>< 목적지 IP > Group, < 목적지 Port > Any                                                                                                           |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                |       |        |     |   |

#### 4.4.3. Group(src) to Any(dst), Any 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                     | 항목 코드 | NF4-03 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 출발지가 특정 IP Address 또는 C-Class이상으로 grouping되어 있으나 출발지 및 목적지 포트가 Any로 정의되어 있기 때문에 목적지/목적지 포트에 대한 접근제어가 이루어지고 있지 않는 보안 정책을 분석한다.                                                                                                                                   |       |        |     |   |
| 진단 기준 | 양호 - Group(src) to Any(dst), Any 서비스 정책을 제한하고 있는 경우<br>취약 - Group(src) to Any(dst), Any 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                                   |       |        |     |   |
| 점검 방법 | 출발지가 특정 IP로 정의되어 있는 경우 목적지/목적지 포트가 Any로 설정되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우 취약하다.<br><br>< 출발지 IP > Group<br>< 목적지 IP > any(내부 네트워크) < 목적지 Port > any                                                                                                           |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client 인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                 |       |        |     |   |

#### 4.4.4. Group(src) to Group(dst), Any 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                     | 항목 코드 | NF4-04 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 출발지 및 목적지가 특정 IP Address 또는 C-Class이상으로 grouping되어 있으나 목적지 포트가 Any로 정의되어 있기 때문에 목적지 포트에 대한 접근제어가 이루어지고 있지 않는 보안 정책을 분석한다.                                                                                                                                       |       |        |     |   |
| 진단 기준 | 양호 - Group(src) to Group(dst), Any 서비스 정책을 제한하고 있는 경우<br>취약 - Group(src) to Group(dst), Any 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                               |       |        |     |   |
| 점검 방법 | 출발지 및 목적지가 특정 IP로 정의되어 있는 경우 목적지 포트가 Any로 설정되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우 취약하다.<br><br>< 출발지 IP >Group<br>< 목적지 IP > any(내부 네트워크) <목적지 Port > any                                                                                                           |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client 인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                 |       |        |     |   |



#### 4.4.5. Any(src) to Group(dst), CML 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                     | 항목 코드 | NF4-05 | 중요도 | L |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 출발지가 Any로 정의되어 있으며 목적지가 Grouping되어 있으나 목적지 포트에 Command Line Protocol(Telnet, FTP, RSH, RLOGIN 등)이 정의되어 있기 때문에 반복적인 Brute Force 공격 등에 대한 위험성이 존재하는 보안 정책을 분석한다.                                                                                                  |       |        |     |   |
| 진단 기준 | 양호 - Any(src) to Group(dst), CML 서비스 정책을 제한하고 있는 경우<br>취약 - Any(src) to Group(dst), CML 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                                   |       |        |     |   |
| 점검 방법 | 출발지가 Any로, 목적지가 Group으로 정의되어 있는 경우 목적지 포트에 CML 서비스가 제한되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우 취약하다.<br><br>< 출발지 IP > any(외부네트워크),<br>< 목적지 IP > Group(내부 네트워크), < 목적지 Port > CML서비스                                                                                  |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client 인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                 |       |        |     |   |

#### 4.4.6. Group(src) to Any(dst), CML 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                     | 항목 코드 | NF4-06 | 중요도 | L |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 출발지가 특정 IP Address 또는 C-Class이상으로 정의되어 있으며 목적지가 Any되어 있기 때문에 목적지 포트의 Command Line Protocol(Telnet, FTP, RSH, RLOGIN 등)에 대하여 반복적인 Brute Force 공격 등에 대한 위험성이 존재하는 보안 정책을 분석한다.                                                                                    |       |        |     |   |
| 진단 기준 | 양호 - Group(src) to Any(dst), CML 서비스 정책을 제한하고 있는 경우<br>취약 - Group(src) to Any(dst), CML 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                                   |       |        |     |   |
| 점검 방법 | 출발지가 특정 IP로, 목적지가 Any로 정의되어 있는 경우 목적지 포트의 CML 서비스가 제한되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우 취약하다.<br><br>< 출발지 IP > Group(외부네트워크)<br>< 목적지 IP > Any(내부 네트워크), < 목적지 Port > CML서비스                                                                                    |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client 인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                 |       |        |     |   |

#### 4.4.7. Group(src) to Group(dst), CML 서비스 정책 제한

| 분류    | 정책 관리 관련 진단                                                                                                                                                                                                                                                    | 항목 코드 | NF4-07 | 중요도 | L |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                            |       |        |     |   |
| 설명    | 출발지 및 목적지가 특정 IP Address 또는 C-Class이상으로 정의되어 있으나 서비스 포트에 Command Line Protocol(Telnet, FTP, RSH, RLOGIN 등)이 정의되어 반복적인 Brute Force 공격 등에 대한 위험성이 존재하는 보안 정책을 분석한다.                                                                                              |       |        |     |   |
| 진단 기준 | 양호 - Group(src) to Group(dst), CML 서비스 정책을 제한하고 있는 경우<br>취약 - Group(src) to Group(dst), CML 서비스 정책을 제한하고 있지 않은 경우                                                                                                                                              |       |        |     |   |
| 점검 방법 | 출발지 및 목적지가 특정 IP로 정의되어 있는 경우 서비스 포트의 CML서비스가 제한되어 있는지 확인한다.<br>다음과 같이 설정되어 있는 경우 취약하다.<br><br>< 출발지 IP > Group(외부네트워크),<br>< 목적지 IP > Group(내부 네트워크), <목적지 Port > CML서비스                                                                                       |       |        |     |   |
| 조치 방법 | 1. 출발지 IP Address의 검증<br>- 접근하고자 하는 출발지의 IP Address의 유효성을 검증하고 제한한다<br>2. 목적지 IP Address 검증<br>- 접근하고자 하는 목적지의 IP Address의 유효성을 검증하고 제한한다<br>3. 서비스포트가 Any로 정의된 경우<br>- 접근하고자 하는 포트의 유효성을 검증하고 제한한다<br>4. 기타 사항<br>- 사용자 및 Client인증의 경우에는 해당 사용자 ID의 유효성을 검증한다 |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                |       |        |     |   |

#### 4.4.8. Internal Outbound

| 분류    | 정책 관리 관련 진단                                                                                                                                                                  | 항목 코드 | NF4-08 | 중요도 | L |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                          |       |        |     |   |
| 설명    | <p>외부 네트워크에서 내부 네트워크에 존재하는 시스템에 불법적으로 접근 성공하였을 경우 이를 경유지 시스템으로 이용하여 다른 네트워크상에 존재하는 시스템으로 불법적인 행위를 할 수 있다.</p> <p>따라서, 보안적인 측면에서는 내부 네트워크에서의 OutBound에 대한 접근 제어 구현이 필요하다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 내부 네트워크에서 OutBound의 접근제어를 하고 있는 경우</p> <p>취약 - 내부 네트워크에서 OutBound의 접근제어를 하고 있지 않은 경우</p>                                                                             |       |        |     |   |
| 점검 방법 | 내부 네트워크에서 외부 네트워크의 접근이 필요한 포트만 허용하고 있는지 침입차단 시스템에서 확인한다.                                                                                                                     |       |        |     |   |
| 조치 방법 | 내부 네트워크에는 특정 서비스만을 제공하는 서버들로만 구성되어 있는 경우 내부 네트워크 망에서 외부 네트워크로 접속하는 OutBound 접속은 제한된 서비스만이 접속할 필요가 있으므로 해당 접속을 검토한 후 꼭 필요한 서비스 포트만을 허용한다.                                     |       |        |     |   |
| 비고    |                                                                                                                                                                              |       |        |     |   |

#### 4.4.9. Drop All

| 분류    | 정책 관리 관련 진단                                                                                                                                                  | 항목 코드 | NF4-09 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                          |       |        |     |   |
| 설명    | 침입차단시스템이 접근통제규칙에 해당되지 않는 모든 패킷들을 Drop 시키도록 설정되어있는지 점검한다.(대부분 장비는 default로 적용됨)<br>또한 filtering rule로써 설정되는 경우 접근통제규칙의 마지막에 DROP & LOG option으로 적용되어 있는지 점검한다 |       |        |     |   |
| 진단 기준 | 양호 - 접근통제규칙에 해당되지 않는 패킷을 Drop 설정하고 있는 경우<br>취약 - 접근통제규칙에 해당되지 않는 패킷을 Drop 설정하고 있지 않은 경우                                                                      |       |        |     |   |
| 점검 방법 | 접근통제규칙에 해당되지 않는 패킷들을 Drop 시키도록 설정되어 있는지 침입차단시스템에서 확인한다.                                                                                                      |       |        |     |   |
| 조치 방법 | 부분의 침입차단시스템은 Default로 접근통제규칙 마지막 항목에 Drop ALL 규칙을 추가하고 있으나 명시적으로 모든 Source에서 모든 Destination으로 모든 Service를 drop 하는 규칙을 추가한다.                                  |       |        |     |   |
| 비고    |                                                                                                                                                              |       |        |     |   |

#### 4.4.10. 침입탐지 룰 적용

| 분류    | 정책 관리 관련 진단                                                                                   | 항목 코드 | NF4-10 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | IPS, IDS                                                                                      |       |        |     |   |
| 설명    | IP spoofing, DDOS 공격 등과 주요한 침입 패턴에 대해서 침입탐지 룰을 설정하고 Alert 경보 및 담당자 메일 등의 관리 조치를 설정하여 중점 관리한다. |       |        |     |   |
| 진단 기준 | 양호 - 침입탐지 룰이 설정되어 있는 경우<br>취약 - 침입탐지 룰이 설정되어 있지 않은 경우                                         |       |        |     |   |
| 점검 방법 | 침입탐지/방지 시스템에 침입탐지 룰이 설정되어 있는지 확인한다.                                                           |       |        |     |   |
| 조치 방법 | 주요한 침입 패턴에 대한 침입탐지 룰을 설정하고 Alert 기능을 활성화 한다.                                                  |       |        |     |   |
| 비고    |                                                                                               |       |        |     |   |

#### 4.4.11. False Positive 관리

| 분류    | 정책 관리 관련 진단                                                                                                                                                                | 항목 코드 | NF4-11 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | IPS, IDS                                                                                                                                                                   |       |        |     |   |
| 설명    | 침입탐지시스템은 DOS(Denial of Service)와 같은 경우 임계값을 설정해서 침입 여부를 판단하고 있으며 해당 임계값은 시스템이 구성된 네트워크에 따라 달라지므로 관리자가 지속적으로 임계값을 조정해서 False Positive (잘못된 침입탐지) 발생률을 낮추어야 한다.              |       |        |     |   |
| 진단 기준 | 양호 - 임계값이 적절하게 설정되어 있는 경우<br>취약 - 임계값이 적절하게 설정되어 있지 않은 경우                                                                                                                  |       |        |     |   |
| 점검 방법 | 침입여부를 판단하는 임계값에 대해 적절하게 설정되어 있는지 침입탐지시스템에서 확인한다.                                                                                                                           |       |        |     |   |
| 조치 방법 | 다음과 같은 순서로 임계값을 조정한다.<br>1. 일정기간동안 지속적으로 탐지되는 침입 Alert를 파악한다.<br>2. 해당 침입 Alert의 정확성을 파악한다.<br>3. 해당 Alert가 임계값을 조정하는 항목인 경우 해당 탐지 임계치를 수정하여 정상적인 서비스가 침입으로 탐지되는 것을 방지 한다. |       |        |     |   |
| 비고    |                                                                                                                                                                            |       |        |     |   |

## 4.5. 로그 관리 관련 진단

### 4.5.1. 보안장비 로그 설정

| 분류                      | 로그 관리 관련 진단                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드                    | NF5-01                   | 중요도                      | M                                   |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------|--------------|-----------|---------------|----------------|--------|--|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|----------|--------------------------|--|--|--|-------------------------------------|-------------------------------------|--|--------------|--------------------------|--|--------------------------|--|-------------------------------------|-------------------------------------|--|-------------|--------------------------|--|--------------------------|--|-------------------------------------|-------------------------------------|--|----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|---------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|---------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|--------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|
| 대상                      | 방화벽, IPS, IDS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                          |                          |                          |                                     |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 설명                      | 로그 정보를 사용함으로써 관리자는 보안장비의 작동과 손상 여부를 파악할 수 있으며 어떤 종류의 침입이나 공격이 진행되고 있는지 알 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |                          |                          |                                     |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 진단 기준                   | 양호 - 정책에 따른 로그설정이 되어 있는 경우<br>취약 - 정책에 따른 로그 설정이 되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |                          |                          |                                     |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 점검 방법                   | 보안장비의 로그 설정 메뉴 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                          |                          |                          |                                     |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 조치 방법                   | <div>정책에 따른 로깅 설정 (각 벤더마다 설정방법이 상이)</div> <table><tr><td></td><td>전체 선택</td><td>FortiLog 애플리케이션 설정</td><td>로컬 고정 디스크 설정</td><td>메모리 백업 설정</td><td>원격 시스로그 서버 설정</td><td>웹 트랜드 로그 서버 설정</td><td>경고 이메일</td></tr><tr><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>▼ 트래픽 로그</td><td><input type="checkbox"/></td><td></td><td></td><td></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td></td></tr><tr><td>정책에서 허용한 트래픽</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td></td></tr><tr><td>정책을 위반한 트래픽</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td></td></tr><tr><td>▼ 이벤트 로그</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>시스템 활동 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>IPSec 터널 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>DHCP 서비스 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>L2TP/PPTP/PPPoE 서비스 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>Admin 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>미종화 활동 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>방화벽 인증 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>패턴 업데이트 이벤트</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>▼ 바이러스 로그</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>바이러스 감염</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>파일명 차단</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>용량초과 파일</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>▼ 웹 필터 로그</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>콘텐츠 차단</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>URL 차단</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>URL 차단 예외</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>분류별 차단 빈도</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>분류별 빈도 감시</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>분류별 빈도 오류</td><td><input type="checkbox"/></td><td></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr></table> |                          |                          |                          |                                     |                                     | 전체 선택                    | FortiLog 애플리케이션 설정 | 로컬 고정 디스크 설정 | 메모리 백업 설정 | 원격 시스로그 서버 설정 | 웹 트랜드 로그 서버 설정 | 경고 이메일 |  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ▼ 트래픽 로그 | <input type="checkbox"/> |  |  |  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  | 정책에서 허용한 트래픽 | <input type="checkbox"/> |  | <input type="checkbox"/> |  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  | 정책을 위반한 트래픽 | <input type="checkbox"/> |  | <input type="checkbox"/> |  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  | ▼ 이벤트 로그 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 시스템 활동 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | IPSec 터널 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | DHCP 서비스 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | L2TP/PPTP/PPPoE 서비스 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Admin 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 미종화 활동 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 방화벽 인증 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 패턴 업데이트 이벤트 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ▼ 바이러스 로그 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 바이러스 감염 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 파일명 차단 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 용량초과 파일 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ▼ 웹 필터 로그 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 콘텐츠 차단 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | URL 차단 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | URL 차단 예외 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 분류별 차단 빈도 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 분류별 빈도 감시 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 분류별 빈도 오류 | <input type="checkbox"/> |  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
|                         | 전체 선택                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | FortiLog 애플리케이션 설정       | 로컬 고정 디스크 설정             | 메모리 백업 설정                | 원격 시스로그 서버 설정                       | 웹 트랜드 로그 서버 설정                      | 경고 이메일                   |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
|                         | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| ▼ 트래픽 로그                | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          |                          |                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 정책에서 허용한 트래픽            | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> |                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 정책을 위반한 트래픽             | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> |                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| ▼ 이벤트 로그                | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 시스템 활동 이벤트              | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| IPSec 터널 이벤트            | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| DHCP 서비스 이벤트            | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| L2TP/PPTP/PPPoE 서비스 이벤트 | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| Admin 이벤트               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 미종화 활동 이벤트              | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 방화벽 인증 이벤트              | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 패턴 업데이트 이벤트             | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| ▼ 바이러스 로그               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 바이러스 감염                 | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 파일명 차단                  | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 용량초과 파일                 | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| ▼ 웹 필터 로그               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 콘텐츠 차단                  | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| URL 차단                  | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| URL 차단 예외               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 분류별 차단 빈도               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 분류별 빈도 감시               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 분류별 빈도 오류               | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |
| 비고                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                          |                          |                          |                                     |                                     |                          |                    |              |           |               |                |        |  |                          |                          |                          |                          |                                     |                                     |                          |          |                          |  |  |  |                                     |                                     |  |              |                          |  |                          |  |                                     |                                     |  |             |                          |  |                          |  |                                     |                                     |  |          |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |              |                          |  |                          |                          |                                     |                                     |                          |                         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |            |                          |  |                          |                          |                                     |                                     |                          |             |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |         |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |        |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |           |                          |  |                          |                          |                                     |                                     |                          |



#### 4.5.2. 보안장비 로그 정기적 검토

| 분류    | 로그 관리 관련 진단                                                                                                                                 | 항목 코드 | NF5-02 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽, IPS, IDS                                                                                                                               |       |        |     |   |
| 설명    | 로그를 정기적으로 조사해야 하는 것이 중요하며 로그를 정기적으로 검사함으로써, 해당 장비와 네트워크 상태의 동향을 파악할 수 있음. 정상적 운영상태 및 그 상태가 로그에 반영되어 있음을 확인함으로써 비정상적인 상태 또는 공격 상태를 식별할 수 있다. |       |        |     |   |
| 진단 기준 | 양호 - 로그 수집이 설정되어 있고, 분석이 정기적으로 되고 있는 경우<br>취약 - 로그 수집이 설정되어 있지 않고, 분석이 되고 있지 않는 경우                                                          |       |        |     |   |
| 점검 방법 | 보안장비 로그를 정기적으로 분석하여 보관하는지 확인                                                                                                                |       |        |     |   |
| 조치 방법 | 보안장비 로그를 정기적으로 분석하여 보관<br>1. 로그 수집 설정<br>2. 로그 분석 도구를 사용하여 결과 생성 및 리포트 제공<br>(로그를 수집하여 수작업으로 분석하는 것은 시간과 인적으로 무리가 있으므로 자동 로그 분석 도구를 사용)     |       |        |     |   |
| 비고    |                                                                                                                                             |       |        |     |   |

## 4.6. 보안기능 설정관련 진단

### 4.6.1. ICMP Flooding 차단 설정

| 분류    | 보안기능 설정관련 진단                                                                                                                                                                                                                                                                                                                 | 항목 코드 | NF6-01 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 설명    | <p>Ping Flooding 공격은 과도한 ICMP echo request packet 발생을 이용한 DoS 공격의 하나이다.</p> <p>Inbound 체크박스과 Outbound 체크박스를 활성화 시킴으로써 내부 혹은 외부에서 발생하는 트래픽 중 ICMP echo request packet 패킷을 감시할 수 있다. 또한 탐지와 차단 체크박스를 통해 침입에 대한 대응을 수행할 수 있다.</p>                                                                                               |       |        |     |   |
| 진단 기준 | <p>양호 - ICMP Flooding 차단 설정이 되어 있는 경우</p> <p>취약 - ICMP Flooding 차단 설정이 되어 있지 않은 경우</p>                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | ICMP Flooding 차단하고 있는지 침입차단시스템에서 확인한다.                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 조치 방법 | <p>Ping Flooding 창에서 검토 후 해당 보안옵션을 활성화시켜 Ping flooding 침해시도를 침입차단시스템 단에서 차단할 수 있도록 관리하는 것을 권고한다.</p> <p>&lt;Netscreen&gt;</p> <ul style="list-style-type: none"> <li>- 메뉴얼 설정으로 ICMP-Flood공격차단 옵션 사용</li> <li>- Outside에 해당하는 인터페이스에 적용</li> </ul> <p>적용방법</p> <p>-&gt; set zone zone screen icmp-flood threshold number</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                              |       |        |     |   |

#### 4.6.2. Port Scan 차단 설정

| 분류    | 보안기능 설정관련 진단                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | NF6-02 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | <p>스캔 공격은 호스트에 대해, 현재 서비스 중인 TCP와 UDP 포트를 탐색하는 도구이다. 해커가 내부 네트워크의 구조를 파악한 후, 어떤 호스트가 어떤 공격에 대해서 취약한 지를 알아내기 위해서 가장 자주 사용되는 도구이다.</p> <p>침입차단시스템은 Default로 아래의 기준으로 탐지한다.</p> <p>1) IP Scan 의 경우 UDP, TCP, ICMP(Ping) 스캔 패킷의 수가 각각 초당 관리자가 설정한 수를 초과하는 경우.(Default : 10)</p> <p>2) Port Scan 의 경우 특정한 값 이하의 포트에 대해 UDP, TCP 스캔 패킷의 수가 각각 초당 관리자가 설정한 수를 초과하는 경우.(Default : 10)</p> |       |        |     |   |
| 진단 기준 | <p>양호 - Port-Scan 차단 설정이 되어 있는 경우</p> <p>취약 - Port-Scan 차단 설정이 되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 점검 방법 | Port-Scan 차단 설정이 되어 있는지 침입차단시스템에서 확인한다.                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 조치 방법 | <p>스캔 공격 창에서 검토 후 해당 보안옵션을 활성화시켜 Scan 공격을 침입차단시스템 단에서 차단할 수 있도록 관리하는 것을 권고한다.</p> <p>&lt;Netscreen&gt;</p> <p>- 매뉴얼 설정으로 내부로 향하는 port scan방지함</p> <p>적용방법</p> <p>-&gt; set zone zone screen port scan-threshold number</p>                                                                                                                                                        |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |

#### 4.6.3. Winnuke 차단설정

|       |                                                                                   |       |        |     |   |
|-------|-----------------------------------------------------------------------------------|-------|--------|-----|---|
| 분류    | 보안기능 설정관련 진단                                                                      | 항목 코드 | NF6-03 | 중요도 | H |
| 대상    | 방화벽                                                                               |       |        |     |   |
| 설명    | 윈도우를 대상으로한 DOS공격의 한 종류인 winnuke는 주로 NetBIOS port 139번과 URG flag셋을 이용하여 시스템을 공격한다. |       |        |     |   |
| 진단 기준 | 양호 - Winnuke 차단 설정이 되어 있는 경우<br>취약 - Winnuke 차단 설정이 되어 있지 않은 경우                   |       |        |     |   |
| 점검 방법 | Winnuke 차단 설정이 되어 있는지 침입차단시스템 내에서 확인한다.                                           |       |        |     |   |
| 조치 방법 | CLI 환경에서 아래와 같이 Winnuke 차단을 설정한다.<br>set zone zone screen winnuke                 |       |        |     |   |
| 비고    |                                                                                   |       |        |     |   |

#### 4.6.4. Session threshold 설정

| 분류    | 보안기능 설정관련 진단                                                                                                                                     | 항목 코드 | NF6-04 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                              |       |        |     |   |
| 설명    | 특정 IP 에서 많은 Session을 발생하여 DOS(Denail of Service) 공격을 수행할 수 있으므로 Source IP 별로 Session 통과 가능한 Session에 대해서 상한선을 부여하여 공격을 방어 할 수 있다.                |       |        |     |   |
| 진단 기준 | 양호 - Session-threshold 설정이 되어 있는 경우<br>취약 - Session-threshold 설정이 되어 있지 않은 경우                                                                    |       |        |     |   |
| 점검 방법 | Session-threshold 설정이 되어 있는지 침입차단시스템 내에서 확인한다.                                                                                                   |       |        |     |   |
| 조치 방법 | The command line interface (CLI) 환경에서 아래와 같이 source-ip-based의 Session-threshold를 설정한다.<br>=> set firewall session-threshold source-ip-based 3000 |       |        |     |   |
| 비고    |                                                                                                                                                  |       |        |     |   |

#### 4.6.5. Source Routing 차단 옵션

| 분류    | 보안기능 설정관련 진단                                                                                                                                                                                        | 항목 코드 | NF6-05 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                                                                 |       |        |     |   |
| 설명    | 침입차단시스템에서 패킷의 목적지에 따라 패킷을 라우팅하는 것이 기본이지만, 경우에 따라 송신측에서 라우팅 경로 정보를 송신 데이터에 포함시켜 라우팅 시키는 방법을 사용하는 경우가 있다. 현재, 거의 사용되지 않는 방법이지만 내부의 라우팅 경로를 파악하여 라우팅이 되지 않는 중요 서버로 접근 할 수 있기 때문에 소스 라우팅을 기본적으로 막아야 한다. |       |        |     |   |
| 진단 기준 | 양호 - Source Routing 차단 옵션이 설정되어 있는 경우<br>취약 - Source Routing 차단 옵션이 설정되어 있지 않은 경우                                                                                                                   |       |        |     |   |
| 점검 방법 | Source Routing 차단 옵션이 설정되어 있는지 침입차단시스템에서 확인한다.                                                                                                                                                      |       |        |     |   |
| 조치 방법 | 침입차단시스템에서 Source Routing 차단 옵션을 사용하여 내부 네트워크 구조 누출 및 외부에서 접근 불가능한 서버의 접근을 차단한다.<br><br>< Netscreen ><br>-> set zone zone screen ip-filter-src                                                       |       |        |     |   |
| 비고    |                                                                                                                                                                                                     |       |        |     |   |

#### 4.6.6. 장비 리셋 기능 비활성화 여부

| 분류    | 보안기능 설정관련 진단                                                                                                                               | 항목 코드 | NF6-06 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                        |       |        |     |   |
| 설명    | 장비복구 목적으로 default enabled 되어있는 기능인 Factory Default Settings으로의 'Device Reset'은, 관리자의 오용, 실수에 의한 침해 또는 기능불능을 가져올 수 있기 때문에 disable하는 것이 안전하다 |       |        |     |   |
| 진단 기준 | 양호 - 장비 리셋 기능이 비활성화 되어 있는 경우<br>취약 - 장비 리셋 기능이 비활성화 되어 있지 않은 경우                                                                            |       |        |     |   |
| 점검 방법 | 장비 리셋 기능이 비활성화 되어 있는지 침입차단시스템에서 확인한다.                                                                                                      |       |        |     |   |
| 조치 방법 | The command line interface (CLI) 환경에서 아래와 같이 Device Reset을 disable 설정한다.<br>=> unset admin device-reset.                                   |       |        |     |   |
| 비고    |                                                                                                                                            |       |        |     |   |

#### 4.6.7. Alert & Monitoring 활성화

| 분류    | 보안기능 설정관련 진단                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | NF6-07 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽, IPS, IDS                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | 주요 침입 등 주요 관심 상황이 발생할 경우 담당자가 해당 상황이 발생함을 신속히 인지할 수 있도록 경보를 발생하거나 Mail 등을 통하여 알려야 한다.                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | 양호 - Alert & Monitoring 활성화 되어 있는 경우<br>취약 - Alert & Monitoring 활성화 되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 점검 방법 | Alert & Monitoring 활성화 되어 있는지 침입차단시스템, 침입탐지/방지시스템에서 확인한다.                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 조치 방법 | <p>[침입차단시스템]</p> <p>Properties Setup -&gt; Log and Alert 창에서 Popup Alert Command 및 Mail Alert Command 을 설정하여 담당자가 신속하게 주요 이벤트 발생을 인지할 수 있도록 설정함을 권고한다.</p> <ul style="list-style-type: none"> <li>- 로그분석기간 이후 시스템에 적합한 정책수립 후 Alert 기능 활성화함</li> <li>- E-mail, SMS의 alert 건수가 많을 시에는 Serverity를 이용한 최상위급 경고에 해당하는 alert을 먼저 사용하도록 함</li> </ul> <p>[침입탐지/방지시스템]</p> <p>시스템에서 제공하는 서비스에 대한 주요 해킹 패턴에 대해서 탐지정책을 수립할 경우 운영담당자가 신속하게 인지할 수 있도록 경보를 설정한다.</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |



#### 4.6.8. TCP/UDP Session Timeout 활성화

| 분류    | 보안기능 설정관련 진단                                                                                                                                                    | 항목 코드 | NF6-08 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | 방화벽                                                                                                                                                             |       |        |     |   |
| 설명    | stateful inspection기능을 이용하여 외부에서의 서비스 사용자가 일정시간 동안 세션의 통신이 없을 시 해당 통신에 대하여 connect kill을 하는 것으로 각 TCP/UDP등에 대하여 time out을 설정하여 불필요한 session을 정리하는 것으로 보안을 강화한다. |       |        |     |   |
| 진단 기준 | 양호 - TCP/UDP Session Timeout 활성화 되어 있는 경우<br>취약 - TCP/UDP Session Timeout 활성화 되어 있지 않은 경우                                                                       |       |        |     |   |
| 점검 방법 | TCP/UDP Session Timeout 설정이 되어 있는지 침입차단시스템에서 확인한다.                                                                                                              |       |        |     |   |
| 조치 방법 | Properties Setup -> Security Policy 창에서 서비스의 특징을 고려하여 TCP session Timeout 및 UDP session Timeout 시간을 조정한다.                                                       |       |        |     |   |
| 비고    |                                                                                                                                                                 |       |        |     |   |

#### 4.6.9. Agent Activity Check

|       |                                                                           |       |        |     |   |
|-------|---------------------------------------------------------------------------|-------|--------|-----|---|
| 분류    | 보안기능 설정관련 진단                                                              | 항목 코드 | NF6-09 | 중요도 | L |
| 대상    | IPS, IDS                                                                  |       |        |     |   |
| 설명    | 침입탐지시스템이 Console과 Agent로 구성된 경우 Agent는 활성화 되어 있어야 한다.                     |       |        |     |   |
| 진단 기준 | 양호 - 침입탐지시스템의 Agent가 활성화 되어 있는 경우<br>취약 - 침입탐지시스템의 Agent가 활성화 되어 있지 않은 경우 |       |        |     |   |
| 점검 방법 | Agent가 활성화 되어 있는지 침입차단시스템에서 확인한다.                                         |       |        |     |   |
| 조치 방법 | Agent가 비 활성화 되어 있는 경우 원인을 파악하여 제거하고 활성화 한다.                               |       |        |     |   |
| 비고    |                                                                           |       |        |     |   |

#### 4.6.10. Agent, Console 통신 암호화

| 분류    | 보안기능 설정관련 진단                                                                                                                | 항목 코드 | NF6-10 | 중요도 | L |
|-------|-----------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | IPS, IDS                                                                                                                    |       |        |     |   |
| 설명    | 침입탐지시스템이 Console과 Agent로 구성된 경우 Console과 Agent가 통신시 암호화 채널을 구성하여야 하며 관리자 원격관리 시에도 암호화 채널을 통해 통신하여 네트워크 상에서 자료의 누설을 방지해야 한다. |       |        |     |   |
| 진단 기준 | 양호 - Agent, Console 통신 암호화를 적용하고 있는 경우<br>취약 - Agent, Console 통신 암호화를 적용하고 있지 않은 경우                                         |       |        |     |   |
| 점검 방법 | Agent, Console 통신 암호화를 적용 여부를 침입차단시스템에서 확인한다.                                                                               |       |        |     |   |
| 조치 방법 | Console과 Agent 통신 및 관리자 원격관리 시 암호화 채널을 통해 통신하는 솔루션을 도입한다.                                                                   |       |        |     |   |
| 비고    |                                                                                                                             |       |        |     |   |

## 5. DBMS 취약성 점검항목 및 가이드

### 5.1. 계정관리

#### 5.1.1. 기본 계정의 패스워드, 정책 등을 변경하여 사용

| 분류                         | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드  | D1-01    | 중요도 | H |                            |  |  |  |      |          |      |          |       |                 |        |         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------|-----|---|----------------------------|--|--|--|------|----------|------|----------|-------|-----------------|--------|---------|
| 대상                         | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |        |          |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| 설명                         | <div>■ Oracle - 데이터베이스의 기본 계정(system, scott 등)의 패스워드 또는, 접근제어 정책을 변경하지 않고 사용할 경우 공격자는 알려진 정보를 이용하여 데이터베이스에 쉽게 접근할 수 있는 취약점이 존재한다.</div> <div>■ MSSQL - sa 계정 null 암호 취약점은 비인가자에 의해 sa 계정으로 데이터베이스에 침입하여 정보 삭제, 변경 등의 행위를 할 수 있는 위험이 있다.</div> <div>■ MySQL - root 계정의 패스워드가 디폴트 설정 값인 null을 사용할 경우, 시스템에 접근한 임의의 모든 사용자가 root 권한으로 접속하여 mysql의 모든 작업을 할 수 있어 mysql DB에 저장된 모든 정보가 유출 되는 등의 침해사고를 일으킬 위험이 있다. 기본 계정을 변경하지 않고 사용하는 경우 공격자에게 정보가 노출될 가능성이 있으므로 변경하여야 한다.</div>                                                                                                                                                       |        |          |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| 진단 기준                      | <div>양호 - 기본 계정의 패스워드를 변경하여 사용하는 경우</div> <div>취약 - 기본 계정의 디폴트 설정을 변경하지 않고 사용하는 경우</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |        |          |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| 점검 방법                      | <div>■ Oracle</div> <div>1. SQL*Plus에서 알려진 계정 정보(system/manager, scott/tiger 등)를 이용하여 데이터베이스에 접근 가능한지 확인함</div> <div>2. chkpassword 프로그램을 이용하여 system 계정의 패스워드를 확인하였을 경우 이를 이용하여 기본 정보를 사용하는 계정 존재 여부 확인함</div> <div>3. SQL*Plus를 통한 확인</div>                                                                                                                                                                                                                                                                                                                                                                                     |        |          |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| 조치 방법                      | <div>기본(관리자) 계정의 패스워드 및 정책 변경</div> <div>■ Oracle</div> <div>1. 불필요한 계정인 경우 계정 삭제</div> <div>SQL&gt; DROP USER username;</div> <div>2. 사용되는 계정인 경우 계정의 기본 패스워드 변경 후 사용</div> <div>SQL&gt; alter user username identified by new_passwd;</div> <div>※ 그 이외에 객체 권한 부여 및 기본 role 확인 및 변경 수행</div> <div>※ DBSNMP 파일의 접근권한 설정이 필요함</div> <div>chmod 700 snmp_rw.ora (결과값 -rwx—snmp_rw.ora)</div> <div><table><tr><th colspan="4">Oracle 설치 시 생성되는 디폴트 계정 정보</th></tr><tr><th>User</th><th>Password</th><th>User</th><th>Password</th></tr><tr><td>scott</td><td>tiger or tigger</td><td>system</td><td>manager</td></tr></table></div> |        |          |     |   | Oracle 설치 시 생성되는 디폴트 계정 정보 |  |  |  | User | Password | User | Password | scott | tiger or tigger | system | manager |
| Oracle 설치 시 생성되는 디폴트 계정 정보 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |          |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| User                       | Password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | User   | Password |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |
| scott                      | tiger or tigger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | system | manager  |     |   |                            |  |  |  |      |          |      |          |       |                 |        |         |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |        |                  |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------|------------------|
|    | dbsnmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | dbsnmp     | sys    | changeon_install |
|    | tracesvr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | trace      | outln  | outln            |
|    | ordplugins                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ordplugins | ordsys | ordsys           |
|    | ctxsys                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ctxsys     | mdsys  | mdsys            |
|    | adams                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | wood       | blake  | papr             |
|    | clark                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | clth       | jones  | steel            |
|    | lbacsys                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | lbacsys    |        |                  |
|    | <p>■ MSSQL</p> <p>sa 계정 패스워드 변경</p> <p>Alter login sa with password='new password'</p> <p>■ MySQL</p> <p>root 계정 패스워드 변경</p> <p>mysql&gt; use mysql</p> <p>mysql&gt; update user set password=password('new password') where user='root';</p> <p>mysql&gt; flush privileges; 또는,</p> <p>mysql&gt; set password for root=password('new password')</p> <p>※ 패스워드가 취약하게 설정된 경우 패스워드를 아래 기준을 준수하여 변경함</p> <p>&lt; 패스워드 관리 방법 &gt;</p> <ol style="list-style-type: none"> <li>영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정</li> </ol> <p>※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성</p> <ol style="list-style-type: none"> <li>영문 대문자(26개)</li> <li>영문 소문자(26개)</li> <li>숫자(10개)</li> <li>특수문자(32개)</li> </ol> <ol style="list-style-type: none"> <li>시스템마다 상이한 패스워드 사용</li> <li>패스워드를 기록해 놓을 경우 변형하여 기록</li> <li>가급적 자주 패스워드를 변경할 것</li> </ol> |            |        |                  |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |        |                  |

## 5.1.2. Scott 등 Demonstration 및 불필요한 계정을 제거하거나 잠금 설정 후 사용

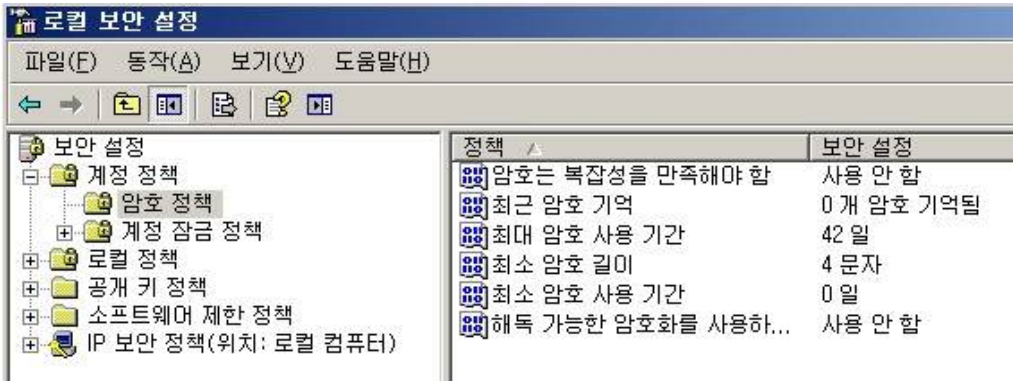
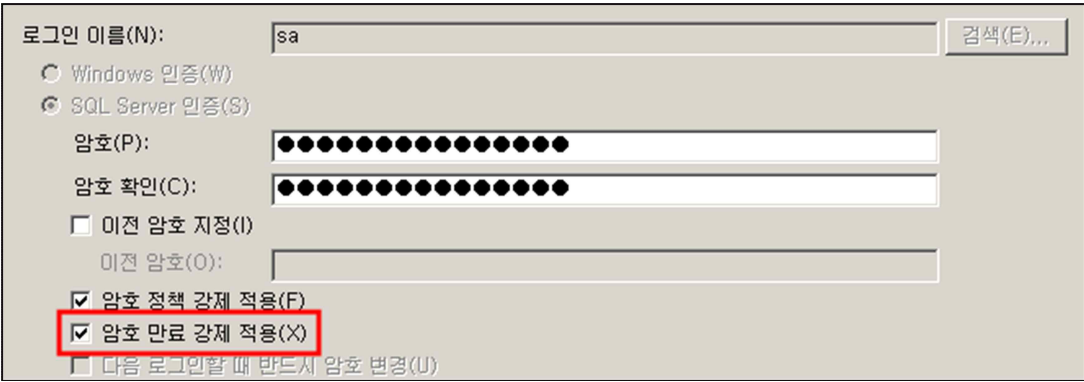
| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | D1-02 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 설명    | 데이터베이스의 계정 중 실질적으로 업무에 사용하지 않는 SCOTT, PM, ADAMS, CLARK 등의 Demonstration 계정이 삭제되지 않고 존재하면 공격자가 데이터베이스 시스템에 쉽게 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 진단 기준 | 양호 - 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 없는 경우<br>취약 - 불필요한 계정이 존재하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 점검 방법 | <p>불필요한 계정 존재유무 확인</p> <p>■ Oracle</p> <p>SQL*Plus를 통한 확인 예시</p> <pre>SQL&gt; select username from dba_users where username in ( 'SCOTT','HR','OE','PM','SH', 'COMPANY','MFG','FINANCE','ANYDATA_USER', 'ANYDSET_USER','ANYTYPE_USER','AQJAVA','AQUSER', 'AQXMLUSER','GPFD','GPLD','MMO2','XMLGEN1', 'BLAKE','ADAMS','CLARK','JONES') or username like 'QS%' or username like 'USER%' or username like '%DEMO%' or username like 'SERVICECONSUMER%'; 어떠한 사용자라도 리스트 되면 취약함</pre> <p>■ MSSQL</p> <p>비인가 사용자 계정을 점검</p> <pre>[SQL 2000] SQL&gt; select name from sysxlogins where name is not null and name &lt;&gt; 'sa' order by name  [SQL 2005] SQL&gt; select name from sys.syslogins where name is not null and name &lt;&gt; 'sa' order by name</pre> <p>■ MySQL</p> <pre>mysql&gt; use mysql; Database changed mysql&gt; select User, Password from user; +-----+-----+   User   Password   +-----+-----+   root   *3F44F330C756F7BB2855662A999C160F6AA9B68E     root   *3F44F330C756F7BB2855662A999C160F6AA9B68E   +-----+-----+</pre> |       |       |     |   |

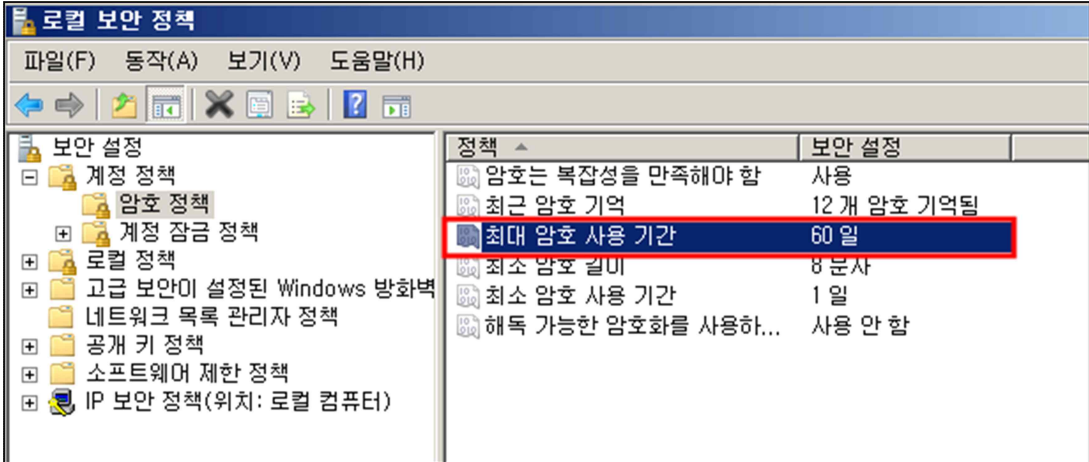
|       |                                                                                                                                                                                                                                                                                                                                |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>■ Oracle</p> <p>1. 불필요한 Demonstration 계정 및 오브젝트 삭제<br/>SQL&gt; DROP USER '삭제할 계정'</p> <p>2. 계정 잠금/만료<br/>SQL&gt; ALTER USER '잠금/만료 계정' ACCOUNT LOCK PASSWORD EXPIRE</p> <p>■ MSSQL</p> <p>불필요한 계정 삭제<br/>Exec sp_droplogin '삭제할 계정'</p> <p>■ MySQL</p> <p>불필요한 계정 삭제<br/>mysql&gt; Delete from user where user='삭제할 계정'</p> |
| 비고    |                                                                                                                                                                                                                                                                                                                                |

### 5.1.3. 패스워드의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | D1-03 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 설명    | <p>주기적인 패스워드 변경이 없을 경우 공격자는 Brute force 공격을 통하여 패스워드를 획득할 위험이 존재한다.</p> <p>■ Oracle - PASSWORD_LIFE_TIME 값은 패스워드가 만기된 이후에 사용가능한 일수에 대한 제한을 제공한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 진단 기준 | <p>양호 - 패스워드를 주기적으로 변경하고, 패스워드 정책이 적용되어 있는 경우</p> <p>취약 - 패스워드를 주기적으로 변경하지 않거나, 패스워드 정책이 없는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>1. 패스워드 사용기간 확인</p> <pre>SQL&gt; select profile,limit from dba_profiles, (select limit as def_pwd_life_tm from dba_profiles where profile='DEFAULT' and resource_name='PASSWORD_LIFE_TIME') where resource_name='PASSWORD_LIFE_TIME' and ((replace(limit,'DEFAULT',def_pwd_life_tm) in ('UNLIMITED',NULL)) or (lpad(replace(limit,'DEFAULT',def_pwd_life_tm),40,'0') )&gt; lpad('60',40,'0')));</pre> <p>2. 패스워드 복잡도 확인</p> <pre>SQL&gt; select profile,limit from dba_profiles where profile='DEFAULT' and resource_name='PASSWORD_VERIFY_FUNCTION';</pre> <p>■ MSSQL</p> <p>윈도우 로컬보안정책 확인</p> <p>[시작]&gt; [설정]&gt; [제어판]&gt; [관리도구]&gt; [로컬 보안 정책]&gt; [계정 정책]&gt; [암호 정책]</p> |       |       |     |   |

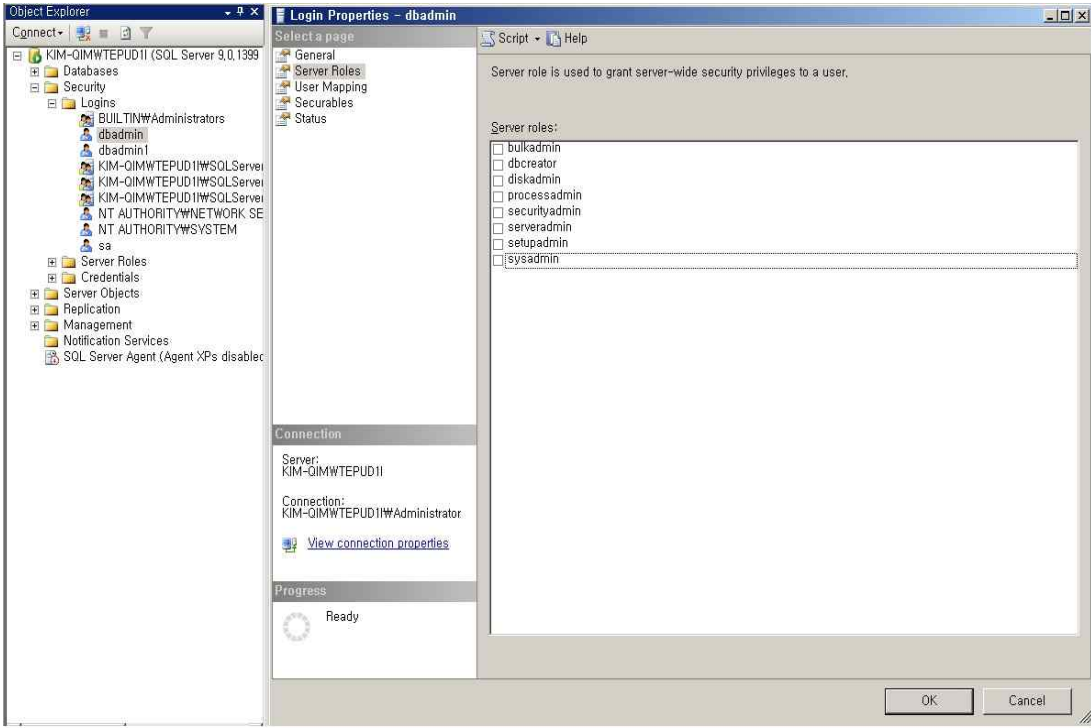


|                    |  <p><b>로컬 보안 설정</b></p> <p>파일(F) 동작(A) 보기(V) 도움말(H)</p> <p>← → [폴더 아이콘] [목록 아이콘] [설정 아이콘] [도움말 아이콘]</p> <p>보안 설정</p> <ul style="list-style-type: none"> <li>계정 정책 <ul style="list-style-type: none"> <li>암호 정책</li> <li>계정 잠금 정책</li> </ul> </li> <li>로컬 정책</li> <li>공개 키 정책</li> <li>소프트웨어 제한 정책</li> <li>IP 보안 정책(위치: 로컬 컴퓨터)</li> </ul> <table border="1"> <thead> <tr> <th>정책</th> <th>보안 설정</th> </tr> </thead> <tbody> <tr> <td>암호는 복잡성을 만족해야 함</td> <td>사용 안 함</td> </tr> <tr> <td>최근 암호 기억</td> <td>0 개 암호 기억됨</td> </tr> <tr> <td>최대 암호 사용 기간</td> <td>42 일</td> </tr> <tr> <td>최소 암호 길이</td> <td>4 문자</td> </tr> <tr> <td>최소 암호 사용 기간</td> <td>0 일</td> </tr> <tr> <td>해독 가능한 암호화를 사용하...</td> <td>사용 안 함</td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 정책 | 보안 설정 | 암호는 복잡성을 만족해야 함 | 사용 안 함 | 최근 암호 기억 | 0 개 암호 기억됨 | 최대 암호 사용 기간 | 42 일 | 최소 암호 길이 | 4 문자 | 최소 암호 사용 기간 | 0 일 | 해독 가능한 암호화를 사용하... | 사용 안 함 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-------|-----------------|--------|----------|------------|-------------|------|----------|------|-------------|-----|--------------------|--------|
| 정책                 | 보안 설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 암호는 복잡성을 만족해야 함    | 사용 안 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최근 암호 기억           | 0 개 암호 기억됨                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최대 암호 사용 기간        | 42 일                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최소 암호 길이           | 4 문자                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최소 암호 사용 기간        | 0 일                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 해독 가능한 암호화를 사용하... | 사용 안 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 조치 방법              | <p>■ Oracle</p> <ol style="list-style-type: none"> <li>PASSWORD_LIFE_TIME 프로파일 파라미터 변경<br/> SCREATE PROFILE grace_5 LIMIT<br/> FAILED_LOGIN_ATTEMPTS 3 (패스워드 실패 3번까지만 가능)<br/> PASSWORD_LIFE_TIME 30 (30일 동안만 패스워드 사용 가능)<br/> PASSWORD_REUSE_TIME 30 (사용한 패스워드 30일 후부터 재사용 가능)<br/> PASSWORD_VERIFY_FUNCTION verify_function<br/> PASSWORD_GRACE_TIME 5 ; (life time이 끝나고 5일 동안 메시지를 보여줌)</li> </ol> <p>■ MSSQL</p> <ol style="list-style-type: none"> <li>패스워드 변경 주기가 60일 이내로 설정되지 않은 경우 패스워드 변경 주기 설정<br/> MSSQL에서 ‘암호 만료 강제 적용’을 체크함으로써 주기적으로 변경이 가능하며, 변경기간은 OS의 ‘암호정책’에서 적용 받으므로 ‘암호 정책 &gt; 최대 암호 사용 기간’ 설정도 같이 변경해야 함</li> <li>암호 만료 강제 적용<br/> [보안]&gt; [로그인]&gt; [각 로그인 계정]&gt; [속성]&gt; 암호 만료 강제 적용: 설정(체크) 확인</li> </ol>  <p>로그인 이름(N): sa [검색(E)...]</p> <p><input type="radio"/> Windows 인증(W)<br/> <input checked="" type="radio"/> SQL Server 인증(S)</p> <p>암호(P): [ masked ]</p> <p>암호 확인(C): [ masked ]</p> <p><input type="checkbox"/> 이전 암호 지정(I)<br/> 이전 암호(O): [ ]</p> <p><input checked="" type="checkbox"/> 암호 정책 강제 적용(F)<br/> <input checked="" type="checkbox"/> 암호 만료 강제 적용(X)<br/> <input type="checkbox"/> 다음 로그인할 때 반드시 암호 변경(U)</p> <ol style="list-style-type: none"> <li>OS의 암호 정책 설정<br/> [관리도구]&gt; [로컬 보안 정책]&gt; [보안 설정]&gt; [계정 정책]&gt; [암호 정책]에서<br/> ‘최대 암호 사용 기간 : ’60일’ 설정</li> </ol> |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |

|                    |  <p>로컬 보안 정책</p> <p>파일(F) 동작(A) 보기(V) 도움말(H)</p> <p>보안 설정</p> <ul style="list-style-type: none"> <li>계정 정책</li> <li>암호 정책 <ul style="list-style-type: none"> <li>계정 잠금 정책</li> </ul> </li> <li>로컬 정책</li> <li>고급 보안이 설정된 Windows 방화벽</li> <li>네트워크 목록 관리자 정책</li> <li>공개 키 정책</li> <li>소프트웨어 제한 정책</li> <li>IP 보안 정책(위치: 로컬 컴퓨터)</li> </ul> <table border="1"> <thead> <tr> <th>정책</th> <th>보안 설정</th> </tr> </thead> <tbody> <tr> <td>암호는 복잡성을 만족해야 함</td> <td>사용</td> </tr> <tr> <td>최근 암호 기억</td> <td>12 개 암호 기억됨</td> </tr> <tr> <td><b>최대 암호 사용 기간</b></td> <td><b>60 일</b></td> </tr> <tr> <td>최소 암호 길이</td> <td>8 문자</td> </tr> <tr> <td>최소 암호 사용 기간</td> <td>1 일</td> </tr> <tr> <td>해독 가능한 암호화를 사용하...</td> <td>사용 안 함</td> </tr> </tbody> </table> <p>■ MySQL</p> <ol style="list-style-type: none"> <li>패스워드 설정 규칙 적용<br/>패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공</li> <li>패스워드 관리 적용<br/>패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(One-Way Encryption)</li> <li>패스워드 변경기능 구현<br/>사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공</li> </ol> <p>패스워드 설정은 다음과 같은 방법으로 가능</p> <pre>mysql&gt; use mysql mysql&gt; update user set password=password('new password') where user='user name'; mysql&gt; flush privileges; 또는, mysql&gt; set password for 'user name'@'%'=password('new password') mysql&gt; flush privileges;</pre> | 정책 | 보안 설정 | 암호는 복잡성을 만족해야 함 | 사용 | 최근 암호 기억 | 12 개 암호 기억됨 | <b>최대 암호 사용 기간</b> | <b>60 일</b> | 최소 암호 길이 | 8 문자 | 최소 암호 사용 기간 | 1 일 | 해독 가능한 암호화를 사용하... | 사용 안 함 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-------|-----------------|----|----------|-------------|--------------------|-------------|----------|------|-------------|-----|--------------------|--------|
| 정책                 | 보안 설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 암호는 복잡성을 만족해야 함    | 사용                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 최근 암호 기억           | 12 개 암호 기억됨                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| <b>최대 암호 사용 기간</b> | <b>60 일</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 최소 암호 길이           | 8 문자                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 최소 암호 사용 기간        | 1 일                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 해독 가능한 암호화를 사용하... | 사용 안 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |
| 비고                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |       |                 |    |          |             |                    |             |          |      |             |     |                    |        |

#### 5.1.4. 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용

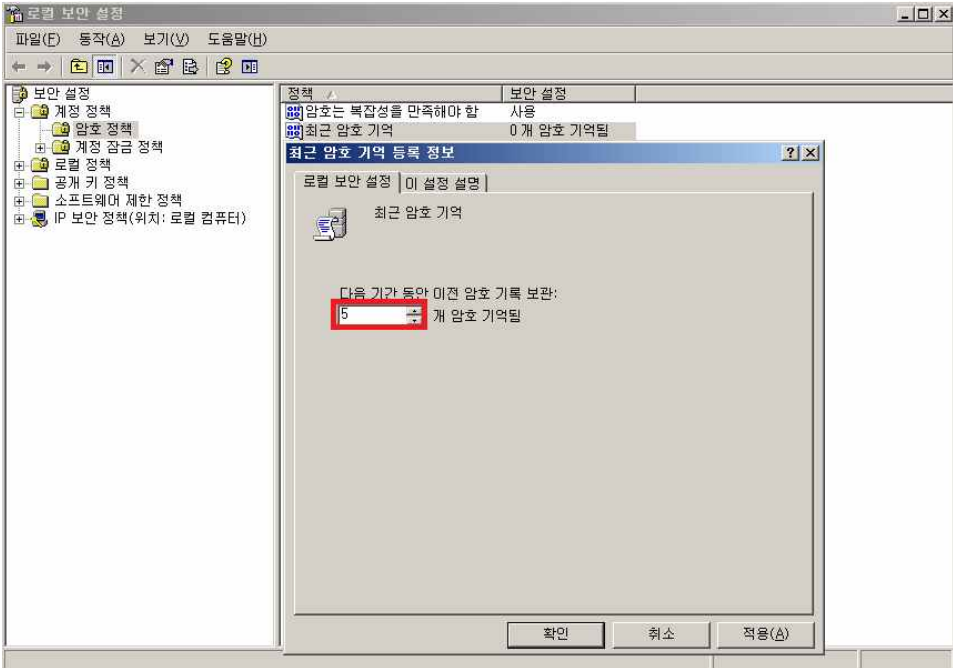
| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | D1-04 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | DBA에게만 허용되어야 하는 SYSDBA 권한이 응용프로그램 계정 또는 일반 사용자 계정에 허용되어 있는 경우 공격자는 이를 이용하여 쉽게 DBA 권한으로 데이터베이스에 접근 가능하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 진단 기준 | <p>양호 - 계정별 관리자 권한이 차등 부여 되어 있는 경우</p> <p>취약 - 일반 사용자 계정에 불필요하게 관리자 권한이 부여되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>1. SYSDBA 권한 점검</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>SQL&gt; SELECT USERNAME FROM V\$PWFILERS WHERE USERNAME NOT IN (SELECT GRANTEE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA') and USERNAME !='INTERNAL' and sysdba='TRUE'; 어떠한 계정이라도 나오면 취약함</pre> </div> <p>2. Admin에 부적합 계정 존재 여부 점검</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>SQL&gt; select grantee,privilege from dba_sys_privs where grantee not in ( 'SYS', 'SYSTEM', 'AQ_ADMINISTRATOR_ROLE' , 'DBA' , 'MDSYS' , 'LBACSYS', 'SCHEDULER_ADMIN','WMSYS') and admin_option='YES' and grantee not in (select grantee from dba_role_privs where granted_role='DBA');</pre> <p>어떠한 계정 결과라도 나오면 취약함</p> </div> <p>■ MSSQL</p> <p>SYSADMIN(System Administrators)에 인증되지 않은 사용자가 설정되어 있는지 구성원을 확인</p> <p>1. SQL 2000</p> <p>[가체탐색기]&gt; [보안]&gt; [서버 역할]&gt; [System Administrators]&gt; [등록정보]&gt; [일반]에서 구성원 확인</p> <p>2. SQL 2005</p> |       |       |     |   |

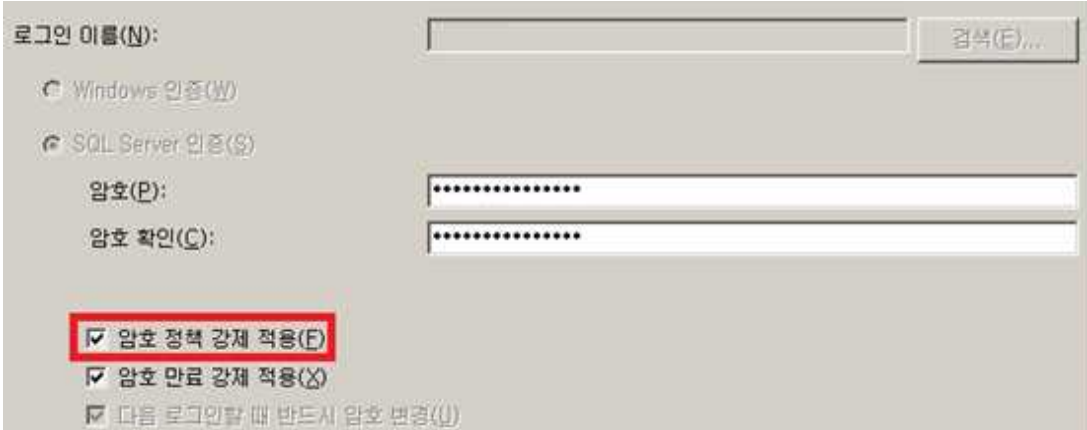
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |  <p>■ MySQL</p> <pre>mysql&gt; SHOW GRANTS FOR &lt;USERID&gt;;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 조치 방법 | <p>계정별 관리자 권한 차등 부여, 삭제</p> <p>■ Oracle</p> <ol style="list-style-type: none"> <li>1. 불필요하게 시스템 권한을 부여한 계정의 권한 변경</li> <li>2. 반드시 필요한 경우 필요한 테이블에만 권한 한정</li> <li>3. 인가된 사용자는 관리자의 권한에 role을 grant 한 후, 시스템 권한을 grant 하고, role을 인가된 사용자에게 grant를 함</li> </ol> <p>■ MSSQL</p> <ol style="list-style-type: none"> <li>1. sysadmin 서버 역할의 계정 목록을 확인 후 해당 서버 역할에 불필요한 계정이 있는 경우 서버 역할에서 삭제<br/>sysadmin 서버 역할에서 불필요한 계정 삭제<br/>Exec sp_droprolemember 'user_name', 'sysadmin' <p>(예) Exec sp_dropsvrolemember 'user01', 'sysadmin'</p> <p>(user01 계정을 sysadmin 서버 역할에서 삭제)</p> </li> <li>2. [개체탐색기]&gt; [보안]&gt; [서버 역할]&gt; [System Administrators]&gt; [등록정보]&gt; [일반] 에서 인증되지 않은 사용자는 제거</li> </ol> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>■ MySQL</p> <p>1. mysql.user 테이블에 적용된 권한은 모든 데이터베이스에 적용되므로 host, user, password를 제외한 나머지 권한은 허용하지 않음('N')으로 설정</p> <ul style="list-style-type: none"> <li>• 사용자 등록</li> </ul> <pre>mysql&gt; insert into mysql.user (host, name, password) values('%', 'user name', password ('password')) ※ 디폴트로 모든 권한 'N' 설정</pre> <ul style="list-style-type: none"> <li>• 권한 변경</li> </ul> <pre>mysql&gt; update mysql.user set &lt;권한&gt;='N' where user='user name'</pre> <p>2. 각 사용자는 접근하고자 하는 DB를 mysql.db에 등록 후 접근 권한을 부여하여 사용</p> <ul style="list-style-type: none"> <li>• DB등록 시 권한 부여</li> </ul> <pre>mysql&gt; insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y')</pre> <pre>mysql&gt; flush privileges</pre> <ul style="list-style-type: none"> <li>• DB 권한 업데이트</li> </ul> <pre>mysql&gt; update mysql.db set &lt;권한&gt;='Y' where db=&lt;DB name&gt; and user='user name'</pre> <pre>mysql&gt; flush privileges</pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### 5.1.5. 비밀번호 재사용에 대한 제약 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | D1-05 | 중요도 | M |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 설명    | <p>■ Oracle - PASSWORD_REUSE_TIME 값은 비밀번호가 재사용될 수 있기 전에 일수를 명시하는 파라미터이며, PASSWORD_REUSE_MAX는 횟수 설정 파라미터이다. 파라미터 미설정 시 비밀번호 노출 가능성이 증가한다.</p> <p>■ MSSQL - 비밀번호 재사용에 대한 제약 미 설정 시 비밀번호 노출 가능성이 증가한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | <p>양호 - 비밀번호 재사용에 대한 설정이 적용된 경우<br/>(Oracle - PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정)</p> <p>취약 - 비밀번호 재사용에 대한 설정이 적용되지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 점검 방법 | <p>■ Oracle<br/>SQL*Plus를 통한 확인</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>- Check for both reuse max and reuse time not set:<br/>SQL&gt; select profile from DBA_PROFILES<br/>where (resource_name='PASSWORD_REUSE_MAX'<br/>and limit in ('UNLIMITED','NULL'))<br/>or profile in<br/>(select profile from DBA_PROFILES<br/>where resource_name='PASSWORD_REUSE_TIME')<br/>and limit in ('UNLIMITED','NULL');</p> <p>- Check for reuse max with value that is less than allowed minimum<br/>SQL&gt; select profile from DBA_PROFILES<br/>where resource_name='PASSWORD_REUSE_MAX'<br/>and limit not in ('UNLIMITED','NULL')<br/>and limit &lt; '10';</p> <p>- Check for reuse time that is less than allowed minimum<br/>SQL&gt; select profile from DBA_PROFILES<br/>where resource_name='PASSWORD_REUSE_TIME'<br/>and limit not in ('UNLIMITED','NULL')<br/><b>and limit &lt; '365';</b></p> </div> <p>■ MSSQL<br/>윈도우 로컬보안정책 확인<br/>[시작]&gt; [설정]&gt; [제어판]&gt; [관리 도구]&gt; [로컬 보안 정책]&gt; [계정 정책]&gt; [암호 정책]에서 최근 암호 기억 확인</p> |       |       |     |   |

|                    |  <p>The screenshot shows the 'Local Security Policy' window. On the left, the tree view is expanded to 'Security Settings' &gt; 'Account Policies' &gt; 'Password Policy'. The right pane shows the 'Policy' list with the following settings:</p> <table border="1"> <thead> <tr> <th>정책</th> <th>보안 설정</th> </tr> </thead> <tbody> <tr> <td>암호는 복잡성을 만족해야 함</td> <td>사용 안 함</td> </tr> <tr> <td>최근 암호 기억</td> <td>0 개 암호 기억됨</td> </tr> <tr> <td>최대 암호 사용 기간</td> <td>42 일</td> </tr> <tr> <td>최소 암호 길이</td> <td>4 문자</td> </tr> <tr> <td>최소 암호 사용 기간</td> <td>0 일</td> </tr> <tr> <td>해독 가능한 암호화를 사용하...</td> <td>사용 안 함</td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                | 정책 | 보안 설정 | 암호는 복잡성을 만족해야 함 | 사용 안 함 | 최근 암호 기억 | 0 개 암호 기억됨 | 최대 암호 사용 기간 | 42 일 | 최소 암호 길이 | 4 문자 | 최소 암호 사용 기간 | 0 일 | 해독 가능한 암호화를 사용하... | 사용 안 함 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-------|-----------------|--------|----------|------------|-------------|------|----------|------|-------------|-----|--------------------|--------|
| 정책                 | 보안 설정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 암호는 복잡성을 만족해야 함    | 사용 안 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최근 암호 기억           | 0 개 암호 기억됨                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최대 암호 사용 기간        | 42 일                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최소 암호 길이           | 4 문자                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 최소 암호 사용 기간        | 0 일                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| 해독 가능한 암호화를 사용하... | 사용 안 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |
| <p>조치 방법</p>       | <p>■ Oracle</p> <p>PASSWORD_REUSE_TIME 및 프로파일 파라미터 설정</p> <pre>SQL&gt; alter profile default limit password_reuse_time 365 password_reuse_max 10;  SQL&gt; alter profile [profile name] limit password_reuse_time default password_reuse_max default;</pre> <p>■ MSSQL</p> <p>1. 윈도우 로컬보안정책 변경</p> <p>[시작]&gt; [설정]&gt; [제어판]&gt; [관리 도구]&gt; [로컬 보안 정책]&gt; [계정 정책]&gt; [암호 정책]에서 최근암호 기억 - 권장 값 : 5</p>  <p>The screenshot shows the 'Local Security Policy' window with the 'Account Policies' &gt; 'Password Policy' path selected. The 'Recent Passwords Remembered' dialog box is open, showing the 'Local Security Policy   Policy Settings' tab. The 'Recent Passwords Remembered' section has a value of '5' entered in the text box, which is highlighted with a red rectangle. The dialog box also includes a description: '다음 기간 동안 이전 암호 기록 보관: 5 개 암호 기억됨' and buttons for '확인', '취소', and '적용(A)'.</p> |    |       |                 |        |          |            |             |      |          |      |             |     |                    |        |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>2. 패스워드 복잡도를 강제하는 패스워드 검증 함수를 생성 또는 사용해야 함</p>  <p>The screenshot shows the 'Local Security Policy' window for Windows. Under the 'Account Policies' tab, the 'Password Policy' is configured. The 'Enforce password complexity' checkbox is checked and highlighted with a red box. Other options include 'Enforce password history' (checked), 'Maximum password age' (set to 42 days), and 'Minimum password age' (set to 1 day). The 'Require password change at next logon' checkbox is also checked.</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



### 5.1.6. DB 사용자 계정을 개별적으로 부여하여 사용

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | D1-06 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |
| 설명    | 데이터베이스의 사용자 계정이 사용자, 프로세스와 응용 프로그램 등에 동일하게 사용하게 될 경우 침해사고 발생 시 책임 추적에 영향을 주며, 계정별 권한 부여가 불가능해지고 사용하지 않는 계정을 이용한 비인가 사용자 접속이 가능하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 진단 기준 | 양호 - 사용자별 계정을 사용하고 있는 경우<br>취약 - 공용 계정을 사용하고 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 점검 방법 | <p>■ Oracle<br/>사용하지 않거나 모르는 계정 확인<br/>SQL&gt; select username from dba_users order by username;</p> <p>■ MSSQL<br/>사용하지 않거나 모르는 계정 확인<br/>SQL&gt; select name from sys.syslogins where name is not null order by name</p> <p>■ MySQL<br/>사용하지 않거나 모르는 계정 확인<br/>mysql&gt; select User, Password from user;</p>                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 조치 방법 | <p>■ Oracle<br/>1. 공통으로 사용하는 계정 삭제<br/>SQL&gt; DROP USER username<br/>2. 각 응용에 적합한 계정 생성<br/>SQL&gt; Create user username identified by passwd<br/>3. 권한 부여<br/>SQL&gt; grant connect, resource to username</p> <p>■ MSSQL<br/>사용자별, 응용프로그램별 계정 생성<br/>CREATE login '생성 계정' WITH password = '패스워드'<br/>CREATE user '생성 계정' FOR login '생성 계정' WITH default_schema ='생성 계정' ;<br/>ALTER USER '생성 계정' WITH DEFAULT_SCHEMA = '생성 계정'<br/>EXEC sp_adduser '생성 계정', '생성 계정', 'db_owner'<br/>EXEC sp_adduser '생성 계정', '생성 계정', '생성 계정'<br/>EXEC sp_grantdbaccess '생성 계정','생성 계정'</p> <p>■ MySQL<br/>사용자별, 응용프로그램별 계정 생성, 권한 설정<br/>mysql&gt; insert into user('localhost','user', 'password') values('localhost', '생성 계정', 'password('패스워드'));</p> |       |       |     |   |

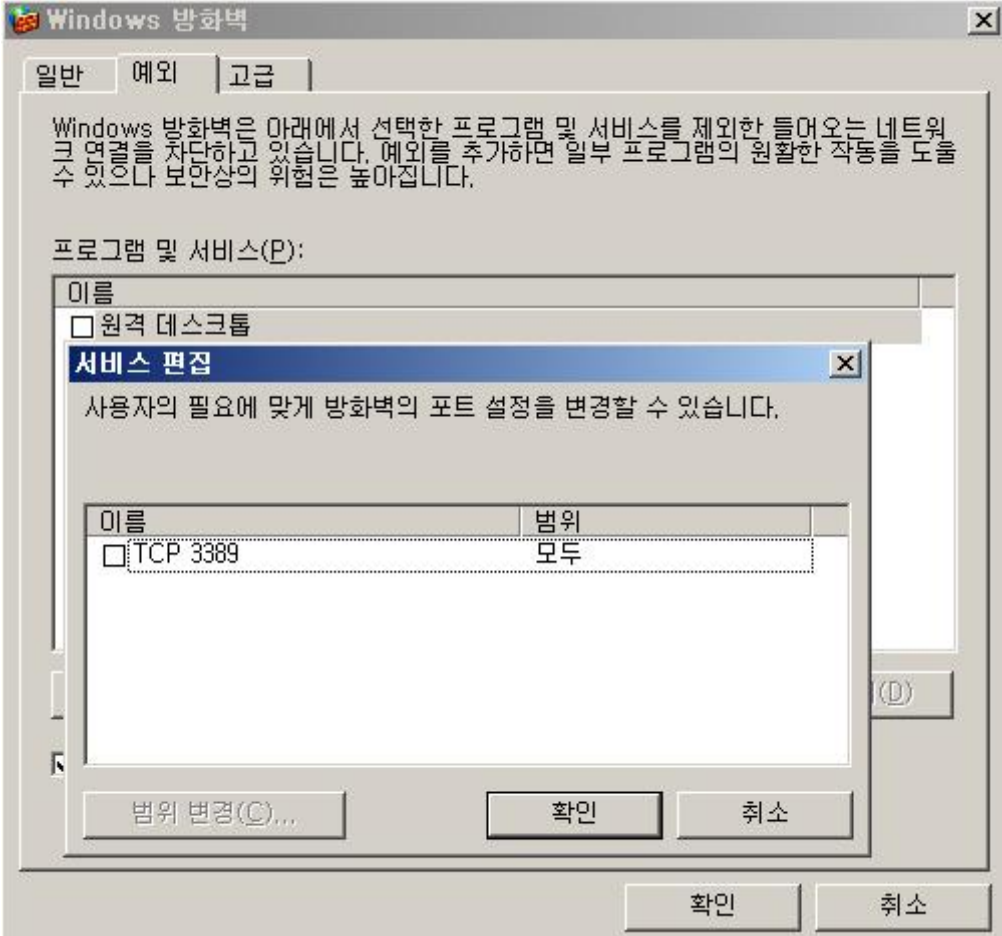
|    |                                                                                                                                                                                             |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <pre>mysql&gt; insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y') mysql&gt; flush privileges</pre> |
| 비고 |                                                                                                                                                                                             |

### 5.1.7. Guest 계정의 관리

| 분류    | 계정관리                                                                                                                                                                                | 항목 코드 | D1-07 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                               |       |       |     |   |
| 설명    | Guest계정은 특별한 로그인 계정으로 이 계정을 데이터베이스에 지정함으로써 SQL 서버의 정상 사용자 모두가 데이터베이스에 접근 가능하다.                                                                                                      |       |       |     |   |
| 진단 기준 | 양호 - Guest 계정이 존재하지 않을 경우<br>취약 - Guest 계정이 존재할 경우                                                                                                                                  |       |       |     |   |
| 점검 방법 | 해당 데이터베이스상에서 Guest 계정의 삭제 또는 잠금이 여부를 확인<br><br>■ MSSQL<br>[개체탐색기]> [해당 데이터베이스]> [사용자]에서 Guest 계정이 잠겨있는지 점검                                                                          |       |       |     |   |
| 조치 방법 | master와 tempdb 데이터베이스의 Guest 계정은 삭제할 수 없으므로, 최소한의 권한을 부여하며, 그 외 데이터베이스 내의 Guest 계정은 삭제를 권장<br><br>■ MSSQL<br>[개체탐색기]> [해당 데이터베이스]> [사용자] 에서 Guest 계정을 선택한 후 우측버튼을 클릭하여 Guest 계정을 삭제 |       |       |     |   |
| 비고    |                                                                                                                                                                                     |       |       |     |   |

## 5.2. 권한관리

### 5.2.1. 원격에서 DB 서버로의 접속 제한

| 분류    | 권한관리                                                                                                                                                                                                                                                                       | 항목 코드 | D2-01 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | OS, Oracle, MySQL                                                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | <p>허용되지 않은 IP에서 원격으로 DB에 접속이 허용되어 있는 경우 공격자에 의해 네트워크 서비스 스캐닝을 통한 DB 사용 여부가 확인되어 공격 대상이 될 수 있으며, DB 내의 데이터 유출이 가능하다.</p> <p>■ Oracle - REMOTE_OS_AUTHENT 값이 TRUE로 설정되어 있으면 안전하지 않은 연결을 통한 원격지의 OS의 인증을 허용함. 이는 원격지 OS의 사용자인 것처럼 속이는 공격자를 허용할 수 있으며, 패스워드 없이 DB 접근을 허용함.</p> |       |       |     |   |
| 진단 기준 | <p>양호 - 허용된 IP 및 포트에 대한 접근 통제가 되어 있는 경우</p> <p>취약 - IP에 대해 접근 통제가 이루어지지 않는 경우</p>                                                                                                                                                                                          |       |       |     |   |
| 점검 방법 | <p>■ OS</p> <p>[시작]&gt; [제어판]&gt; [Windows 방화벽]&gt; [예외]&gt; [편집] 에서 특정 IP에서만 접속 가능하도록 설정되어 있는지 확인</p>                                                                                 |       |       |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>■ OS</p> <p>특정 IP에서만 접속 가능하도록 방화벽 등이 설정되어 있는지 확인</p> <p>시작&gt; 제어판&gt; 보안 센터&gt; windows 방화벽 설정</p> <ul style="list-style-type: none"> <li>• 예외 tab -&gt; 포트추가 -&gt; 1433 -&gt; TCP 추가 -&gt; 범위 변경</li> <li>• 예외 tab -&gt; 포트추가 -&gt; 135 -&gt; TCP 추가 -&gt; 범위 변경</li> <li>• 예외 tab -&gt; 포트추가 -&gt; 1434 -&gt; UDP 추가 -&gt; 범위 변경</li> </ul> <p>■ Oracle</p> <p>1. 원격 OS 인증 방식이 불필요한 경우, SYS 계정으로 접속하여 'REMOTE_OS_AUTHENT=FALSE'로 설정</p> <ul style="list-style-type: none"> <li>• spfile 사용하는 경우 아래와 같이 설정</li> </ul> <p>SQL&gt; ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=spfile</p> <ul style="list-style-type: none"> <li>• pfile 사용하는 경우 init&lt;SID&gt;.ora 파일 안에 아래와 같이 설정</li> </ul> <p>SQL&gt; ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE</p> <p>2. 원격 OS 인증 방식이 필요한 경우</p> <ul style="list-style-type: none"> <li>• 방화벽을 통한 원격 접근 IP 제한</li> <li>• NAT(Network Address Translation)를 사용하여 비공인 IP 부여 후 외부 접근 제한</li> </ul> <p>■ MySQL</p> <p>mysql.user 테이블과 mysql.db 테이블을 조회하여 host가 “%”인 필드 삭제하고 접속 IP를 지정하여 등록</p> <p>mysql&gt; delete from user where host='%';</p> <p>mysql&gt; delete from db where host='%';</p> |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## 5.2.2. DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | D2-02 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 설명    | DBA만 접근 가능해야 할 테이블을 잘못 설정할 경우 비인가 사용자가 시스템의 주요 정보를 획득하거나, 주요 데이터베이스 설정 변경이 가능하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 진단 기준 | <p>양호 - DBA만 접근 가능한 테이블에 일반 사용자 접근이 불가능 할 경우</p> <p>취약 - DBA만 접근 가능한 테이블에 일반 사용자 접근이 가능한 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>DBA만 접근 가능한 테이블의 권한 확인</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>SQL&gt; select grantee, privilege, owner, table_name from dba_tab_privs where (owner='SYS' or table_name like 'DBA_%') and privilege &lt;&gt; 'EXECUTE' and grantee not in ('PUBLIC','AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'AURORA\$JIS\$UTILITY\$', 'OSE\$HTTP\$ADMIN', 'TRACESVR', 'CTXSYS', 'DBA', 'DELETE_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE', 'EXP_FULL_DATABASE', 'GATHER_SYSTEM_STATISTICS', 'HS_ADMIN_ROLE', 'IMP_FULL_DATABASE', 'LOGSTDBY_ADMINISTRATOR', 'MDSYS','ODM', 'OEM_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN','RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE', 'SNMPAGENT', 'SYSTEM', 'WKSYS','WKUSER', 'WMSYS', 'WM_ADMIN_ROLE', 'XDB', 'LBACSYS', 'PERFSTAT', 'XDBADMIN') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee; (어떤 계정이나 role이 나타나지 않으면 양호)</pre> </div> <p>■ MySQL</p> <p>User 테이블에 대한 접근 권한(select_priv)이 존재하는 사용자 점검</p> <pre>mysql&gt; use mysql mysql&gt; select user, Select_priv from user;</pre> |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>불필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우</p> <pre>SQL&gt; REVOKE 권한 on 객체 FROM User</pre> <p>■ MSSQL</p> <p>1. System tables 접근 권한이 Public, Guest 또는 비 인가된 사용자에게 부여된 경우 접근 권한을 Public, Guest, 비인가된 사용자로부터 권한 제거</p> <pre>Use database name Revoke &lt;권한&gt; on &lt;object&gt; from [user name][[public]][[guest]]</pre> <p>2. 시스템 테이블에 접근하기 위해서는 stored procedure 또는, information_schema views를 통해 접근해야 함</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                              |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>3. 시스템 테이블에 접근 가능한 stored procedure는 사용이 제한되어야 함</p> <p>■ MySQL</p> <p>1. 일반 사용자로부터 mysql.user 테이블 모든 접근 권한 제거<br/>mysql&gt; revoke all on mysql.user from '[user name]@[hosts]';<br/>mysql&gt; flush privileges</p> <p>2. 일반 사용자로부터 mysql.user 테이블 접근 권한 제거<br/>mysql&gt; revoke [권한] on mysql.user from [user name];<br/>mysql&gt; flush privileges</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                              |

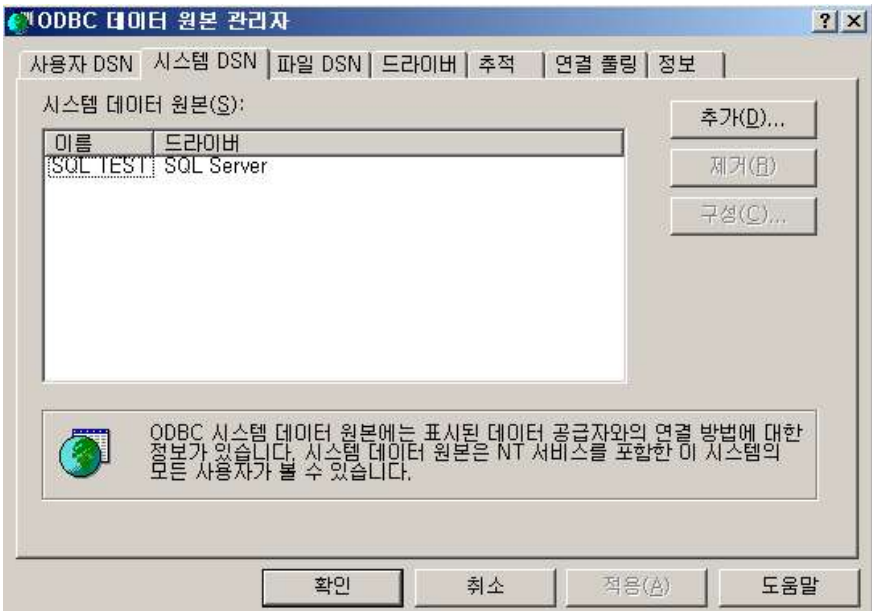
### 5.2.3. Listener의 패스워드 설정 및 디폴트 포트 변경

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | D2-03 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 설명    | 리스너의 패스워드가 설정되지 않을 경우 인가되지 않은 사용자가 데이터베이스에 직접 접속할 수 있는 취약점 존재한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 진단 기준 | 양호 - Listener의 패스워드가 설정되어 있는 경우<br>취약 - Listener의 패스워드가 설정되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 점검 방법 | <div> <div> <div>■ Oracle</div> <div>1. Listener 패스워드 설정 여부 점검</div> <div> <pre># cat \$ORACLE_HOME/network/admin/listener.ora #-----ADDED BY TNSLSNR 24-OCT-2005 17:02:28----- PASSWORDS_LISTENER_ODSSDB01 = 75CD180DE6C75466 #-----</pre> </div> </div> <div>2. Listener에 설정된 포트 정보를 확인</div> <div> <pre># cat \$ORACLE_HOME/network/admin/listener.ora LISTENER =   (DESCRIPTION_LIST =     (DESCRIPTION =       (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC))       (ADDRESS = (PROTOCOL = TCP)(HOST = localhost.localdomain)(PORT = 1521))     )   )</pre> </div> </div>                                                |       |       |     |   |
| 조치 방법 | <div> <div> <div>■ Oracle</div> <div>1. Listener 파일의 패스워드를 입력</div> <div> <p>패스워드를 암호화하여 리스너 매개변수 파일에 저장</p> <pre># ./\$ORACLE_HOME/bin/lsnrctl LSNRCTL&gt; change_password LSNRCTL&gt; save_config</pre> <p>-listener.ora 파일 내용-</p> <pre>#-----ADDED BY TNSLSNR 24-OCT-2005 17:02:28----- PASSWORDS_LISTENER_ODSSDB01 = 75CD180DE6C75466</pre> <pre>LSNRCTL&gt; services Connecting to (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521)) TNS-01169: The listener has not recognized the password</pre> <p>패스워드 입력 방법</p> <pre>LSNRCTL&gt; set password mypassword The command completed successfully</pre> </div> </div> </div> |       |       |     |   |



|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>2. Listener에 설정된 Default 포트를 변경</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>① Listener.ora 파일의 port 변경<br/> # cat \$ORACLE_HOME/network/admin/listener.ora<br/> LISTENER =<br/> (DESCRIPTION_LIST =<br/> (DESCRIPTION =<br/> (AADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC))<br/> (AADDRESS = (PROTOCOL = TCP)(HOST = localhost.localdomain)(PORT = 1521))<br/> )<br/> )</p> <p>② spfile의 Listener 포트 변경<br/> SQL&gt;alter system set local_listener =<br/> “(ADDRESS = (PROTOCOL=tcp)(HOST=hostname)(PORT=1522))”;<br/> System altered.<br/> SQL&gt;alter system register;<br/> <b>System altered.</b></p> </div> |
| <p><b>비고</b></p> | <p>■ Oracle기본값<br/> 오라클 8i, 9i: 리스너 Security 옵션 OFF<br/> 오라클 10g, 11g: Local OS authentication (로컬 운영체제의 계정만이 리스너 관리 가능, 11g에서는 리스너를 실행한 로컬 운영체제의 계정만이 리스너를 종료할 수 있음)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

#### 5.2.4. 불필요한 ODBC/OLE DB 데이터 소스와 드라이브 제거

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | D2-04 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Windows OS                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |
| 설명    | 애플리케이션에 따라 샘플 데이터베이스를 위해서 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이브를 설치하여 사용하는 경우 임의의 명령어 실행, 임의의 파일 수정, 시스템 관리자 권한 획득이 가능하다.                                                                                                                                                                                                                                                                                |       |       |     |   |
| 진단 기준 | 양호 - 불필요한 ODBC/OLEDB가 설치되지 않은 경우<br>취약 - 불필요한 ODBC/OLEDB가 설치된 경우                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <p>■ Windows NT<br/>[시작]&gt; [설정]&gt; [제어판]&gt; [데이터 원본(ODBC)]&gt; [시스템 DSN] 에서 확인</p> <p>■ Windows 2000, 2003<br/>[시작]&gt; [설정]&gt; [제어판]&gt; [관리도구]&gt; [데이터 원본 (ODBC)]&gt; [시스템DSN]&gt; 해당 드라이브에서 확인</p>                                                                                                                                                                                                        |       |       |     |   |
| 조치 방법 | <p>■ Windows NT<br/>1. 사용하지 않는 불필요한 ODBC 데이터 소스 제거<br/>[시작]&gt; [설정]&gt; [제어판]&gt; [데이터 원본(ODBC)]&gt; [시스템 DSN]<br/>2. 사용하지 않는 데이터 소스 제거</p> <p>■ Windows 2000, 2003<br/>1. 사용하지 않는 불필요한 ODBC 데이터 소스 제거<br/>[시작]&gt; [설정]&gt; [제어판]&gt; [관리도구]&gt; [데이터 원본 (ODBC)]&gt; [시스템DSN]&gt; 해당 드라이브에서 클릭<br/>2. 사용하지 않는 데이터 소스 제거</p>  |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |

## 5.2.5. 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 설정

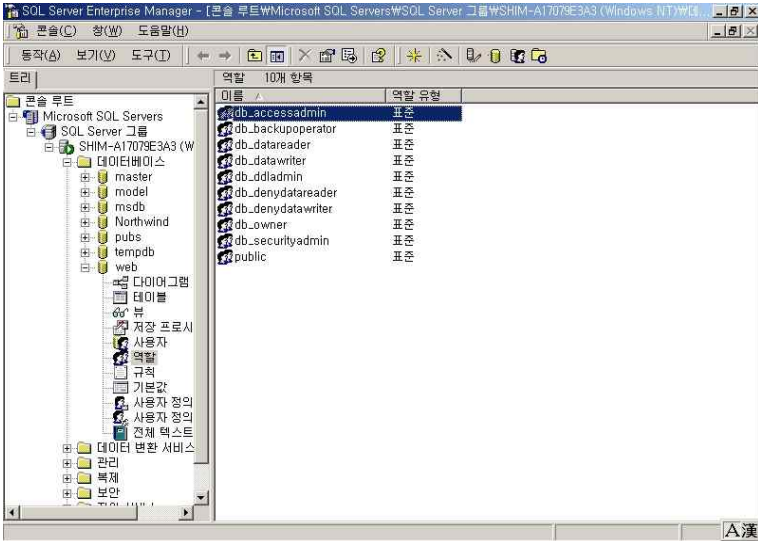
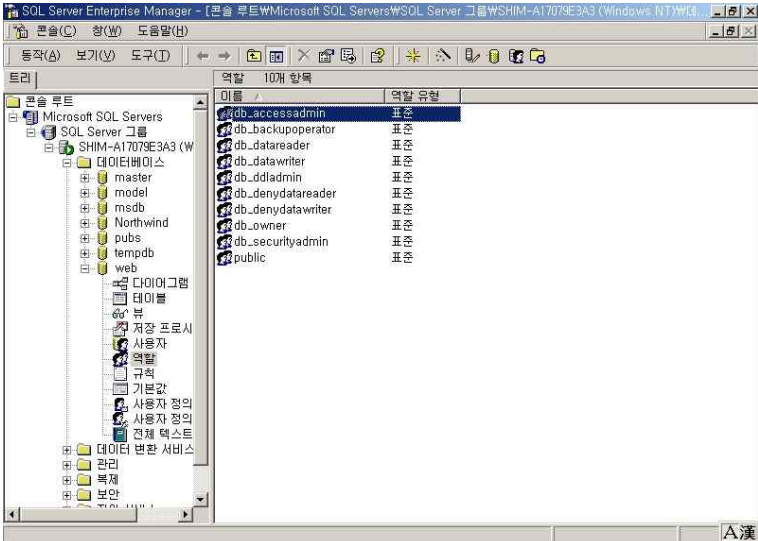
| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | D2-05 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |
| 설명    | 일정한 횟수의 로그인 실패 횟수 발생 시 이를 제한하지 않으면 무작위 추측 공격 (Brute force)을 통하여 데이터베이스에 접근이 가능하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 진단 기준 | 양호 - 로그인 시도 횟수를 제한하는 값을 설정한 경우<br>취약 - 로그인 시도 횟수가 UNLIMITED로 설정된 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 점검 방법 | <div> <div>■ Oracle</div> <div>Tnslnr를 통한 확인(windows)</div> <div> <pre>SQL&gt; select profile from dba_profiles       where resource_name='FAILED_LOGIN_ATTEMPTS'       and limit not in ('UNLIMITED','DEFAULT');</pre>                     결과가 리스트 되지 않으면 취약점이 존재하고, UNLIMITED 값의 경우 직접 Lock을 풀 때까지 계정이 잠겨있음을 의미함                 </div> </div>                                                                                                                                                                                                                                                                              |       |       |     |   |
| 조치 방법 | <div> <div>■ Oracle</div> <div>1. FAILED_LOGIN_ATTEMPTS 프로파일 파라미터 변경</div> <div>SQL&gt; ALTER PROFILE LIMIT FAILED_LOGIN_ATTEMPTS xx</div> <div>2. 프로파일 값과 관련된 사용자들 변경</div> <div>SQL&gt; ALTER USER PROFILE</div> <div>3. SQL*Plus를 통한 확인 예시</div> <div>SQL&gt; CREATE PROFILE grace_5 LIMIT</div> <div>FAILED_LOGIN_ATTEMPTS 3 (패스워드 실패를 3번까지만 가능)</div> <div>PASSWORD_LIFE_TIME 30 (30일동안만 패스워드를 사용)</div> <div>PASSWORD_REUSE_TIME 30 (한번 사용한 패스워드를 다시 사용하려면 30일 후부터 재사용 가능)</div> <div>PASSWORD_VERIFY_FUNCTION verify_function</div> <div>PASSWORD_GRACE_TIME 5;</div> <div>(life time이 끝나고 5일동안 메시지를 보여줌)</div> </div> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |

## 5.2.6. 데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 항목 코드 | D2-06 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Unix OS, Windows OS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 설명    | 비인가자가 redo 파일, 데이터베이스 설정 파일, 데이터 파일, 네트워크 설정 파일, Oracle 패스워드 관련 파일인 orapw.ora, listener.ora, init<SID>.ora 등의 주요 파일에 접근하여 수정·삭제하면 Oracle 데이터베이스 운영에 오류가 발생한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 진단 기준 | <p>양호 - 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있는 경우</p> <p>취약 - 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |
| 점검 방법 | <p>■ Oracle / Unix OS</p> <p>1. 디렉터리 또는 파일의 퍼미션 점검</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>\$ORACLE_HOME/bin/oracle (퍼미션 755) \$ORACLE_HOME/bin/ 아래 (퍼미션 755) sqlplus, sqlldr, sqlload, proc, oraenv, oerr, exp, imp, tkprof, tnsping, wrap \$ORACLE_HOME/bin 아래 (퍼미션 750) svrmgrl, lsnrctl, dbsnmp \$ORACLE_HOME/network (퍼미션 755) \$ORACLE_HOME/network/admin (퍼미션 755) listener.ora, sqlnet.ora 등 \$ORACLE_HOME/lib (퍼미션 755) \$ORACLE_HOME/network/admin 아래 환경파일 (퍼미션 644) tnsnames.ora, protocol.ora, sqlnet.ora \$ORACLE_HOME/dbs/init.ora (퍼미션 640) \$ORACLE_HOME/dbs/init&lt;SID&gt;.ora (퍼미션 640) Find \$ORACLE_HOME -name init*.ora -print</pre> </div> <p>2. redo 파일, 데이터베이스 설정 파일, 데이터 파일 위치(SQL*Plus)</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>SQL&gt; Select value from v\$parameter where name='spfile'; SQL&gt; Select 'Control Files: '  value from v\$parameter where name='control_files'; SQL&gt; select 'Control Files: '  value from v\$parameter where name='spfile'; SQL&gt; select 'Logfile: '  member from v\$logfile; SQL&gt; select 'Datafile: '  name from v\$datafile;</pre> </div> |       |       |     |   |
| 조치 방법 | <p>■ Oracle / Unix OS</p> <p>해당 파일 및 디렉터리의 퍼미션 설정 변경</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |

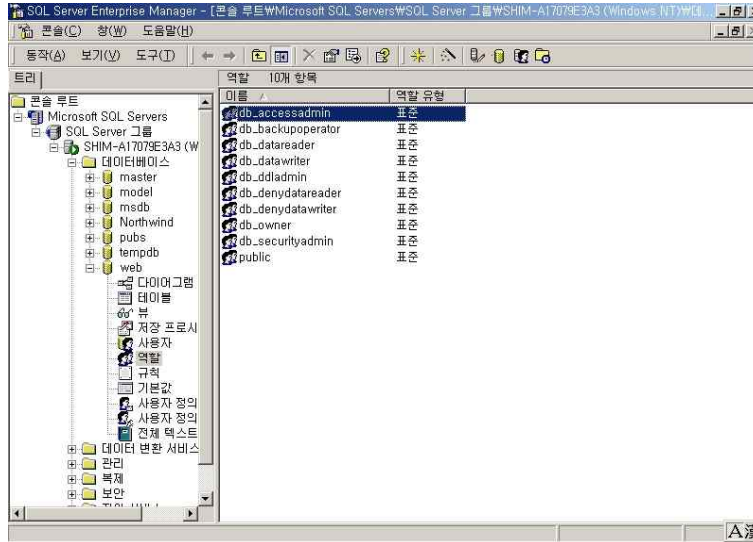
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>■ Oracle / Windows OS<br/>패스워드 파일(orapw&lt;SID&gt;) 접근 권한은 administrators, system group, owner group, oracle service account, DBAs에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함</p> <p>■ MySQL / Unix OS<br/>초기화 파일(my.cnf, my.ini)의 접근 권한을 초기화 파일에 대한 보호를 위하여 600 또는, 640으로 설정<br/>my.cnf 파일 디폴트 위치: /etc/my.cnf, &lt;각 홈디렉터리&gt;/my.cnf<br/># chmod 600 ./my.cnf</p> <p>■ MySQL / Windows OS<br/>초기화 파일의 접근 권한은 Administrators, SYSTEM, Owner에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 5.2.7. Application 사용자의 권한의 최소화

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | D2-07 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | 필요이상의 권한이 부여된 사용자에게 의해 데이터베이스상의 중요 정보의 변경 및 삭제 등의 비인가 접근이 발생한다.                                                                                                                                                                                                                                                                                            |       |       |     |   |
| 진단 기준 | <p>양호 - 불필요한 권한이 존재하는 계정이 없는 경우</p> <p>취약 - 불필요한 권한이 존재하는 계정이 있는 경우</p>                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>Application Role을 인터뷰를 통해서 확인</p> <p>[개체탐색기]&gt; [해당 데이터베이스]&gt; [역할] 에서 Application Role 을 선택하여 불필요한 권한이 설정되어 있는지 점검</p> <p>1. SQL 2000</p>  <p>2. SQL 2005</p>  |       |       |     |   |

### ■ MSSQL

Application Role을 인터뷰를 통해서 불필요한 권한이 존재하는 계정은 권한의 삭제 또는 변경을 통해 최소한의 권한을 부여

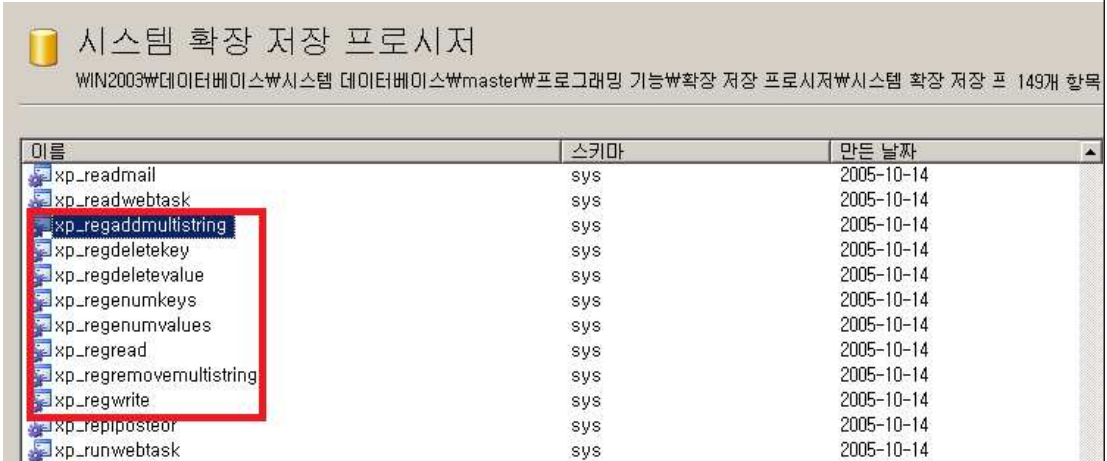


#### 조치 방법

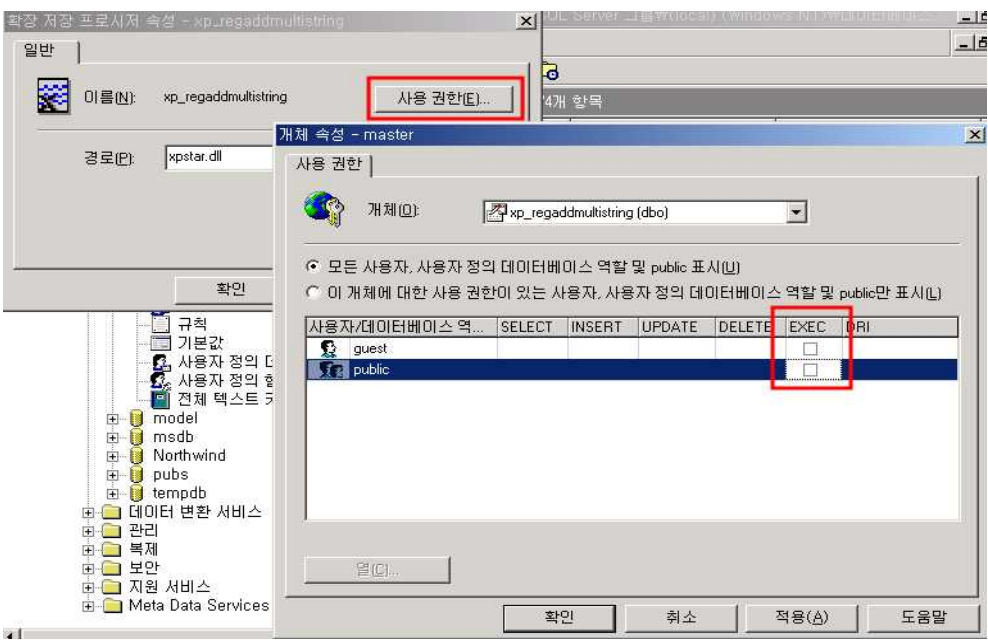
| 고정 데이터베이스 역할      | 설명                                                             |
|-------------------|----------------------------------------------------------------|
| db_accessadmin    | Windows 로그인, Windows 그룹 및 SQL Server 로그인에 대한 액세스를 추가, 제거할 수 있음 |
| db_backupoperator | 데이터베이스를 백업할 수 있음                                               |
| db_datareader     | 사용자 테이블의 모든 데이터를 읽을 수 있음                                       |
| db_datawriter     | 사용자 테이블에서 데이터를 추가, 삭제, 변경할 수 있음                                |
| db_ddladmin       | 데이터베이스에서 모든 DDL 명령을 실행할 수 있음                                   |
| db_denydatareader | 데이터베이스 내에 있는 사용자 테이블의 데이터를 읽을 수 없음                             |
| db_denydatawriter | 데이터베이스 내의 사용자 테이블의 데이터를 추가, 수정, 삭제할 수 없음                       |
| db_owner          | 데이터베이스에서 모든 구성 및 유지 관리 작업을 수행할 수 있음                            |
| db_securityadmin  | 멤버 자격을 수정하고 사용권한을 관리할 수 있음                                     |
| public            | 모든 데이터베이스 사용자에게 디폴트로 부여되는 최소 권한을 갖는 역할                         |

#### 비고

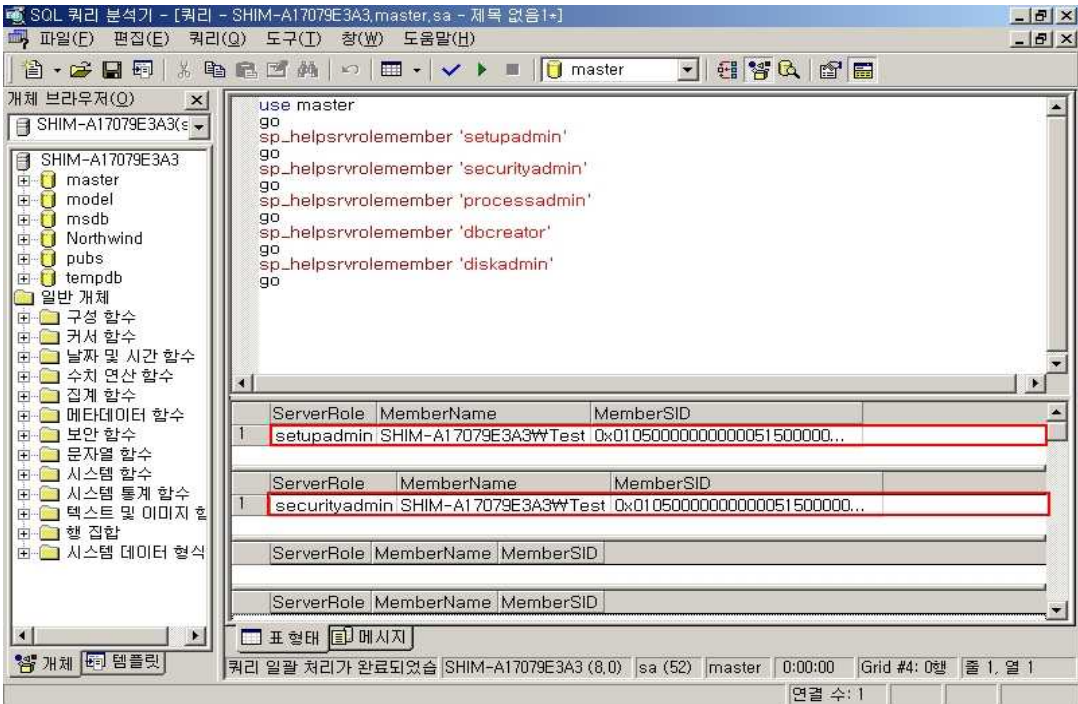
## 5.2.8. Registry procedure permission

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | D2-08 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 설명    | 확장 Stored Procedure인 Registry Procedure를 이용하면 SQL Server상에서 Windows NT 서버의 함수호출이 가능합니다. Registry Procedure가 비인가된 사용자에게 접근 허용되면, 이 사용자는 함수호출을 이용하여 Windows NT 서버의 패스워드 변경 가능하다.                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 진단 기준 | <p>양호 - guest/public 권한이 부여되지 않은 경우</p> <p>취약 - guest/public 권한이 부여된 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>Xp_reg* 프로시저의 사용권한을 점검</p> <p>[개체탐색기]&gt; [데이터베이스]&gt; [master]&gt; [확장 저장 프로시저] 에서 xp_reg*의 사용권한에 guest 또는 public 에 권한이 부여되어 있는지 확인</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>[Xp_reg 프로시저]</p> <p>xp_regaddmultistring, xp_regdeletekey, xp_regdeletevalue, xp_regread, xp_regwrite<br/>xp_regenumvalues, xp_regremovemultistring</p> </div>  |       |       |     |   |
| 조치 방법 | <p>■ MSSQL</p> <p>인가된 사용자만이 OLE Automation Procedure에 접근이 허용하고, public 권한은 제거</p>                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |



|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the 'xp_regaddmultistring' stored procedure properties in SQL Server Enterprise Manager. The 'Permissions' tab is active, displaying a table of permissions for the 'public' role. The 'EXEC' permission is checked for the 'public' role. Red boxes highlight the 'Permissions' button in the top right and the 'EXEC' checkbox in the permissions table.</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## 5.2.9. Fixed server 및 DB Role 부여

| 분류    | 권한관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 항목 코드 | D2-09 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |
| 설명    | Fixed Server 및 DB Role이 제한없이 일반 사용자에게 부여될 경우, 비인가된 DB 접근 및 침해가 발생할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 진단 기준 | <p>양호 - 일반 사용자에게 고정 서버 및 DB 역할이 설정되어 있지 않은 경우</p> <p>취약 - 일반 사용자에게 고정 서버 및 DB 역할이 설정되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>SQL 쿼리를 이용하여 고정 서버 및 DB 역할이 일반 사용자에게 부여되었는지 확인</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>&gt;&gt; Use master go sp_helpsrvrolemember 'setupadmin' go sp_helpsrvrolemember 'securityadmin' go sp_helpsrvrolemember 'processadmin' go sp_helpsrvrolemember 'dbcreator' go sp_helpsrvrolemember 'diskadmin' go</pre> </div>  |       |       |     |   |

|       |                                                                                                                                               |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>■ MSSQL</p> <p>일반 사용자에게 설정된 고정 서버 및 DB 역할을 제거</p> <pre>&gt;&gt; use master</pre> <pre>exec sp_dropsvrolemember '일반 사용자 계정', '삭제할 역할'</pre> |
| 비고    |                                                                                                                                               |

### 5.3. 보안 관리

#### 5.3.1. 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정

| 분류    | 보안관리                                                                                                                                                                                                                                                                                    | 항목 코드 | D3-01 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL                                                                                                                                                                                                                                                                           |       |       |     |   |
| 설명    | 응용 프로그램 계정의 Role 또는 DBA 계정의 Role이 Public으로 설정되어 있으면, 일반 계정에서도 응용 프로그램 테이블 또는 DBA 테이블로의 접근이 가능하다.                                                                                                                                                                                        |       |       |     |   |
| 진단 기준 | <p>양호 - DBA 계정의 Role이 Public으로 설정되어있지 않은 경우</p> <p>취약 - DBA 계정의 Role이 Public으로 설정되어있는 경우</p>                                                                                                                                                                                            |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>DBA Role 설정 확인</p> <p>SQL&gt; Select granted_role from dba_role_privs where grantee='PUBLIC';</p> <p>위와 같이 롤(role)이 설정되어 있는 경우 취약</p> <p>■ MSSQL</p>  <p>어떠한 Role이라도 나오면 취약함</p> |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>Public 그룹의 권한 취소</p> <p>SQL&gt; Revoke role from public;</p> <p>■ MSSQL</p> <p>1. 각 Object의 사용 권한이 불필요하게 Public, Guest에 부여된 경우 권한 제거</p> <p>Use database name</p> <p>(1) 권한 제거</p>                                                                                   |       |       |     |   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>REVOKE &lt;권한&gt; on &lt;object&gt; FROM public guest;</p> <p>(2) 권한 부여</p> <p>GRANT &lt;권한&gt; on &lt;object&gt; TO public guest;</p> <p>(예) syscolumns 테이블에 대한 SELECT 권한 제거</p> <p>USE master</p> <p>REVOKE select on sys.syscolumns FROM public;</p> <p>※ Object 사용 권한이 Public에 부여된 경우, 사용 권한이 없는 모든 계정이 Object에 접근 가능하여 Object의 정보를 획득할 수 있으므로 Object 사용 권한을 Public에 부여하는 것을 제한하여야 함</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                 |

### 5.3.2. OS\_ROLES, REMOTE\_OS\_AUTHENTICATION, REMOTE\_OS\_ROLES를 FALSE로 설정

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | D3-02 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | <p>OS_ROLES 설정 파라미터는 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락되며, REMOTE_OS_ROLES가 TRUE로 설정되어 있는 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있다.</p> <p>REMOTE_OS_AUTHENT가 TRUE로 설정되어있는 경우 신뢰하는 원격 호스트에서 인증 절차 없이 데이터베이스에 접속할 수 있다.</p>                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 진단 기준 | <p>양호 - OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 FALSE로 되어있는 경우</p> <p>취약 - OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 TRUE로 되어있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>1. OS_ROLES에 대한 확인</p> <p>show parameter os_roles;</p> <p>또는, select value from v\$parameter where name='os_roles';</p> <p>결과값이 False가 아니면 취약함</p> <p>2. REMOTE_OS_AUTHENTICATION에 대한 확인</p> <p>show parameter remote_os_authent;</p> <p>또는 select value from v\$parameter where name='remote_os_authent';</p> <p>결과가 FALSE가 아니면 취약함</p> <p>3. REMOTE_OS_ROLES에 대한 확인</p> <p>show parameter remote_os_roles;</p> <p>또는 Select value from v\$parameter where name='remote_os_roles';</p> <p>결과가 FALSE가 아니면 취약함</p>                        |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>파라미터를 FALSE로 설정</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>SPFILE: ALTER SYSTEM SET [파라미터이름=values] [SCOPE=(MEMORY/SPFILE/BOTH)]</p> <p>PFILE: ALTER SYSTEM SET [파라미터이름=values] [SCOPE=(MEMORY)]</p> <p>(예)</p> <p>SQL&gt; alter system set remote_os_roles = true scope=spfile;</p> <p>SQL&gt; alter system set os_roles = true scope=spfile;</p> <p>SQL&gt; alter system set remote_os_authent = true scope=spfile;</p> <p>버전 9i 이후 버전은 SPFILE을 재 생성해야 하므로, 데이터베이스를 셧다운 시키면 spfile이 재 생성됨</p> </div> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |

### 5.3.3. 세션 Idle timeout 설정

| 분류    | 보안관리                                                                                                                                     | 항목 코드 | D3-03 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                   |       |       |     |   |
| 설명    | 사용하지 않는 세션에 대한 timeout이 설정되어 있지 않을 경우, 비인가 된 사용자가 시스템에 해당 세션을 통해 접근하는 취약점이 발생할 수 있을 뿐만 아니라 해당 서버의 가용성 측면에서 문제점이 발생할 수 있다.                |       |       |     |   |
| 진단 기준 | 양호 - 세션에 대한 timeout이 설정되어 있을 경우<br>취약 - 세션에 대한 timeout이 설정되어 있지 않는 경우                                                                    |       |       |     |   |
| 점검 방법 | ■ Oracle<br>사용자 프로파일에서 세션 timeout 시간을 확인<br>SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='IDLE_TIME'; |       |       |     |   |
| 조치 방법 | ■ Oracle<br>세션 timeout 시간을 3분 이하로 설정하는 것을 권고<br>ALTER PROFILE profile_name LIMIT<br>IDLE_TIME 3                                          |       |       |     |   |
| 비고    |                                                                                                                                          |       |       |     |   |

### 5.3.4. SYSDBA 로그인 제한 설정

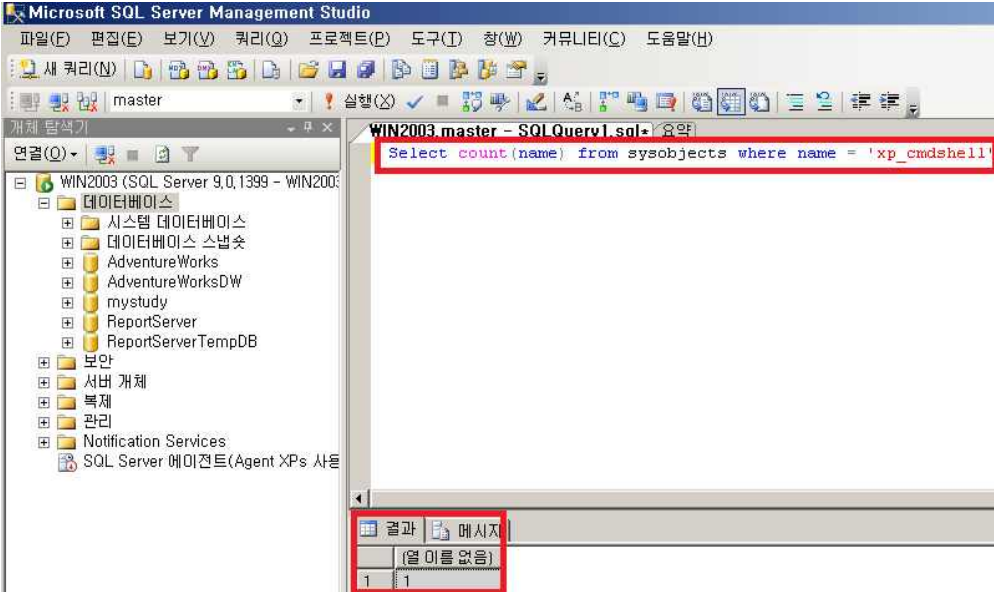
| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | D3-04 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 설명    | DBA가 SYS 패스워드를 기억하거나 입력할 필요가 없는 경우, DBA 그룹 멤버로 로그인할 수 있는 모든 사용자는 SYS 권한으로 DB에 접근 가능하다.                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | <p>양호 - SYS 계정을 통해 자동 로그인이 수행되지 않을 경우</p> <p>취약 - SYS 계정을 통해 자동 로그인이 수행되는 경우</p>                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>SYS계정을 통해 자동 로그인이 수행되는지 확인</p> <pre>grep -I SQLNET.AUTHENTICATION_SERVICES \$ORACLE_HOME/network/admin/SQLNET.ORA</pre> <p>SYSDBA 계정으로 DBMS 접근 시도</p> <pre>#sqlplus '/as sysdba' SQL*Plus: Release 10.2.0.2.0 -Production on Web Mar 4 15:23:16 2009 Copyright © 1982, 2005, Oracle, All Rights Reserved.</pre>                                  |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>SYS계정의 로그인 접근통제(SQLNET.AUTHENTICATION_SERVICES)를 적용</p> <pre>vi \$ORACLE_HOME/network/admin/SQLNET.ORA SQLNET.AUTHENTICATION_SERVICES=(NONE)</pre> <p>\$sqlplus / as sysdba</p> <p>다음과 같은 에러를 확인</p> <p>ERROR:ORA-01031: insufficient privileges</p> <p>Enter user-name:scott</p> <p>Enter password:</p> <p>성공적인 연결을 위해서 SYS계정과 패스워드를 입력해야 함</p> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |



### 5.3.5. OS 명령 수행 제한

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                               | 항목 코드 | D3-05 | 중요도 | H |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 설명    | SQL*Plus 상에서 대상 서버에 명령 수행이 가능하면 DB 서버 자체에 접근이 가능한 명령 실행 등으로 DB 서버 자체가 악의적인 공격에 노출된다.                                                                                                                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | 양호 - SQL*Plus 상에서 대상 서버에 명령 수행이 가능하지 않은 경우<br>취약 - SQL*Plus 상에서 대상 서버에 명령 수행이 가능한 경우                                                                                                                                                                                                                                                                               |       |       |     |   |
| 점검 방법 | <div> <div>■ Oracle</div> <div>OS 명령 수행 가능 여부를 점검</div> <div> <pre>SQL&gt; select count(*) from system.sqlplus_product_profile where      product='SQL*Plus'      and      attribute='HOST'      and char_value='DISABLED'; COUNT(*) _____ 0</pre> </div> </div>                                                                                                   |       |       |     |   |
| 조치 방법 | <div> <div>■ Oracle</div> <div>Scott 계정을 OS 명령어 제한</div> <div> <pre>SQL&gt;                                insert                                into PRODUCT_USER_PROFILE(product,userid,attribute,char_value) values('SQL*Plus','scott','HOST ','DISABLED');  PRODUCT  USERID  ATTRIBUTE  VALUE _____ SQL*Plus  SCOTT    HOST       DISABLED</pre> </div> </div> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |

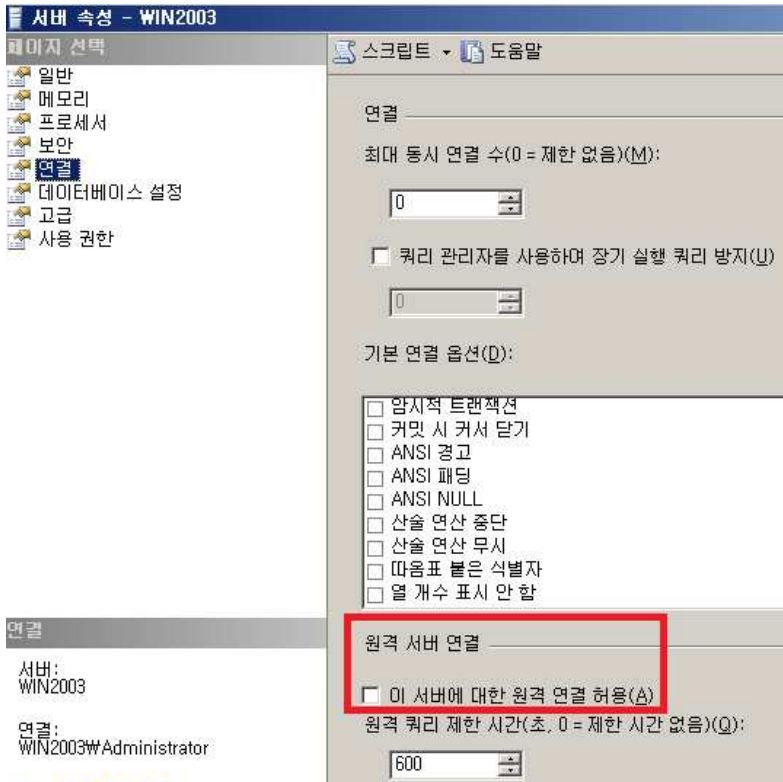
### 5.3.6. XP\_cmdshell procedure 사용

| 분류    | 보안관리                                                                                                                                                                                                                                                                                     | 항목 코드 | D3-06 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 설명    | xp_cmdshell Procedure 를 이용하면 SQL Server 상에서 대상 서버 운영체제의 명령어 실행이 가능하며, DB 서버 자체에 접근이 가능한 명령을 실행할 수 있으므로 DB 서버가 악의적인 공격에 노출된다.                                                                                                                                                             |       |       |     |   |
| 진단 기준 | 양호 - xp_cmdshell Procedure가 활성화되어 있지 않은 경우<br>취약 - xp_cmdshell Procedure가 활성화되어 있는 경우(결과값 : 1)                                                                                                                                                                                           |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>SQL 쿼리를 이용하여 xp_cmdshell procedure가 활성화 되어 있는지 점검</p> <p>SQL&gt; Select count(name) from sysobjects where name = 'xp_cmdshell'</p> <p>(결과가 1이면 xp_cmdshell Procedure 가 활성화 의미)</p>  |       |       |     |   |
| 조치 방법 | <p>■ MSSQL</p> <p>Xp_cmdshell procedure를 제거</p> <pre> use master go if object_id('[dbo].[xp_cmdshell]') is not null begin exec sp_dropextendedproc 'xp_cmdshell' end go exec sp_addextendedproc 'xp_cmdshell', 'xplog70.dll' go                     </pre>                               |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                          |       |       |     |   |

### 5.3.7. Sample DB 사용

| 분류    | 보안관리                                                                                                                                                                                                                       | 항목 코드 | D3-07 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | 운영 시스템에 불필요한 Sample DB에는 알려지지 않은 잠재적인 취약점이 존재할 가능성이 있으므로 운영 시스템에 영향을 줄 수 있다.                                                                                                                                               |       |       |     |   |
| 진단 기준 | <p>양호 - 불필요한 sample DB가 존재하지 않은 경우</p> <p>취약 - 불필요한 sample DB가 존재할 경우</p>                                                                                                                                                  |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>Sample DB 존재 유무를 인터뷰를 통해 확인</p> <p>Sample DB - pubs, Northwind</p> <p>[개체탐색기]&gt; [데이터베이스] 에서 pubs, Northwind 확인</p>  |       |       |     |   |
| 조치 방법 | <p>■ MSSQL</p> <p>운영상 불필요한 Sample DB 제거</p> <p>SQL&gt; drop database 샘플DB이름</p>                                                                                                                                            |       |       |     |   |
| 비고    |                                                                                                                                                                                                                            |       |       |     |   |

### 5.3.8. 외부 DB와의 연동

| 분류    | 보안관리                                                                                                                                                                                                                                                        | 항목 코드 | D3-08 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MSSQL                                                                                                                                                                                                                                                       |       |       |     |   |
| 설명    | DB 연동을 위해 외부의 다른 SQL 서버로부터 접근이 가능하도록 설정하여 놓은 경우, 외부의 공격자가 DB에 비인가된 접근을 수행할 수 있다.                                                                                                                                                                            |       |       |     |   |
| 진단 기준 | 양호 - 외부 접근 기능이 설정되어 있지 않은 경우<br>취약 - 외부 접근 기능이 설정되어 있는 경우(결과값 1)                                                                                                                                                                                            |       |       |     |   |
| 점검 방법 | <p>■ MSSQL</p> <p>SQL 쿼리를 이용하여 외부 접근이 가능한 지 점검</p> <p>SQL&gt; Select value from sysconfigures where comment = 'Allow remote access'</p> <p>(결과가 1이면 외부 접근이 가능함을 의미)</p>  |       |       |     |   |
| 조치 방법 | <p>■ MSSQL</p> <p>외부 접근이 가능하지 않도록 다음과 같이 설정</p> <p>[서버 우클릭]&gt; [속성]&gt; [연결]&gt; [원격 서버 연결] 에서</p> <p>‘이 서버에 대한 원격 연결 허용’ 체크 해제</p>                                    |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                             |       |       |     |   |

### 5.3.9. My SQL 설치 시 제공된 test 데이터베이스 제거

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 항목 코드 | D3-09 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |       |     |   |
| 설명    | test 데이터베이스는 암호 없이 접근할 수 있으므로 삭제하며, 설치된 불필요한 디렉토리 및 파일들은 보안상 위험이 존재하므로 삭제한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |
| 진단 기준 | 양호 - test 데이터베이스, 불필요한 디렉터리나 파일이 존재하지 않는 경우<br>취약 - test 데이터베이스, 불필요한 디렉터리나 파일이 존재하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |       |     |   |
| 점검 방법 | <b>■ MySQL</b><br>1. test 데이터베이스 관련 삭제<br>2. 불필요한 디렉터리나 파일을 삭제                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 조치 방법 | <b>■ MySQL</b><br>1. test 데이터베이스 관련 삭제 <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>mysql&gt; use mysql; mysql&gt; delete from user where User=''; mysql&gt; delete from db where Host='%'; mysql&gt; drop database 'test';</pre> </div> 2. 불필요한 파일 삭제 <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>먼저 \$MySQL_HOME에서 불필요한 디렉토리 및 파일이 존재하는지 확인 # ls -al -rw-r--r-- 1 root mysql 5806 Nov 3 2006 EXCEPTIONS-CLIENT -rw-r--r-- 1 root mysql 8117 Nov 3 2006 INSTALL-BINARY drwxr-xr-x 2 root mysql 4096 Nov 3 2006 bin -rwxr-xr-x 1 root mysql 801 Nov 3 2006 configure drwxr-x-- 4 mysql mysql 4096 Aug 15 22:27 data drwxr-xr-x 3 root mysql 4096 Nov 3 2006 include drwxr-xr-x 2 root mysql 4096 Nov 3 2006 lib drwxr-xr-x 4 root mysql 4096 Nov 3 2006 man drwxr-xr-x 8 root mysql 4096 Nov 3 2006 mysql-test drwxr-xr-x 2 root mysql 4096 Nov 3 2006 scripts drwxr-xr-x 2 root mysql 4096 Nov 3 2006 support-files drwxr-xr-x 2 root mysql 4096 Nov 3 2006 tests</pre> </div> 3. 불필요한 디렉터리나 파일을 삭제<br><pre># rm -rf '불필요한 디렉터리나 파일'</pre> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |

## 5.4. 운영관리

### 5.4.1. Listener 감사 설정

| 분류    | 운영관리                                                                                                                                                                                                                            | 항목 코드 | D4-01 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | DBMS의 Listener Audit Trail Log가 설정되어 DBMS로 로그인하는 계정의 DBMS 리모트 로그인 내역이 기록되고 있는지 점검한다.                                                                                                                                            |       |       |     |   |
| 진단 기준 | 양호 - DBMS 리모트 로그인 내역이 기록되고 있는 경우<br>취약 - DBMS 리모트 로그인 내역이 기록되고 있지 않은 경우                                                                                                                                                         |       |       |     |   |
| 점검 방법 | ■ Oracle<br>Listener 감사 설정 확인<br><pre>grep -i logging_listener listener.ora</pre>                                                                                                                                               |       |       |     |   |
| 조치 방법 | ■ Oracle<br>1. Oracle환경파일(listener.ora) 설정<br><pre>Vi \$ORACLE_HOME/network/admin/listener.ora</pre> logging_listener=ON 으로 설정한다.<br><br>2. 솔루션을 이용한 변경 방안<br>DB접근통제 솔루션을 이용하여 DB에 접근하는 사용자의 접근ID, 시간, IP 등을 솔루션에서 통제 경우 예외처리함. |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                 |       |       |     |   |

## 5.4.2. 로그 관련 디렉터리 접근권한

| 분류    | 운영관리                                                                                                                                                                                                  | 항목 코드 | D4-02 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                |       |       |     |   |
| 설명    | 로그 파일 대한 접근 통제 설정이 제대로 되어 있지 않은 경우 해커는 자신이 들어왔던 흔적을 지우기 위하여 로그 파일에 대한 변조 및 삭제를 시도할 수 있으므로 적절하게 접근 통제 설정해야 한다.                                                                                         |       |       |     |   |
| 진단 기준 | 양호 - 적절한 접근 통제 설정이 되어있는 경우<br>취약 - 적절한 접근 통제 설정이 되어있지 않은 경우                                                                                                                                           |       |       |     |   |
| 점검 방법 | <b>■ Oracle</b><br>로그파일(Listener.log)의 접근권한을 점검<br><pre>grep -i log_file_listener \$ORACLE_HOME/network/admin/listener.ora</pre> 파일 위치: \$ORACLE_HOME/network/log/listener.log                        |       |       |     |   |
| 조치 방법 | <b>■ Oracle</b><br>Listener.log 파일의 접근권한을 640이하로 변경<br><pre>#chmod 640 W \$ORACLE_HOME/network/log/listener.log</pre> <pre>#chown oracleuser.oraclegroup \$ORACLE_HOME/network/log/listener.log</pre> |       |       |     |   |
| 비고    |                                                                                                                                                                                                       |       |       |     |   |

### 5.4.3. Control File의 물리적 DISK 관리

| 분류    | 운영관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | D4-03 | 중요도 | M |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 설명    | Control File은 DBMS 상태를 담고 있는 중요한 파일이므로 파일시스템 장애 또는 관리자의 실수로 파일이 DELETE 되었을 경우 복구 될 수 있는 환경이 되어야 한다. 이에 대한 대응책으로 몇 개의 Control 파일이 있을 경우 다른 파일 시스템으로 Mirroring이 되도록 설정 되어야 한다. 운영중인 Control File들이 동일한 Disk Device에 위치해 있으면 이로 인하여 한 개의 Disk Device에 물리적 문제 발생 시 가용성 유지에 어려움이 발생한다.                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 진단 기준 | 양호 - Control File이 분리되어 있는 경우<br>취약 - Control File이 분리되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |
| 점검 방법 | <div> <div> <div>■ Oracle</div> <div>1. 명령문을 통한 Control File의 분리여부 점검</div> <div> <pre>grep -i control_files init.ora ls -al</pre> <div>-출력 화면 -</div> <pre>control_files=("/dev/vx/rdisk/oracle_dg/clustdb_raw_controlfile1_110m", "/dev/vx/rdisk/oracle_dg/clustdb_raw_controlfile2_110m")</pre> </div> </div> <div> <div>2. 쿼리문을 이용하여 Control File의 분리여부 점검</div> <div> <pre>SQL&gt; select name from v\$controlfile;</pre> <div>- 출력 화면 -</div> <pre>NAME ----- /u01/app/oracle/oradata/orcl/control01.ctl /u01/app/oracle/oradata/orcl/control02.ctl /u01/app/oracle/oradata/orcl/control03.ctl</pre> </div> </div> </div> |       |       |     |   |
| 조치 방법 | <div> <div> <div>■ Oracle</div> <div>1. 권한은 Oracle 소유자와 DBA 그룹으로 제한</div> <pre>#chmod 640 control_file</pre> <pre>#chown oracleuser.oraclegroup control_file_name</pre> </div> <div> <div>2. 동시에 운영중인 시스템볼륨에서 Control File 분리</div> <div>새로운 Control File을 추가</div> <div>1) 인스턴스를 셧다운</div> <div>2) 기존 Control File을 새로운 위치에 복사</div> <div>3) 새로운 위치를 init&lt;SID&gt;.ora 파일의 CONTROL_FILES 파라미터 설정 사항에 추가</div> <div>4) 인스턴스를 다시 시작</div> </div> </div>                                                                                                                                                                        |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |



#### 5.4.4. 백업 및 복구 설정

| 분류    | 운영관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 항목 코드 | D4-04 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 설명    | <p>Backup을 통해 고의/비고의적 사고로 인한 데이터 손실로부터 데이터를 복구 할 수 있으며, Backup파일의 퍼미션이 잘못 설정되어 있을 경우 비인가자가 Backup파일을 절취함으로써 중요 데이터가 누출될 수 있으므로 Backup은 적절한 정책에 의해 실행되어야 하며 생성된 Backup 파일의 관리가 철저히 이루어져야 한다.</p> <p>또한 주기적인 백업이 수행되어야 하며 특히 DBMS의 유지보수 및 Upgrade 작업에는 전체 Full 백업을 실시하여 장애 및 외부 침입 등에 대한 변수가 발생할 경우를 대비해야 한다.</p>                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | <p>양호 - 주기적으로 백업을 수행하며 정책에 따라 수행되고 있는 경우</p> <p>취약 - 주기적으로 백업을 수행하며 정책에 따라 수행되고 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 점검 방법 | <p>■ Oracle</p> <p>인터뷰를 통해 현황을 확인</p> <ol style="list-style-type: none"> <li>1. 백업설정에 대하여 해당 DBA와 인터뷰 실시</li> <li>2. 담당자와 인터뷰하여 주기적인 백업 수행 여부 점검</li> <li>3. 백업 및 복구 수행 이력을 점검하여 백업이 정책에 따라 수행되고 있는지 점검</li> </ol>                                                                                                                                                                                                                                                                                                                                                                           |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>시스템에 따른 백업 및 복구 정책 결정</p> <ol style="list-style-type: none"> <li>1. 백업 정책을 바탕으로 주기적인 백업 절차를 수립한다 <ul style="list-style-type: none"> <li>- 백업전략 계획시 고려사항 <ol style="list-style-type: none"> <li>① 상실될 경우의 위험성에 따른 데이터의 유형 분류 및 그 때의 필요한 공간</li> <li>② 데이터가 복구되는 동안 시스템이 다운되는 시간</li> <li>③ Standby 데이터베이스를 유지할 경우 소요되는 비용 등</li> </ol> </li> </ul> </li> <li>2. DBMS의 유지보수 및 Upgrade 작업 시에는 전체 Full 백업 절차를 수립한다(권고)</li> <li>3. 데이터 파일 및 시스템 구성 파일 백업한다 <p>Ex) datafile, controlfile, doline redo log file, 환경설정(init.ora, config.ora), archive log file 등</p> </li> </ol> |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |

## 5.5. 패치관리

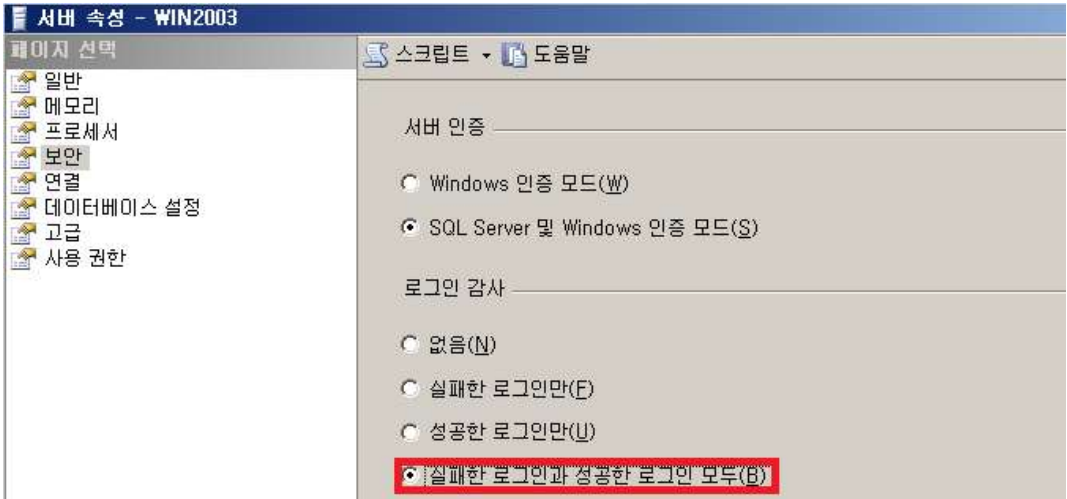
### 5.5.1. 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용

| 분류                   | 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 항목 코드 | D5-01 | 중요도 | H |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|----------|-------|----------------------|--------------------------------|----------------------|----------------------------|----------------------|-----------------|----------------------|----------|---------------------|---------|---------------------|---------|---------------------|---------|-----------|---------|
| 대상                   | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| 설명                   | 데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능하다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| 진단 기준                | 양호 - 버전별 최신 패치를 적용한 경우<br>취약 - 버전별 최신 패치를 적용하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| 점검 방법                | <div>■ Oracle</div> <p>ORACLE_HOME에 설치된 오라클 제품 컴포넌트를 조회하거나, 적용된 임시 패치를 조회할 때는 lsinventory 명령어를 사용함</p> <div>1. oracle 제공 패치 명령을 이용하여 확인함</div> <div>· \$opatch lsinventory [ -all ] [ -detail ] [ -invPtrLoc ] [ -jre ] [ -oh ]</div> <div>· all : ORACLE_BASE 밑에 설치된 모든ORACLE_HOME 정보를 표시</div> <div>· detail : 설치된 패치 내에 포함된 라이브러리 파일까지 표시하므로 패치 적용 시 충돌되는 객체 파일을 확인 가능함</div> <div>2. Unix 시스템 경우</div> <div>\$ORACLE_HOME/OPatch/ 명령어: ./opatch lsinventory -detail</div> <div>3. Windows 시스템 경우</div> <div>%ORACLE_HOME%\WOPatch\wopatch lsinventory -detail</div> <div>http://metalink.oracle.com에서 최신 패치 버전을 확인하고 opatch 명령을 통해 도출된 결과를 비교함</div> <table><tr><th>데이터베이스 명</th><th>적용 패치</th></tr><tr><td>Oracle 10g Release 2</td><td>10.2.0.5 Windows 64bit itanium</td></tr><tr><td>Oracle 10g Release 2</td><td>10.2.0.4 Windows, MAC OS X</td></tr><tr><td>Oracle 10g Release 2</td><td>10.2.0.1 All OS</td></tr><tr><td>Oracle 10g Release 1</td><td>10.1.0.5</td></tr><tr><td>Oracle 9i Release 2</td><td>9.2.0.8</td></tr><tr><td>Oracle 9i Release 1</td><td>9.0.1.4</td></tr><tr><td>Oracle 8i Release 3</td><td>8.1.7.4</td></tr><tr><td>Oracle 8i</td><td>8.0.6.3</td></tr></table> <div>※ 참고 사이트</div> <div><a href="http://www.oracle.com/technetwork/database/enterprise-dition/downloads/index.html">http://www.oracle.com/technetwork/database/enterprise-dition/downloads/index.html</a></div> |       |       |     |   | 데이터베이스 명 | 적용 패치 | Oracle 10g Release 2 | 10.2.0.5 Windows 64bit itanium | Oracle 10g Release 2 | 10.2.0.4 Windows, MAC OS X | Oracle 10g Release 2 | 10.2.0.1 All OS | Oracle 10g Release 1 | 10.1.0.5 | Oracle 9i Release 2 | 9.2.0.8 | Oracle 9i Release 1 | 9.0.1.4 | Oracle 8i Release 3 | 8.1.7.4 | Oracle 8i | 8.0.6.3 |
|                      | 데이터베이스 명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 적용 패치 |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 10g Release 2 | 10.2.0.5 Windows 64bit itanium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 10g Release 2 | 10.2.0.4 Windows, MAC OS X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 10g Release 2 | 10.2.0.1 All OS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 10g Release 1 | 10.1.0.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 9i Release 2  | 9.2.0.8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 9i Release 1  | 9.0.1.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 8i Release 3  | 8.1.7.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |
| Oracle 8i            | 8.0.6.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |       |     |   |          |       |                      |                                |                      |                            |                      |                 |                      |          |                     |         |                     |         |                     |         |           |         |

|                                 | <p>■ MSSQL</p> <p>SQL쿼리를 이용하여 SQL 버전 확인</p> <p>SQL&gt; Select @@version</p>  <p>■ MySQL</p> <p>SQL 쿼리를 이용하여 현재 사용하고 있는 버전을 확인</p> <p>mysql&gt; select version();</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------------|----------------------|-----------|----------------------|-----------|----------------------|----------|----------------------|----------|---------------------|----------|--------------------------|-----------|---------------------------|-----------|---------------------------|-----------|---------------------|-----------|---------------------|-----------|------------------------------|---------------|------------------------------|---------------|-------------------------------|---------------|---------------------------|---------------|----------------------------|---------------|----------------------------|---------------|----------------------------|---------------|---------------------------------|---------------|
| 조치 방법                           | <p>■ Oracle</p> <p><a href="http://metalink.oracle.com">http://metalink.oracle.com</a>을 통해 발표되는 오라클 패치 수행</p> <p>■ MSSQL</p> <p>데이터베이스에 대한 버전을 확인 후 업그레이드 및 패치 적용</p> <table border="1" data-bbox="493 1039 1310 1973"> <thead> <tr> <th>Release</th><th>Sqlserver.exe</th></tr> </thead> <tbody> <tr><td>SQL Server 2000 SP 4</td><td>8.00.2283</td></tr> <tr><td>SQL Server 2000 SP 3</td><td>8.00.1007</td></tr> <tr><td>SQL Server 2000 SP 2</td><td>8.00.534</td></tr> <tr><td>SQL Server 2000 SP 1</td><td>8.00.384</td></tr> <tr><td>SQL Server 2000 RTM</td><td>8.00.194</td></tr> <tr><td>SQL Server 2005 SP4 CU#3</td><td>9.00.5266</td></tr> <tr><td>SQL Server 2005 SP3 CU#15</td><td>9.00.4325</td></tr> <tr><td>SQL Server 2005 SP2 CU#17</td><td>9.00.3356</td></tr> <tr><td>SQL Server 2005 SP1</td><td>9.00.2047</td></tr> <tr><td>SQL Server 2005 RTM</td><td>9.00.1399</td></tr> <tr><td>SQL Server 2008 R2 SP2 CU #3</td><td>10.50.4266.00</td></tr> <tr><td>SQL Server 2008 R2 SP1 CU #9</td><td>10.50.2866.00</td></tr> <tr><td>SQL Server 2008 R2 RTM CU #13</td><td>10.50.1815.00</td></tr> <tr><td>SQL Server 2008 SP3 CU #8</td><td>10.00.5785.00</td></tr> <tr><td>SQL Server 2008 SP2 CU #11</td><td>10.00.4333.00</td></tr> <tr><td>SQL Server 2008 SP1 CU #16</td><td>10.00.2850.00</td></tr> <tr><td>SQL Server 2008 RTM CU #10</td><td>10.00.1835.00</td></tr> <tr><td>SQL Server 2012 SP1 + KB2765331</td><td>11.00.3321.00</td></tr> </tbody> </table> <p>※ 참고 사이트</p> <p><a href="http://support.microsoft.com/kb/321185/en-us">http://support.microsoft.com/kb/321185/en-us</a></p> <p><a href="http://www.sqlsecurity.com/FAQs/SQLServerVersionDatabase/tabid/63/Default.aspx">http://www.sqlsecurity.com/FAQs/SQLServerVersionDatabase/tabid/63/Default.aspx</a></p> | Release | Sqlserver.exe | SQL Server 2000 SP 4 | 8.00.2283 | SQL Server 2000 SP 3 | 8.00.1007 | SQL Server 2000 SP 2 | 8.00.534 | SQL Server 2000 SP 1 | 8.00.384 | SQL Server 2000 RTM | 8.00.194 | SQL Server 2005 SP4 CU#3 | 9.00.5266 | SQL Server 2005 SP3 CU#15 | 9.00.4325 | SQL Server 2005 SP2 CU#17 | 9.00.3356 | SQL Server 2005 SP1 | 9.00.2047 | SQL Server 2005 RTM | 9.00.1399 | SQL Server 2008 R2 SP2 CU #3 | 10.50.4266.00 | SQL Server 2008 R2 SP1 CU #9 | 10.50.2866.00 | SQL Server 2008 R2 RTM CU #13 | 10.50.1815.00 | SQL Server 2008 SP3 CU #8 | 10.00.5785.00 | SQL Server 2008 SP2 CU #11 | 10.00.4333.00 | SQL Server 2008 SP1 CU #16 | 10.00.2850.00 | SQL Server 2008 RTM CU #10 | 10.00.1835.00 | SQL Server 2012 SP1 + KB2765331 | 11.00.3321.00 |
| Release                         | Sqlserver.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2000 SP 4            | 8.00.2283                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2000 SP 3            | 8.00.1007                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2000 SP 2            | 8.00.534                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2000 SP 1            | 8.00.384                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2000 RTM             | 8.00.194                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2005 SP4 CU#3        | 9.00.5266                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2005 SP3 CU#15       | 9.00.4325                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2005 SP2 CU#17       | 9.00.3356                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2005 SP1             | 9.00.2047                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2005 RTM             | 9.00.1399                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 R2 SP2 CU #3    | 10.50.4266.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 R2 SP1 CU #9    | 10.50.2866.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 R2 RTM CU #13   | 10.50.1815.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 SP3 CU #8       | 10.00.5785.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 SP2 CU #11      | 10.00.4333.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 SP1 CU #16      | 10.00.2850.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2008 RTM CU #10      | 10.00.1835.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |
| SQL Server 2012 SP1 + KB2765331 | 11.00.3321.00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |               |                      |           |                      |           |                      |          |                      |          |                     |          |                          |           |                           |           |                           |           |                     |           |                     |           |                              |               |                              |               |                               |               |                           |               |                            |               |                            |               |                            |               |                                 |               |

|         | <p>■ MySQL</p> <p>패치는 주기적으로 <a href="http://www.mysql.com">http://www.mysql.com</a> 에서 확인하여 적용</p> <table border="1" data-bbox="539 392 1264 846"> <thead> <tr> <th>Version</th><th>Last Version</th></tr> </thead> <tbody> <tr> <td>6.0</td><td>6.0.11</td></tr> <tr> <td>5.6</td><td>5.6.9</td></tr> <tr> <td>5.5</td><td>5.5.6</td></tr> <tr> <td>5.4</td><td>5.4.2</td></tr> <tr> <td>5.1</td><td>5.1.40</td></tr> <tr> <td>5.0</td><td>5.0.88</td></tr> <tr> <td>4.1</td><td>4.1.22</td></tr> </tbody> </table> <p>※ 참고 사이트</p> <p>버그패치 된 릴리즈 사이트 <a href="http://downloads.mysql.com/archives.php">http://downloads.mysql.com/archives.php</a></p> <p>버그 현황 사이트 <a href="http://bugs.mysql.com/bugstats.php">http://bugs.mysql.com/bugstats.php</a></p> | Version | Last Version | 6.0 | 6.0.11 | 5.6 | 5.6.9 | 5.5 | 5.5.6 | 5.4 | 5.4.2 | 5.1 | 5.1.40 | 5.0 | 5.0.88 | 4.1 | 4.1.22 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|-----|--------|-----|-------|-----|-------|-----|-------|-----|--------|-----|--------|-----|--------|
| Version | Last Version                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 6.0     | 6.0.11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 5.6     | 5.6.9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 5.5     | 5.5.6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 5.4     | 5.4.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 5.1     | 5.1.40                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 5.0     | 5.0.88                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 4.1     | 4.1.22                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |
| 비고      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |         |              |     |        |     |       |     |       |     |       |     |        |     |        |     |        |

## 5.5.2. 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정

| 분류    | 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | D5-02 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | 데이터베이스의 감사 기록이 기관에서 정의한 감사 기록 정책에 적합하도록 기록해야 한다. 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립해야 하며, 지속적으로 준수하지 않을 경우 데이터베이스에 문제 발생 시 이를 효과적으로 대처할 수 없다.                                                                                                                                                                                                                                                                                                                          |       |       |     |   |
| 진단 기준 | 양호 - DBMS의 감사 로그 저장 정책이 수립되어 있으며, 정책이 적용되어있는 경우<br>취약 - DBMS에 대한 감사 로그 저장을 하지 않거나, 정책이 수립되어있지 않은 경우                                                                                                                                                                                                                                                                                                                                                                       |       |       |     |   |
| 점검 방법 | <p>■ Oracle, MSSQL, MySQL</p> <p>인터뷰를 통해 데이터베이스 감사기록, 백업 정책 관련 지침이 존재하는지 확인<br/>확인된 내용을 토대로 실제 감사 기록 및 백업이 이루어지는지 확인함</p>                                                                                                                                                                                                                                                                                                                                                 |       |       |     |   |
| 조치 방법 | <p>■ Oracle</p> <p>데이터베이스 감사 기록 정책 및 백업 정책 수립</p> <p>■ MSSQL</p> <p>데이터베이스 감사 기록 정책 및 백업 정책 수립</p> <p>[개체탐색기]&gt; [해당 서버 오른쪽 마우스]&gt; [속성]&gt; [보안]&gt; [로그인 옵션] 에서<br/>‘실패한 로그인과 성공한 로그인 모두’ 설정</p>  <p>■ MySQL</p> <p>데이터베이스 감사 기록 정책 및 백업 정책을 설정</p> <pre>1. mysql&gt; set global general_log=1; mysql&gt; show variables where Variable_name in ('version', 'general_log');</pre> |       |       |     |   |

|    |                                                                                                             |
|----|-------------------------------------------------------------------------------------------------------------|
|    | 2. set global general_log='on';<br>mysql> show variables where Variable_name in ('version', 'general_log'); |
| 비고 |                                                                                                             |

### 5.5.3. Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정

| 분류    | 패치관리                                                                                                                                    | 항목 코드 | D5-03 | 중요도 | L |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | Oracle                                                                                                                                  |       |       |     |   |
| 설명    | Audit Table은 반드시 SYS, SYSTEM과 같은 데이터베이스 관리자 계정에 속해 있어야 한다. 그렇지 않은 경우 인가되지 않은 사용자가 감사 데이터의 수정, 삭제수행 가능하다.                                |       |       |     |   |
| 진단 기준 | 양호 - Audit Table이 데이터베이스 관리자 계정에 속해있는 경우<br>취약 - Audit Table이 데이터베이스 관리자 계정에 속해있지 않은 경우                                                 |       |       |     |   |
| 점검 방법 | <b>■ Oracle</b><br>SQL*Plus를 이용하여 확인 예시<br>select owner from dba_tables where table_name='AUD\$';<br>SYS 또는 SYSTEM이 아닌 계정이 나오면 확인하여 평가함 |       |       |     |   |
| 조치 방법 | <b>■ Oracle</b><br>Audit table에 접근할 권한이 없는 계정이 있다면 권한을 삭제                                                                               |       |       |     |   |
| 비고    |                                                                                                                                         |       |       |     |   |

#### 5.5.4. Show processlist 기능 제거

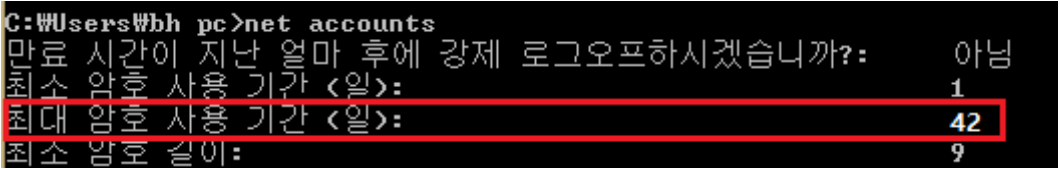
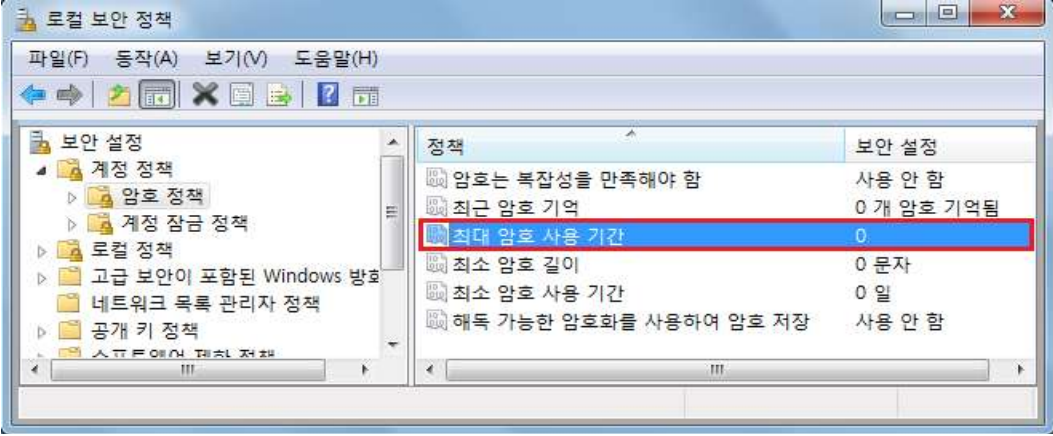
| 분류    | 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | D5-04 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-----|---|
| 대상    | MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |       |     |   |
| 설명    | MySQL 관리자가 아닌 일반 유저에게 process 권한이 주어질 경우 “show processlist;”를 실행하면 현재 실행되는 query를 모니터링할 수 있으며, 이중에는 “UPDATE user SET password=PASSWORD(‘xxxxxxx’)”과 같은 query도 직접 볼 수 있으며, 결국 암호가 쉽게 유출될 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |       |     |   |
| 진단 기준 | 양호 - user테이블에서 계정의 Process_priv권한이 관리자에게만 Y권한일 경우<br>취약 - user테이블에서 계정의 Process_priv권한이 관리자에게만 N권한일 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 점검 방법 | <p>■ MySQL</p> <p>현재 계정들에 대하여 Process_priv 권한을 검사</p> <pre>mysql&gt; select User, Process_priv from user; +----+-----+   User   Process_priv   +----+-----+   root   Y               root   Y             +----+-----+ 2 rows in set (0.00 sec)</pre> <p>2. 일반 유저에게 Process_priv 권한이 ‘Y’일 경우 다음과 같이 “show processlist” 명령을 사용하여 실행중인 query를 모니터링</p> <pre>mysql&gt; show processlist; +----+----+-----+----+-----+----+-----+-----+   Id   User   Host        db    Command   Time   State   Info   +----+----+-----+----+-----+----+-----+-----+   2    root   localhost   NULL   Query     0      NULL    show processlist   +----+----+-----+----+-----+----+-----+-----+ 1 row in set (0.00 sec)</pre> |       |       |     |   |
| 조치 방법 | <p>■ MySQL</p> <p>user테이블에서 계정의 Process_priv 권한을 관리자 계정에게만 ‘Y’권한을 허용</p> <pre>mysql&gt; UPDATE user SET Process_priv='N' WHERE user='&lt;계정&gt;;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |       |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |       |     |   |



## 6. PC 취약성 점검항목 및 가이드

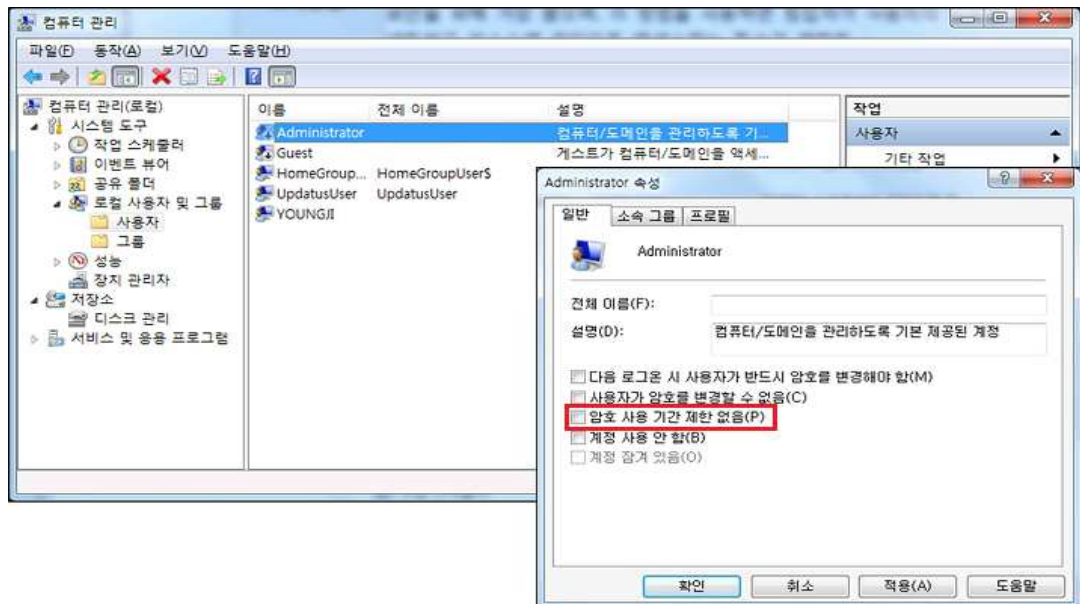
### 6.1. 계정관리

#### 6.1.1. 패스워드의 주기적 변경

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | PC1-01 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | 계정의 패스워드를 주기적으로 변경하지 않고 오랫동안 사용할 경우 계정 패스워드가 외부에 유출될 수 있으며, 관리자 계정의 패스워드가 유출될 시 자료 유출 등 심각한 사고 발생 가능성이 존재한다.                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 진단 기준 | 양호 - 최대 암호 사용 기간이 “90일”로 설정되어 있는 경우<br>취약 - 암호 사용 기간이 “제한 없음”으로 설정되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>최대 암호 사용 기간이 “90일”로 설정되어 있는지 확인한다.</p> <p>[Windows 7]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net accounts 명령어 실행하여 “최대 암호 사용 기간(일)” 확인</p>  <p>■ 로컬 보안 정책에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 설정 &gt; 계정 정책 &gt; 암호 정책 에서 “최대 암호 사용 기간” 확인</p>  |       |        |     |   |
| 조치 방법 | <p>최대 암호 사용 기간을 “90일”로 설정하고, 이 정책이 활성화 되기 위해 우선적으로 암호 사용 기간 제한을 없음으로 설정한다.</p> <p>※ 환경에 따라 30에서 90일마다(기본값: 42) 암호가 만료되도록 설정하는 것이 보안을 위해 가장 좋으며, 이 방법을 사용하면 침입자가 사용자의 암호를 도용하여 네트워크 리소스에 무단으로 액세스하는 횟수가 제한된다.</p>                                                                                                                                                                                                                                      |       |        |     |   |

## 1. 암호 사용 기간 제한 설정

제어판 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > Administrator  
마우스 우 클릭 > 속성 에서 “암호 사용 기간 제한 없음” 해제



## 2. 최대 암호 사용 기간 설정

[Windows 7]

### ■ 명령 프롬프트에서 설정

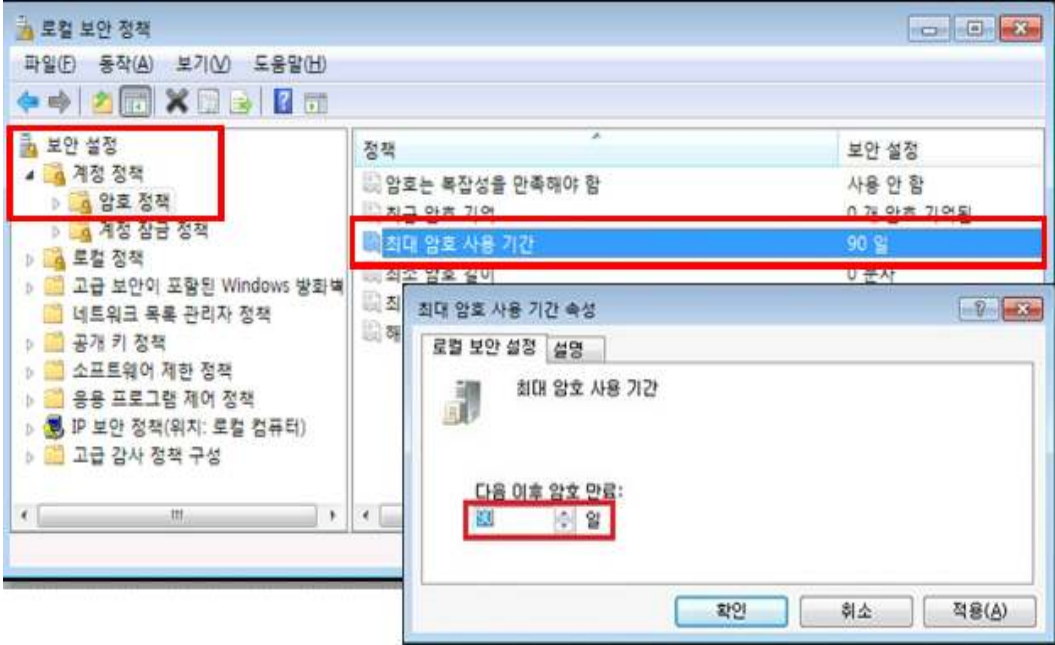
시작 > 실행 > cmd > net accounts /MAXPWAGE:90 명령어를 입력하여 설정

※ 명령 프롬프트(CMD)는 관리자 권한으로 실행해야 한다.

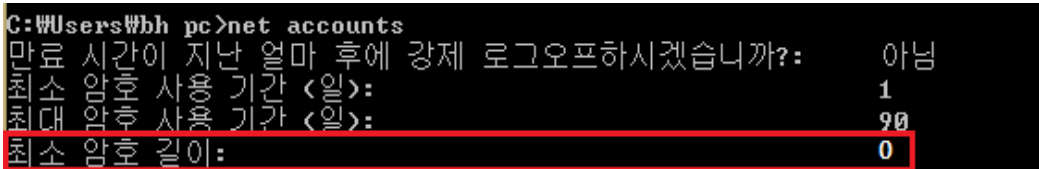
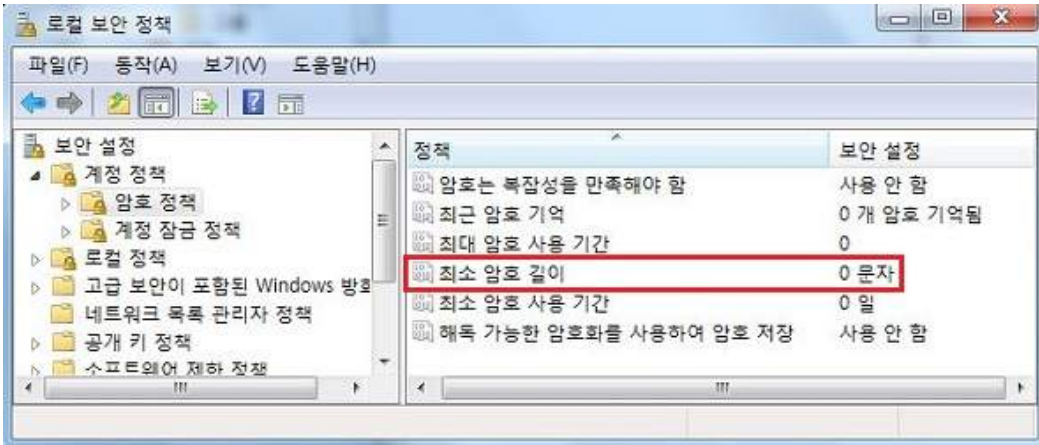


### ■ 로컬 보안 정책에서 설정

제어판 > 관리도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > “최대 암호 사용 기간” 정책의 속성 > “다음 이후 암호 만료” 값을 “90일” 로 설정

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the Windows Security Policy console. In the left-hand tree, 'Security Policies' is expanded, and 'Account Policies' is selected. The right-hand pane shows the 'Account Policies' list, with 'Maximum password age' highlighted. Below this, a dialog box titled 'Maximum password age' is open, showing the 'Local Security Settings' tab. The 'Maximum password age' is set to 90 days, and the 'Next password must be different from' checkbox is checked. The 'Apply' button is highlighted.</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

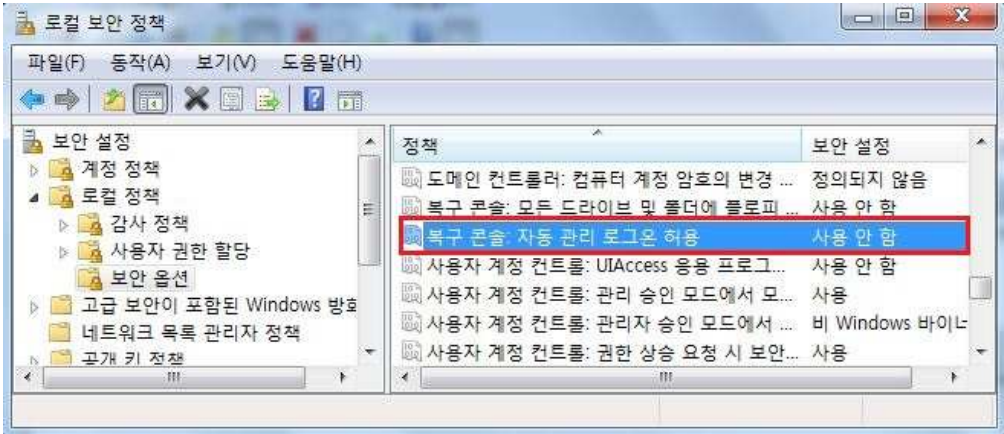
## 6.1.2. 비밀번호 정책이 해당 조직의 보안 정책에 적합하게 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | PC1-02 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | <p>대부분의 환경에서 3종류(영문·숫자·특수문자) 조합의 경우 8자리 비밀번호 사용, 2종류(영문·숫자) 조합의 경우 10자리 암호 사용을 권고하고 있다.</p> <p>비밀번호 정책에 적합하게 비밀번호가 설정된 경우 *무작위 대입 공격(Brute Force Attack)이나 비밀번호 추측 공격&gt;Password Guessing)에 대한 대비가 가능하다.</p> <p>* 무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.</p>                                                                                                                                                                                                                                                                                                    |       |        |     |   |
| 진단 기준 | <p>양호 - 최소 암호 길이가 해당 기관의 보안 정책을 반영하여 설정되어 있는 경우</p> <p>취약 - 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 비밀번호를 사용하고 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |     |   |
| 점검 방법 | <p>최소 암호 길이가 해당 기관의 보안 정책에 적합하게 설정되어 있는지 확인한다.<br/>[Windows 7]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net accounts 명령어를 실행하여 “최소 암호 길이” 확인</p>  <pre>C:\Users\Wbh pc&gt;net accounts 만료 시간이 지난 얼마 후에 강제 로그오프하시겠습니까?: 아님 최소 암호 사용 기간 &lt;일&gt;: 1 최대 암호 사용 기간 &lt;일&gt;: 90 최소 암호 길이: 0</pre> <p>■ 로컬 보안 정책에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 설정 &gt; 계정 정책 &gt; 암호 정책 &gt; “최소 암호 길이 속성” 값 확인</p>  |       |        |     |   |
| 조치 방법 | <p>최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정한다.<br/>[Windows 7]</p> <p>■ 명령 프롬프트에서 설정</p> <p>시작 &gt; 실행 &gt; cmd &gt; net accounts /MINPWLEN:8 명령어를 입력하여 “최소 암호 길이” 설정</p> <p>※ 명령 프롬프트(CMD)는 관리자 권한으로 실행해야 한다.</p>                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |

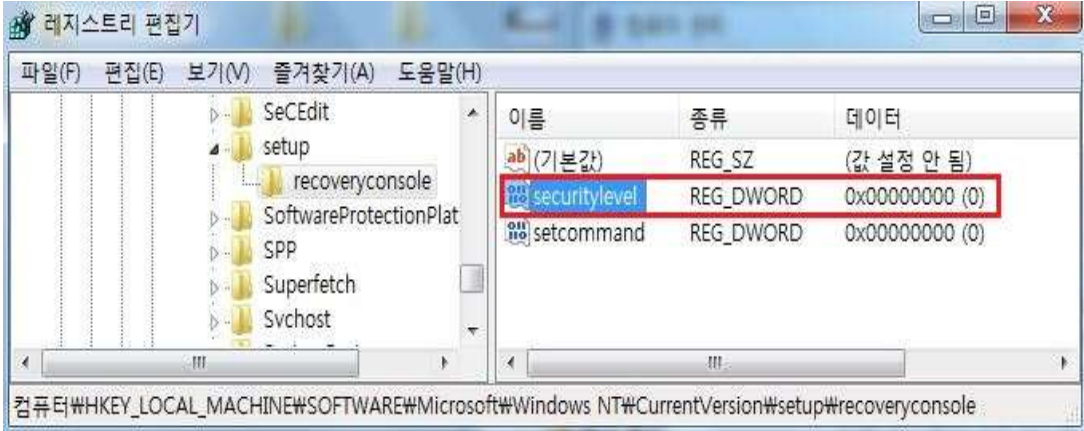
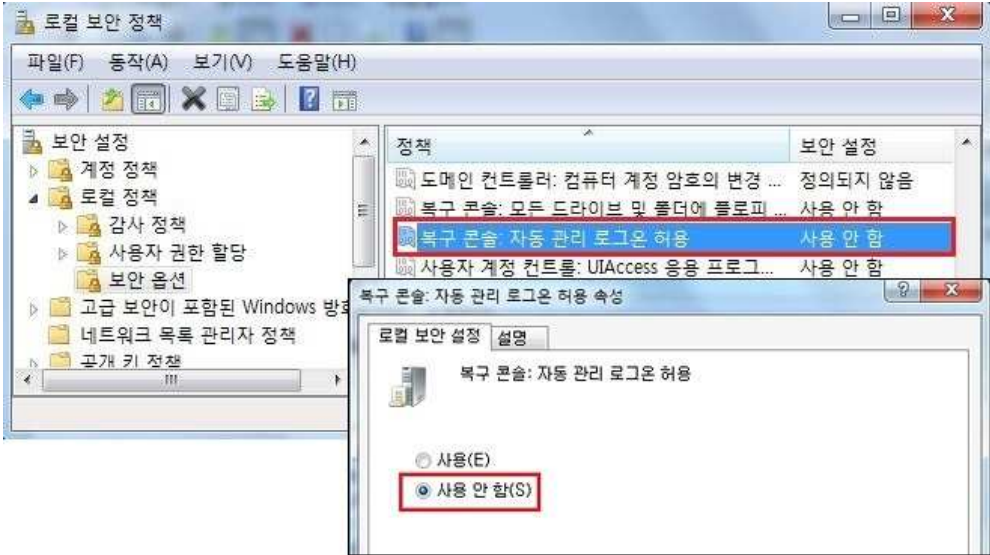
|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <div data-bbox="352 300 1310 436" data-label="Image"> </div> <p>■ 로컬 보안 정책에서 설정</p> <p>제어판 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 설정 &gt; 계정 정책 &gt; “최소 암호 길이” 정책의 속성 &gt; “암호에 필요한 최소 문자” 값을 “8문자” 로 설정</p> <div data-bbox="352 622 1453 1355" data-label="Image"> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>비고</p> | <p>&lt; 패스워드 설정 기준 &gt;</p> <ol style="list-style-type: none"> <li>영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정<br/>             ※ 다음 각 항목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성             <ol style="list-style-type: none"> <li>영문 대문자(26개)</li> <li>영문 소문자(26개)</li> <li>숫자(10개)</li> <li>특수문자(32개)</li> </ol> </li> <li>패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계             <ol style="list-style-type: none"> <li>(1) Null(공백) 패스워드 사용 금지</li> <li>(2) 문자 또는 숫자만으로 구성 금지</li> <li>(3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지</li> <li>(4) 연속적인 문자나 숫자 사용 (예) 1111, 1234, abcd) 사용 금지</li> <li>(5) 주기성 패스워드 재사용 금지</li> <li>(6) 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지</li> </ol> </li> </ol> |

|  |                                                                                                                                                                                                                                                                                                      |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>3. SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용을 권장 (8자로 이루어진 암호 사용 권장)</p> <p>4. 아래와 같은 암호 설정 지양<br/> Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명<br/> “root”, “rootroot”, “root123”, “123root”, “admin”, “admin123”, “123admin”, “osadmin”, “adminos”</p> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

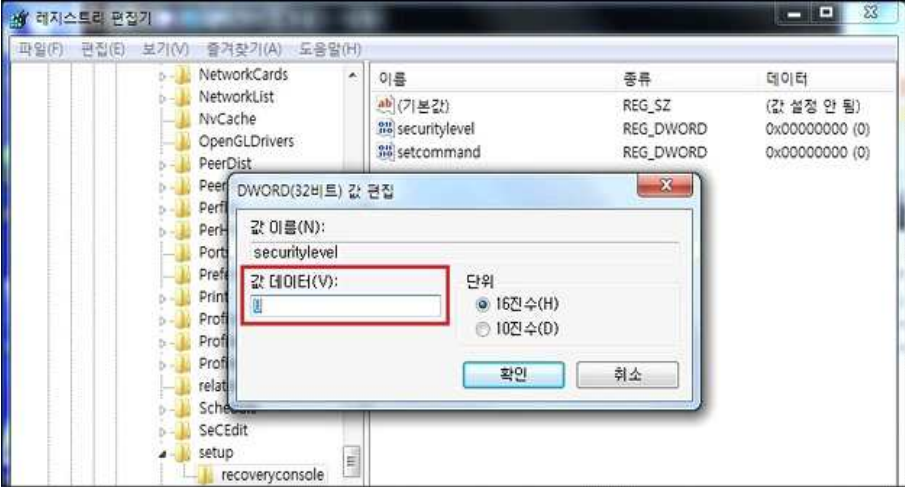
### 6.1.3. 복구 콘솔 자동 로그인 금지 설정

| 분류    | 계정관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | PC1-03 | 중요도 | M |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | <p>윈도우 *복구 콘솔(Recovery Console) 자동 로그인 설정은 시스템 액세스 허가 전 Administrator 계정의 암호 제공 여부를 결정하는 것으로 이 옵션을 사용하면 복구 콘솔에 암호를 입력하지 않아도 시스템에 자동으로 로그인 된다.</p> <p>이 경우 비인가자가 관리자 권한으로 시스템에 접근하여 주요 정보를 획득할 수 있는 위험이 존재한다.</p> <p>* 복구 콘솔(Recovery Console): 윈도우 2000, 윈도우 XP, 윈도우 서버 2003 운영 체제의 기능 가운데 하나로 윈도우가 그래픽 사용자 인터페이스(GUI)가 나타날 때까지 시동이 되지 않는 상황에서 관리자들이 복구할 수 있게 하는 것이 주된 기능이다.</p> <p>이 콘솔을 통해 관리자들이 명령 줄 인터페이스를 이용하여 제한된 영역의 작업을 수행할 수 있다.</p>                                                                                       |       |        |     |   |
| 진단 기준 | <p>양호 - 복구 콘솔 자동 로그인 허용이 “사용 안 함” 으로 설정되어 있는 경우</p> <p>취약 - 복구 콘솔 자동 로그인 허용이 “사용” 으로 설정되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 점검 방법 | <p>복구 콘솔 자동 로그인 허용 정책의 설정을 확인한다.</p> <p>[Windows 7]</p> <p>■ 로컬 보안 정책에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 설정 &gt; 로컬 정책 &gt; 보안 옵션 &gt; “복구 콘솔 : 자동 관리 로그인 허용” 정책의 설정 확인</p>  <p>■ 레지스트리에서 확인</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; regedit 입력</li> <li>다음 레지스트리 경로로 이동<br/>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole</li> <li>SecurityLevel 의 데이터 값 확인 (값이 0일 경우 양호)</li> </ol> |       |        |     |   |



|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 조치 방법 | <p>복구 콘솔 자동 로그인 허용 정책을 “사용 안 함” 으로 설정한다.<br/>[Windows 7]</p> <p>■ 로컬 보안 정책에서 설정</p> <p>제어판 &gt; 관리도구 &gt; 로컬 보안 정책 &gt; 보안 설정 &gt; 로컬 정책 &gt; 보안 옵션 &gt; “복구 콘솔 : 자동 관리 로그인 허용” 정책의 속성 에서 “사용 안 함” 설정</p>  <p>■ 레지스트리에서 설정</p> <ol style="list-style-type: none"> <li>1. 시작 &gt; 실행 &gt; regedit 입력</li> <li>2. 다음 레지스트리 경로로 이동<br/>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole</li> <li>3. SecurityLevel 의 데이터 값을 0 으로 설정</li> </ol> |

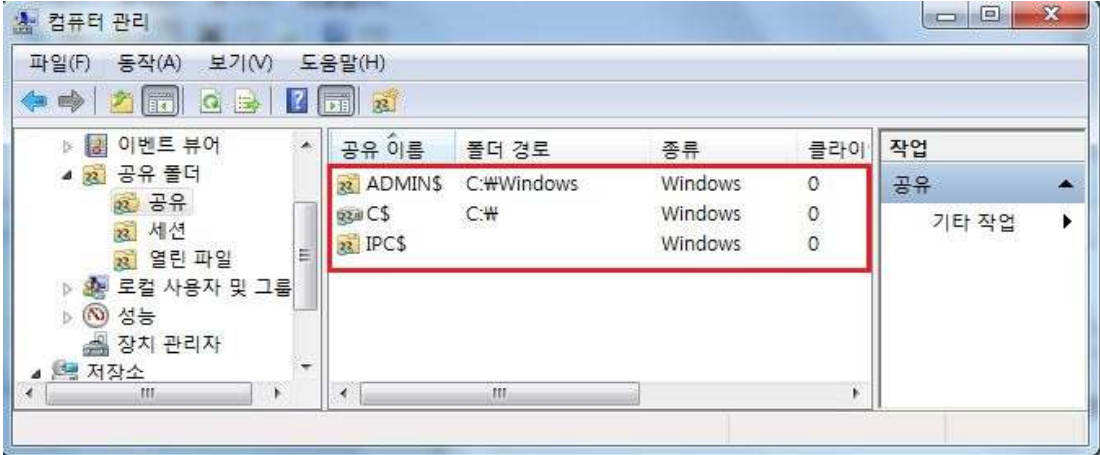
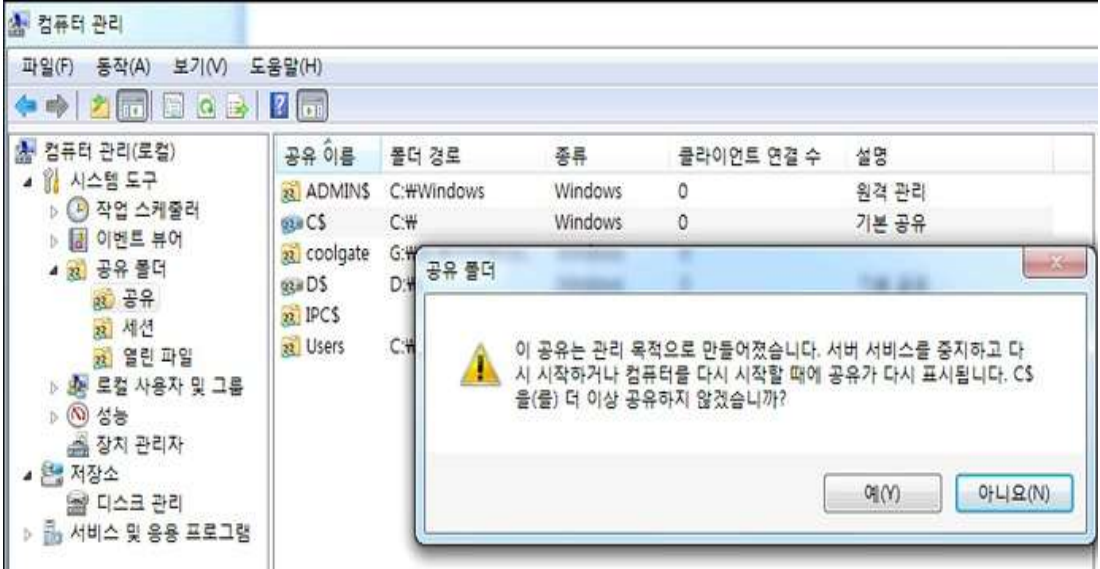


|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                    |

## 6.2. 서비스관리

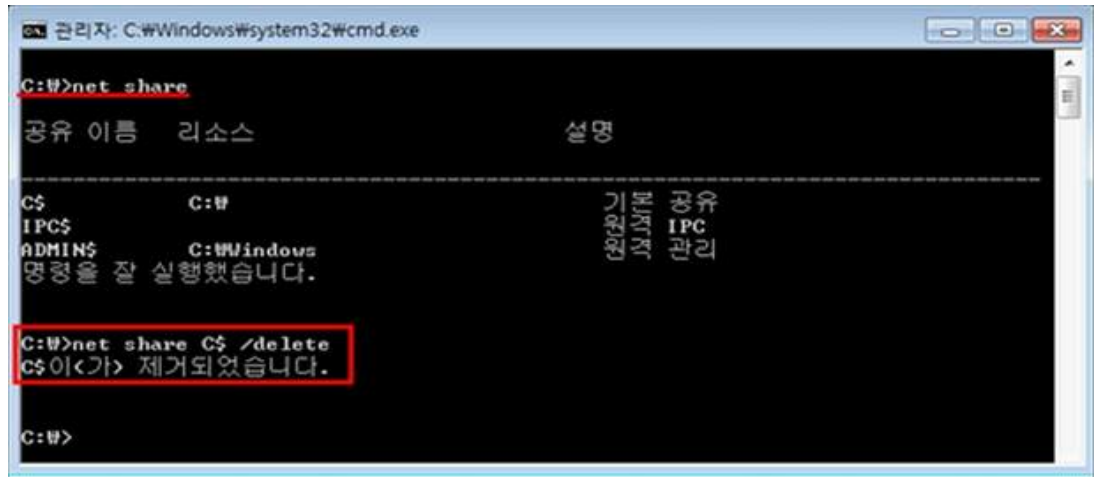
### 6.2.1. 공유 폴더 제거

| 분류      | 서비스관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드  | PC2-01 | 중요도 | H |       |     |    |         |             |       |       |  |        |     |     |       |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------|-----|---|-------|-----|----|---------|-------------|-------|-------|--|--------|-----|-----|-------|
| 대상      | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |        |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| 설명      | <p>시스템의 기본 공유 항목이 제거되지 않으면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있다. 2001년에 발생한 *Win32.Nimda 바이러스도 여러가지 방법 중에서 이러한 공유 기능 침투의 한 경로를 이용한 것이다.</p> <p>따라서 불필요한 공유라고 판단되면 공유를 해제해야 하며, 공유를 해제한 후에 레지스트리 AutoShareServer 값 설정을 통해 재부팅 시 기본 공유 폴더의 자동 공유 설정을 방지할 수 있다. (하드디스크 기본 공유 폴더 예: C\$, D\$, Admin\$, IPC\$ 등)</p> <p>또한, 기본 공유 폴더를 제외한 일반 공유 폴더의 권한이 Everyone으로 설정되었는지 확인하고, 공유 금지 설정을 통해 익명 사용자에게 의한 접근을 차단해야 한다.</p> <p>*Win32.Nimda 바이러스: 2001년 9월 17일 미국·유럽·라틴아메리카에서 동시에 발생한 뒤 한국에서도 다음 날 저녁 발견될 정도로 빠르게 확산하는 악성 컴퓨터 바이러스이다. 두 종류가 있는데, 하나는 정부를 뜻하는 영어 단어 'admin'의 철자를 거꾸로 나열해 명명한 것이고, 다른 하나는 제3차 세계대전을 뜻하는 'To 3W'를 거꾸로 나열한 'W32' 이다. 이 바이러스는 이메일 뿐만 아니라 감염된 웹 사이트를 통해서도 전염되며, 네트워크 상에서 패스워드 없이 읽기·쓰기가 가능한 공유 디렉터리를 통해서도 감염되는 특징을 가진다.</p> |        |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| 진단 기준   | <p>양호 - 불필요한 공유 폴더가 존재하지 않는 경우</p> <p>취약 - 불필요한 공유 폴더가 존재하는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| 점검 방법   | <p>불필요한 기본 공유 폴더 및 일반 공유 폴더가 존재하는지 확인한다.</p> <p>[Windows 7]</p> <p>■ 명령 프롬프트에서 확인</p> <p>시작 &gt; 실행 &gt; cmd &gt; net share 명령어를 입력하여 불필요한 공유 폴더 확인</p> <div><div>C:₩&gt;net share</div><table><tr><th>공유 이름</th><th>리소스</th><th>설명</th></tr><tr><td>ADMIN\$</td><td>C:₩₩WINDOWS</td><td>원격 관리</td></tr><tr><td>IPC\$</td><td></td><td>원격 IPC</td></tr><tr><td>C\$</td><td>C:₩</td><td>기본 공유</td></tr></table></div> <p>■ 컴퓨터 관리에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유 에서 불필요한 공유 폴더 확인</p>                                                                                                                                                                                                                                 |        |        |     |   | 공유 이름 | 리소스 | 설명 | ADMIN\$ | C:₩₩WINDOWS | 원격 관리 | IPC\$ |  | 원격 IPC | C\$ | C:₩ | 기본 공유 |
| 공유 이름   | 리소스                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 설명     |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| ADMIN\$ | C:₩₩WINDOWS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 원격 관리  |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| IPC\$   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 원격 IPC |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |
| C\$     | C:₩                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 기본 공유  |        |     |   |       |     |    |         |             |       |       |  |        |     |     |       |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 조치 방법 | <p>기본 공유 폴더 및 일반 공유 폴더 존재 시 제거하고, 재부팅 후 자동 공유 되지 않도록 설정한다.</p> <p>&lt; 공유 폴더 설정 기준 &gt;</p> <ol style="list-style-type: none"> <li>1. C\$, D\$, Admin\$ 등의 기본 공유 폴더 제거</li> <li>2. 기본 공유 폴더 제거 후 시스템 재부팅 시 “기본 공유 폴더가 자동으로 공유되는 것”을 방지하기 위해 해당 레지스트리의 AutoShareServer 값을 “0”으로 설정</li> <li>3. 일반 공유 폴더 사용 시 공유 폴더 접근 권한에 “Everyone” 제거</li> <li>4. 일반 공유 폴더 사용 시 접근이 필요한 계정에만 적절한 (읽기, 변경)권한 설정</li> <li>5. 일반 공유 폴더 사용 시 공유 폴더 접근을 위한 암호 설정</li> </ol> <p>[Windows 7]</p> <ol style="list-style-type: none"> <li>1. C\$, D\$, Admin\$ 등의 기본 공유 폴더 제거</li> </ol> <p>■ 컴퓨터 관리에서 기본 공유 중지</p> <p>제어판 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 공유 폴더 &gt; 공유 &gt; 불필요한 공유 폴더 우클릭 &gt; 공유 중지 (하드디스크 기본 공유 폴더는 C\$, D\$, Admin\$, IPC\$ 가 있으며, C\$, D\$, Admin\$ 폴더의 공유 제거)</p>  |

■ 명령 프롬프트에서 기본 공유 중지

시작 > 실행 > cmd > net share “삭제할 공유 폴더명” /delete 명령을 통해 공유 디렉터리 삭제



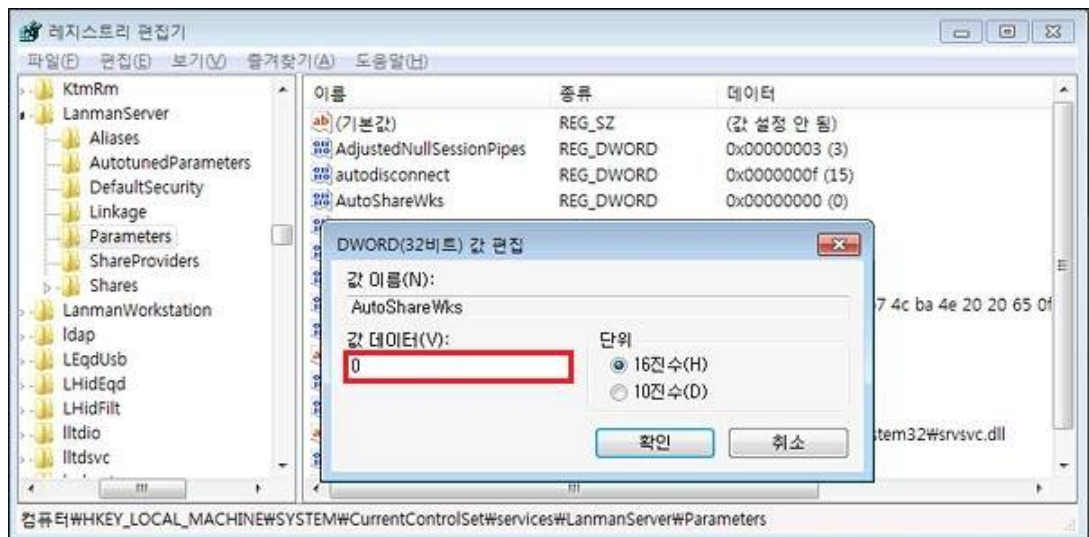
2. 시스템 재부팅 시 기본 공유 폴더 자동 공유 방지 설정

① 시작 > 실행 > regedit 입력

② 다음 레지스트리 경로로 이동

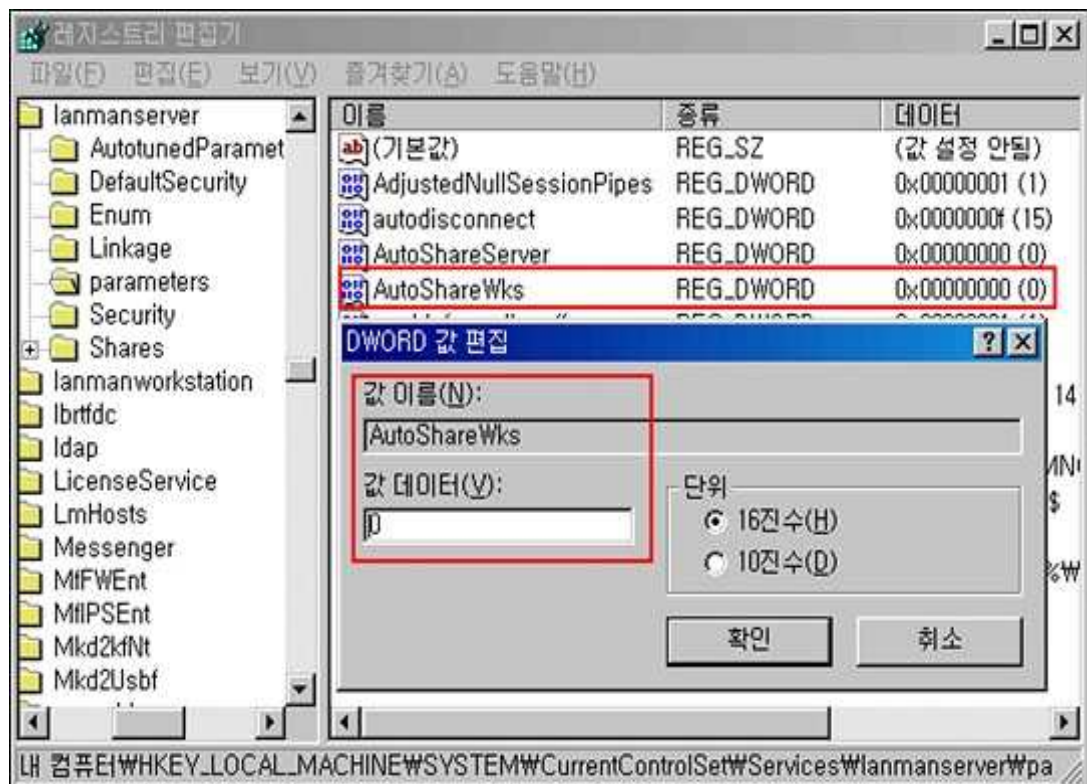
HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

③ AutoShareWks의 데이터 값을 0으로 설정



④ 값이 없는 경우,

아래 그림과 같이 새로 만들기 > “DWORD 값” 선택하고 AutoShareServer(또는 AutoShareWks)를 추가하여 값을 “0”으로 입력



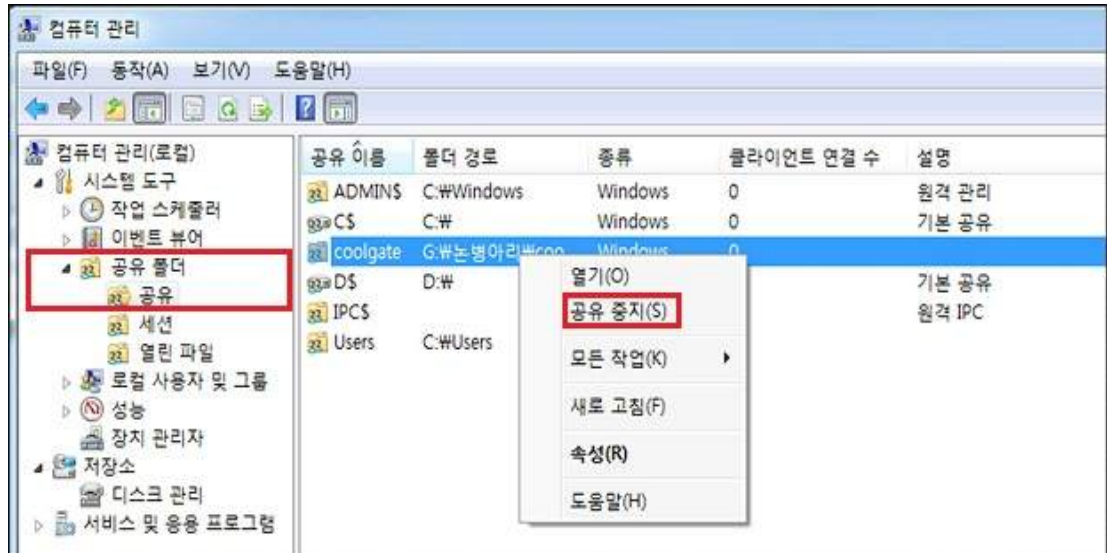
※ 기본 공유에 대한 조치 시 반드시 [기본 공유 삭제], [비활성화 레지스트리 값]을 모두 설정해야 한다.

### 3. 불필요한 일반 공유 폴더 제거

■ 컴퓨터 관리에서 일반 공유 중지



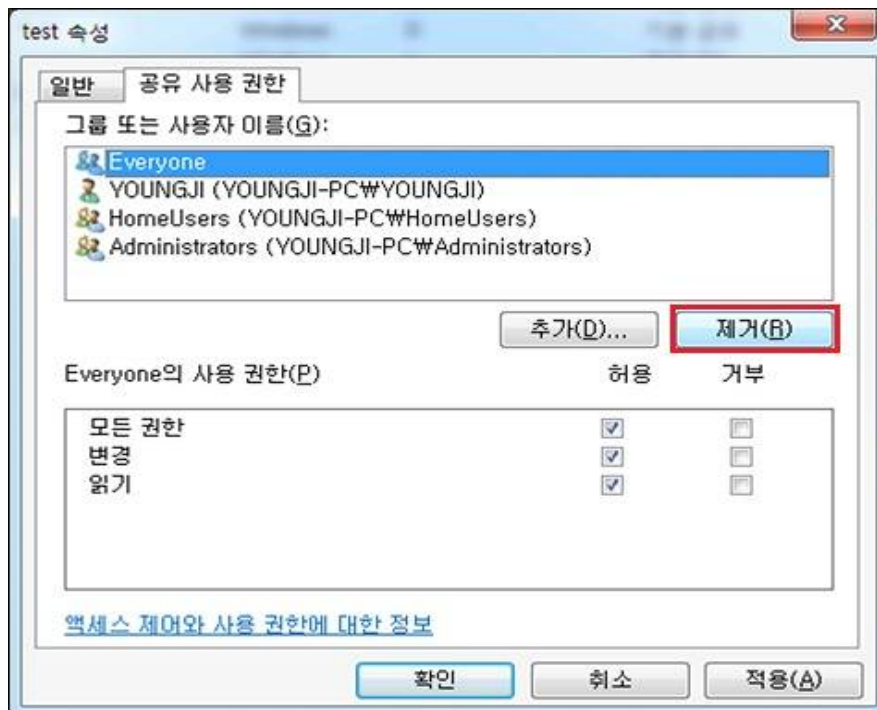
제어판 > 관리도구 > 컴퓨터 관리 > 공유 폴더 > 공유 > 불필요한 공유 폴더 우클릭 > 공유 중지



#### 4. 일반 공유 폴더 사용 시 접근 권한 설정

##### ① 일반 공유 폴더에 Everyone 공유 제거

제어판 > 관리 도구 > 컴퓨터 관리 > 공유 폴더 > 공유 > 사용할 공유 폴더 우클릭 > 속성 > [공유 사용 권한] 탭 에서 “Everyone” 으로 된 공유를 제거하고, 접근이 필요한 계정에만 적절한 권한 추가

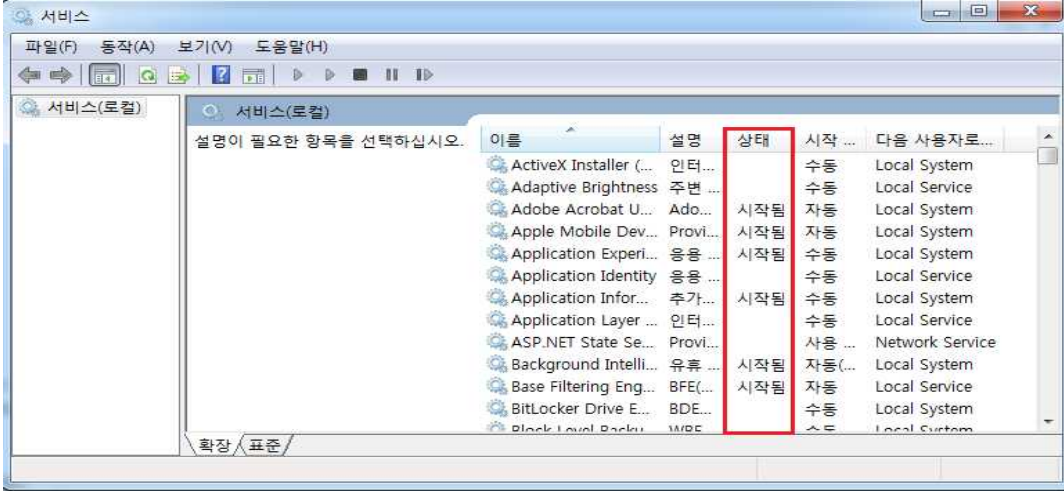


##### ② 공유 폴더의 접근 암호 설정

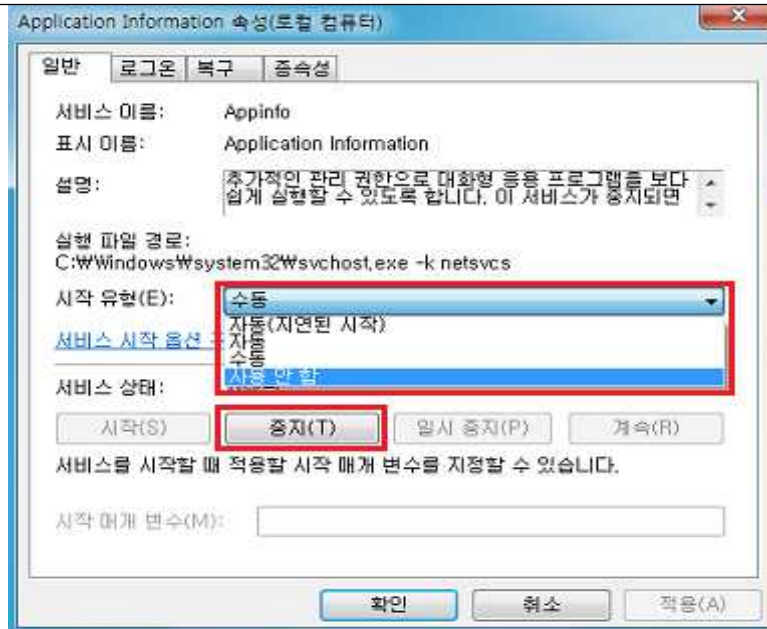
제어판 > 네트워크 및 공유 센터 > 고급 공유 설정 에서 “암호 보호 공유 켜기” 설정

|                  |                                                                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <div data-bbox="349 318 1458 788" data-label="Image"> </div> <p>③ 공유 폴더 접근 가능 여부 확인</p> <p>시작 &gt; 실행 &gt; 공유 폴더 PC 계정명 또는 IP 주소 입력 후 패스워드 입력 팝업 확인</p> <div data-bbox="349 927 1458 1308" data-label="Image"> </div> |
| <p><b>비고</b></p> | <ul style="list-style-type: none"> <li>- 업무에 필요한 공유 폴더 사용 시 사용자별 권한 부여 필요</li> <li>- 방화벽과 라우터에서 135,139(TCP/UDP)포트를 차단하여 외부로부터 위험을 제거함으로써 보안성을 높일 수 있다.</li> </ul>                                                    |

## 6.2.2. 불필요한 서비스 제거

| 분류    | 서비스관리                                                                                                                                                                                                                                               | 항목 코드 | PC2-02 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                           |       |        |     |   |
| 설명    | <p>불필요한 서비스가 시스템에 디폴트로 설치되어 실행되는 경우 시스템 자원을 낭비하게 될 뿐만 아니라, 이 서비스를 통해 악의적인 공격자가 침입할 수 있으므로 필요하지 않은 서비스는 중지시켜야 한다.</p> <p>시스템 관리자는 대상 시스템의 용도를 정확히 파악한 후 특별한 목적으로 사용하는 업무 관련 서비스를 제외한 다른 불필요한 서비스를 제거해야 한다.</p>                                       |       |        |     |   |
| 진단 기준 | <p>양호 - 업무에 필요한 서비스만 실행되고 있는 경우</p> <p>취약 - 디폴트로 설치된 서비스가 실행되고 있는 경우</p>                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>업무에 불필요한 서비스가 실행되고 있는지 확인한다.</p> <p>[Windows 7]</p> <p>■ 서비스에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 서비스 &gt; 해당 서비스 상태를 확인하여 불필요한 서비스가 실행 중인지 확인</p>                  |       |        |     |   |
| 조치 방법 | <p>업무에 불필요한 서비스를 중지시키고, 시작 유형을 “사용 안 함”으로 설정한다.</p> <p>[Windows 7]</p> <p>■ 서비스에서 설정</p> <ol style="list-style-type: none"> <li>제어판 &gt; 관리도구 &gt; 서비스 &gt; 해당 서비스 선택 &gt; 속성 &gt; [일반] 탭</li> <li>불필요한 서비스 → 중지</li> <li>시작 유형 → 사용 안 함</li> </ol> |       |        |     |   |





※ 해당 서비스의 속성에서 “시작 유형” 선택 및 “시작 시 로그인 계정” 별도 설정이 가능하다.

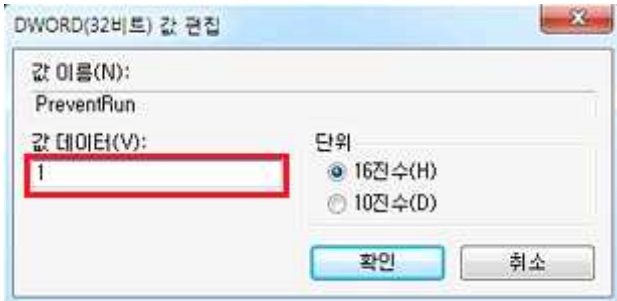
| 서비스 시작 유형 | 설 명                                    |
|-----------|----------------------------------------|
| 사용 안 함    | 설치되어 있으나 실행되지 않음                       |
| 수동        | 다른 서비스나 응용 프로그램에서 당 기능을 필요로 할 때만 시작됨   |
| 자동        | 부팅 시에 해당 장치 드라이버가 로드된 후에 운영 체제에 의해 시작됨 |

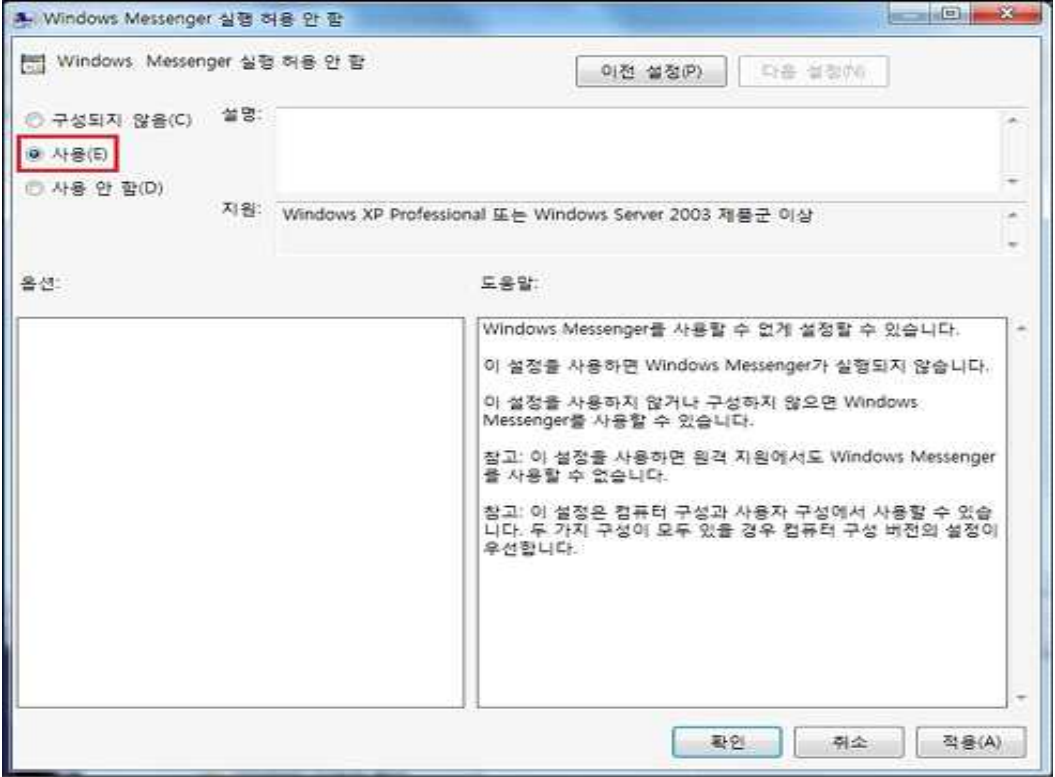
#### # 서비스 리스트

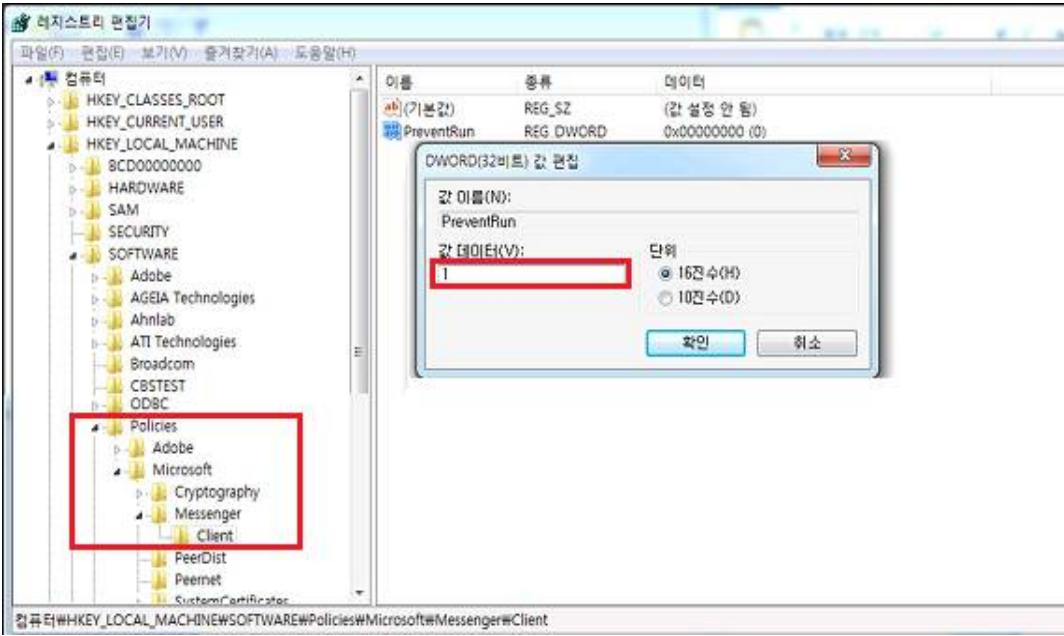
| 서비스 리스트                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 불필요한 서비스 리스트                                                                                                                                                                                                                                                                  | Windows 운영을 위한 최소한의 서비스                                                                                                                                                                                                                                                         |
| <ul style="list-style-type: none"> <li>- Alerter</li> <li>- Clipboard</li> <li>- ComputerBrowser</li> <li>- DHCP Client</li> <li>- FTP Publishing Service</li> <li>- InternetConnectionSharingService</li> <li>- IndexingService</li> <li>- InfraredMonitorService</li> </ul> | <ul style="list-style-type: none"> <li>- Logical Logging Manager</li> <li>- NetworkConnections</li> <li>- NTLMSecuritySupportProvider</li> <li>- PlugandPlay</li> <li>- Server</li> <li>- Workstation</li> <li>- RemoveableStrage</li> <li>- SecurityAccountsManager</li> </ul> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                 |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <ul style="list-style-type: none"> <li>- Messenger</li> <li>- NetLogon</li> <li>- Network DDE</li> <li>- Network DDE DSDM</li> <li>- NetMeetingRemoteDesktopSharingService</li> <li>- Print spooler</li> <li>- RemoteRegistryService</li> <li>- RoutingandRemoteAccessService</li> <li>- SimpleTCP/IPService</li> <li>- SMTPService</li> <li>- TaskSchedulerService</li> <li>- TCPIP NetBIOS Helper</li> <li>- TerminalService</li> </ul> | <ul style="list-style-type: none"> <li>- WindowsManagementInstrumentation</li> <li>- WindowsManagem nt Instrumentation driver extensions</li> <li>- WMDMPMSPService</li> <li>- ApplicationManagement</li> </ul> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                 |

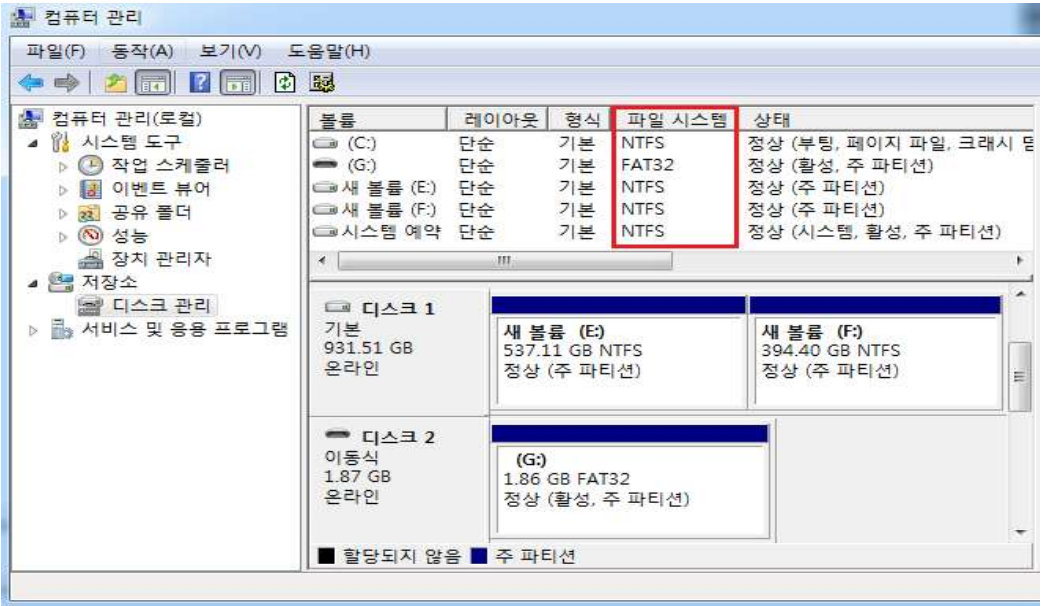
### 6.2.3. Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지

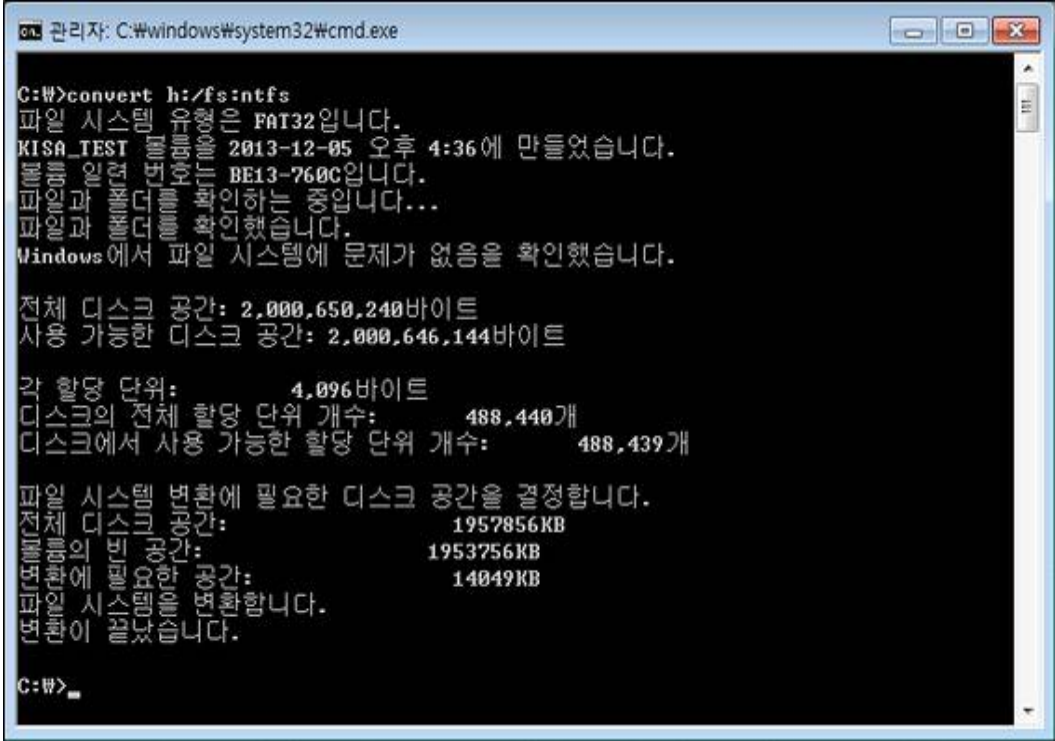
| 분류    | 서비스관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | PC2-03 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 설명    | <p>일반 사용자 PC에서 Windows Messenger를 사용할 경우, *메신저(Messenger)를 통해서 주요 정보가 유출될 수 있을 뿐만 아니라 *악성코드가 유입될 수 있음.</p> <p>* 메신저(Messenger): 인터넷을 통해 실시간으로 대화를 나눌 수 있는 서비스.</p> <p>* 악성코드: 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 진단 기준 | <p>양호 - Windows Messenger가 실행되고 있지 않은 경우</p> <p>취약 - Windows Messenger가 실행되고 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |     |   |
| 점검 방법 | <p>Windows Messenger가 실행되고 있는지 확인한다.</p> <p>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 확인</p> <p>시작 &gt; 실행 &gt; gpedit.msc 입력 &gt; 컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; Windows Messenger 에서 “Windows Messenger를 실행 허용 안 함” 확인 (“사용” 으로 설정되어 있는 경우 양호)</p>  <p>■ 레지스트리에서 확인</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; regedit 입력</li> <li>다음 레지스트리 경로로 이동<br/>HKLM\Software\Policies\Microsoft\Messenger\Client</li> <li>PreventRun 의 데이터 값이 1로 설정되어 있는지 확인 (1일 경우 양호)</li> </ol>  |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>Windows Messenger를 실행하지 않음 으로 설정<br/>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 설정</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; gpedit.msc 입력 &gt; 컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; Windows Messenger</li> <li>“Windows Messenger를 실행 허용 안 함” 정책 마우스 우클릭 &gt; 편집 에서 “사용” 으로 설정</li> </ol>  <p>■ 레지스트리에서 설정</p> <ol style="list-style-type: none"> <li>시작 &gt; 실행 &gt; regedit 입력</li> <li>다음 레지스트리 경로로 이동<br/>HKLM\Software\Policies\Microsoft\Messenger\Client</li> <li>PreventRun 마우스 우 클릭 &gt; 수정 에서 값 데이터를 1로 설정</li> </ol> |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the Windows Registry Editor with the following tree structure:</p> <ul style="list-style-type: none"> <li>컴퓨터             <ul style="list-style-type: none"> <li>HKEY_CLASSES_ROOT</li> <li>HKEY_CURRENT_USER</li> <li>HKEY_LOCAL_MACHINE                     <ul style="list-style-type: none"> <li>8CD0000000</li> <li>HARDWARE</li> <li>SAM</li> <li>SECURITY</li> <li>SOFTWARE                             <ul style="list-style-type: none"> <li>Adobe</li> <li>AGEIA Technologies</li> <li>Ahnlab</li> <li>ATI Technologies</li> <li>Broadcom</li> <li>CBSTEST</li> <li>ODBC</li> <li>Policies                                     <ul style="list-style-type: none"> <li>Adobe</li> <li>Microsoft                                             <ul style="list-style-type: none"> <li>Cryptography</li> <li>Messenger                                                     <ul style="list-style-type: none"> <li>Client</li> </ul> </li> <li>PeerDist</li> <li>Peernet</li> <li>SystemCertificates</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>The 'PreventRun' value is highlighted in the list, and the 'DWORD(32비트) 값 편집' dialog box shows the value '1'.</p> |
| 비고 | <p>Windows Messenger 사용 불가<br/>원격 지원에서도 Windows Messenger를 사용할 수 없음</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

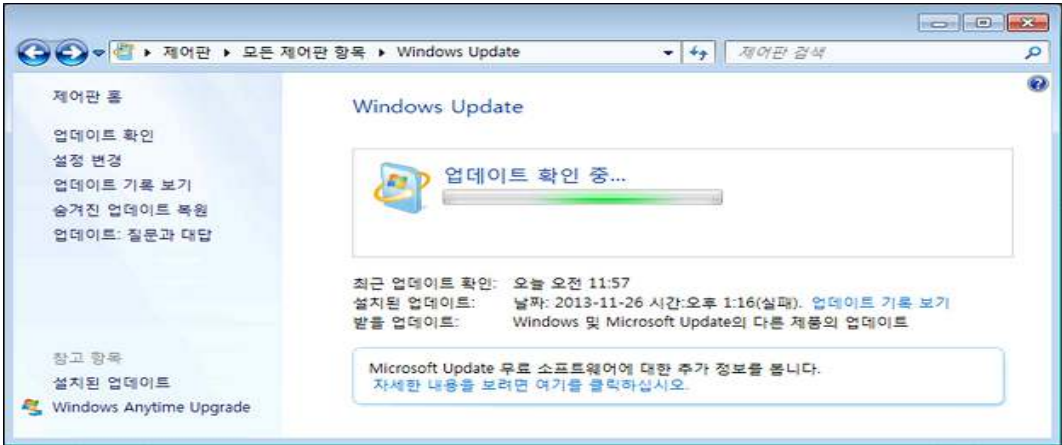
## 6.2.4. 파일 시스템을 NTFS로 포맷

| 분류    | 서비스관리                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | PC2-04 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                |       |        |     |   |
| 설명    | <p>*NTFS 파일 시스템은 포맷 시 모든 파일과 디렉터리에 소유권과 사용 권한 설정이 가능하고 ACL(접근 통제 목록)을 제공함으로써 *FAT32 파일 시스템에 비해 보다 강화된 보안 기능을 제공한다.</p> <p>기존에 FAT 파일 시스템을 사용하다가 NTFS로 변환하기 위해서는 convert.exe 명령을 사용할 수 있지만 FAT 파일 시스템으로 운영 중 변환해야 하는 경우 Default ACL이 적용되지 않으므로 가능한 초기 설치 시 NTFS 파일 시스템을 선택하는 것을 권장한다.</p> <p>*NTFS, FAT32 파일 시스템 비교: FAT32에는 NTFS가 제공하는 보안 기능이 없으므로 컴퓨터에 FAT32 파티션 또는, 볼륨이 있는 경우 컴퓨터에 액세스 가능한 모든 사용자가 파일을 읽을 수 있으며 FAT32에는 크기 제한이 있다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 모든 디스크 볼륨의 파일 시스템이 NTFS인 경우</p> <p>취약 - 모든 디스크 볼륨의 파일 시스템이 FAT32인 경우</p>                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |
| 점검 방법 | <p>디스크 볼륨의 파일 시스템이 NTFS 인지 확인한다.</p> <p>[Windows 7]</p> <p>■ 컴퓨터 관리에서 확인</p> <p>제어판 &gt; 관리도구 &gt; 컴퓨터 관리 &gt; 저장소 &gt; 디스크 관리 에서 파일 시스템 확인</p>                                                                                                                                                                                                      |       |        |     |   |
| 조치 방법 | <p>모든 디스크 볼륨에 대해 파일 시스템 NTFS로 변경한다.</p> <p>[Windows 7]</p> <p>■ 명령 프롬프트에서 설정</p> <p>시작 &gt; 실행 &gt; cmd 입력 &gt; “convert 드라이브명:/fs:ntfs” 입력</p> <p>※ 관리자 권한으로 명령 프롬프트 실행</p> <p>(예) convert h: /fs:ntfs 입력하면 H 드라이브는 NTFS 형식으로 포맷됨</p>                                                                                                                                                                                                   |       |        |     |   |

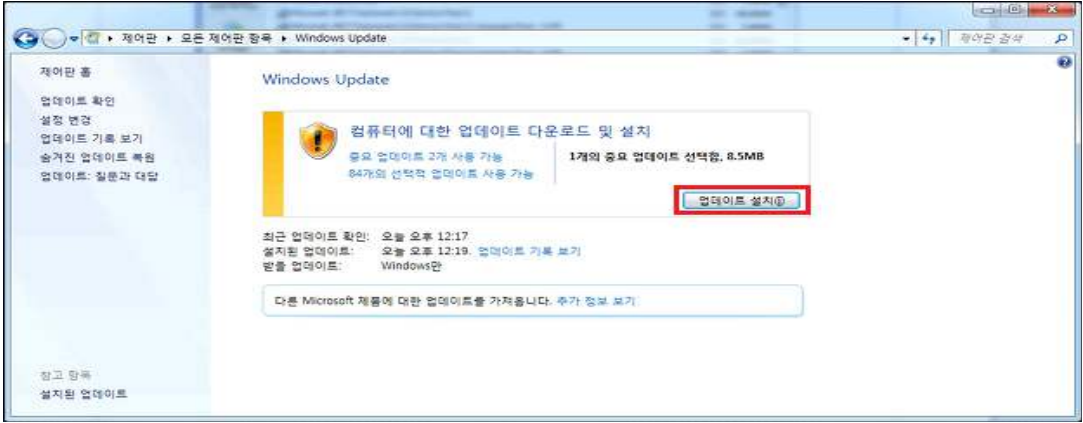
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <pre> ca. 관리자: C:\windows\system32\cmd.exe  C:\W&gt;convert h:/fs:ntfs 파일 시스템 유형은 FAT32입니다. KISA_TEST 볼륨을 2013-12-05 오후 4:36에 만들었습니다. 볼륨 일련 번호는 BE13-760C입니다. 파일과 폴더를 확인하는 중입니다... 파일과 폴더를 확인했습니다. Windows에서 파일 시스템에 문제가 없음을 확인했습니다.  전체 디스크 공간: 2,000,650,240바이트 사용 가능한 디스크 공간: 2,000,646,144바이트  각 할당 단위: 4,096바이트 디스크의 전체 할당 단위 개수: 488,440개 디스크에서 사용 가능한 할당 단위 개수: 488,439개  파일 시스템 변환에 필요한 디스크 공간을 결정합니다. 전체 디스크 공간: 1957856KB 볼륨의 빈 공간: 1953756KB 변환에 필요한 공간: 14049KB 파일 시스템을 변환합니다. 변환이 끝났습니다.  C:\W&gt;         </pre> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## 6.3. 패치관리

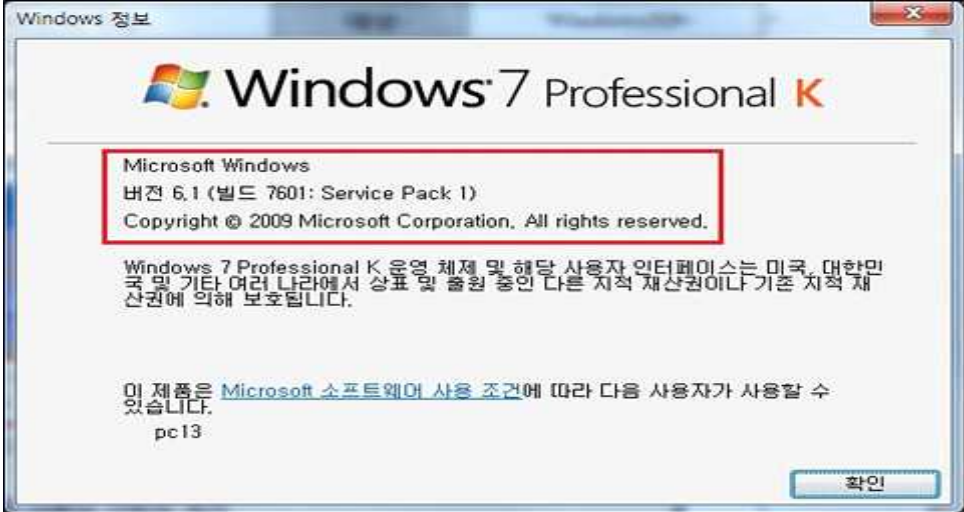
### 6.3.1. HOT FIX 등 최신 보안패치

| 분류    | 패치관리                                                                                                                                                                                                                                                                                                                             | 항목 코드 | PC3-01 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | <p>*HOT FIX 설치 및 자동 *업데이트가 설정되어 있지 않은 경우 취약점으로 인한 공격이 발생할 수 있으므로 Hot Fix 출시 즉시 신속하게 설치하고 항상 최신의 보안 업데이트가 이루어져야 한다.</p> <p>*Hot Fix: 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련)을 패치하기 위해 배포되는 프로그램으로 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표된다.</p> <p>*업데이트(Update): 문제를 예방 또는 해결하거나 컴퓨터 작동 방식을 향상시키거나 컴퓨팅 경험을 향상시킬 수 있도록 추가되는 소프트웨어를 말한다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - HOT FIX 설치 및 자동 업데이트 설정이 되어 있는 경우</p> <p>취약 - HOT FIX가 설치되어 있지 않은 경우</p>                                                                                                                                                                                                                                                 |       |        |     |   |
| 점검 방법 | <p>시스템의 최신 패치 여부를 확인한다.</p> <p>[Windows 7]</p> <p>제어판 &gt; Windows Update &gt; “업데이트 확인” 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인</p>                                                                                                             |       |        |     |   |
| 조치 방법 | <p>HOT FIX, 최신 보안 업데이트 등을 설치한다.</p> <p>[Windows 7]</p> <p>제어판 &gt; Windows Update &gt; “업데이트 확인”, “설정 변경”, “업데이트 기록 보기”를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경</p>                                                                                                                                                         |       |        |     |   |



|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>The screenshot shows the Windows Update interface. On the left, there is a sidebar with links like '업데이트 확인' (Check for updates), '설정 변경' (Change settings), '업데이트 기록 보기' (View update history), '숨겨진 업데이트 확인' (Check for hidden updates), and '업데이트: 질문과 대답' (Updates: Questions and answers). The main area displays 'Windows Update' with a yellow banner stating '컴퓨터에 대한 업데이트 다운로드 및 설치' (Download and install updates for your computer). Below the banner, it says '중요 업데이트 2개 사용 가능' (2 important updates available) and '64개의 선택적 업데이트 사용 가능' (64 optional updates available). A box indicates '1개의 중요 업데이트 선택됨, 8.5MB' (1 important update selected, 8.5MB). The '업데이트 설치' button is highlighted with a red rectangle. Below this, it shows '최근 업데이트 확인: 오늘 오후 12:17' (Check for updates: Today at 12:17 PM), '숨겨진 업데이트: 오늘 오후 12:19, 업데이트 기록 보기' (Hidden updates: Today at 12:19 PM, View update history), and '받은 업데이트: Windows만' (Updates received: Windows only). At the bottom, there is a link '다른 Microsoft 제품에 대한 업데이트를 가져옵니다. 추가 정보 보기' (Get updates for other Microsoft products. View more information).</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### 6.3.2. 최신 서비스팩 적용

| 분류    | 패치관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 항목 코드 | PC3-02 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |        |     |   |
| 설명    | <p>최신 *서비스팩을 적용하지 않을 경우, 공격에 쉽게 노출될 수 있다.</p> <p>*서비스팩 : Windows 시스템을 마이크로소프트에서 출시하고 난 뒤 Windows와 관련된 응용프로그램, 서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 프로그램을 말한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 진단 기준 | <p>양호 - 최신 서비스팩이 적용 되어 있는 경우</p> <p>취약 - 최신 서비스팩이 적용 되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 점검 방법 | <p>최신 서비스팩이 설치되어 있는지 확인한다.</p> <p>[Windows 7]</p> <p>시작&gt; 실행&gt; “winver” 입력&gt; Windows 정보 확인</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 조치 방법 | <p>최신 서비스팩을 설치한다.</p> <p>[Windows 7]</p> <p>서비스팩 확인 후 최신 버전이 아닐 경우 Microsoft 홈페이지에서 다운로드 하여 설치 (현재까지 발표된 최신의 Windows XP의 서비스팩은 SP3 이며, Windows 7은 SP1)</p> <p>※ 아래의 Microsoft 홈페이지에서 다운로드 받을 수 있다.</p> <p><a href="http://windows.microsoft.com/ko-kr/windows/service-packs-download#sptabs=win7">http://windows.microsoft.com/ko-kr/windows/service-packs-download#sptabs=win7</a></p> <p>※ 네트워크와 분리된 상태에서 서비스팩 설치를 권장</p> <p>현재 많은 인터넷 *웜(Worm)이 Windows의 취약점을 이용하여 공격하므로 OS 설치 후 곧바로 네트워크에 연결하는 것은 서버에 피해를 입을 수 있다.</p> <p>*웜(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와는 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말한다.</p> |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |

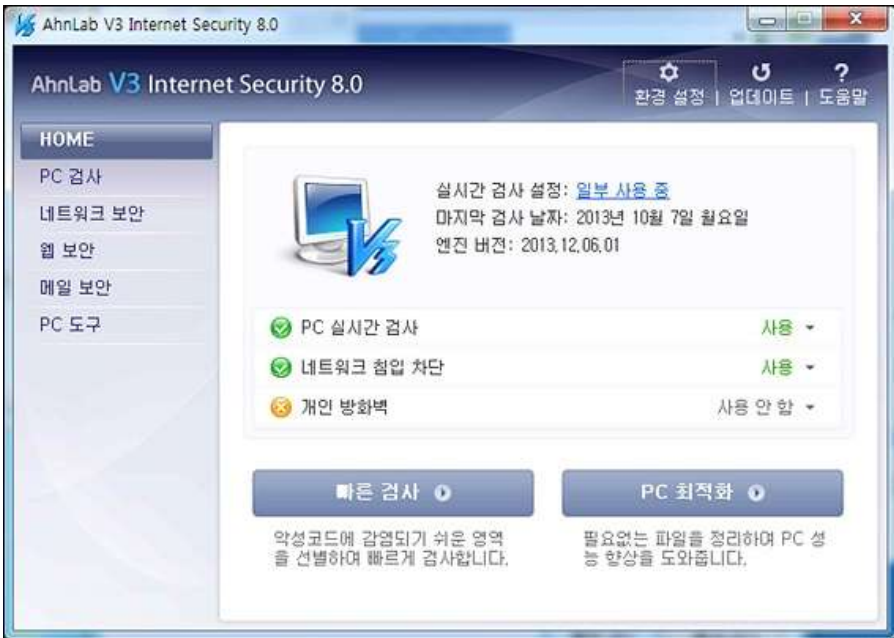
## 6.4. 보안관리

### 6.4.1. 바이러스 백신 프로그램 설치 및 주기적 업데이트

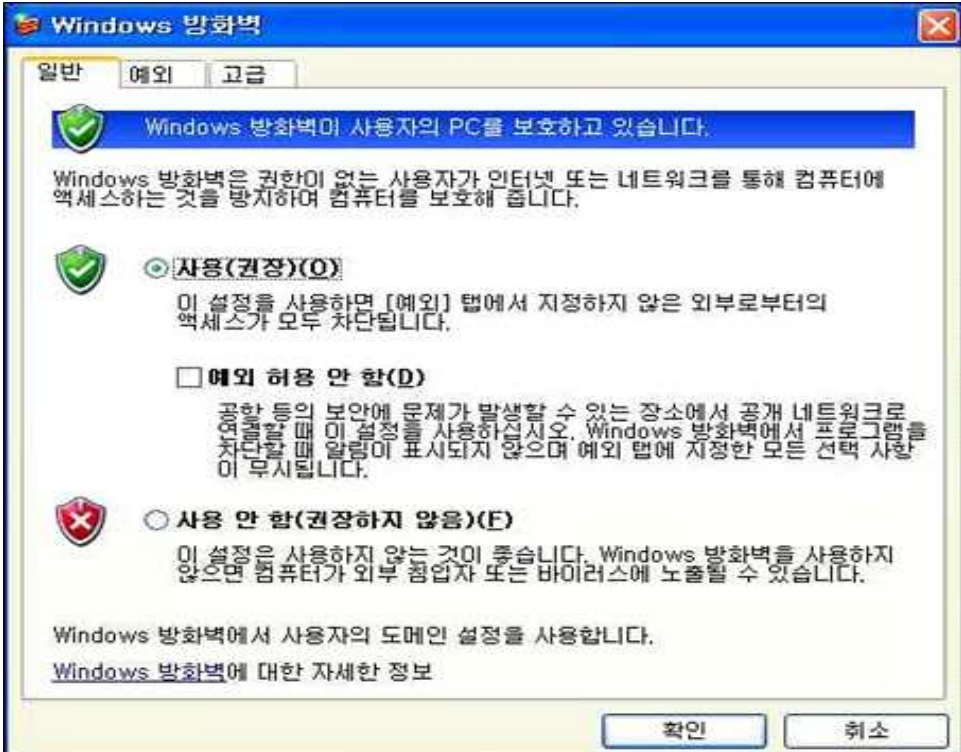
| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | PC4-01 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 설명    | <p>바이러스 백신 프로그램은 *바이러스, *웜 등으로부터 시스템을 보호하기 위한 중요한 보안 요소이다. 최신 바이러스 탐지를 위하여 패턴 업데이트가 자주 발생하므로 이를 즉각적으로 반영하는 것이 중요하다.</p> <p>*바이러스(Virus): 바이러스는 스스로를 복제하려는 명백한 의도를 갖고 만들어진 코드 사용을 통해 호스트 프로그램에 침투하여 컴퓨터 사이에서 확산을 시도한다. 호스트가 실행되면 바이러스도 함께 실행되어 새로운 숙주를 감염시키는 등 시스템에 직접적인 피해를 줄 수 있고, 이메일이나 다른 외부저장장치를 통해서 다른 PC들로도 전파가 가능하고 전염성이 매우 강해서 PC 내로 들어오면 다른 파일들까지 급속하게 감염시킬 수 있다.</p> <p>*웜(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와 비슷하지만, 바이러스가 다른 실행프로그램에 기생하여 실행되는 데 반해 웜은 독자적으로 실행되며, 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말한다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 백신이 설치되어 있고, 최신 업데이트가 적용 되어 있는 경우</p> <p>취약 - 백신이 설치되어 있지 않거나, 최신 업데이트가 적용 되어 있지 않은 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | <p>[Windows 7]</p> <p>백신 프로그램의 설치 여부와 최신 Update 여부를 수동으로 점검한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 조치 방법 | <p>바이러스 백신 설치 후 최신 업데이트를 적용한다.</p> <p>[Windows 7]</p> <ol style="list-style-type: none"> <li>1. V3 Internet security 8.0 설치 여부 및 업데이트 설정 확인</li> <li>2. V3 Internet security 8.0 업데이트 적용</li> </ol>                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |

|    |                                                                                        |
|----|----------------------------------------------------------------------------------------|
|    | <div data-bbox="349 293 1426 1070"> </div> <div data-bbox="349 1126 1426 1794"> </div> |
| 비고 |                                                                                        |

#### 6.4.2. 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 항목 코드 | PC4-02 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |        |     |   |
| 설명    | <p>바이러스 백신 프로그램의 실시간 감시 기능으로 *바이러스, *스파이웨어 탐지 및 방화벽 설정 등이 가능하다. 시스템에 대한 위협 발생 시 즉시 대응이 가능하도록 실시간 감시 기능을 사용할 것을 권고한다.</p> <p>*바이러스(Virus): 바이러스는 스스로를 복제하려는 명백한 의도를 갖고 만들어진 코드 사용을 통해 호스트 프로그램에 침투하여 컴퓨터 사이에서 확산을 시도한다. 호스트가 실행 되면 바이러스도 함께 실행되어 새로운 숙주를 감염시키는 등 시스템에 직접적인 피해를 준다. 이메일이나 다른 외부저장장치를 통해서 다른 PC들로도 전파가 가능하고 전염성이 매우 강해서 PC 내로 들어오면 다른 파일들까지 급속하게 감염시킨다.</p> <p>*스파이웨어: 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성코드로, 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집한다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 설치된 백신의 실시간 감시 기능이 활성화 되어 있는 경우</p> <p>취약 - 백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화 되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                       |       |        |     |   |
| 점검 방법 | <p>[Windows 7]</p> <p>백신의 실시간 감시 기능이 활성화 되어 있는지 수동으로 점검한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 조치 방법 | <p>백신의 실시간 감시 기능을 활성화 시킨다.</p> <p>[Windows 7]</p> <p>■ 백신의 실시간 검사 기능 활성화 (V3 Internet Security 8.0 사용 시)</p> <p>PC 실시간 검사 및 네트워크 침입 차단 기능을 “사용”으로 설정</p>                                                                                                                                                                                                                                            |       |        |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |        |     |   |

### 6.4.3. OS에서 제공하는 침입차단 기능 활성화

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | PC4-03 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                 |       |        |     |   |
| 설명    | 윈도우에서 제공하는 침입차단 기능인 윈도우 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 한다.<br>네트워크 방화벽과 더불어 각각의 PC에 윈도우 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상될 수 있다.                                                                                                                                                                                     |       |        |     |   |
| 진단 기준 | 양호 - Windows 방화벽이 “사용” 으로 설정되어 있는 경우<br>취약 - Windows 방화벽이 “사용 안 함” 으로 설정되어 있는 경우                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | [Windows 7]<br>■ 제어판에서 확인<br>제어판 > Windows 방화벽(또는 시작> 실행> “firewall.cpl” 입력) 에서 Windows 방화벽 사용 여부를 확인                                                                                                                                                                                                                                     |       |        |     |   |
| 조치 방법 | <p>Windows 방화벽을 사용하도록 설정한다.</p> <p>[Windows 7]<br/>■ 제어판에서 설정</p> <ol style="list-style-type: none"> <li>1. 시작&gt; 제어판&gt; Windows 방화벽&gt; Windows 방화벽 설정 또는 해제</li> <li>2. Windows 방화벽 “사용” 설정<br/>(Windows XP의 경우 [일반] 탭에서 “사용(권장)” 설정)</li> </ol>  |       |        |     |   |





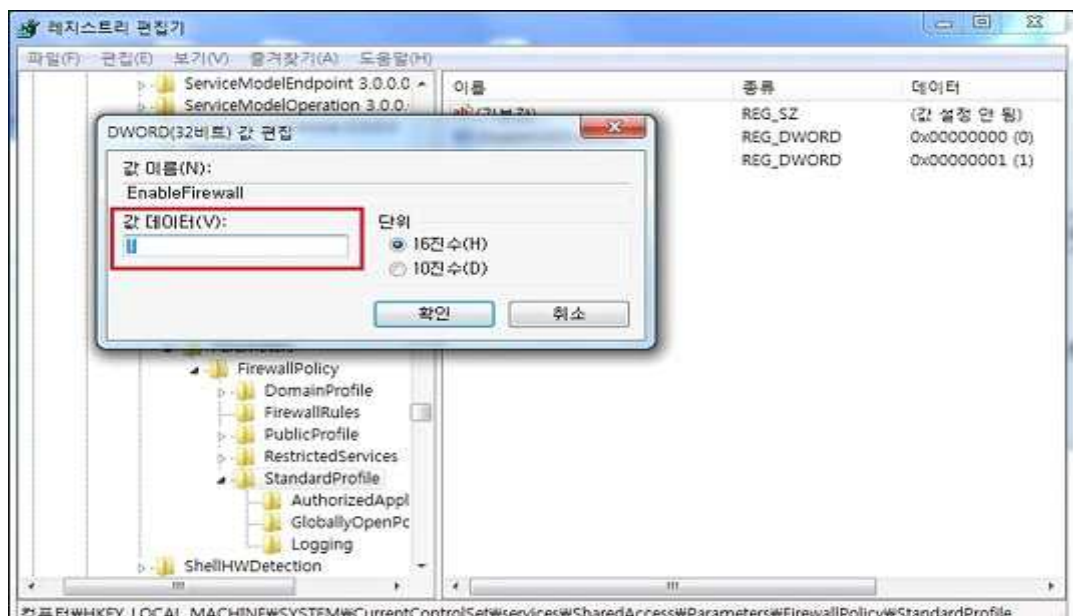
■ 레지스트리에서 설정

1. 시작> 실행> “regedit” 입력
2. 다음 레지스트리 경로로 이동

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPo

lICY

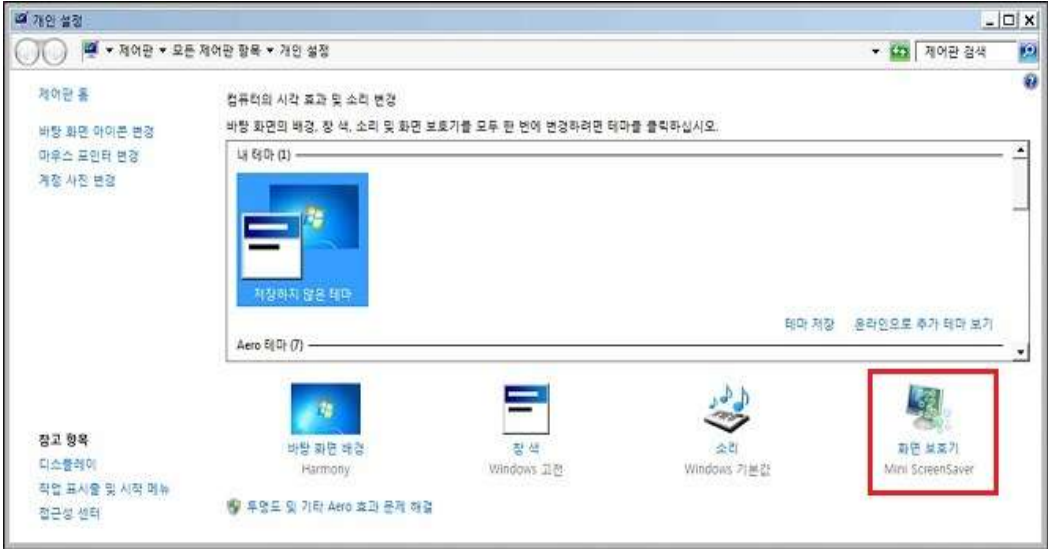
3. EnableFirewall 의 데이터 값을 “1”로 설정



|    |                                                                                                                                                                                                                                                                                                                                |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 비고 | <p>※ 방화벽이란?</p> <p>방화벽은 인터넷 또는 네트워크에서 들어오는 정보를 확인한 다음 방화벽 설정에 따라 이를 컴퓨터로 전달하는 것을 차단하거나 허용하는 소프트웨어 또는 하드웨어를 말한다.</p> <p>방화벽은 해커 또는 악성 소프트웨어가 네트워크나 인터넷을 통해 사용자 컴퓨터에 액세스하지 못하도록 방지하며, 사용자 컴퓨터에서 다른 컴퓨터로 악성 소프트웨어를 보내지 못하도록 방지한다.</p> <p>방화벽은 바이러스 백신 프로그램이 아니며, 컴퓨터를 안전하게 보호하기 위해서는 방화벽, 바이러스 백신 및 맬웨어 방지 프로그램이 모두 설치되어야 한다.</p> |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



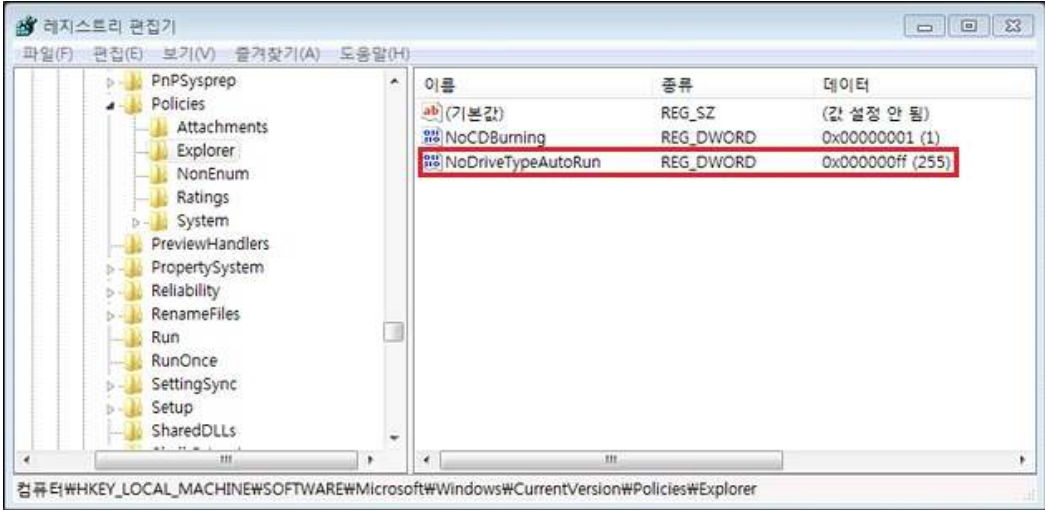
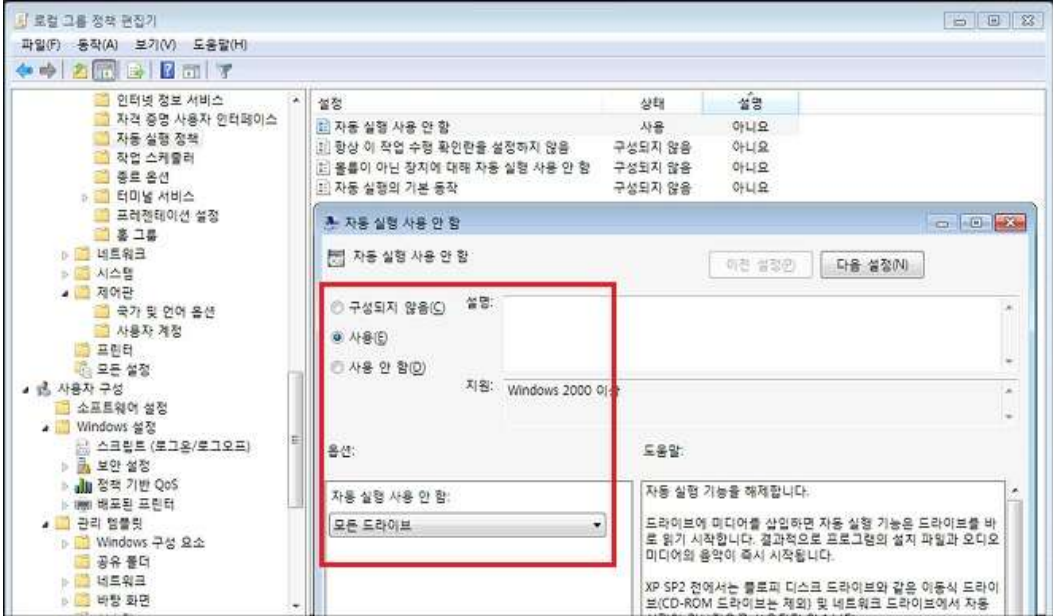
#### 6.4.4. 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정

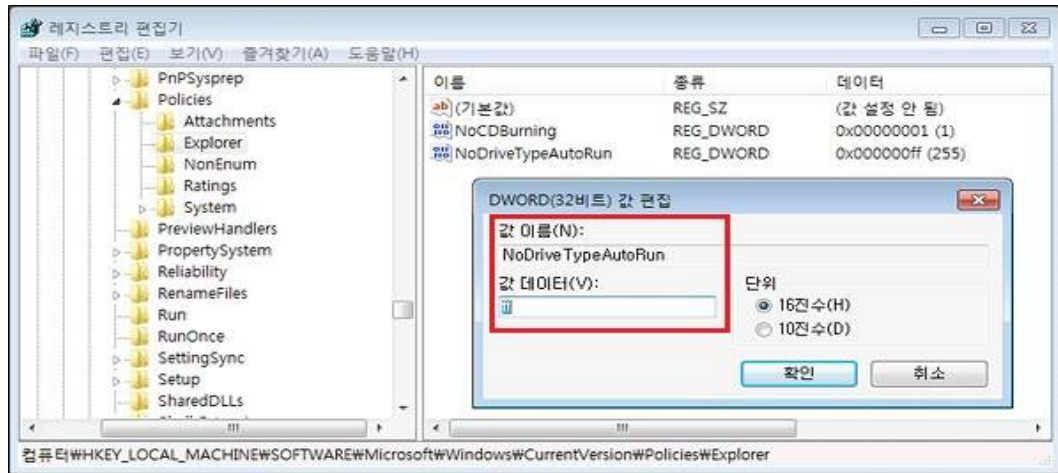
| 분류    | 보안관리                                                                                                                                                                                                                                          | 항목 코드 | PC4-04 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                     |       |        |     |   |
| 설명    | <p>사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프 되거나 워크스테이션이 잠기도록 설정하여야 한다.</p> <p>해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있으므로 화면보호기 대기 시간 및 암호 사용 설정을 이용해서 비인가자의 물리적 접근을 차단한다.</p> |       |        |     |   |
| 진단 기준 | <p>양호 - 화면보호기 설정 및 암호로 보호가 설정되어 있는 경우</p> <p>취약 - 화면보호기 설정 및 암호로 보호가 설정되어 있지 않은 경우</p>                                                                                                                                                        |       |        |     |   |
| 점검 방법 | <p>PC에 화면보호기 설정이 되어 있는지 확인한다.</p> <p>[Windows 7]</p> <p>시작 &gt; 제어판 &gt; 개인 설정 &gt; 화면보호기 에서 화면보호기 설정 확인</p>                                               |       |        |     |   |
| 조치 방법 | <p>PC에 화면보호기가 실행될 수 있도록 설정한다..</p> <p>[Windows 7]</p> <ol style="list-style-type: none"> <li>1. 시작 &gt; 제어판 &gt; 개인 설정 &gt; 화면보호기 에서 화면보호기 설정</li> <li>2. 대기 시간을 5분~10분 사이로 설정 후 “다시 시작할 때 로그인 화면 표시(R)” 체크</li> </ol>                        |       |        |     |   |

|    |                                                                                     |
|----|-------------------------------------------------------------------------------------|
|    |  |
| 비고 |                                                                                     |

#### 6.4.5. CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립

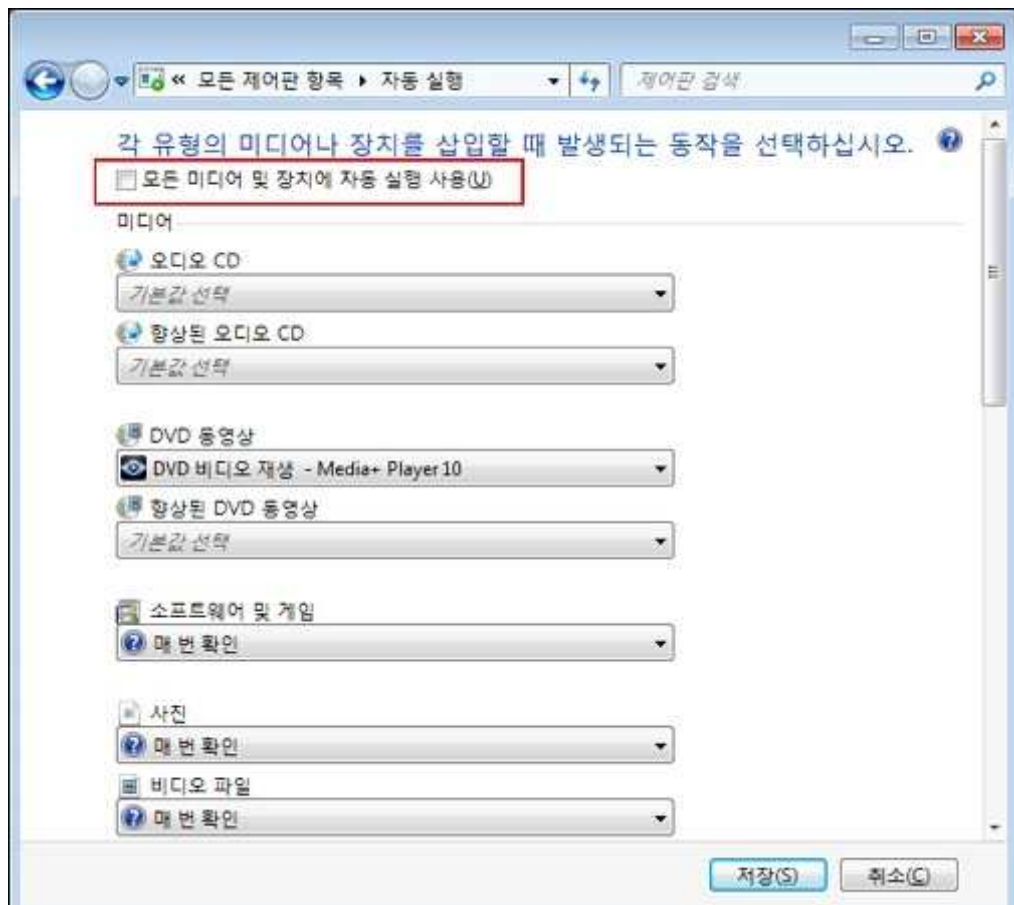
| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 항목 코드 | PC4-05 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 설명    | <p>CD/DVD, USB 메모리 등과 같은 미디어에 탑재된 *Autorun.inf 파일을 통해 다른 응용 프로그램이 자동 실행될 수 있다. 대부분의 USB 관련 악성코드들은 Autorun.inf 파일을 통해 자동 실행되도록 제작되므로 이를 통해 악성코드가 PC로 쉽게 유입될 가능성이 존재한다.</p> <p>*Autorun.inf 파일: 윈도우 운영체제의 AutoRun, AutoPlay 기능에 사용되는 텍스트 파일.</p> <p>미디어 장치의 루트 디렉터리에 위치하며, 미디어(CD/DVD, USB) 연결 시 특정 프로그램이 자동으로 실행되도록 제어한다.</p>                                                                                                                                                                                                                                                                                |       |        |     |   |
| 진단 기준 | <p>양호 - 미디어 사용 시 자동 실행되지 않는 경우</p> <p>취약 - 미디어 사용 시 자동 실행되는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |        |     |   |
| 점검 방법 | <p>미디어 사용 시 자동 실행 되지 않도록 설정되어 있는지 확인한다.</p> <p>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 확인</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; Windows 구성 요소&gt; 자동 실행 정책</li> <li>“자동 실행 사용 안 함” 정책이 “사용”으로 되어 있는지 확인</li> </ol>  <p>■ 레지스트리에서 확인</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “regedit” 입력</li> <li>레지스트리 경로<br/>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer</li> <li>NoDriveTypeAutoRun 의 데이터 값이 ff로 되어 있는지 확인</li> </ol> |       |        |     |   |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 조치 방법 | <p>미디어 사용 시 자동 실행 되지 않도록 설정한다.<br/>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 설정</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; Windows 구성 요소&gt; 자동 실행 정책</li> <li>“자동 실행 사용 안 함” 정책을 “사용 – 모든 드라이브”로 설정</li> </ol>  <p>■ 레지스트리에서 설정</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “regedit” 입력</li> <li>레지스트리 경로<br/>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer</li> <li>NoDriveTypeAutoRun 의 데이터 값을 ff 로 설정</li> </ol> |



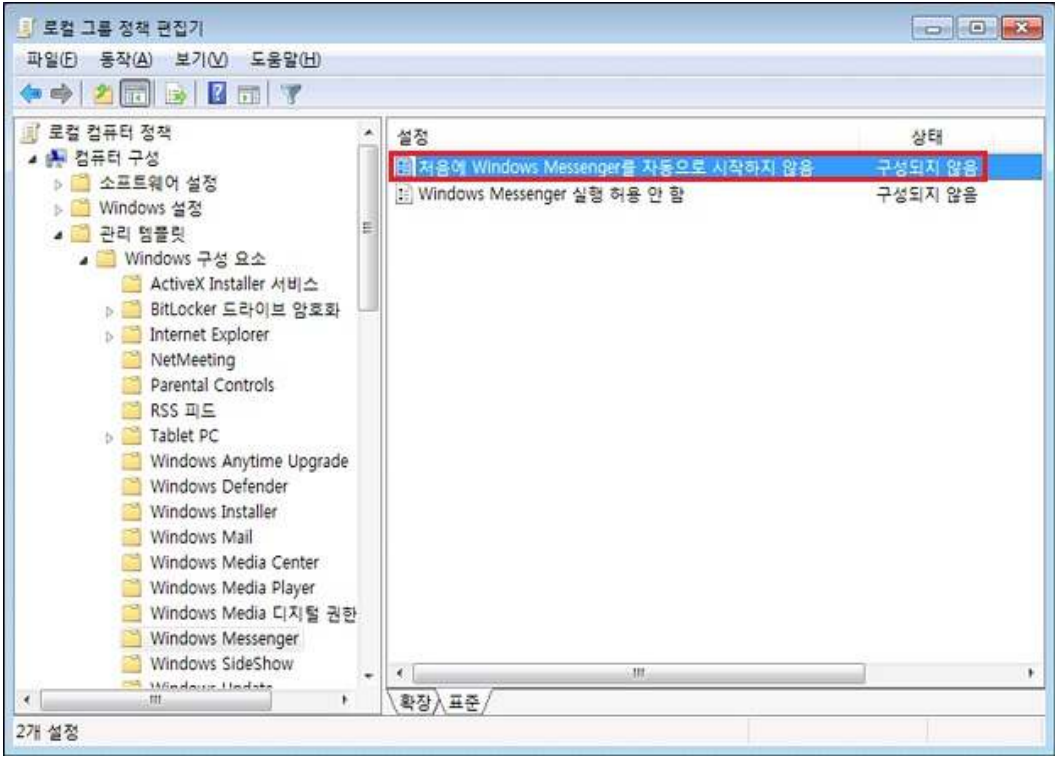
■ 제어판에서 설정

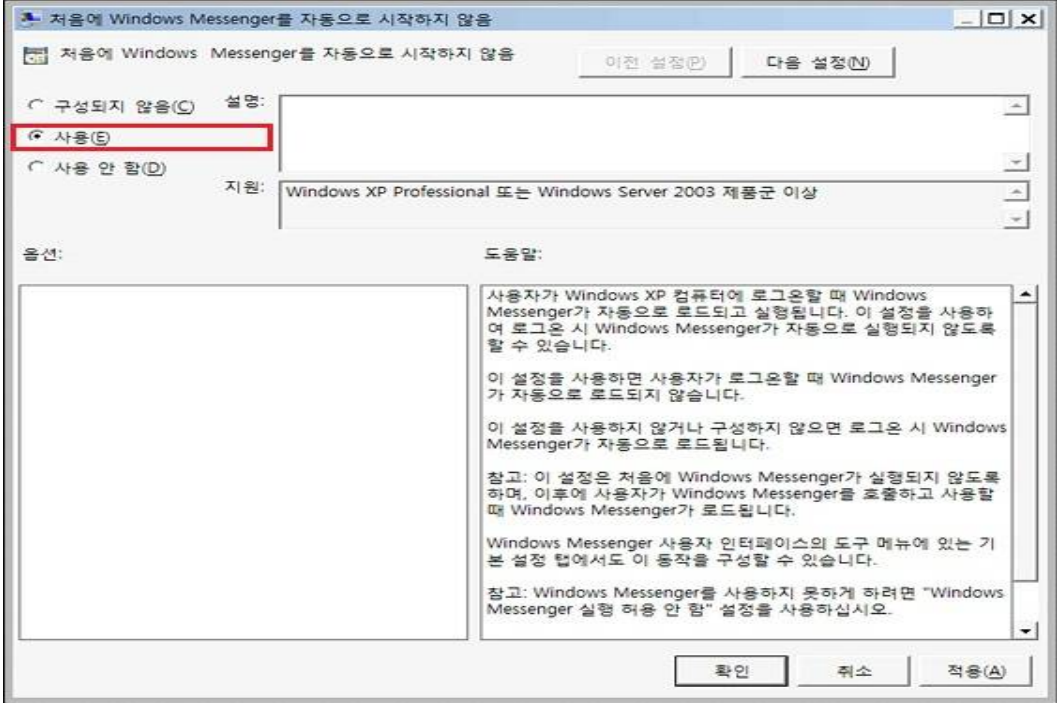
시작 > 제어판 > 자동 실행 > “모든 미디어 및 장치에 자동 실행 사용(U)” 체크 해제



비고

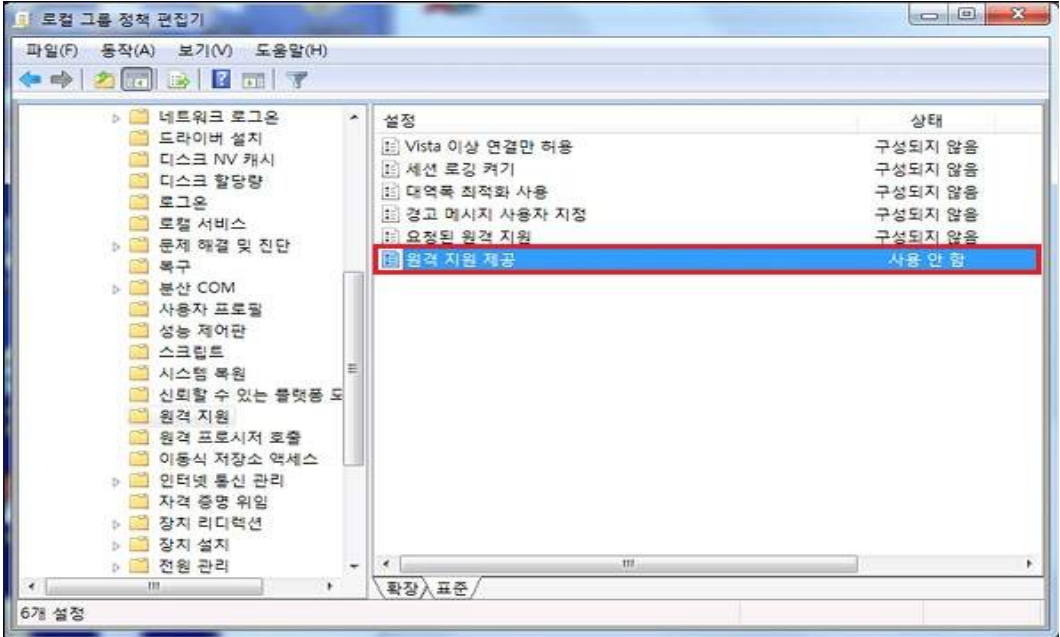
#### 6.4.6. 시스템 부팅 시 Windows Messenger 자동시작 금지

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 항목 코드 | PC4-06 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |     |   |
| 설명    | 윈도우 시작 시 자동으로 Windows Messenger가 시작되도록 설정할 수 있으나 Messenger를 통한 정보 유출 및 악성코드 유입이 발생할 수 있으므로 자동시작으로 설정된 경우 시스템에 대한 위협이 증가할 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |     |   |
| 진단 기준 | 양호 - Windows Messenger 자동시작 금지 설정이 되어있는 경우<br>취약 - Windows Messenger 자동시작 금지 설정이 되어있지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |        |     |   |
| 점검 방법 | <p>Windows Messenger 가 자동시작 설정 여부를 확인한다.</p> <p>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 확인</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; Windows 구성 요소&gt; Windows Messenger</li> <li>“Windows Messenger를 자동으로 시작하지 않음” 정책의 설정 확인 (“사용”으로 설정되어 있는 경우 양호)</li> </ol>  <p>■ 레지스트리에서 확인</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “regedit” 입력</li> <li>다음 레지스트리 경로로 이동<br/>HKLM\Software\Policies\Microsoft\Messenger\Client</li> <li>PreventAutoRun 의 데이터 값이 “1”로 설정되어 있는지 확인 (“1”로 설정되어 있는 경우 양호)</li> </ol> |       |        |     |   |

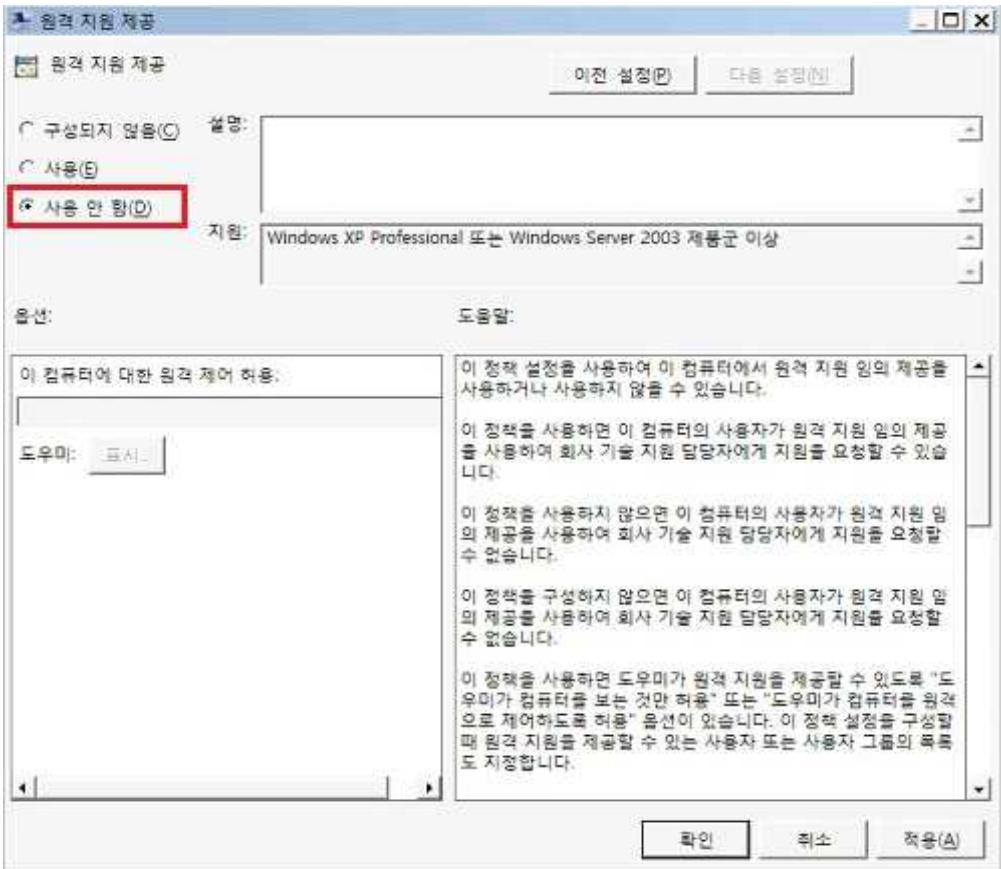
|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치 방법 | <p>Windows Messenger 가 자동시작 되지 않도록 설정한다.<br/>[Windows 7]</p> <p>■ 로컬 그룹 정책 편집기에서 설정</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; Windows 구성 요소&gt; Windows Messenger</li> <li>“Windows Messenger를 자동으로 시작하지 않음” 설정을 “사용” 으로 설정</li> </ol>  <p>■ 레지스트리에서 설정</p> <ol style="list-style-type: none"> <li>시작&gt; 실행&gt; “regedit” 입력</li> <li>다음 레지스트리 경로로 이동<br/>HKLM\Software\Policies\Microsoft\Messenger\Client</li> <li>PreventAutoRun 의 데이터 값을 “1” 로 설정</li> </ol> <p>※ “Windows Messenger를 실행하지 않음” 설정이 “사용 안 함” 으로 설정되어 있는 경우 레지스트리 편집기 내 Messenger 항목이 존재하며, “사용” 인 경우는 존재하지 않음</p> |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



#### 6.4.7. 원격 지원 금지 정책 설정

| 분류    | 보안관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 항목 코드 | PC4-07 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-----|---|
| 대상    | Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |        |     |   |
| 설명    | 시스템 관리 등의 목적으로 원격 지원 기능을 활용할 수 있으나 원격 지원 기능이 비인가자에게 허용될 경우 시스템 제어 권한이 악용될 수 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 진단 기준 | <p>양호 - 원격 지원이 “사용 안 함” 으로 설정되어 있는 경우</p> <p>취약 - 원격 지원이 “사용” 으로 설정되어 있는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |     |   |
| 점검 방법 | <p>원격 지원 정책이 “사용 안 함” 으로 설정되어 있는지 확인한다.</p> <p>[Windows 7]</p> <ol style="list-style-type: none"> <li>1. 시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; 시스템&gt; 원격 지원</li> <li>2. “원격 지원 제공” 정책의 설정 값 확인 (“사용 안 함” 으로 되어 있는 경우 양호)</li> </ol>  <p>The screenshot shows the 'Group Policy Editor' window. On the left, the tree view is expanded to 'Computer Configuration' &gt; 'Administrative Templates' &gt; 'System' &gt; 'Remote Assistance'. On the right, the 'Settings' pane shows a list of policies. The policy 'Remote Assistance' is highlighted with a red box, and its state is 'Disabled'.</p> |       |        |     |   |
| 조치 방법 | <p>원격 지원 정책을 “사용 안 함” 으로 설정한다.</p> <p>[Windows 7]</p> <ol style="list-style-type: none"> <li>1. 시작&gt; 실행&gt; “gpedit.msc” 입력&gt; 컴퓨터 구성&gt; 관리 템플릿&gt; 시스템&gt; 원격 지원</li> <li>2. “원격 지원 제공”을 “사용 안 함” 으로 설정</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |        |     |   |



|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |  <p>원격 지원 제공</p> <p>원격 지원 제공</p> <p>이전 설정(P) 다음 설정(N)</p> <p> <input type="radio"/> 구성되지 않음(C)         <input type="radio"/> 사용(E)         <input checked="" type="radio"/> 사용 안 함(D)     </p> <p>지원: Windows XP Professional 또는 Windows Server 2003 제품군 이상</p> <p>         옵션:         <span style="margin-left: 100px;">도움말:</span> </p> <p>이 컴퓨터에 대한 원격 제어 허용:</p> <p>도우미: 프시...</p> <p>         이 정책 설정을 사용하여 이 컴퓨터에서 원격 지원 임의 제공을 사용하거나 사용하지 않을 수 있습니다.<br/>         이 정책을 사용하면 이 컴퓨터의 사용자가 원격 지원 임의 제공을 사용하여 회사 기술 지원 담당자에게 지원을 요청할 수 있습니다.<br/>         이 정책을 사용하지 않으면 이 컴퓨터의 사용자가 원격 지원 임의 제공을 사용하여 회사 기술 지원 담당자에게 지원을 요청할 수 없습니다.<br/>         이 정책을 구성하지 않으면 이 컴퓨터의 사용자가 원격 지원 임의 제공을 사용하여 회사 기술 지원 담당자에게 지원을 요청할 수 없습니다.<br/>         이 정책을 사용하면 도우미가 원격 지원을 제공할 수 있도록 "도우미가 컴퓨터를 보는 것만 허용" 또는 "도우미가 컴퓨터를 원격으로 제어하도록 허용" 옵션이 있습니다. 이 정책 설정을 구성할 때 원격 지원을 제공할 수 있는 사용자 또는 사용자 그룹의 목록도 지정합니다.     </p> <p>확인 취소 적용(A)</p> |
| 비고 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



## 7. 웹 취약성 점검항목 및 가이드

### 7.1. 중요 정보 노출

#### 7.1.1. SQL Injection.

| 분류    | SQL Injection                                                                                                                                                                                                                                                                            | 항목 코드 | WAS1-01 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 웹 사이트는 DBMS와 연동하므로 웹 애플리케이션에서 사용자의 입력값을 통하여 데이터 트랜잭션이 발생한다. 만일 사용자 입력값에 대한 유효성 검증이 누락될 경우, 악의적인 사용자는 정상적인 입력값 대신 SQL 쿼리문이 포함된 조작된 입력값을 전송하여 서버측 쿼리문의 구조를 변경할 수 있으며, 이를 통해서 사용자 인증을 우회하거나 데이터베이스의 정보를 유출시키고 서버의 시스템 명령어를 실행시킬 수도 있다.                                                      |       |         |     |   |
| 진단 기준 | 양호 - 데이터베이스 질의어를 요청할 때 특수문자를 필터링 하는 경우<br>취약 - 데이터베이스 질의어를 요청할 때 특수문자를 필터링 하지 않는 경우                                                                                                                                                                                                      |       |         |     |   |
| 점검 방법 | 로그인 등 데이터베이스 질의어를 요청하는 곳에 'or 1=1# 입력후 확인(MySQL일 경우 #, MsSQL일 경우 - 로 작성)<br>                                                                                                                           |       |         |     |   |
| 조치 방법 | 사용자측으로부터 전달되는 파라미터 중 DB 쿼리문에 사용되는 모든 파라미터 (게시판 ID, 글 번호, 검색 keyword, 사용자 번호, 항목 번호, 분류명칭 등)로부터 입력되는 데이터에 대하여 아래와 같이 특수 문자 및 Query 예약어를 필터링해 에러처리를 하거나 'W' 문자 또는 공백 문자로 치환해야 한다.<br>예) \$login_id = mysql_escape_string(\$login_id);<br>\$login_pass = mysql_escape_string(\$login_pass); |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                          |       |         |     |   |

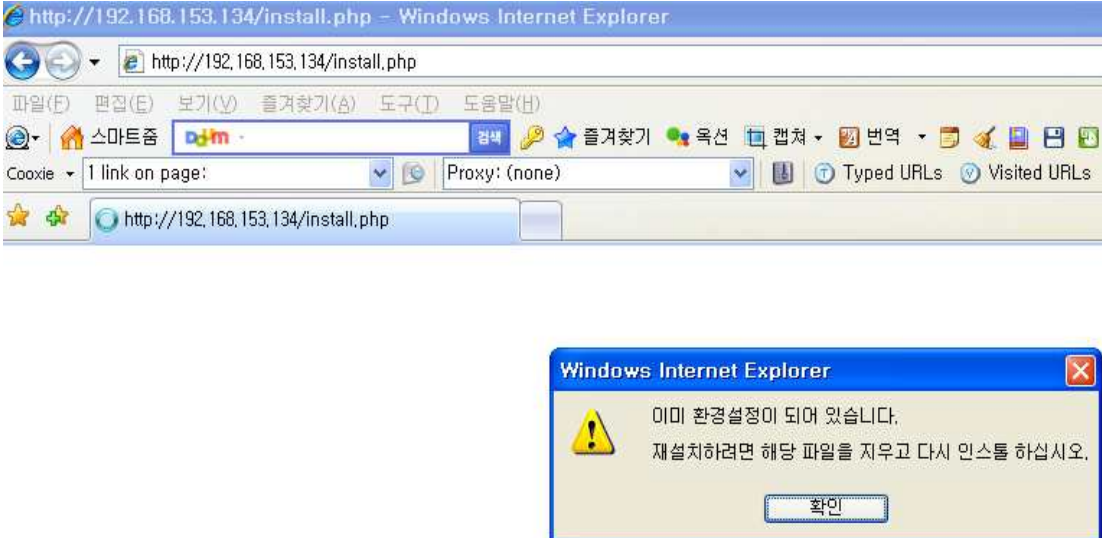
### 7.1.2. 부적절한 에러 처리

| 분류    | 부적절한 에러 처리                                                                                                                                                                                                                                                                        | 항목 코드 | WAS1-02 | 중요도 | L |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 공격자가 대상 시스템의 현황을 파악하기 위하여 다양한 에러를 유발시킴으로써 반응하는 에러 결과값으로 웹 프로그램의 구조 및 환경설정을 추측하여 공격에 이용된다. 그러므로 Error를 위한 별도의 페이지를 작성하여 Error발생시 기본 Error Page로 Redirect 시킴으로써, 불필요한 정보가 노출되지 않도록 해야 한다. SQL Injection 공격으로 대상 시스템의 SQL Query문장의 구성을 알아내기 위한 Foot Printing 시도와 같은 것이 이 항목에 해당된다    |       |         |     |   |
| 진단 기준 | 양호 - 별도의 에러페이지를 작성하여 리다이렉트 하는 경우<br>취약 - 별도의 에러페이지를 작성하여 리다이렉트 하지 않는 경우                                                                                                                                                                                                           |       |         |     |   |
| 점검 방법 | 무작위 에러를 산출하여 결과 확인<br>                                                                                                                                                                          |       |         |     |   |
| 조치 방법 | Apache 설정에서 에러 페이지 리다이렉트 설정<br>1. 보통의 텍스트<br>ErrorDocument 500 "The server made a boo."<br>(" 표시는 텍스트임을 알려주는 것으로서 그 자체는 출력되지 않음.)<br>2. 지역적인 방향 전환<br>#ErrorDocument 404 /missing.html 지역적인 방향 전환<br>3. 외부 방향 전환<br>#ErrorDocument 402 http://some.othercom.com/subscription.html |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                   |       |         |     |   |

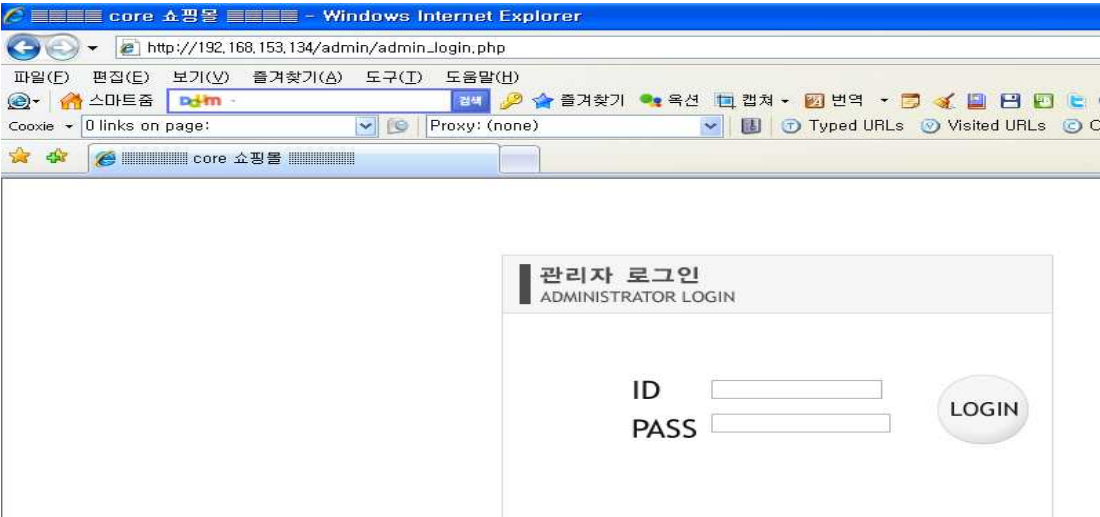
### 7.1.3. 백업 페이지 존재

| 분류    | 부적절한 에러 처리                                                                                                                                                                                                  | 항목 코드 | WAS1-03 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 웹 Root Directory 내에 백업용 압축파일, 테스트 파일 등이 존재하고 유추 가능한 이름으로 되어 있는 경우, 별도의 과정 없이 다운로드가 가능하거나 내용이 브라우저 상으로 출력될 수 있으므로 이를 통해서 중요한 정보가 노출될 위험이 있다.                                                                 |       |         |     |   |
| 진단 기준 | 양호 - 웹 디렉터리에 *.asp.bak , *.jsp.bak, *.php.old와 같은 백업파일이 존재하지 않는 경우<br>취약 - 웹 디렉터리에 *.asp.bak , *.jsp.bak, *.php.old와 같은 백업파일이 존재할 경우                                                                        |       |         |     |   |
| 점검 방법 | 웹 디렉터리 마다 백업 파일이 존재 하는지 확인<br> <a href="http://192.168.153.134/m_login.php.old">http://192.168.153.134/m_login.php.old</a> |       |         |     |   |
| 조치 방법 | *.txt 같은 웹 페이지의 작업 도중 생성된 일반 텍스트 파일이나 그 밖에 이미지 파일 등도 본래 파일 이외에는 제거하여야 하며 *.asp.bak, *.jsp.bak 파일 이외의 *.bak 파일도 불필요한 경우는 삭제해야 한다.                                                                            |       |         |     |   |
| 비고    |                                                                                                                                                                                                             |       |         |     |   |

#### 7.1.4. 디폴트 페이지 존재

| 분류    | 디폴트 페이지 존재                                                                                                                                                                                                           | 항목 코드 | WAS1-04 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | <p>웹서버, WAS 등 널리 사용되는 유명 플랫폼의 경우, 설치 당시 자동으로 생성되는 각종 디폴트 페이지 및 관리용 콘솔의 경로가 일반에 공개되어 있어 쉽게 접근할 수 있으므로 이를 그대로 사용하면 악의적인 공격에 이용될 수 있다.</p> <p>따라서 이러한 디폴트 페이지 및 관리 콘솔에 대한 접근을 적절히 통제해야 하며, 사용하지 않는 경우 삭제하는 것이 바람직하다</p> |       |         |     |   |
| 진단 기준 | <p>양호 - 웹 디렉터리리 phpinfo, sample파일 등 디폴트 페이지가 존재 하지 않는 경우</p> <p>취약 - 웹 디렉터리리 phpinfo, sample파일 등 디폴트 페이지가 존재 할 경우</p>                                                                                                |       |         |     |   |
| 점검 방법 | <p>install, sample 파일이 존재하는지 확인</p>                                                                                               |       |         |     |   |
| 조치 방법 | <p>설치된 웹 서버에 대한 Default Page와 Banner를 삭제하여 Banner Grab에 의한 시스템 기본 정보 유출을 사전에 차단해야 하며, Tomcat, Apache 등을 사용할 경우, Install 혹은 Default Page등을 삭제하고 sample 파일 역시 삭제해야 한다.</p>                                             |       |         |     |   |
| 비고    |                                                                                                                                                                                                                      |       |         |     |   |

### 7.1.5. 관리자 페이지 접근

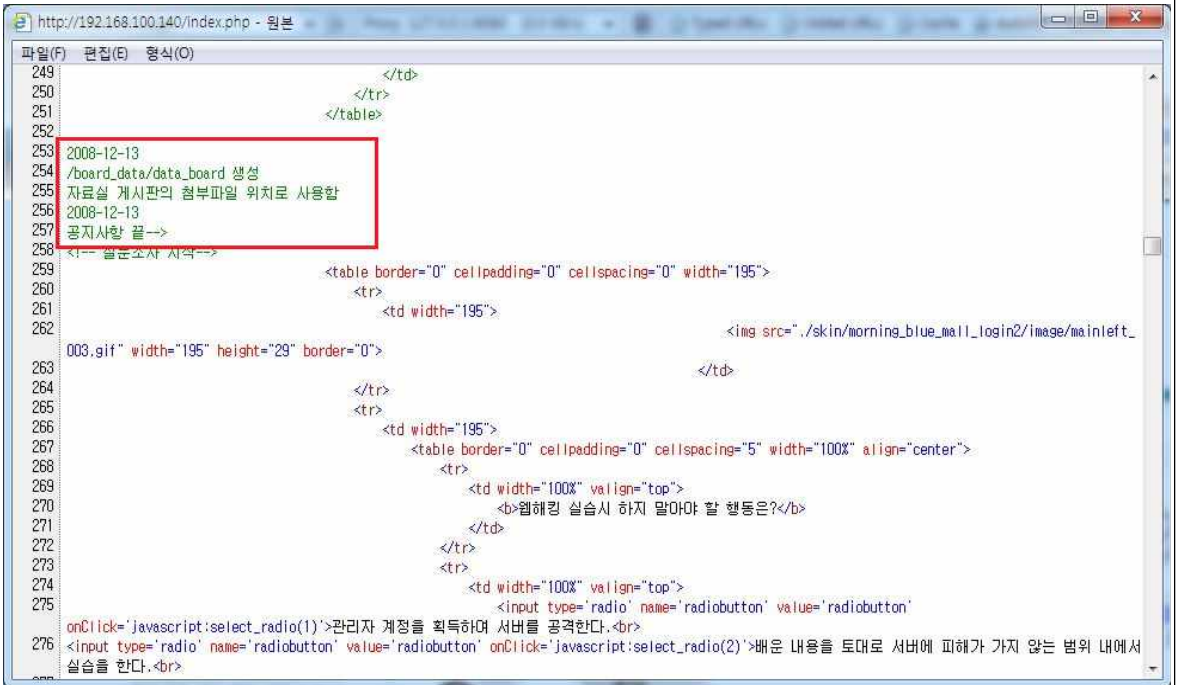
| 분류    | 관리자 페이지 접근                                                                                                                                                                                                                                                                                    | 항목 코드 | WAS1-05 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | <p>관리자 기능이 일반 사용자 기능과 분리되어있지 않을 경우, 해당 기능의 경로가 노출되기 쉬우며, 노출된 경로를 통해서 일반 사용자의 접근 시도가 발생하거나 또는 악의적인 공격자에 의한 지속적인 공격을 유발할 수 있다.</p> <p>관리자 페이지는 적절한 접근 통제가 이루어져야 하며, 접근 통제 없이 임의의 위치에서 접근 가능할 경우, 해당 경로를 유추하거나 기타 다양한 방법에 의해서 위치가 노출될 수 있으므로 이를 통해서 악의적인 공격자에 의한 brute force 공격 등이 발생할 수 있다.</p> |       |         |     |   |
| 진단 기준 | <p>양호 - 관리자 페이지의 경로가 노출 되지 않은 경우</p> <p>취약 - 관리자 페이지의 경로가 노출 된 경우</p>                                                                                                                                                                                                                         |       |         |     |   |
| 점검 방법 | <p>관리자 페이지로 추측 되는 URL 접근</p>                                                                                                                                                                               |       |         |     |   |
| 조치 방법 | <p>관리자 페이지는 다음과 같은 보안 정책에 의해서 보호되어야 한다.</p> <ol style="list-style-type: none"> <li>1. 관리자 페이지는 일반 사용자용 인터페이스와 분리되어 작성되어야 한다. (별도의 포트, 도메인 등)</li> <li>2. 관리자 페이지는 임의의 위치에서 접근할 수 없도록 적절한 접근 통제 절차가 적용되어야 한다 (IP 접근 제어, SMS 인증 등)</li> <li>3. 추측하기 쉬운 디렉터리명이나 파일명을 사용해서는 안된다.</li> </ol>       |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                               |       |         |     |   |

## 7.1.6. 디렉터리 리스팅

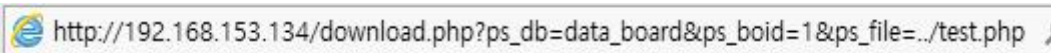
| 분류    | 디렉터리 리스팅                                                                                                                                                                                                                                                                                | 항목 코드 | WAS1-06 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 웹서버 설정상의 오류나 개발 과정의 편의를 위해서 웹 디렉터리 내부의 파일 리스트가 웹 브라우저를 통해서 출력되도록 설정되어있는 경우, 이 정보를 이용해서 중요한 파일을 다운로드 하거나 웹사이트 구조를 파악하여 공격에 이용할 수 있다.                                                                                                                                                     |       |         |     |   |
| 진단 기준 | 양호 - 설정파일에서 Directory Indexing을 허용하지 않은 경우<br>취약 - 설정파일에서 Directory Indexing을 허용 했을 경우                                                                                                                                                                                                  |       |         |     |   |
| 점검 방법 | URL 경로에 디렉터리 경로 삽입 후 확인<br>                                                                                                                                                                          |       |         |     |   |
| 조치 방법 | DocumentRoot 디렉터리 내의 모든 파일들이 리스팅 되는 것을 방지하기 위해서 httpd.conf 파일 내의 "Options" 지시자 에서 "Indexes" 라는 옵션을 제거해야 한다. 이 옵션은 해당 디렉터리 안에 DirectoryIndex에 명기된 파일(index.html, index.jsp 등등..)이 없을 경우 디렉터리와 파일 목록을 보여주는 옵션이다. 이 옵션을 제거하면 "Forbidden"이 표시되면서 permission error 페이지가 뜨고 디렉터리 인덱싱이 되지 않는다. |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                         |       |         |     |   |



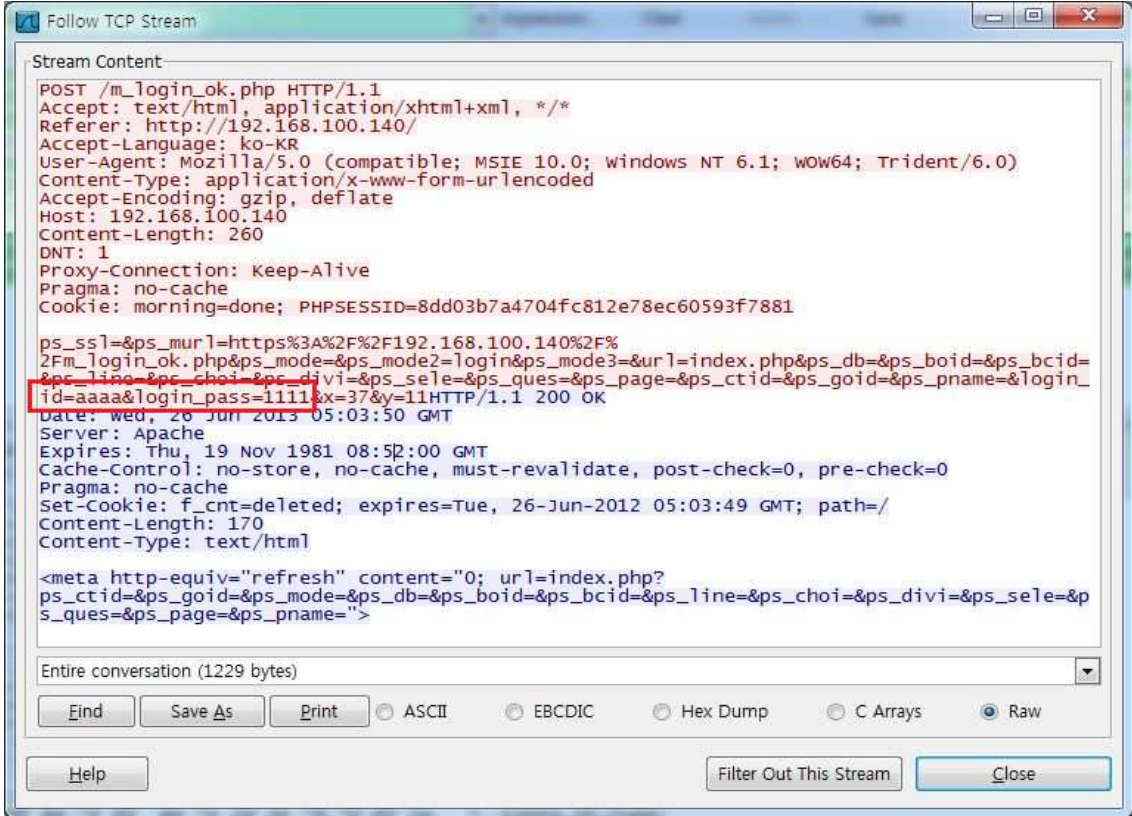
### 7.1.7. 소스코드 노출

| 분류    | 중요정보 노출                                                                                                                                                                                                                                                                                                                                                      | 항목 코드 | WAS1-07 | 중요도 | M |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 홈페이지에서 중요정보 및 개인정보 노출은 웹페이지, 첨부파일, 소스코드, 외부 검색엔진(구글 등) 등의 형태로 발생한다. 또한 각 형태 별로 다양한 유형의 개인정보 노출이 발생할 수 있다. 따라서 개인정보 노출관리자는 관리하는 홈페이지에서 발생할 수 있는 모든 유형의 개인정보 노출에 대해서 점검하여야 한다.                                                                                                                                                                                 |       |         |     |   |
| 진단 기준 | <p>양호 - 소스 코드 보기를 통해 중요 정보가 노출 되지 않은 경우</p> <p>취약 - 소스 코드 보기를 통해 중요 정보가 노출 될 경우</p>                                                                                                                                                                                                                                                                          |       |         |     |   |
| 점검 방법 | <p>마우스 오른쪽 클릭 - 소스 보기를 통해 중요 정보가 노출 되는 지 확인</p>                                                                                                                                                                                                                           |       |         |     |   |
| 조치 방법 | <p>1. Html 소스코드 특히 hidden 필드를 통해 중요정보가 노출되고 있지 않는지 철저히 점검하여 중요정보 및 개인정보 침해 요소를 제거 한다.</p> <p>2. 개인정보, 기타 주요 정보가 포함된 게시물, 첨부파일을 발견한 경우에는 해당 페이지를 즉시 삭제하거나 민감한 정보의 일부를 * 처리하는 등의 조치를 취해야 한다.</p> <p>3. 현재 운영중이 아니지만 과거 운영 했던 정보가 웹 서버에 남아 개인정보, 중요정보가 노출되는 경우에는 관리자는 관리하는 웹서버 내에 잔존하는 휴면 홈페이지를 모두 삭제하거나 휴면 홈페이지의 개인정보 노출여부를 일제히 점검하여 삭제처리 하는 등의 관리를 해야 한다.</p> |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                              |       |         |     |   |

### 7.1.8. 파일 다운로드

| 분류    | 파일 다운로드                                                                                                                                                           | 항목 코드 | WAS1-08 | 중요도 | H |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | Web Application 의 download 관련 모듈의 파라미터에 path traversal 문자열을 삽입하여 웹 루트 디렉터리의 상위 경로에 위치하는 OS파일 시스템까지 접근할 수 있으며, 이를 이용하여 시스템의 각종 중요 파일 및 웹 프로그램의 소스 코드를 다운로드 할 수 있다. |       |         |     |   |
| 진단 기준 | 양호 - 파라미터를 조작하여 중요파일을 다운 받을 수 없는 경우<br>취약 - 파라미터를 조작하여 중요파일을 다운 받을 수 있는 경우                                                                                        |       |         |     |   |
| 점검 방법 | 파라미터에 path traversal를 변조하여 시스템 접근 여부 확인<br>                                     |       |         |     |   |
| 조치 방법 | 파일 다운로드 모듈의 경로를 처리하는 파라미터 변수에 대해서 다음의 특수문자(path traversal 문자열)을 필터링 한다.<br>[../], [..W] ,[/]                                                                      |       |         |     |   |
| 비고    |                                                                                                                                                                   |       |         |     |   |

### 7.1.9. 중요정보 전송구간 암호화

| 분류    | 중요정보 전송구간 암호화                                                                                                                                                    | 항목 코드 | WAS1-09 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | Web Application 의 download 관련 모듈의 파라미터에 path traversal 문자열을 삽입하여 웹 루트 디렉터리의 상위 경로에 위치하는 OS파일 시스템까지 접근할 수 있으며, 이를 이용해서 시스템의 각종 중요 파일 및 웹 프로그램의 소스 코드를 다운로드할 수 있다. |       |         |     |   |
| 진단 기준 | 양호 - ID, PassWord등 중요정보가 암호화 되어 전송되는 경우<br>취약 - ID, PassWord등 중요정보가 평문으로 전송되는 경우                                                                                 |       |         |     |   |
| 점검 방법 | WireShark를 사용하여 패킷 내용 확인<br>                                                  |       |         |     |   |
| 조치 방법 | 모든 인증된 연결이나 민감한 데이터가 전송되는 곳에 SSL을 사용                                                                                                                             |       |         |     |   |
| 비고    |                                                                                                                                                                  |       |         |     |   |

## 7.2. 취약한 인증 권한

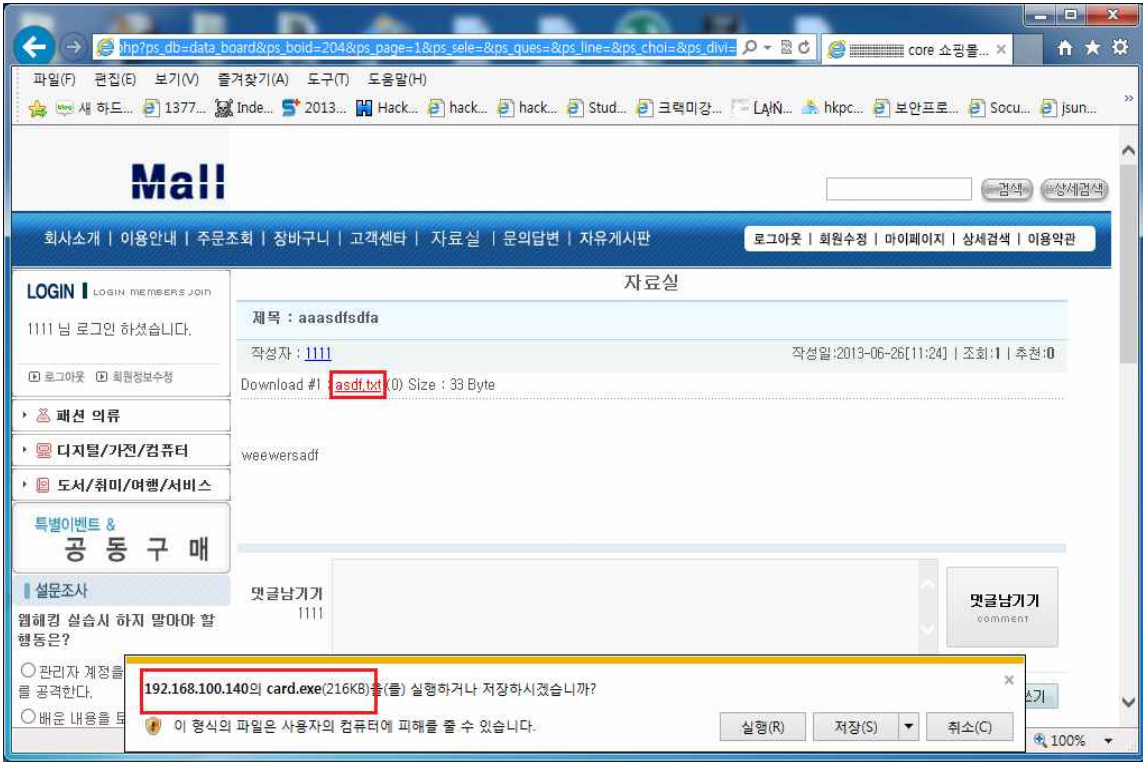
### 7.2.1. XSS(크로스 사이트 스크립트)

| 분류    | 취약한 인증 권한                                                                                                                                                                                                      | 항목 코드 | WAS2-01 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 웹사이트에서 게시판 등을 통해서 사용자가 문자열을 입력하여 웹사이트에 게시할 수 있는 기능을 제공할 경우, 악의적인 사용자는 문자열에 javascript 등 스크립트를 삽입하여 게시한 후, 이를 열람한 사용자의 웹브라우저에서 스크립트가 실행되도록 함으로써, PC에 저장된 인증정보를 유출시키거나 악성 코드를 다운로드하여 설치하도록 유도하는 등의 공격이 발생할 수 있다. |       |         |     |   |
| 진단 기준 | 양호 - 게시글에 HTML 및 스크립트를 작성 할 수 있는 경우<br>취약 - 게시글에 HTML 및 스크립트를 작성 할 수 없는 경우                                                                                                                                     |       |         |     |   |
| 점검 방법 | <p>게시글에 &lt;script&gt; alert("XSS");&lt;/script&gt; 작성 후 확인</p>                                                             |       |         |     |   |
| 조치 방법 | 취약점이 존재하는 해당 페이지의 게시물 입력 창에 대한 특수문자(<, >,  , ", ', %, &, =, ` 등)에 대한 필터링을 수행하고 사용자로부터 폼을 입력 받아 페이지에 표시하는 모든 어플리케이션에서 HTML 및 스크립트(iframe, script, xmp, xml 등)를 금지해야 한다.                                         |       |         |     |   |
| 비고    |                                                                                                                                                                                                                |       |         |     |   |

## 7.2.2. 디폴트/취약한 계정 사용

| 분류    | 취약한 인증 권한                                                                                                                              | 항목 코드 | WAS2-02 | 중요도 | M |
|-------|----------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 시스템의 디폴트/취약한 계정 및 패스워드를 사용할 경우 추측 공격, 사전 공격, 무작위 대입 공격에 인증정보가 쉽게 노출이 되어 타 사용자나 관리자 계정을 가로챌 수 있고, 권한 및 책임 추구성 관리를 악화시키며, 개인정보 침해를 유발한다. |       |         |     |   |
| 진단 기준 | 양호 - 디폴트/취약한 계정을 사용하고 있지 않은 경우<br>취약 - 디폴트/취약한 계정을 사용하고 있는 경우                                                                          |       |         |     |   |
| 점검 방법 | 디폴트/취약한 계정 추측                                                                                                                          |       |         |     |   |
| 조치 방법 | 시스템의 디폴트 계정과 추측하기 쉬운 계정 사용을 사용하지 않을 것을 권장한다.                                                                                           |       |         |     |   |
| 비고    |                                                                                                                                        |       |         |     |   |

### 7.2.3. URL 직접 접근

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                                      | 항목 코드 | WAS2-03 | 중요도 | H |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | <p>인증 / 권한 관리 모듈은 안전하게 설계되어야 하며, 그렇지 않을 경우, 사용자는 javascript를 수정하거나 기타 다른 여러 가지 방법을 통해서 인증을 우회하여 특정 페이지에 접근하여 서비스를 무단으로 이용하는 등의 문제가 발생할 수 있다.</p> <p>또한 모든 웹페이지는 개별적으로 인증 및 권한 관리 모듈을 포함하고 있어야 하며, 그렇지 않을 경우 로그인 인증을 통과해야만 접근할 수 있는 웹페이지나 상위 권한이 필요한 웹페이지에 해당 페이지의 URL을 웹브라우저에 직접 입력하여 무단 접근을 시도할 수 있다.</p>     |       |         |     |   |
| 진단 기준 | <p>양호 - 페이지 각각에 대하여 인증을 위한 세션관리를 하고 있는 경우</p> <p>취약 - 페이지 각각에 대하여 인증을 위한 세션관리를 하고 있지 않은 경우</p>                                                                                                                                                                                                                 |       |         |     |   |
| 점검 방법 | <p>비밀글의 글 번호를 파악 하여 접근하여 확인</p> <p><a href="http://192.168.153.134/download.php?ps_db=data_board&amp;ps_boid=글번호&amp;ps_file=1">http://192.168.153.134/download.php?ps_db=data_board&amp;ps_boid=글번호&amp;ps_file=1</a></p>  |       |         |     |   |
| 조치 방법 | <p>인증을 통과해야 접속할 수 있는 페이지의 경우 해당 페이지 주소를 직접 입력하여 들어가지 못하도록 페이지 각각에 대하여 인증을 위한 세션관리를 해야 한다.</p> <p>접근제어가 필요한 모든 페이지에 통제수단(로그인 체크 및 권한 체크)을 구현해야 한다.</p> <p>특히, 하나의 프로세스가 여러 개의 페이지 또는 모듈로 이루어져 있을 때 권한 체크가 누락되는 경우를 방지하기 위해서 공통 모듈을 사용하는 것을 권장한다.</p>                                                            |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                |       |         |     |   |

## 7.2.4. 히든필드 조작

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                | 항목 코드 | WAS2-04 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 히든필드는 사용자 정보를 포함시켜 페이지를 이동 할때마다 인증 정보 등을 전달한다. 이때 노출되는 변수를 통해서 서버 측 프로그램의 로직 및 역할 등을 유추할 수 있으므로, 공격자는 변수에 임의의 값을 입력하여 관리자 권한을 획득 할 수 있으며 관리자를 사칭하여 특정 악성 사이트로 피싱을 유도 할 수 있다.                                                                                                             |       |         |     |   |
| 진단 기준 | 양호 - 사용자로부터 전송된 값에 대해 검증을 하는 경우<br>취약 - 사용자로부터 전송된 값에 대해 검증을 하지 않는 경우                                                                                                                                                                                                                    |       |         |     |   |
| 점검 방법 | <p><a href="http://192.168.153.134/m_board.php?ps_db=data_board">http://192.168.153.134/m_board.php?ps_db=data_board</a> 에서 파라미터를 조작하여 확인</p> <p style="text-align: center;">자유게시판</p>                |       |         |     |   |
| 조치 방법 | 사용자로부터 전송되어온 URL 파라미터, Cookie변수, HTTP Header, Referer 등 모든 HTTP 코드는 항상 변조되어 있을 가능성을 염두에 두고 프로그래밍 해야 하며, 데이터 업데이트 및 인증 등 중요한 작업을 수행하기 위해서는 사용자로부터 전송되어온 HTTP 데이터의 사용을 가능한 자제하고, DB, 세션 등 서버 측에서 입력된 정보를 이용해서 작업을 진행해야 함. 만일 사용자로부터 전송된 값을 꼭 사용해야 한다면 반드시 이들 값의 변조 여부에 대한 유효성 검토를 거쳐야만 한다. |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                          |       |         |     |   |

## 7.2.5. 쿠키 인증 취약점

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                     | 항목 코드 | WAS2-05 | 중요도 | H |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 적절히 보호되지 않은 쿠키를 사용하면 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능하다.                                                                                                                                                                                                                    |       |         |     |   |
| 진단 기준 | 암호 - 쿠키 정보를 암호화 하고 있는 경우<br>취약 - 쿠키 정보를 암호화 하고 있지 않는 경우                                                                                                                                                                                                                                       |       |         |     |   |
| 점검 방법 | Cooxie툴을 사용하여 쿠키 확인<br><pre> user%5Fid=aaaa user%5Fno=8 user%5Fname=aaaa ASPSESSIONIDASSTQRS=BFNPCKCJAAEBAlJDIEPDFFI                     </pre>                                                                                                                                               |       |         |     |   |
| 조치 방법 | 쿠키 인증 취약점을 제거하려면 쿠키정보를 암호화 하거나 Server Side Session을 사용해야 한다.<br>- 중요정보 암호화<br>Client 브라우저에 저장되는 쿠키 내에 중요 정보(ID, PASSWORD, 기타 개인정보)를 포함하는 경우 이를 암호화 한다.<br>- Server Side Session 사용<br>Client Side Session 방식인 Cookie는 그 구조상 다양한 취약점에 노출될 수 있으므로 가능한 웹 서버에서 제공되는 Server Side Session을 사용해야 한다. |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                               |       |         |     |   |



## 7.2.6. 세션/쿠키 타임아웃 설정

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 항목 코드 | WAS2-06 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 세션/쿠키 타임아웃을 설정 하지 않은 경우 사용자가 자리를 비웠을 시 타인이 그 계정을 도용할 가능성이 있다.                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |         |     |   |
| 진단 기준 | 양호 - 세션/쿠키 타임아웃을 설정 했을 경우<br>취약 - 세션/쿠키 타임아웃을 설정하지 않았을 경우                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |         |     |   |
| 점검 방법 | 로그인후 타임아웃이 설정되어 있는지 확인한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |         |     |   |
| 조치 방법 | <p>[ASP]<br/>web.config 에서 설정(분단위)<br/> <code>&lt;system.web&gt;</code><br/> ...생략...<br/> <code>&lt;sessionState mode="InProc" timeout="60" /&gt;</code><br/> ...생략...<br/> <code>&lt;/system.web&gt;</code></p> <p>[JSP]<br/>web.xml에서 설정(분단위)<br/> <code>&lt;session-config&gt;</code><br/> <code>&lt;session-timeout&gt;50&lt;/session-timeout&gt;</code><br/> <code>&lt;/session-config&gt;</code></p> <p>[PHP]<br/>php.ini 에서 설정(초단위)<br/> <code>session.gc_maxlifetime = 1440(기본값)</code></p> |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |         |     |   |

### 7.2.7. 다중 세션 허용

| 분류    | 취약한 인증 권한                                                                                                              | 항목 코드 | WAS2-07 | 중요도 | M |
|-------|------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 사용자가 동일한 세션을 사용할 경우 공격자가 세션을 가로채서 로그인을 할 경우 다중 세션이 허용 된다면 사용자의 정보가 공격자에게 노출이 된다.                                       |       |         |     |   |
| 진단 기준 | 양호 - 다른 2개의 IP로 동시 로그인이 되지 않을 경우<br>취약 - 다른 2개의 IP로 동시 로그인이 되는 경우                                                      |       |         |     |   |
| 점검 방법 | 2개의 다른 IP에서 동시에 로그인을 시도한다.                                                                                             |       |         |     |   |
| 조치 방법 | [JSP]<br>HttpSessionBindingListener를 사용하여 중복로그인 방지<br><br>[ASP, PHP]<br>로그인시 접속자 정보를 DB에 저장하여 다른 세션에서 로그인시 DB를 조회하여 확인 |       |         |     |   |
| 비고    |                                                                                                                        |       |         |     |   |

## 7.2.8. 파라미터 변조

| 분류                                                                                                          | 취약한 인증 권한                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 항목 코드 | WAS2-08            | 중요도 | H    |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------|-----|------|----------|----|-------------------------------------------------------------------------------------------------------------|--------------------|--------|--------------------|--|--|------|-----|------|--------|------|---------|--|--|------|------|--|--|--------|-------------------|--|--|----------|--------|--|--|------------|--|--|--|----------|-------------------------------------------------------------|--|--|------|-------------------------------|--|--|------------|--|--|--|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|-----|------|----|----|-------------------------------------------------------------------------------------------------------------|--------------------|---|--------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| 설명                                                                                                          | 웹 사이트의 URL 파라미터 또는 HTML 코드의 Form 파라미터, Hidden field 등을 통해서 노출되는 변수를 통해서 서버측 프로그램의 로직 및 역할 등을 유추할 수 있으므로, 공격자는 변수에 임의의 값을 입력하여 자신이 원하는 특정 작업을 시도할 수 있다. 만일 웹사이트 로직이 신중하게 설계되지 않았을 경우, 공격자의 조작된 입력값에 의해서 서버측 프로그램이 의도되지 않은 오동작을 일으킬 수 있으며 이를 통해서 인증 및 권한을 우회하여 무단으로 서비스를 이용하거나 결제 금액 변조 등 다양한 문제를 발생시킬 수 있다                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 진단 기준                                                                                                       | 양호 - 사용자로부터 전송된 값에 대해 검증을 하는 경우<br>취약 - 사용자로부터 전송된 값에 대해 검증을 하지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 점검 방법                                                                                                       | <p>http://192.168.100.140/m_userinfo.php에서 파라미터를 조작하여 확인</p> <table><tr><th colspan="4">주문 정보 확인</th></tr><tr><td>성명(실명)</td><td colspan="3">운영자</td></tr><tr><td>전화번호</td><td>111</td><td>휴대전화</td><td>000000</td></tr><tr><td>우편번호</td><td colspan="3">444 - 4</td></tr><tr><td>자택주소</td><td colspan="3">4444</td></tr><tr><td>E-MAIL</td><td colspan="3">admin@fskmail.com</td></tr><tr><td>기타 하실 말씀</td><td colspan="3">000000</td></tr><tr><th colspan="4">배송 &amp; 포장 방법</th></tr><tr><td>배송(택배)선택</td><td colspan="3">core택배,배송비용:2500원,무료배송:30000원 이상,배송문의:1533-8282,많은 이용 바랍니다.</td></tr><tr><td>포장선택</td><td colspan="3">기본포장,포장비용:0원,배송에 무리 없는 튼튼한 포장</td></tr><tr><th colspan="4">주문 &amp; 결제 정보</th></tr><tr><td rowspan="2">주문 내역</td><td colspan="3"><table><tr><th>상품명</th><th>판매가격</th><th>수량</th><th>합계</th></tr><tr><td> +16 페리얼 듀얼소드!! [W30000]</td><td>130,000원<br/>6,500점</td><td>1</td><td>130,000원<br/>6,500점</td></tr></table></td></tr><tr><td>주문 금액</td><td colspan="3"><p>구입총액(130,000원) - 특별할인(0원) = 총액(130,000원)<br/>+ 배송료(0원) + 포장료(0원) - 적립금사용(130,000원)<br/>적립금(6,500점)+특별적립금(0점)</p><div>결제하실 총 금액은 0원 입니다.</div></td></tr></table> |       |                    |     |      | 주문 정보 확인 |    |                                                                                                             |                    | 성명(실명) | 운영자                |  |  | 전화번호 | 111 | 휴대전화 | 000000 | 우편번호 | 444 - 4 |  |  | 자택주소 | 4444 |  |  | E-MAIL | admin@fskmail.com |  |  | 기타 하실 말씀 | 000000 |  |  | 배송 & 포장 방법 |  |  |  | 배송(택배)선택 | core택배,배송비용:2500원,무료배송:30000원 이상,배송문의:1533-8282,많은 이용 바랍니다. |  |  | 포장선택 | 기본포장,포장비용:0원,배송에 무리 없는 튼튼한 포장 |  |  | 주문 & 결제 정보 |  |  |  | 주문 내역 | <table><tr><th>상품명</th><th>판매가격</th><th>수량</th><th>합계</th></tr><tr><td> +16 페리얼 듀얼소드!! [W30000]</td><td>130,000원<br/>6,500점</td><td>1</td><td>130,000원<br/>6,500점</td></tr></table> |  |  | 상품명 | 판매가격 | 수량 | 합계 |  +16 페리얼 듀얼소드!! [W30000] | 130,000원<br>6,500점 | 1 | 130,000원<br>6,500점 | 주문 금액 | <p>구입총액(130,000원) - 특별할인(0원) = 총액(130,000원)<br/>+ 배송료(0원) + 포장료(0원) - 적립금사용(130,000원)<br/>적립금(6,500점)+특별적립금(0점)</p> <div>결제하실 총 금액은 0원 입니다.</div> |  |  |
| 주문 정보 확인                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 성명(실명)                                                                                                      | 운영자                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 전화번호                                                                                                        | 111                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 휴대전화  | 000000             |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 우편번호                                                                                                        | 444 - 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 자택주소                                                                                                        | 4444                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| E-MAIL                                                                                                      | admin@fskmail.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 기타 하실 말씀                                                                                                    | 000000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 배송 & 포장 방법                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 배송(택배)선택                                                                                                    | core택배,배송비용:2500원,무료배송:30000원 이상,배송문의:1533-8282,많은 이용 바랍니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 포장선택                                                                                                        | 기본포장,포장비용:0원,배송에 무리 없는 튼튼한 포장                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 주문 & 결제 정보                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 주문 내역                                                                                                       | <table><tr><th>상품명</th><th>판매가격</th><th>수량</th><th>합계</th></tr><tr><td> +16 페리얼 듀얼소드!! [W30000]</td><td>130,000원<br/>6,500점</td><td>1</td><td>130,000원<br/>6,500점</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |                    | 상품명 | 판매가격 | 수량       | 합계 |  +16 페리얼 듀얼소드!! [W30000] | 130,000원<br>6,500점 | 1      | 130,000원<br>6,500점 |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
|                                                                                                             | 상품명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 판매가격  | 수량                 | 합계  |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
|  +16 페리얼 듀얼소드!! [W30000] | 130,000원<br>6,500점                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 1     | 130,000원<br>6,500점 |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 주문 금액                                                                                                       | <p>구입총액(130,000원) - 특별할인(0원) = 총액(130,000원)<br/>+ 배송료(0원) + 포장료(0원) - 적립금사용(130,000원)<br/>적립금(6,500점)+특별적립금(0점)</p> <div>결제하실 총 금액은 0원 입니다.</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 조치 방법                                                                                                       | 사용자로부터 전송되어온 URL 파라미터, Cookie변수, HTTP Header, Referer 등 모든 HTTP 코드는 항상 변조되어 있을 가능성을 염두에 두고 프로그래밍 해야 하며, 데이터 업데이트 및 인증 등 중요한 작업을 수행하기 위해서는 사용자로부터 전송되어온 HTTP 데이터의 사용을 가능한 자제하고, DB, 세션 등 서버 측에서 입력된 정보를 이용해서 작업을 진행해야 함. 만일 사용자로부터 전송된 값을 꼭 사용해야 한다면 반드시 이들 값의 변조 여부에 대한 유효성 검토를 거쳐야만 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |
| 비고                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |                    |     |      |          |    |                                                                                                             |                    |        |                    |  |  |      |     |      |        |      |         |  |  |      |      |  |  |        |                   |  |  |          |        |  |  |            |  |  |  |          |                                                             |  |  |      |                               |  |  |            |  |  |  |       |                                                                                                                                                                                                                                                                        |  |  |     |      |    |    |                                                                                                             |                    |   |                    |       |                                                                                                                                                   |  |  |

## 7.2.9. 검증되지 않은 리다이렉트와 포워드

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                   | 항목 코드 | WAS2-09 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 어플리케이션은 종종 다른 페이지로 사용자를 리다이렉트 시키거나, 비슷한 방식으로 내부 포워드를 사용한다. 때로는 목적 페이지는 승인되지 않은 파라미터 내에 지정할 수 있고, 공격자가 목적지 페이지를 선택하도록 한다. 따라서 목적 페이지에 대한 검증이 미흡할 경우 공격자가 의도한 악성 사이트로 리다이렉트 되어 악성코드 설치되거나 권한 없는 페이지에 접근을 시도할 수 있다.                                                                            |       |         |     |   |
| 진단 기준 | 양호 - 목적지를 조작 할 수 있는 사용자 파라미터 값이 포함되지 않은 경우<br>취약 - 목적지를 조작 할 수 있는 사용자 파라미터 값이 포함된 경우                                                                                                                                                                                                        |       |         |     |   |
| 점검 방법 | 게시판에서 리다이렉트 파라미터를 변조하여 확인<br><div>                         쿼리                         <input type="text" value="test"/> </div> <div> <a href="http://www.naver.com/redirect?url=http://www.google.com">www.naver.com/redirect?url=http://www.google.com</a>Naver                     </div> |       |         |     |   |
| 조치 방법 | 리다이렉트와 포워드에 대한 안전한 사용은 아래와 같은 몇 가지 방법에 의해 할 수 있다.<br>- 단순히 리다이렉트와 포워드의 사용을 피한다.<br>- 만약 사용한다면, 목적지를 계산하는 사용자 파라미터를 포함하지 않는다.<br>- 목적 파라미터를 사용할 수밖에 없다면, 제공된 값이 유효한지, 그 사용자에게 허용된 것 인지를 확실히 검증 해야 한다.                                                                                        |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                             |       |         |     |   |

## 7.2.10. 불충분한 인증

| 분류    | 취약한 인증 권한                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 항목 코드 | WAS2-10 | 중요도 | H |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | 민감한 데이터에 접근 가능한 경로에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 사용자가 권한 외의 페이지에 접근하여 정보를 유출하거나 변조할 수 있으므로 추가적인 인증 절차를 구현하여야 한다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |         |     |   |
| 진단 기준 | 양호 - 중요 정보 페이지 접근 시 추가 인증을 하는 경우<br>취약 - 중요 정보 페이지 접근에 대한 추가 인증을 하지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |         |     |   |
| 점검 방법 | 1. 개인정보 수정 및 비밀번호 수정 기능 페이지 접근 전에 본인인증에 대한 재인증 여부 확인<br>2. 인증 후 페이지에 아이디만을 인증값으로 하여 변수로 관리 되고 있는지 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |         |     |   |
| 조치 방법 | <p>중요 정보 페이지에 대한 추가 인증 로직 추가 구현</p> <ol style="list-style-type: none"> <li>1. 개인정보 및 비밀번호 수정 페이지와 같은 중요 정보를 표시하는 페이지에서는 본인 인증을 재확인하는 로직을 구현하고, 인증 후 사용자가 이용 가능 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증하여야 함</li> <li>2. 접근 통제 정책을 구현하고 있는 코드는 구조화, 모듈화가 되어 있어야 함</li> <li>3. 접근제어가 필요한 모든 페이지에 통제수단(로그인 체크 및 권한 체크)을 구현해야 하며 특히, 하나의 프로세스가 여러 개의 페이지 또는 모듈로 이루어져 있을 때 권한 체크가 누락되는 경우를 방지하기 위해서 공통 모듈을 사용하는 것을 권장함</li> <li>4. 인증 과정을 처리하는 부분에 Client Side Script(Javascript, VBScript 등)를 사용하면 사용자가 임의로 수정할 수 있으므로 Server Side Script(PHP, ASP, JSP 등)를 통하여 인증 및 필터링 과정을 수행함</li> </ol> |       |         |     |   |
| 비고    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |         |     |   |

## 7.3. 원격명령실행

### 7.3.1. 파일 업로드

| 분류    | 원격명령실행                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 항목 코드 | WAS3-01 | 중요도 | H |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|---|
| 설명    | <p>첨부 파일 업로드 기능이 있는 게시판 등에서 실행 가능한 확장자를 가진 스크립트 파일의 업로드가 허용되는 경우, 공격자에 의해 악성 프로그램이 업로드 되어 실행 될 수 있다.</p> <p>공격자는 첨부한 악성 프로그램을 실행하여 웹 서버 사용자 권한을 획득한 후 내부 네트워크로의 침입을 시도하거나 DB에 연결하여 중요 정보를 유출시킬 수 있다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |         |     |   |
| 진단 기준 | <p>양호 - 첨부 파일 업로드시 스크립트 파일이 업로드 되지 않을 경우</p> <p>취약 - 첨부 파일 업로드시 스크립트 파일이 업로드 되는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |         |     |   |
| 점검 방법 | <p>파일 업로드시 스크립트 파일 업로드 가능 여부 확인</p> <p><b>파일첨부_1</b> <code>Documents and Settings\Administrator\바탕 화면\test file upload.php</code> <a href="#">찾아보기...</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |         |     |   |
| 조치 방법 | <p>사용자 입력 값 전체에 대해 문자열 필터링을 수행해야 하며 ..., ', W0, %00, % 등과 같은 특수 문자 탐지 시 제거 또는 replace 시키는 형태로 필터링 처리를 해야 한다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |         |     |   |
| 비고    | <p>자료실, 게시판 등에서 사용자에게 파일을 서버로 업로드 할 수 있는 기능을 제공할 경우, 사용자가 실행 가능한 파일을 웹서버에 업로드하여 시스템 명령어를 사용할 수 있을 가능성이 있으므로 다음과 같은 보안 대책을 적용해야 한다.</p> <ul style="list-style-type: none"> <li>- 파일업로드 기능 제공시, 업로드가 허용된 확장자만 가능토록 Server Side에서 컨트롤해야 한다.</li> <li>- 업로드를 허용할 확장자 리스트를 제외한 모든 파일의 업로드를 금지하는 white list 방식의 필터링을 적용해야 한다.</li> <li>- 파일의 확장자 검사를 할 때, 대소문자 구분없이 비교하는 함수를 사용해야 하며, 이중 확장자(ex: file.jpg.jsp 등)나 확장자 끝에 “.”를 사용하는 등의 trick에 의해서 확장자 검사가 우회되지 않도록 주의깊게 처리해야 한다.</li> <li>- 파일이 업로드 되는 디렉토리는 실행 권한 및 스크립트 수행설정이 제거되어야 한다.</li> <li>- 업로드 디렉토리를 별도의 드라이브 또는 별도의 물리적 서버에 분리하여 저장하고, 웹사이트에서 다운로드 모듈 및 출력 모듈을 작성하여 처리함으로써, 외부로부터 업로드 디렉토리에 대한 URL을 통한 접근이 불가능하도록 해야한다.</li> <li>- 업로드되는 파일을 저장할 때, 파일명과 확장자를 추측할 수 없는 무작위 문자열 및 실행 불가능한 확장자로 변경하여 저장 해야한다.</li> <li>- 저장 경로 및 파일명은 DB에 저장한 후, index 번호를 통해서 호출하도록 함으로써 파일명 및 경로를 외부에 노출되지 않도록 해야한다.</li> </ul> |       |         |     |   |