

주요정보통신기반시설

기술적 취약점 분석·평가 방법 상세가이드

01

**Unix fl¢**

1. 계정 관리 ····································· 기본 5 / 선택 90

2. 파일 및 디렉터리 관리 ············· 기본 18 / 선택 113

3. 서비스 관리 ······························ 기본 39 / 선택 119

4. 패치 관리 ································· 기본 85

5. 로그 관리 ································· 기본 89 / 선택 142



Unix 서버 취약점 분석·평가 항목

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 점검항목 | 항목 중요도 | 항목코드 |
| 1. 계정 관리 | root 계정 원격 접속 제한 | 상 | U-01 |
| 패스워드 복잡성 설정 | 상 | U-02 |
| 계정 잠금 임계값 설정 | 상 | U-03 |
| 패스워드 파일 보호 | 상 | U-04 |
| root 이외의 UID가 ‘0’금지 | 중 | U-44 |
| root 계정 su 제한 | 하 | U-45 |
| 패스워드 최소 길이 설정 | 중 | U-46 |
| 패스워드 최대 사용기간 설정 | 중 | U-47 |
| 패스워드 최소 사용기간 설정 | 중 | U-48 |
| 불필요한 계정 제거 | 하 | U-49 |
| 관리자 그룹에 최소한의 계정 포함 | 하 | U-50 |
| 계정이 존재하지 않는 GID 금지 | 하 | U-51 |
| 동일한 UID 금지 | 중 | U-52 |
| 사용자 shell 점검 | 하 | U-53 |
| Session Timeout 설정 | 하 | U-54 |
| 2. 파일 및 디렉터리 관리 | root 홈, 패스 디렉터리 권한 및 패스 설정 | 상 | U-05 |
| 파일 및 디렉터리 소유자 설정 | 상 | U-06 |
| /etc/passwd 파일 소유자 및 권한 설정 | 상 | U-07 |
| /etc/shadow 파일 소유자 및 권한 설정 | 상 | U-08 |
| /etc/hosts 파일 소유자 및 권한 설정 | 상 | U-09 |
| /etc/(x)inetd.conf 파일 소유자 및 권한 설정 | 상 | U-10 |
| /etc/syslog.conf 파일 소유자 및 권한 설정 | 상 | U-11 |
| /etc/services 파일 소유자 및 권한 설정 | 상 | U-12 |
| SUID, SGID, Sticky bit 설정 파일 점검 | 상 | U-13 |
| 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 | 상 | U-14 |
| world writable 파일 점검 | 상 | U-15 |
| /dev에 존재하지 않는 device 파일 점검 | 상 | U-16 |
| $HOME/.rhosts, hosts.equiv 사용 금지 | 상 | U-17 |
| 접속 IP 및 포트 제한 | 상 | U-18 |
| hosts.lpd 파일 소유자 및 권한 설정 | 하 | U-55 |
| UMASK 설정 관리 | 중 | U-56 |
| 홈디렉토리 소유자 및 권한 설정 | 중 | U-57 |
| 홈디렉토리로 지정한 디렉토리의 존재 관리 | 중 | U-58 |
| 숨겨진 파일 및 디렉토리 검색 및 제거 | 하 | U-59 |

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 점검항목 | 항목 중요도 | 항목코드 |
| 3. 서비스 관리 | finger 서비스 비활성화 | 상 | U-19 |
| Anonymous FTP 비활성화 | 상 | U-20 |
| r 계열 서비스 비활성화 | 상 | U-21 |
| cron 파일 소유자 및 권한설정 | 상 | U-22 |
| Dos 공격에 취약한 서비스 비활성화 | 상 | U-23 |
| NFS 서비스 비활성화 | 상 | U-24 |
| NFS 접근 통제 | 상 | U-25 |
| automountd 제거 | 상 | U-26 |
| RPC 서비스 확인 | 상 | U-27 |
| NIS, NIS+ 점검 | 상 | U-28 |
| tftp, talk 서비스 비활성화 | 상 | U-29 |
| Sendmail 버전 점검 | 상 | U-30 |
| 스팸 메일 릴레이 제한 | 상 | U-31 |
| 일반사용자의 Sendmail 실행 방지 | 상 | U-32 |
| DNS 보안 버전 패치 | 상 | U-33 |
| DNS Zone Transfer 설정 | 상 | U-34 |
| 웹서비스 디렉토리 리스팅 제거 | 상 | U-35 |
| 웹서비스 웹 프로세스 권한 제한 | 상 | U-36 |
| 웹서비스 상위 디렉토리 접근 금지 | 상 | U-37 |
| 웹서비스 불필요한 파일 제거 | 상 | U-38 |
| 웹서비스 링크 사용 금지 | 상 | U-39 |
| 웹서비스 파일 업로드 및 다운로드 제한 | 상 | U-40 |
| 웹서비스 영역의 분리 | 상 | U-41 |
| ssh 원격접속 허용 | 중 | U-60 |
| ftp 서비스 확인 | 하 | U-61 |
| ftp 계정 shell 제한 | 중 | U-62 |
| Ftpusers 파일 소유자 및 권한 설정 | 하 | U-63 |
| Ftpusers 파일 설정 | 중 | U-64 |
| at 파일 소유자 및 권한 설정 | 중 | U-65 |
| SNMP 서비스 구동 점검 | 중 | U-66 |
| SNMP 서비스 커뮤니티스트링의 복잡성 설정 | 중 | U-67 |
| 로그온 시 경고 메시지 제공 | 하 | U-68 |
| NFS 설정파일 접근 제한 | 중 | U-69 |
| expn, vrfy 명령어 제한 | 중 | U-70 |
| Apache 웹 서비스 정보 숨김 | 중 | U-71 |
| 4. 패치 관리 | 최신 보안패치 및 벤더 권고사항 적용 | 상 | U-42 |
| 5. 로그 관리 | 로그의 정기적 검토 및 보고 | 상 | U-43 |
| 정책에 따른 시스템 로깅 설정 | 하 | U-72 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | [Telnet]  #cat /etc/default/login CONSOLE=/dev/console [SSH]  #cat /etc/ssh/sshd\_config  PermitRootLogin no |
| LINUX | [Telnet]  #cat /etc/pam.d/login  auth required /lib/security/pam\_securetty.so #cat /etc/securetty |

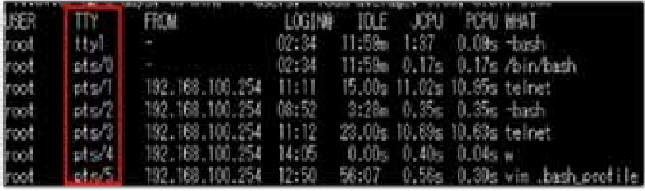
|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-01 | (상) | 1. | 계정관리 | > | 1.1 | root | 계정 | 원격접속 제한 | | | |
| 취약점 개요 | | | | | | | | | | | |
| 점검내용 | | * 시스템 정책에 root 계정의 원격터미널 접속차단 설정이 적용되어 있는지 점검 | | | | | | | | | |
| 점검목적 | | * 관리자계정 탈취로 인한 시스템 장악을 방지하기 root 계정 접근 시도를 원천적으로 차단하기 위함 | | | | | | | 위해 | 외부 | 비인가자의 |
| 보안위협 | | * root 계정은 운영체제의 모든기능을 설정 및 변경이 가능하여(프로세스, 커 널변경 등) root 계정을 탈취하여 외부에서 원격을 이용한 시스템 장악 및 각종 공격으로(무작위 대입 공격) 인한 root 계정 사용 불가 위협 | | | | | | | | | |
| 참고 | | ※ root 계정: 여러 사용자가 사용하는 컴퓨터에서 모든 기능을 관리할 수 있는 총괄권한 을 가진 유일한 특별 계정. 유닉스 시스템의 루트(root)는 시스템 관리자인 운용 관리 자(Super User)로서 윈도우의 Administrator 보다 높은 System 계정에 해당하며, 사용 자 계정을 생성하거나 소프트웨어를 설치하고, 환경 및 설정을 변경하거나 시스템의 동작을 감시 및 제어할 수 있음  ※ 무작위 대입 공격(Brute Force Attack): 특정한 암호를 풀기 위해 가능한 모든 값을 대 입하는 공격 방법  ※ 사전 대입 공격(Dictionary Attack): 사전에 있는 단어를 입력하여 암호를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법 | | | | | | | | | |
| 점검대상 및 판단기준 | | | | | | | | | | | |
| 대상 | | * SOLARIS, LINUX, AIX, HP-UX 등 | | | | | | | | | |
| 판단기준 | | 양호 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우 | | | | | | | | | |
| 취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우 | | | | | | | | | |
| 조치방법 | | 원격 접속 시 root 계정으로 ~~바로 접속 할 수 없도록 설정파일 수정~~ | | | | | | | | | |
| 점검 및 조치사례 | | | | | | | | | | | |
|  | | | | | | | | | | | |

UNIX 서버

|  |  |
| --- | --- |
|  | pts/0 ~ pts/x 관련 설정이 존재하지 않음  [SSH]  #cat /etc/sshd\_config  PermitRootLogin no |
| AIX | [Telnet]  #cat /etc/security/user rlogin = false  [SSH]  #cat /etc/sshd\_config  PermitRootLogin no |
| HP-UX | [Telnet]  #cat /etc/securetty console  [SSH]  #cat /etc/sshd\_config  PermitRootLogin no |
| 위에 제시한 내용으로 설정되어 있을 경우 root 원격 접속이 차단됨 / 내용 설정에 대해서는 아래의 보안설정방법을 참고함 | |

|  |  |
| --- | --- |
| U-01 (상) | 1. 계정관리 > 1.1 root 계정 원격접속 제한 |
| * SOLARIS   [Telnet 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/default/login” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입  (수정 전) #CONSOLE=/dev/console  (수정 후) CONSOLE=/dev/console  [SSH 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/ssh/sshd\_config” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입  (수정 전) #PermitRootLogin Yes (수정 후) PermitRootLogin No   * LINUX   [Telnet 서비스 사용시]  Step 1) “/etc/securetty” 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리 Step 2) “/etc/pam.d/login” 파일 수정 또는, 신규 삽입 | |

UNIX 서버



|  |  |
| --- | --- |
| U-01 (상) | 1. 계정관리 > 1.1 root 계정 원격접속 제한 |
| (수정 전) #auth required /lib/security/pam\_securetty.so  (수정 후) auth required /lib/security/pam\_securetty.so  ※ /etc/securetty : Telnet 접속 시 root 접근 제한 설정 파일  “/etc/securetty” 파일 내 \*pts/x 관련 설정이 존재하는 경우 PAM 모듈 설정과 관계없이 root 계정 접속을 허용하므로 반드시 "securetty" 파일에서 pts/x 관련 설정 제거 필요  \*pts/0 ~ pts/x 설정 :  tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함 pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함  [SSH 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/ssh/sshd\_config” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입  (수정 전) #PermitRootLogin Yes (수정 후) PermitRootLogin No   * AIX   [Telnet 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/security/user” 파일 열기  Step 2) rlogin 설정을 아래와 같이 수정 또는, 신규 삽입 (root 설정에 해당되는 부분 수정) (수정 전) rlogin = true  (수정 후) rlogin = false  rlogin(remote-login): 자주 접속하는 호스트에 대해 자동으로 원격 접속을 할 수 있도록 사용 하는 명령어  [SSH 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/ssh/sshd\_config” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입  (수정 전) #PermitRootLogin Yes (수정 후) PermitRootLogin No   * HP-UX   [Telnet 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/securetty” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입 | |

UNIX 서버

|  |  |
| --- | --- |
| U-01 (상) | 1. 계정관리 > 1.1 root 계정 원격접속 제한 |
| (수정 전) #console  (수정 후) console  ※ “/etc/securetty” 파일은 디폴트로 존재하지 않으므로 /etc 디렉터리 내에 "securetty" 파일 이 존재하지 않는 경우 새로 생성한 후 적용함  (※ vi 편집기를 사용한 파일 내용 수정: 부록 참고)  #vi /etc/securetty  [SSH 서비스 사용시]  Step 1) vi 편집기를 이용하여 “/etc/ssh/sshd\_config” 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입  (수정 전) #PermitRootLogin Yes (수정 후) PermitRootLogin No | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | /etc/default/passwd |
| INUX - RHEL5 | /etc/pam.d/system-auth |
| LINUX - RHEL7 | /etc/security/pwquality.conf |
| AIX | /etc/security/user |
| HP-UX | /etc/default/security |
| OS별 점검 파일을 열어 패스워드 복잡도 관련 설정 확인 후 아래의 보안설정방법 에 따라 설정을 변경함(최소길이, 특수문자, 숫자 포함 등 설정) | |

|  |  |
| --- | --- |
| U-02 (상) | 1. 계정관리 > 1.2 패스워드 복잡성 설정 |
| 취약점 개요 | |
| 점검내용 | * 시스템 정책에 사용자 계정(root 및 일반계정 모두 해당) 패스워드 복잡성 관련 설정이 되어 있는지 점검 |
| 점검목적 | * 패스워드 복잡성 관련 정책이 설정되어 있는지 점검하여 비인가자의 공격(무 작위 대입 공격, 사전 대입 공격 등)에 대비가 되어 있는지 확인하기 위함 |
| 보안위협 | * 복잡성 설정이 되어있지 않은 패스워드는 사회공학적인 유추가 가능 할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크렉이 가능함 |
| 참고 | ※ 패스워드 복잡성: 사용자 패스워드 설정 시 영문(대문자, 소문자), 숫자, 특수문자가 혼 합된 일정 길이 이상으로 패스워드를 설정하는 방법 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 패스워드 최소길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정된 경우 |
| 취약 : 패스워드 최소길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정된 경우 |
| 조치방법 | 계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정 및 패스워드 복잡성 옵션 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   < 부적절한 패스워드 유형 >   * 사전에 나오는 단어나 이들의 조합 * 길이가 너무 짧거나, NULL(공백)인 패스워드 | |

UNIX 서버

|  |  |
| --- | --- |
| U-02 (상) | 1. 계정관리 > 1.2 패스워드 복잡성 설정 |
| * 키보드 자판의 일련의 나열 (예) abcd, qwert, etc * 사용자 계정 정보에서 유추 가능한 단어들   (예) 지역명, 부서명, 계정명, 사용자 이름의 이니셜, root, rootroot, root123, admin 등  < 패스워드 관리 방법 >   * 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정   ※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을  조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개)  나. 영문 소문자(26개) 다. 숫자(10개)  라. 특수문자(32개)   * 시스템마다 상이한 패스워드 사용 * 패스워드를 기록해 놓을 경우 변형하여 기록   < 패스워드 설정 파일 정리 >   * SOLARIS [10 이상버젼]   Step 1) 패스워드 복잡성 설정  #/etc/default/passwd 내용을 내부 정책에 맞도록 편집  권장 값 기능 설명 HISTORY=10 이전 패스워드 기억 개수 이전 10개의 암호를 기억함 MINDIFF=4 이전 암호와 차이 이전 암호와 4자 이상 차이 요구 MINALPHA=1 최소 문자 요구 최소 1자 이상 문자 요구  MINNONALPHA=1 최소 숫자 또는 특수문자 요구 숫자 또는 특수문자 1자 이상 요구 MINUPPER=1 최소 대문자 요구 최소 1자 이상 대문자 요구 MINLOWER=1 최소 소문자 요구 최소 1자 이상 소문자 요구 MAXREPEATS=0 연속문자 사용 허용 0일 경우 문자 연속 사용이 불가 MINSPECIAL=1 최소 특수문자 요구 최소 1자 이상 특수문자 요구 MINDIGIT=1 최소 숫자 요구 최소 1자 이상 숫자 요구 NAMECHECK=YES 아이디와 패스워드 동일 검증 아이디와 동일한 패스워드 사용 불가  ※ DIGIT 이나 SPECIAL 이 설정되어 있을 경우 NONALPHA 설정 안 됨   * LINUX - RHEL5   Step 1) 패스워드 복잡성 설정 파일 확인  #/etc/pam.d/system-auth, /etc/login.defs 내용을 내부 정책에 맞도록 편집  Step 2) /etc/pam.d/system-auth 파일 설정  ※ 다음 라인에 패스워드 정책을 설정함 | |

UNIX 서버



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 권장 | 값 |  | 기능 | | 설명 |
| lcredit=-1 | 최소 | | 소문자 요구 |  | 소문자 최소 1자 이상 요구 |
| ucredit=-1 | 최소 | | 대문자 요구 |  | 최소 대문자 1자 이상 요구 |
| dcredit=-1 | 최소 | | 숫자 요구 |  | 최소 숫자 1자 이상 요구 |
| ocredit=-1 | 최소 | | 특수문자 요구 |  | 최소 특수문자 1자 이상 요구 |
| minlen=8 | 최소 | | 패스워드 길이 | 설정 | 최소 8자리 이상 설정 |
| difok=N | | 기존 패스워드와 비교 | | | 기본값 10(50%)) |

|  |  |
| --- | --- |
| U-02 (상) | 1. 계정관리 > 1.2 패스워드 복잡성 설정 |
| - 패스워드 정책 설정 예시  # vi /etc/pam.d/system-auth  password requisite /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1   * LINUX - RHEL7   Step 1) 패스워드 복잡성 설정 파일 확인  #/etc/security/pwquality.conf 파일 수정  ※ 다음 라인에 패스워드 정책을 설정함  - 패스워드 정책 설정 예시  # vi /etc/security/pwquality.conf  password requisite pam\_cracklib.so try\_first\_pass retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1  ※ 각 변수에 대한 설명 / 각 항목에서 -1 값은 반드시 해당하는 문자를 포함시켜야 함   * AIX   Step 1) 패스워드 복잡성 설정 파일 확인  #/etc/security/user 파일 내용을 내부 정책에 맞도록 설정 | |

UNIX 서버

|  |  |  |  |
| --- | --- | --- | --- |
| 권장 값 | 기능 | | 설명 |
| dictionlist=/usr/share/dict/words | | unix 명령어 포함 여부 검증경로 설정 | |
| histexpire=26 | 동일한 패스워드 재사용 기간 | | 26주 후 사용가능 |
| histsize=10 | 이전 패스워드 기억 개수 이전 10개 패스워드 기억(사용불가) | | |
| maxrepeats=2 | 반복 가능한 동일 문자의 최대 수 2개이상 동일문자 사용 금지 | | |
| minalpha=2 | 최소 알파벳 문자 포함 | | 2개 이상 알파벳 사용 |
| minother=2 | 최소 알파벳 문자 이외의 문자 수 | | 2개 이상 숫자, 특수문자 사용 |
| mindiff=4 | 이전 패스워드와 동일문자 수 | | 이전 패스워드와 4개까지 동일문자 사용 |
| minlen=8 | 패스워드 최소 길이 | | 8자리 이상 패스워드 작성 |

|  |  |  |
| --- | --- | --- |
| 권장 값 | 기능 | 설명 |
| MIN\_PASSWORD\_LENGTH=8 | 암호의 최소 길이 | 최소 8자리 패스워드 |
| PASSWORD\_MIN\_UPPER\_CASE\_CHARS=1 | 최소 대문자 필요 개수 | 최소 1개의 대문자 |
| PASSWORD\_MIN\_LOWER\_CASE\_CHARS=1 | 최소 소문자 필요 개수 | 최소 1개의 소문자 |
| PASSWORD\_MIN\_DIGIT\_CHARS=1 | 최소 숫자 필요 개수 | 최소 1개의 숫자 |
| PASSWORD\_MIN\_SPECIAL\_CHARS=1 | 최소 특수문자 필요 개수 | 최소 1개의 특수문자 |

|  |  |
| --- | --- |
| U-02 (상) | 1. 계정관리 > 1.2 패스워드 복잡성 설정 |
| * HP-UX   Step 1) 패스워드 복잡성 설정  #/etc/default/security 내용을 내부 정책에 맞도록 편집 | |
| 조치 시 영향 | 패스워드 변경 시 Web, WAS, DB연동 구간에서 문제가 발생할 수 있으므로 연  동 구간에 미칠 수 있는 영향을 고려하여 적용 필요 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | #cat /etc/default/login RETRIES=5  SOLARIS 5.9 이상 버전일 경우 추가적으로 “policy.conf” 파일  확인  #cat /etc/security/policy.conf  LOCK\_AFTER\_RETRIES=YES |
| LINUX | #cat /etc/pam.d/system-auth  auth required /lib/security/pam\_tally.so deny=5 unlock\_time=120 no\_magic\_root  account required /lib/security/pam\_tally.so  no\_magic\_root reset |
| AIX | #cat /etc/security/user loginretries=10 |
| HP-UX | #cat /tcb/files/auth/system/default |

|  |  |
| --- | --- |
| U-03 (상) | 1. 계정관리 > 1.3 계정 잠금 임계값 설정 |
| 취약점 개요 | |
| 점검내용 | * 사용자 계정 로그인 실패 시 계정잠금 임계값이 설정되어 있는지 점검 |
| 점검목적 | * 계정탈취 목적의 무작위 대입 공격 시 해당 계정을 잠금하여 인증 요청에 응답하는 리소스 낭비를 차단하고 대입 공격으로 인한 비밀번호 노출 공격 을 무력화하기 위함 |
| 보안위협 | * 패스워드 탈취 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)의 인 증 요청에 대해 설정된 패스워드와 일치 할 때까지 지속적으로 응답하여 해 당 계정의 패스워드가 유출 될 수 있음 |
| 참고 | ※ 사용자 로그인 실패 임계 값: 시스템에 로그인 시 몇 번의 로그인 실패에 로그인을 차 단할 것인지 결정하는 값 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 계정 잠금 임계값이 10회 이하의 값으로 설정되어 있는 경우 |
| 취약 : 계정 잠금 임계값이 설정되어 있지 않거나, 10회 이하의 값으로 설정되 지 않은 경우 |
| 조치방법 | 계정 잠금 임계값을 10회 이하로 설정 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버

|  |  |
| --- | --- |
|  | u\_maxtries#5  HP-UX 11.v3 이상일 경우 “security” 파일 확인 #cat /etc/default/security AUTH\_MAXTRIES=10 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| 옵션 | 설명 |
| no\_magic\_root | root에게는 패스워드 잠금 설정을 적용하지 않음 |
| deny=5 | 5회 입력 실패 시 패스워드 잠금 |
| unlock\_time | 계정 잠김 후 마지막 계정 실패 시간부터 설정된 시간이 지나면 자동 계정 잠김 해제 (단위: 초) |
| reset | 접속 시도 성공 시 실패한 횟수 초기화 |

|  |  |
| --- | --- |
| U-03 (상) | 1. 계정관리 > 1.3 계정 잠금 임계값 설정 |
| * SOLARIS   - SOLARIS 5.9 이하 버전 -  Step 1) vi 편집기를 이용하여 “/etc/default/login” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) #RETRIES=2  (수정 후) RETRIES=10  - SOLARIS 5.9 이상 버전 -  Step 1) vi 편집기를 이용하여 “/etc/default/login” 파일 열기  Step 2) 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 횟수 설정) (수정 전) #RETRIES=2  (수정 후) RETRIES=10  Step 3) vi 편집기를 이용하여 “/etc/security/policy.conf” 파일 열기 Step 4) 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 정책사용 설정)  (수정 전) #LOCK\_AFTER\_RETRIES=NO  (수정 후) LOCK\_AFTER\_RETRIES=YES   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/pam.d/system-auth” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  auth required /lib/security/pam\_tally.so deny=5 unlock\_time=120 no\_magic\_root  account required /lib/security/pam\_tally.so no\_magic\_root reset | |

UNIX 서버



|  |  |
| --- | --- |
| U-03 (상) | 1. 계정관리 > 1.3 계정 잠금 임계값 설정 |
| * AIX   Step 1) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) loginretries = 0 (수정 후) loginretries = 10   * HP-UX   - HP-UX 11.v2 이하 버전 -  Step 1) vi 편집기를 이용하여 /tcb/files/auth/system/default 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) u\_maxtries#  (수정 후) u\_maxtries#10  ※ HP-UX 서버에 계정 잠금 정책 설정을 위해서는 HP-UX 서버가 Trusted Mode로 동작하고 있어야하므로 Trusted Mode로 전환한 후 잠금 정책 적용  - HP-UX 11.v3 이상 버전 -  Step 1) vi 편집기를 이용하여 /etc/default/security 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) #AUTH\_MAXTRIES=0  (수정 후) AUTH\_MAXTRIES=10  ※ Standard and Shadow modes only | |
|  | HP-UX 경우 Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 |
|  | 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode |
| 조치 시 영향 | 로의 전환이 필요함  Liunx의 pam.d/system-auth의 내용 수정 시 해당 라이브럴리가 실제 존재하 |
|  | 는지 확인 필요(/lib/security/pam\_tally.so – 파일 미존재시 모든 계정 |
|  | 로그인 안되는 장애가 발생될 수 있음) |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
|  | Step 1) /shadow 파일의 패스워드 암호화 존재 확인 |
|  | (일반적으로 /etc 디렉터리 내 존재) |
| SOLARIS, LINUX | #ls /etc  Step 2) /etc/passwd 파일 내 두 번째 필드가 “x” 표시되는지 확인  #cat /etc/passwd |
|  | root:x:0:0:root:/root:/bin/bash |
|  | (※ “passwd” 파일 구조: 부록 참조} |
| HP-UX | /etc/security/passwd 파일 내 설정된 패스워드 점검 |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-04 (상) | 1. 계정관리 > 1.4 패스워드 파일 보호 |
| 취약점 개요 | |
| 점검내용 | * 시스템의 사용자 계정(root, 일반계정) 정보가 저장된 파일(예 /etc/passwd,   /etc/shadow)에 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검 |
| 점검목적 | * 일부 오래된 시스템의 경우 /etc/passwd 파일에 패스워드가 평문으로 저장 되므로 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검하여 비인 가자의 패스워드 파일 접근 시에도 사용자 계정 패스워드가 안전하게 관리 되고 있는지 확인하기 위함 |
| 보안위협 | * 사용자 계정 패스워드가 저장된 파일이 유출 또는 탈취 시 평문으로 저장된   패스워드 정보가 노출될 수 있음 |
| 참고 | ※ 관련 점검 항목 : U-07(상), U-08(상) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 쉐도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우 |
| 취약 : 쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않 는 경우 |
| 조치방법 | 패스워드 암호화 저장∙관리 설정 적용 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX   Step 1) #pwconv ---> 쉐도우 패스워드 정책 적용 방법 Step 2) #pwunconv ---> 일반 패스워드 정책 적용 방법   * AIX | |

UNIX 서버



|  |  |
| --- | --- |
| U-04 (상) | 1. 계정관리 > 1.4 패스워드 파일 보호 |
| Step 1) #cat /etc/security/passwd Step 2) 패스워드 암호화 여부 확인  ※ AIX 서버는 기본적으로 “/etc/security/passwd” 파일에 패스워드를 암호화하여 저장·관리   * HP-UX   HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 “/tcb/files/auth” 디렉터 리에 계정 이니셜과 계정 이름에 따라 파일로 저장∙관리할 수 있으므로 Trusted Mode인지 확 인 후 UnTrusted Mode인 경우 모드를 전환함  Step 1) Trusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행  #/etc/tsconvert  Step 2) UnTrusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행  #/etc/tsconvert -r2 | |
| 조치 시 영향 | HP-UX 경우 Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode 로의 전환 필요 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | #echo $PATH  /usr/local/sbin:/sbin:/usr/sbin:/bin:/usr/bin/X11:  /usr/local/bin:/usr/bin:/usr/X11R6/bin:/root/bin  위와 같이 출력되는 PATH 변수 내에 “.” 또는, “::” 포함 여부 확인 |
| PATH 변수 내에 “.”, “::” 이 맨 앞에 존재하는 경우 아래의 보안설정방법에 따라 설정 을 변경함 | |

|  |  |
| --- | --- |
| 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 |

|  |  |
| --- | --- |
| U-05 (상) | 2. 파일 및 디렉토리 관리 > 2.1 root홈, 패스 디렉터리 권한 및 패스 설정 |
| 취약점 개요 | |
| 점검내용 | * root 계정의 PATH 환경변수에 “.”이(마침표) 포함되어 있는지 점검 |
| 점검목적 | * 비인가자가 불법적으로 생성한 디렉터리 및 명령어를 우선으로 실행되지 않도록 설정하기 위해 환경변수 점검이 필요함 |
| 보안위협 | * root 계정의 PATH(환경변수)에 정상적인 관리자 명령어(예: ls, mv, cp등)의 디렉터리 경로 보다 현재 디렉터리를 지칭하는 “.” 표시가 우선하면 현재 디렉터리에 변조된 명령어를 삽입하여 관리자 명령어 입력 시 악의적인 기 능이 실행 될 수 있음 |
| 참고 | ※ 환경변수: 프로세스가 컴퓨터에서 동작하는 방식에 영향을 미치는 동적인 값들의 집합 으로 Path 환경변수는 실행파일을 찾는 경로에 대한 변수임 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : PATH 환경변수에 “.” 이 맨 앞이나 중간에 포함되지 않은 경우 |
| 취약 : PATH 환경변수에 “.” 이 맨 앞이나 중간에 포함되어 있는 경우 |
| 조치방법 | root 계정의 환경변수 설정파일(“/.profile”, “/.cshrc” 등)과 “/etc/profile” 등에서 PATH 환경변수에 포함되어 있는 현재 디렉터리를 나타내는 “.”을 PATH 환경변 수의 마지막으로 이동  ※ “/etc/profile”, root 계정의 환경변수 파일, 일반계정의 환경변수 파일을 순차 적으로 검색하여 확인 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| /bin/bash | /etc/profile, $HOME/.bash\_profile |
| ※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨 | |

|  |  |
| --- | --- |
| U-05 (상) | 2. 파일 및 디렉토리 관리 > 2.1 root홈, 패스 디렉터리 권한 및 패스 설정 |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile) 열기  #vi /etc/profile  Step 2) 아래와 같이 수정  (수정 전) PATH=.:$PATH:$HOME/bin  (수정 후) PATH=$PATH:$HOME/bin:.  ※ 환경변수 파일은 OS별로 약간씩 다를 수 있음 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | | | | | | | |
| SOLARIS, AIX | 소유자가 nouser, nogroup인 파일이나 디렉터리 검색  #find / -nouser –o –nogroup –xdev –ls 2 > /dev/null | | | | | | |
| HP-UX | #find  {} \; | / \( -nouser –o –nogroup  2> /dev/null | \) | -xdev | –exec | ls | –al |
| LINUX | #find  #find | / -nouser –print  / -nogroup -print |  |  |  |  |  |
| ※ 소유자 또는 그룹이 없는 파일은 파일 속성 해당 필드에 숫자로 표시됨  예시) rwxr-xr-x 500 500 test.txt  ※ 소유자가 nouser, nogroup인 파일이나 디렉터리 존재하는 경우 아래의 보안설  정방법에 따라 디렉터리 및 파일 삭제 또는, 소유자 및 그룹을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-06 (상) | 2. 파일 및 디렉토리 관리 > 2.2 파일 및 디렉터리 소유자 설정 |
| 취약점 개요 | |
| 점검내용 | * 소유자 불분명한 파일이나 디렉터리가 존재하는지 여부를 점검 |
| 점검목적 | * 소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리하여 임의의 사용 자가 해당파일을 열람, 수정하는 행위를 사전에 차단하기 위함 |
| 보안위협 | * 소유자가 존재하지 않는 파일의 UID와 동일한 값으로 특정계정의 UID값을 변경하면 해당 파일의 소유자가 되어 모든 작업이 가능함 |
| 참고 | ※ 소유자가 존재하지 않는 파일 및 디렉터리는 퇴직자의 자료이거나 관리 소홀로 인해 생긴 파일인 경우 또는 해킹으로 인한 공격자가 만들어 놓은 악의적인 파일인 경우가 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 소유자가 존재하지 않는 파일 및 디렉터리가 존재하지 않는 경우 |
| 취약 : 소유자가 존재하지 않는 파일 및 디렉터리가 존재하는 경우 |
| 조치방법 | 소유자가 존재하지 않는 파일 및 디렉터리 삭제 또는, 소유자 변경 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제  #rm <file\_name>  #rm <directory\_name>  ※ 삭제할 파일명 또는, 디렉터리명 입력  Step 2) 필요한 경우 chown 명령으로 소유자 및 그룹 변경  #chown <user\_name> <file\_name> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | “/etc/passwd” 파일의 소유자 및 권한 확인  #ls –l /etc/passwd  rw-r--r-- root <passwd 파일> | | | | | | |
| “passwd” 파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-07 (상) | 2. 파일 및 디렉토리 관리 > 2.3 /etc/passwd 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/passwd 파일 권한 적절성 점검 |
| 점검목적 | * /etc/passwd 파일의 임의적인 변경을 차단하기 위함을 통해 비인가자가 권 한 상승하는 것을 막기 위함 |
| 보안위협 | * 관리자(root) 외 사용자가 "/etc/passwd” 파일의 사용자 정보를 변조하여 shell 변경, 사용자 추가/삭제 등 root를 포함한 사용자 권한 획득 가능 |
| 참고 | ※ /etc/passwd: 사용자의 ID, 패스워드, UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 파일 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : /etc/passwd 파일의 소유자가 root이고, 권한이 644 이하인 경우 |
| 취약 : /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우 |
| 조치방법 | “/etc/passwd” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   “/etc/passwd” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)  #chown root /etc/passwd #chmod 644 /etc/passwd | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX | # ls –l /etc/shadow (※ shadow 파일 구조: 부록 참고)  r-------- root <shadow 파일> | | | | | | |
| AIX | # ls –ld /etc/security/passwd (※ passwd 파일 구조: 부록 참고)  r-------- root <passwd 파일> | | | | | | |
| HP-UX | # ls –ld /tcb/files/auth  r-------- root <auth 디렉터리> | | | | | | |
| 위에 제시된 파일 및 디렉터리의 소유자가 root가 아니거나 파일의 권한이 400이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-08 (상) | 2. 파일 및 디렉토리 관리 > 2.4 /etc/shadow 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/shadow 파일 권한 적절성 점검 |
| 점검목적 | * /etc/shadow 파일을 관리자만 제어할 수 있게 하여 비인가자들의 접근을 차 단하도록 shadow 파일 소유자 및 권한을 관리해야함 |
| 보안위협 | * shadow파일은 패스워드를 암호화하여 저장하는 파일이며 해당 파일의 암호 화된 해쉬값을 복호화하여(크래킹) 비밀번호를 탈취할 수 있음 |
| 참고 | ※ /etc/shadow: 시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리 하고 있는 파일 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | * 양호 : /etc/shadow 파일의 소유자가 root이고, 권한이 400 이하인 경우 |
| * 취약 : /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400 이하가 아닌 경우 |
| 조치방법 | “/etc/shadow” 파일의 소유자 및 권한 변경 (소유자 root, 권한 400) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX   Step 1) “/etc/shadow” 파일의 소유자 및 권한 확인  #ls -l /etc/shadow  Step 2) “/etc/shadow” 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)  #chown root /etc/shadow #chmod 400 /etc/shadow | |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-08 (상) | 2. 파일 및 | | 디렉토리 관리 | | > | 2.4 | /etc/shadow | 파일 | 소유자 | 및 | 권한 | 설정 |
| * AIX   AIX 서버는 기본적으로 “/etc/security/passwd” 파일에 패스워드를 암호화하여 저장·관리하므로 해당 디렉터리 권한을 기준에 맞게 설정  Step 1) /etc/security/passwd 디렉터리의 소유자 및 권한 확인  #ls -ld /etc/security/passwd  Step 2) /etc/security/passwd 디렉터리의 소유자 및 권한 변경 (소유자 root, 권한 400)  #chown root /etc/security/passwd #chmod 400 /etc/security/passwd   * HP-UX   HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 “/tcb/files/auth” 디렉터 리에 계정 이니셜과 계정명에 따라 파일로 저장∙관리 가능  Step 1) /tcb/files/auth 디렉터리의 소유자 및 권한 확인  #ls -ld /tcb/files/auth  Step 2) /tcb/files/auth 디렉터리의 소유자 및 권한 변경 (소유자 root, 권한 400)  #chown root /tcb/files/auth  #chmod 400 /tcb/files/auth | | | | | | | | | | | | |
| 조치 시  영향 | 일반적인 | 경우 | 영향 | 없음 | | | | | | | | |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | # ls –l /etc/hosts  rw------- root <hosts 파일> | | | | | | |
| “hosts” 파일의 소유자가 root가 아니거나 파일의 권한이 600이하가 아닌 경우 아 래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-09 (상) | 2. 파일 및 디렉토리 관리 > 2.5 /etc/hosts 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/hosts 파일의 권한 적절성 점검 |
| 점검목적 | * /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파 일 변조를 방지하기 위함 |
| 보안위협 | * hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악 의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이 트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있음 * hosts파일에 소유자외 쓰기 권한이 부여된 경우, 일반사용자 권한으로 hosts 파일에 변조된 IP주소를 등록하여 정상적인 DNS를 방해하고 악성사이트로 의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있음 |
| 참고 | ※ /etc/hosts: IP 주소와 호스트네임을 매핑하는 파일. 일반적으로 인터넷 통신 시 주소를 찾기 위해 도메인 네임 서비스(DNS)보다 hosts 파일을 먼저 참조함. hosts 파일은 문 자열 주소로부터 IP 주소를 수신받는 DNS 서버와는 달리, 파일 내에 직접 문자열 주소 와 IP 주소를 매칭하여 기록하며, DNS 서버 접근 이전에 확인하여 해당 문자열 주소가 목록에 존재할 시 그 문자열 주소에 해당하는 IP 주소로 연결함  ※ 파밍(Pharming): 사용자의 DNS 또는 hosts 파일을 번조함으로써 정상적인 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 훔치는 새로운 컴퓨터 범죄 수법 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : /etc/hosts 파일의 소유자가 root이고, 권한이 600인 이하경우 |
| 취약 : /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600 이상인 경우 |
| 조치방법 | “/etc/hosts” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   “/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)  #chown root /etc/hosts #chmod 600 /etc/hosts | |
| 조치 시 영향 | hosts 파일의 권한을 600으로 변경시 일반사용자 권한은 해당파일을 사용할 수 없음  hosts 파일에 시스템 정보가 설정되어 있는 경우 hosts파일을 참조하는 서비스를 확인하는 것이 필요함 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | “/etc/inetd.conf” 파일의 소유자 및 권한 확인  #ls –l /etc/inetd.conf  rw------- root <inetd.conf 파일> | | | | | | |
| LINUX  (Xinetd) | “/etc/xinetd.conf” 파일 및 “/etc/xinetd.d/” 하위 모든 파일의 소유자 및 권한 확인  #ls –l /etc/xinetd.conf #ls –al /etc/xinetd.d/\*  rw------- root <xinetd.conf 파일>  rw------- root <xinetd 디렉터리 내 모든 파일> | | | | | | |
| 인터넷 슈퍼데몬 서비스 설정파일의 소유자가 root가 아니거나 파일의 권한이 600 이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함  ※ Linux 운영체제는 버전에 따라 inetd 또는 xinetd을 사용하고 있으므로 사용하고 있는 데몬 확인 필요 | | | | | | | |

|  |  |
| --- | --- |
| U-10 (상) | 2. 파일 및 디렉토리 관리 > 2.6 /etc/(x)inetd.conf 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/(x)inetd.conf 파일 권한 적절성 점검 |
| 점검목적 | * /etc/(x)inetd.conf 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의 적인 파일 변조를 방지하기 위함 |
| 보안위협 | * (x)inetd.conf 파일에 소유자외 쓰기 권한이 부여된 경우, 일반사용자 권한으 로 (x)inetd.conf 파일에 등록된 서비스를 변조하거나 악의적인 프로그램(서 비스)를 등록할 수 있음 |
| 참고 | ※ (x)inetd (슈퍼데몬) : 자주 사용하지 않는 서비스가 상시 실행되어 메모리를 점유하는 것을 방지하기 위해 (x)inetd(슈퍼대몬)에 자주 사용하지 않는 서비스를 등록하여 요청 이 있을시에만 해당 서비스를 실행하고 요청이 끝나면 서비스를 종료하는 역할 수행 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : /etc/inetd.conf 파일의 소유자가 root이고, 권한이 600인 경우 |
| 취약 : /etc/inetd.conf 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우 |
| 조치방법 | “/etc/(x)inetd.conf” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   “/etc/inetd.conf” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600) | |

UNIX 서버

|  |  |
| --- | --- |
| U-10 (상) | 2. 파일 및 디렉토리 관리 > 2.6 /etc/(x)inetd.conf 파일 소유자 및 권한 설정 |
| #chown root /etc/inetd.conf #chmod 600 /etc/inetd.conf   * LINUX - xinetd   “/etc/inetd.conf” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)  #chown root /etc/xinetd.conf #chmod 600 /etc/xinetd.conf  ※ "/etc/xinetd.d/" 하위 디렉터리에 취약한 파일도 위와 동일한 방법으로 조치 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | “/etc/syslog.conf” 파일의 소유자 및 권한 확인  #ls –l /etc/syslog.conf  rw-r----- root <syslog.conf 파일> | | | | | | |
| “syslog.conf” 파일의 소유자가 root가 아니거나 파일의 권한이 640가 아닌 경우 아  래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-11 (상) | 2. 파일 및 디렉토리 관리 > 2.7 /etc/syslog.conf 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/syslog.conf 파일 권한 적절성 점검 |
| 점검목적 | * /etc/syslog.conf 파일의 권한 적절성을 점검하여, 관리자 외 비인가자의 임 의적인 syslog.conf 파일 변조를 방지하기 위함 |
| 보안위협 | * syslog.conf 파일의 설정내용을 참조하여 로그의 저장위치가 노출되며 로그 을 기록하지 않도록 설정하거나 대량의 로그를 기록하게 하여 시스템 과부 하를 유도할 수 있음 |
| 참고 | ※ /etc/syslog.conf : syslogd 데몬 실행시 참조되는 설정파일로 시스템 로그 기록의 종류, 위치 및 Level을 설정할 수 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)이고, 권한이 640 이 하인 경우 |
| 취약 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 640 이하가 아닌 경우 |
| 조치방법 | “/etc/syslog.conf” 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권 한 644 이하) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) “/etc/syslog.conf” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)  #chown root /etc/syslog.conf #chmod 640 /etc/syslog.conf   * LINUX (CentOS 6 이상일 경우) #chown root /etc/rsyslog.conf #chmod 640 /etc/rsyslog.conf   ※ HP-UX 11이상 버전에서는 syslog.conf 소유가 bin 으로 나타남 | |
| 조치 시 영향 | root, bin, sys 등 시스템에서 사용하는 계정이 아닌 일반 계정에게 소유 권한이 부여되지 않도록 하여야 함 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | “/etc/services” 파일의 소유자 및 권한 확인  #ls –l /etc/services  rw-r--r-- root <services 파일> | | | | | | |
| “services” 파일의 소유자가 root가 아니거나 파일의 권한이 644가 아닌 경우 아래 의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-12 (상) | 2. 파일 및 디렉토리 관리 > 2.8 /etc/services 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/services 파일 권한 적절성 점검 |
| 점검목적 | * /etc/services 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함 |
| 보안위협 | * services 파일의 접근권한이 적절하지 않을 경우 비인가 사용자가 운영 포트 번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈 하여 악성 서비스를 의도적으로 실행할 수 있음 |
| 참고 | ※ /etc/services : 서비스 관리를 위해 사용되는 파일. 해당 파일에 서버에서 사용하는 모 든 포트(port)들에 대해 정의되어 있으며, 필요시 서비스 기본사용 포트를 변경하여 네 트워크 서비스를 운용할 수 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : etc/services 파일의 소유자가 root(또는 bin, sys)이고, 권한이 644 이하 인 경우 |
| 취약 : etc/services 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 644 이하가 아닌 경우 |
| 조치방법 | “/etc/ services” 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권한 644 이하) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   “/etc/services” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)  #chown root /etc/services #chmod 644 /etc/services | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | | | | | | | |
| SOLARIS, LINUX, AIX, HP-UX | OS별 주요 실행파일에 대한 SUID/SGID 설정 여부 확인 (※ 불필요한 SUID/SGID 목록: 부록 참고)  #ls –alL [check\_file] | awk ‘{ print $1}’ | grep –i ‘s’ | | | | | | |
| 주요 파일에 불필요한 SUID/SGID를 제거함 | | SUID/SGID가 | 설정된 | 경우 | 아래의 | 보안설정방법에 | 따라 |

|  |  |
| --- | --- |
| U-13 (상) | 2. 파일 및 디렉토리 관리 > 2.9 SUID, SGID, 설정 파일점검 |
| 취약점 개요 | |
| 점검내용 | * 불필요하거나 악의적인 파일에 SUID, SGID 설정 여부 점검 |
| 점검목적 | * 불필요한 SUID, SGID 설정 제거로 악의적인 사용자의 권한상승을 방지하기 위함 |
| 보안위협 | * ~~SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파 일로 특정 명령어를 실행하여 root 권한 획득 가능함~~ |
| 참고 | ※ SUID: 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한 을 얻게 됨  ※ SGID: 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 됨  ※ 불필요한 SUID/SGID 목록: 부록 참고 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우 |
| 취약 : 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우 |
| 조치방법 | Step 1) 불필요한 SUID, SGID 파일 제거  Step 2) 아래의 목록 이외에 애플리케이션에서 생성한 파일이나, 사용자가 임의 로 생성한 파일 등 의심스럽거나 특이한 파일의 발견 시 SUID 제거 필요 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 제거 방법  #chmod -s <file\_name>  Step 2) 주기적인 감사 방법  #find / -user root -type f \( -perm -04000 -o -perm -02000 \) -xdev  -exec ls –al {} \;  Step 3) 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법 | |

UNIX 서버

|  |  |
| --- | --- |
| U-13 (상) | 2. 파일 및 디렉토리 관리 > 2.9 SUID, SGID, 설정 파일점검 |
| 일반 사용자의 Setuid 사용을 제한함 (임의의 그룹만 가능) #/usr/bin/chgrp <group\_name> <setuid\_file\_name> #/usr/bin/chmod 4750 <setuid\_file\_name> | |
| 조치 시  영향 | SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요 |

UNIX 서버



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | | | | | |
| SOLARIS,  LINUX, AIX,  HP-UX | 홈 디렉터리  #ls –l <홈 | 환경변수 디렉터리 | 파일의 소유자 및 환경변수 파일> | 권한 | 확인 |
| 홈 디렉터리 환경변수 파일의 소유자가 root 또는, 해당 계정으로 설정되어 있는지  확인 후 소유자 이외의 사용자에게 쓰기 권한이 부여되어 있을 경우 아래의 보안  설정방법에 따라 설정을 변경함 | | | | | |

|  |  |
| --- | --- |
| U-14 (상) | 2. 파일 및 디렉토리 관리 > 2.10 사용자, 시스템 시작파일 및 환경파일 소유자  및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * 홈 디렉터리 내의 환경변수 파일에 대한 소유자 및 접근권한이 관리자 또는 해당 계정으로 설정되어 있는지 점검 |
| 점검목적 | * 비인가자의 환경변수 조작으로 인한 보안 위험을 방지하기 위함 |
| 보안위협 | * 홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환 경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수 파일을 변조하여 정상 사용중인 사용자의 서비스가 제한 될 수 있음 |
| 참고 | ※ 환경변수 파일 종류: “.profile”, “.kshrc”, “.cshrc”, “.bashrc”, “.bash\_profile”, “.login", “.exrc”, “.netrc” 등 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되 어 있고, 홈 디렉터리 환경변수 파일에 root와 소유자만 쓰기 권한이 부여 된 경우 |
| 취약 : 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되 지 않고, 홈 디렉터리 환경변수 파일에 root와 소유자 외에 쓰기 권한이 부여된 경우 |
| 조치방법 | 환경변수 파일의 권한 중 타 사용자 쓰기 권한 제거 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX , HP-UX   Step 1) 소유자 변경 방법  #chown <user\_name> <file\_name>  Step 2) 일반 사용자 쓰기 권한 제거 방법  #chmod o-w <file\_name> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | world writable 파일 존재 여부 확인  #find / -type f -perm –2 –exec ls –l {} \; | | | | | | |
| “world writable“ 파일 존재 시 사용 목적을 확실히 알고 불필요 시 삭제, 필요 시 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-15 (상) | 2. 파일 및 디렉토리 관리 > 2.11 world writable 파일 점검 |
| 취약점 개요 | |
| 점검내용 | * 불필요한 world writable 파일 존재 여부 점검 |
| 점검목적 | * world writable 파일을 이용한 시스템 접근 및 악의적인 코드 실행을 방지하 기 위함 |
| 보안위협 | * ~~시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 일반사용 자 및 비인가된 사용자가 해당 파일을 임의로 수정, 삭제가 가능함~~ |
| 참고 | ※ world writable 파일: 파일의 내용을 소유자나 그룹 외 모든 사용자에 대해 쓰기가 허  용된 파일 (예 : rwxrwxrwx root root <파일명>) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 시스템 중요 파일에 world writable 파일이 존재하지 않거나, 존재 시 설 정 이유를 확인하고 있는 경우 |
| 취약 : 시스템 중요 파일에 world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우 |
| 조치방법 | world writable 파일 존재 여부를 확인하고 불필요한 경우 제거 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 일반 사용자 쓰기 권한 제거 방법  #chmod o-w <file\_name>  Step 2) 파일 삭제 방법  #rm -rf <world-writable 파일명> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | dev에 존재하지 않는 device 파일 점검  #find /dev –type f –exec ls –l {} \; | | | | | | |
| 존재하지 않는 디바이스가 “dev” 디렉터리 내에 존재하는 경우 아래의 보안설정방 법에 따라 제거함 | | | | | | | |

|  |  |
| --- | --- |
| U-16 (상) | 2. 파일 및 디렉토리 관리 > 2.12 /dev에 존재하지 않는 device 파일 점검 |
| 취약점 개요 | |
| 점검내용 | * 존재하지 않는 device 파일 존재 여부 점검 |
| 점검목적 | * 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하기 위함 |
| 보안위협 | * 공격자는 rootkit 설정파일들을 서버 관리자가 쉽게 발견하지 못하도록 /dev 에 device 파일인 것처럼 위장하는 수법을 많이 사용함 |
| 참고 | ※ /dev 디렉터리: 논리적 장치 파일을 담고 있는 /dev 디렉터리는 /devices 디렉터리에 있는 물리적 장치 파일에 대한 심볼릭 링크임. 예를 들어 rmt0를 rmto로 잘못 입력한 경우 rmto 파일이 새로 생성되는 것과 같이 디바이스 이름 입력 오류 시 root 파일 시스템이 에러를 일으킬 때까지 /dev 디렉터리에 계속해서 파일을 생성함  ※ /dev 디렉터리 내 불필요한 device 파일이 존재할 시 삭제 권고 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : dev에 대한 파일 점검 후 존재하지 않은 device 파일을 제거한 경우 |
| 취약 : dev에 대한 파일 미점검 또는, 존재하지 않은 device 파일을 방치한 경우 |
| 조치방법 | major, minor number를 가지지 않는 device 파일 제거 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) /dev 디렉터리 파일 점검  #find /dev -type f -exec ls -l {} \;  Step 2) major, minor number를 가지지 않는 device일 경우 삭제 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS,  LINUX, AIX, | Step 1) 파일 소유자 및 권한 확인  #ls –al /etc/hosts.equiv |

|  |  |
| --- | --- |
| U-17 (상) | 2. 파일 및 디렉토리 관리 > 2.13 $HOME/.rhosts, hosts.equiv 사용 금지 |
| 취약점 개요 | |
| 점검내용 | * /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root 또는, 해당 계정으로 설정한 뒤 권한을 600으로 설정하고 해당파일 설정에 ‘+’ 설정(모든 호스트 허용)이 포함되지 않도록 설정되어 있는지 점검 |
| 점검목적 | * ‘r’ command 사용을 통한 원격 접속은 인증 없이 관리자 원격접속이 가능 하므로 서비스 포트를 차단해야 함 |
| 보안위협 | * rlogin, rsh 등과 같은 ‘r’ command의 보안 설정이 적용되지 않은 경우, 원 격지의 공격자가 관리자 권한으로 목표 시스템상의 임의의 명령을 수행시킬 수 있으며, 명령어 원격 실행을 통해 중요 정보 유출 및 시스템 장애를 유발 시킬 수 있음. 또한 공격자 백도어 등으로도 활용될 수 있음 * r-command(rlogin, rsh등) 서비스의 접근통제에 관련된 파일로 권한설정을 미 적용한 경우 r-command 서비스 사용 권한을 임의로 등록하여 무단 사 용이 가능함 |
| 참고 | ※ ‘r’command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있으며, 포트번호 512,513,514 (TCP)를 사용함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정 이 적용된 경우   * /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계 정인 경우 * /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600 이하인 경우 * /etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에 ‘+’ 설정이 없는 경우 |
| 취약 : login, shell, exec 서비스를 사용하고, 위와 같은 설정이 적용되지 않은 경 우 |
| 조치방법 | Step 1) /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자를 root 또는, 해당 계 정으로 변경  Step 2) /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한을 600 이하로 변경  Step 3) /etc/hosts.equiv 및 $HOME/.rhosts 파일에서 “+”를 제거하고 반드시 필요한 호스트 및 계정만 등록 (해당 내역 요청) |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| HP-UX | #ls –al $HOME/.rhosts  rw------- root <hosts.equiv 파일> rw------- root <$HOME/.rhosts 파일>  Step 2) 계정 별 ‘+’ 부여 적절성 확인  #cat /etc/hosts.equiv #cat $HOME/.rhosts   * /etc/hosts.equiv : 서버 설정 파일 * $HOME/.rhosts : 개별 사용자의 설정 파일 |
| “/etc/hosts.equiv 및 $HOME/.rhosts” 파일의 소유자가 root가 아니거나 파일의 권 한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| + + | 모든 호스트의 계정을 신뢰 |
| + test | 모든 호스트의 test 계정을 신뢰 |
| Web1 + | Web1 호스트의 모든 계정을 신뢰 |

|  |  |
| --- | --- |
| U-17 (상) | 2. 파일 및 디렉토리 관리 > 2.13 $HOME/.rhosts, hosts.equiv 사용 금지 |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) “/etc/hosts.equiv” 및 “$HOME/.rhosts” 파일의 소유자를 root 또는, 해당 계정으로 변경  #chown root /etc/hosts.equiv #chown <user\_name> $HOME/.rhosts  Step 2) “/etc/hosts.equiv” 및 “$HOME/.rhosts” 파일의 권한을 600 이하로 변경  #chmod 600 /etc/hosts.equiv  #chmod 600 $HOME/.rhosts  Step 3) “/etc/hosts.equiv” 및 “$HOME/.rhosts” 파일에서 “+”를 제거하고 허용 호스트 및 계정 등록  #cat /etc/hosts.equiv (or $HOME/.rhosts) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX | * TCP Warrper 사용할 경우   All deny 적용 확인 및 접근 허용 IP 적절성 확인  #cat /etc/hosts.deny #cat /etc/hosts.allow   * IPtables 사용할 경우 (Linux)   #iptalbes -L   * IPfilter 사용할 경우 (SOLARIS) #cat /etc/ipf/ipf.conf * TCP Warrper (SOLARIS 10 이상) # inetadm –p   tcp\_wrappers=true <- 현재 실행되어 있는 상태 |

|  |  |
| --- | --- |
| U-18 (상) | 2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한 |
| 취약점 개요 | |
| 점검내용 | * 허용할 호스트에 대한 접속 IP 주소 제한 및 포트 제한 설정 여부 점검 |
| 점검목적 | * 허용한 호스트만 서비스를 사용하게 하여 서비스 취약점을 이용한 외부자 공격을 방지하기 위함 |
| 보안위협 | * 허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같 은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해 사고가 발생할 수 있음 |
| 참고 | * 접속 IP 및 포트제한 애플리케이션 종류 예시   ※ TCP Wrapper: 네트워크 서비스에 관련한 트래픽을 제어하고 모니터링 할 수 있는 UNIX 기반의 방화벽 툴  ※ IPFilter: 유닉스 계열에서 사용하는 공개형 방화벽 프로그램으로써 Packet Filter로 시스 템 및 네트워크 보안에 아주 강력한 기능을 보유한 프로그램  ※ IPtables: 리눅스 커널 방화벽이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 응용프로그램 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정한 경우 |
| 취약 : 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않 은 경우 |
| 조치방법 | OS에 기본으로 제공하는 방화벽 애플리케이션이나 TCP Wrapper와 같은 호스 트별 서비스 제한 애플리케이션을 사용하여 접근 허용 IP 등록 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | tcp\_wrappers=false <- 현재 정지된 상태 | | | | |
| HP-UX | | All deny 적용 확인 및 서비스 접근 가능 IP 확인  #cat /var/adm/inetd.sec | | | | |
| 위에 제시한 시스템 접근 | 파일이 제한 IP | | 존재하지 설정 필요 | 않거나 All 시 아래의 | deny 설정이 적용되지 않은 보안설정방법에 따라 설정을 | 경우 또는, 변경함 |

|  |  |
| --- | --- |
| U-18 (상) | 2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한 |
| * IPtables 사용하는 경우   Step 1) iptables 명령어를 통해 접속할 IP 및 포트 정책 추가 (예) SSH 서비스 제한  #iptables –A INPUT –p tcp –s 192.168.1.0/24 —dport 22 –j ACCEPT  #iptables -A INPUT -p tcp --dport 22 -j DROP  Step 2) iptables 설정 저장  #/etc/rc.d/init.d/iptables save   * IPfilter 사용하는 경우   Step 1) vi 편집기를 이용하여 “/etc/ipf/ipf.conf” 파일 열기 Step 2) 접속할 IP 및 포트 정책 추가  (예) SSH 서비스 제한  pass in quick proto tcp from 192.168.1.0/24 to any port = 22 keep state  block in quick proto tcp from any to any port = 22 keep state  Step 3) IPfilter 서비스 재시작   * TCP Wrapper 사용하는 경우   Step 1) vi 편집기를 이용하여 “/etc/hosts.deny” 파일 열기 (해당 파일이 없을 경우 새로 생성) Step 2) 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)  (수정 전) 설정 없음 (수정 후) ALL:ALL  Step 3) vi 편집기를 이용하여 “/etc/hosts.allow” 파일 열기 (해당 파일이 없을 경우 생성) (수정 전) 설정 없음  (수정 후) sshd : 192.168.0.148, 192.168.0.6  (다른 서비스도 동일한 방식으로 설정)  < TCP Wrapper 접근제어 가능 서비스 >   * + SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH   < TCP Wrapper는 다음 두 파일에 의해 접근이 제어됨 > | |

UNIX 서버

|  |  |
| --- | --- |
| U-18 (상) | 2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한 |
| * /etc/hosts.deny --> 시스템 접근을 제한할 IP 설정 * /etc/hosts.allow --> 시스템 접근을 허용할 IP 설정 * 위의 두파일이 존재하지 않은 시 --> 모든 접근 허용 * HP-UX   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 복 사하여 사용함  Step 1) vi 편집기를 이용하여 “/var/adm/inetd.sec” 파일 열기 (해당 파일이 없을 경우 새로 생성)  Step 2) 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)   * + telnet 으로의 모든 접속 차단 => telnet deny \*.\*.\*.\*   + telnet 접속을 허용할 IP 등록 => telnet allow [telnet 접속 허용 IP 등록] (다른 서비스들도 위와 동일한 방법으로 설정) | |
| 조치 시  영향 | 허용되지 않은 IP는 서비스 사용이 불가함 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX,  HP-UX, SOLARIS 5.9  이하 버전 | #cat /etc/inetd.conf  #finger stream tcp nowait bin /usr/lbin/fingered fingerd 주석처리 확인 |
| SOLARIS 5.10  이상 버전 | #inetadm | grep "finger" |
| LINUX  (xinetd일  경우) | #ls -alL /etc/xinetd.d/\* | egrep "echo finger" |
| 위에 제시된 파일 내 “finger" 서비스가 활성화된 경우 아래의 보안설정방법에 따  라 서비스 중지 | |

|  |  |
| --- | --- |
| U-19 (상) | 3. 서비스 관리 > 3.1 Finger 서비스 비활성화 |
| 취약점 개요 | |
| 점검내용 | * finger 서비스 비활성화 여부 점검 |
| 점검목적 | * Finger(사용자 정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템 에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회 되는 것을 차단하고자 함 |
| 보안위협 | * 비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 함 |
| 참고 | ※ Finger(사용자 정보 확인 서비스): who 명령어가 현재 사용 중인 사용자들에 대한 간 단한 정보만을 보여주는 데 반해 finger 명령은 옵션에 따른 시스템에 등록된 사용자뿐 만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : Finger 서비스가 비활성화 되어 있는 경우 |
| 취약 : Finger 서비스가 활성화 되어 있는 경우 |
| 조치방법 | Finger 서비스 비활성화 |
| 점검 및 조치 사례 | |
| * LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전   Step 1) “/etc/inetd.conf” 파일에서 finger 서비cd /스 라인 #처리(주석처리)  (수정 전) finger stream tcp nowait bin /usr/lbin/fingered fingerd (수정 후) #finger stream tcp nowait bin /usr/lbin/fingered fingerd  Step 2) inetd 서비스 재시작 | |

UNIX 서버

|  |  |
| --- | --- |
| U-19 (상) | 3. 서비스 관리 > 3.1 Finger 서비스 비활성화 |
| #ps -ef | grep inetd  root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill -HUP [PID]   * SOLARIS 5.10 이상 버전   inetadm –d “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #inetadm -d svc:/network/finger:default   * LINUX (xinetd일 경우)   Step 1) vi 편집기를 이용하여 “/etc/xinetd.d/finger” 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)  service finger  {  socket\_type = stream  wait = no  user = nobody  server = /usr/sbin/in.fingerd  disable = yes  }  Step 3) xinetd 서비스 재시작  #service xinetd restart | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS,  LINUX, AIX,  HP-UX | /etc/passwd 파일에 ftp 계정 존재 여부 확인  #cat /etc/passwd | grep "ftp" | | | | | | |
| "passwd" 파일 내 ftp 계정이 존재하는 경우 아래의 보안설정방법에 따라 서비스  접속 제한 | | | | | | | |

|  |  |
| --- | --- |
| U-20 (상) | 3. 서비스 관리 > 3.2 Anonymous FTP 비활성화 |
| 취약점 개요 | |
| 점검내용 | * 익명 FTP 접속 허용 여부 점검 |
| 점검목적 | * 실행중인 FTP 서비스에 익명 FTP 접속이 허용되고 있는지 확인하여 접속허 용을 차단하는 것을 목적으로 함 |
| 보안위협 | * Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉 터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사 용하여 시스템에 대한 공격을 가능하게 함 |
| 참고 | ※ Anonymous FTP(익명 FTP): 파일 전송을 위해서는 원칙적으로 상대방 컴퓨터를 사용할 수 있는 계정이 필요하나 누구든지 계정 없이도 anonymous 또는 ftp라는 로그인 명과 임의의 비밀번호를 사용하여 FTP를 실행할 수 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : Anonymous FTP (익명 ftp) 접속을 차단한 경우 |
| 취약 : Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우 |
| 조치방법 | Anonymous FTP를 사용하지 않는 경우 Anonymous FTP 접속 차단 설정 적용 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Case 1) 일반 FTP - Anonymous FTP 접속 제한 설정 방법 “/etc/passwd” 파일에서 ftp 또는, anonymous 계정 삭제   * + SOLARIS, LINUX, HP-UX 설정: #userdel ftp   + AIX 설정: #rmuser ftp   Case 2) ProFTP - Anonymous FTP 접속 제한 설정 방법  conf/proftpd.conf 파일의 anonymous 관련 설정 중 User, Useralias 항목 주석처리 (proftpd.conf 파일의 위치는 운영체제 종류별로 상이함)  <Anonymous ~ftp> <- Anonymous 설정 구간  # User ftp <- anonymous로 사용되는 계정  Group ftp  # UserAlias anonymous ftp <- 별칭으로 사용되는 계정 | |

UNIX 서버

|  |  |
| --- | --- |
| U-20 (상) | 3. 서비스 관리 > 3.2 Anonymous FTP 비활성화 |
| ~~이하생략~~  </Anonymous>  Case 3) vsFTP - Anonymous FTP 접속 제한 설정 방법  vsFTP 설정파일(“/etc/vsftpd/vsftpd.conf” 또는, “/etc/vsftpd.conf”)에서 anonymous\_enable=NO 설정 | |
| 조치 시  영향 | Anonymous FTP를 사용하지 않을 경우 영향 없음 |

UNIX 서버



|  |  |  |
| --- | --- | --- |
| shell(514) | login(513) | exec(512) |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS 5.9  이하 버전 | r-command 서비스 활성화 여부 확인  #vi /etc/inetd.conf | | | | | | |
| AIX | #cat /etc/inetd.conf | grep rlogin (# 처리 되어 있으면  비활성화)  #cat /etc/inetd.conf | grep rsh (# 처리 되어 있으면 비활성화) | | | | | | |
| HP-UX | #vi /etc/inetd.conf  r로 시작하는 필드 존재 시 취약 | | | | | | |
| SOLARIS 5.10  이상 버전 | #inetadm | egrep "shell|rlogin|rexec"  r command 관련 데몬 확인 | | | | | | |
| LINUX  (xinetd일  경우) | rsh, rlogin, rexec (shell, login, exec) 서비스 구동 확인  #ls -alL /etc/xinetd.d/\* | egrep "rsh|rlogin|rexec"  | egrep -v "grep|klogin|kshell|kexec" | | | | | | |
| 위에 제시된 파일 내 "r-command계열“ 서비스가 활성화 된 경우 아래의 보안설정  방법에 따라 서비스 중지 | | | | | | | |

|  |  |
| --- | --- |
| U-21 (상) | 3. 서비스 관리 > 3.3 r 계열 서비스 비활성화 |
| 취약점 개요 | |
| 점검내용 | * r-command 서비스 비활성화 여부 점검 |
| 점검목적 | * r-command 사용을 통한 원격 접속은 NET Backup 또는 클러스터링 등 용 도로 사용되기도 하나, 인증 없이 관리자 원격접속이 가능하여 이에 대한 보 안위협을 방지하고자 함 |
| 보안위협 | * rsh, rlogin, rexec 등의 r command를 이용하여 원격에서 인증절차 없이 터 미널 접속, 쉘 명령어를 실행이 가능함 |
| 참고 | ※ r-command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec, rsync 등이 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요한 r 계열 서비스가 비활성화 되어 있는 경우 |
| 취약 : 불필요한 r 계열 서비스가 활성화 되어 있는 경우 |
| 조치방법 | NET Backup등 특별한 용도로 사용하지 않는다면 아래의 서비스 중지 |
| 점검 및 조치 사례 | |
| * SOLARIS 5.9 이하, HP-UX   Step 1) r 계열 서비스 활성화 여부 확인 | |

UNIX 서버

|  |  |
| --- | --- |
| U-21 (상) | 3. 서비스 관리 > 3.3 r 계열 서비스 비활성화 |
| # vi /etc/inetd.conf  Step 2) r로 시작하는 필드 주석처리 후 재가동 (수정 전)  shell stream tcp nowait root /usr/sbin/in.rshd in.rshd shell stream tcp6 nowait root /usr/sbin/in.rshd in.rshd login stream tcp nowait root /usr/sbin/in.rlogin.d in.rlogind exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd exec stream tcp6 nowait root /usr/sbin/in.rexecd in.rexecd  (수정 후)  #shell stream tcp nowait root /usr/sbin/in.rshd in.rshd #shell stream tcp nowait root /usr/sbin/in.rshd in.rshd #shell stream tcp6 nowait root /usr/sbin/in.rshd in.rshd #login stream tcp6 nowait root /usr/sbin/in.rlogind in.rlogind #exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd #exec stream tcp6 nowait root /usr/sbin/in.rexecd in.rexecd  SOLARIS) # kill -HUP [inetd PID]  HP-UX) # inetd -c   * AIX   Step 1) r 계열 서비스 활성화 여부 확인  #cat /etc/inetd.conf |grep rlogin (# 처리 되어 있으면 비활성화) #cat /etc/inetd.conf |grep rsh (# 처리 되어 있으면 비활성화) #cat /etc/inetd.conf |grep exec (# 처리 되어 있으면 비활성화)  Step 2) /etc/hosts.equiv 파일은 TRUSTED 시스템을 등록  Step 3) .rhosts 파일은 사용자 별로 'r'command를 통해 접근이 가능하도록 설정할 수 있음 ($HOME/.rhosts)   * SOLARIS 5.10 이상 버전   Step 1) r’command 관련 데몬 확인   * + svc:/network/login:rlogin   + svc:/network/rexec:default   + svc:/network/shell:kshell   Step 2) inetadm –d “중지하고자 하는 데몬“ 명령으로 데몬 중지  #inetadm -d svc:/network/login:rlogin | |

UNIX 서버



|  |  |
| --- | --- |
| U-21 (상) | 3. 서비스 관리 > 3.3 r 계열 서비스 비활성화 |
| #inetadm -d svc:/network/rexec:default #inetadm -d svc:/network/shell:kshell   * LINUX (xinetd일 경우)   Step 1) vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 rlogin, rsh, rexec 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)   * + /etc/xinetd.d/rlogin 파일   + /etc/xinetd.d/rsh 파일   + /etc/xinetd.d/rexec 파일   service rlogin  {  socket\_type = stream  wait = no  user = nobody  log\_on\_success += USERID  log\_on\_failure += USERID  server = /usr/sdin/in.fingerd  disable = yes  }  Step 3) xinetd 서비스 재시작  #service xinetd restart   * r-command 사용시 보안설정(U-17 점검항목 참고)   Step 1) r command 사용을 허용하는 호스트 및 계정 설정   * .rhosts, hosts.equiv 파일에 접근을 허용하는 hostname(IP) 명시   ※ IP 등록시 공인 IP 설정은 금지   * .rhosts, hosts.equiv 파일의 퍼미션을 600 이하로 설정 * 필요시 TCP\_Wrapper를 이용하여 접근을 허용하는 IP를 등록하여 추가 보안 설정 | |
|  | rlogin, rshell, rexec 서비스는 backup, 클러스터링 등의 용도로 종종 사용되고 |
|  | 있으므로 해당 서비스 사용 유무를 확인하여 미사용시 서비스 중지 |
| 조치 시  영향 | (/etc/hosts.equiv 또는 각 홈 디렉터리 밑에 있는 .rhosts 파일에 설정 유무를 |
|  | 확인하여 해당 서비스 사용여부 확인 - 파일이 존재하지 않거나 해당파일 내에 |
|  | 설정이 없다면 사용하지 않는 것으로 파악) |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 방법 | |
| SOLARIS, LINUX, AIX,  HP-UX | Cron 관련 파일 권한 확인  #ls -al /usr/bin/crontab  rw-r----- root <cron 접근제어 파일> |

|  |  |  |  |
| --- | --- | --- | --- |
| OS별 점검 파일 위치 | | | |
| SOLARIS | /etc/cron.d/ | crontab <- 예약작업을 등록하는 파일 cron.hourly <- 시간단위 실행 스크립트 등록 cron.daily <- 일단위 실행 스크립트 등록 cron.weekly <- 주단위 실행 스크립트 등록 cron.monthly <- 월 단위 실행 스크립트 등록 cron.allow <- crontab 명령어 허용 사용자  cron.deny <- crontab 명령어 차단 사용자 | |
| LINUX | /etc/ |
| AIX, HP-UX | /var/adm/cron/ |
| 공통 | /var/spool/cron/ 또는  /var/spool/cron/crontabs/ | | 사용자별 설정된 cron 작업 목록 |
| "cron" 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을  변경함 | | | |

|  |  |
| --- | --- |
| U-22 (상) | 3. 서비스 관리 > 3.4 crond 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * Cron 관련 파일의 권한 적절성 점검 |
| 점검목적 | * 관리자외 cron 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 함 |
| 보안위협 | * root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음 |
| 참고 | ※ Cron 시스템: 특정 작업을 정해진 시간에 주기적이고 반복적으로 실행하기 위한 데몬 및 설정  ※ cron.allow: 사용자 ID를 등록하면 등록된 사용자는 crontab 명령어 사용이 가능함  ※ cron.deny: 사용자 ID를 등록하면 등록된 사용자는 crontab 명령어 사용이 불가능함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : crontab 명령어 일반사용자 금지 및 cron 관련 파일 640 이하인 경우 |
| 취약 : crontab 명령어 일반사용자 사용가능하거나, crond 관련 파일 640 이상인 경우 |
| 조치방법 | crontab 명령어 750 이하, cron 관련 파일 소유자 및 권한 변경(소유자 root, 권한 640 이하) |
| 점검 및 조치 사례 | |
| * 공통설정 | |

UNIX 서버



|  |  |
| --- | --- |
| 관련 설정파일 | 설명 |
| <cron 디렉터리>/crontab | <- 예약작업을 등록하는 파일 |
| /etc/cron.hourly, /etc/cron.daily, etc/cron.weekly, /etc/cron.monthly | <- 시간,일, 주, 월 단위 실행스크립트 등록 |
| /var/spool/cron/ 또는  /var/spool/cron/crontabs/ | <- 사용자별 설정된 cron 작업 목록 |
| cron.allow, cron.deny | <- crontab 명령어 허용(차단) 사용자 등록 |

|  |  |
| --- | --- |
| 운영체제 | 관련 설정파일 위치 |
| SOLARIS | /etc/cron.d/ |
| LINUX | /etc/ |
| AIX, HP-UX | /var/adm/cron/ |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-22 (상) | 3. | | 서비스 관리 | | > | 3.4 | crond | 파일 | 소유자 | 및 | 권한 | 설정 |
| Step 1) crontab 명령어 일반사용자 권한 삭제 (crontab 명령어 위치는 OS별 다를수 있음)  ※ crontab 명령어는 SUID가 설정되어 있으므로 SUID 설정 제거  # ls -l /usr/bin/crontab  # chmod 750 /usr/bin/crontab  Step 2) cron 관련 설정파일 소유자 및 권한 설정  # chown root <cron 관련 파일> # chmod 640 <cron 관련 파일>   * crontab 명령어를 일반사용자에게 허용하는 경우   Step 1) “/etc/cron.d/cron.allow” 및 “/etc/cron.d/cron.deny” 파일의 소유자 및 권한 변경  #chown root /etc/cron.d/cron.allow #chmod 640 /etc/cron.d/cron.allow #chown root /etc/cron.d/cron.deny #chmod 640 /etc/cron.d/cron.deny  Step 2) “/etc/cron.d/cron.allow” 및 “/etc/cron.d/cron.deny” 파일에 사용자 등록  # cat /etc/cron.allow (crontab 명령어 사용을 허용하는 사용자 등록)  # cat /etc/cron.deny (crontabl 명령어 사용을 차단하는 사용자 등록) | | | | | | | | | | | | |
| 조치 시  영향 | 일반적인 | 경우 | 영향 | 없음 | | | | | | | | |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS | #svcs -a | grep echo #svcs -a | grep daytime #svcs -a | grep discard #svcs -a | grep chargen  echo, discard, daytime, chargen 서비스 활성 여부 확인 | | | | | | |
| AIX, HP-UX | #vi /etc/inetd.conf  echo, discard, daytime, chargen 필드 주석처리 확인 | | | | | | |
| SOLARIS 5.10  이상 버전 | #inetadm | grep enable | egrep "echo|discard|daytim  e|chargen" 명령으로 기타 서비스 데몬 확인 | | | | | | |
| 아래 제시된 DoS 공격에 취약한 서비스 중 사용하지 않는 서비스가 활성화 된 경우  아래의 보안설정방법에 따라 서비스 중지 | | | | | | | |

|  |  |
| --- | --- |
| DoS 공격에 취약한 서비스 예시 | |
| echo(7) | 클라이언트에서 보내는 메시지를 단순히 재전송 |
| discard(9) | 수신되는 임의 사용자의 데이터를 폐기하는 서비스 |
| daytime(13) | daytime은 클라이언트의 질의에 응답하여 아스키 형태로 현재  시간과 날짜를 출력하는 데몬 |

|  |  |
| --- | --- |
| U-23 (상) | 3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화 |
| 취약점 개요 | |
| 점검내용 | * 사용하지 않는 Dos 공격에 취약한 서비스의 실행 여부 점검 |
| 점검목적 | * 시스템 보안성을 높이기 위해 취약점이 많이 발표된 echo, discard, daytime, chargen, ntp, snmp 등 서비스를 중지함 |
| 보안위협 | * 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있음 |
| 참고 | ※ DoS(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족 하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 사용하지 않는 DoS 공격에 취약한 서비스가 비활성화 된 경우 |
| 취약 : 사용하지 않는 DoS 공격에 취약한 서비스가 활성화 된 경우 |
| 조치방법 | echo, discard, daytime, charge, ntp, dns, snmp 등 서비스 비활성화 설정 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| chargen(19) | 임의 길이의 문자열을 반환하는 서비스 |
| NTP(123) | 네트워크로 연결되어 있는 컴퓨터들끼리 클록 시각을  동기화시키는데 사용되는 서비스 |
| DNS(53) | 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그  반대의 변환을 수행하는데 사용되는 서비스 |
| SNMP(161/162) | 네트워크 장비들로부터 필요한 정보를 가져와 장비 상태를  모니터링 하거나 설정값을 변경하는 등의 작업을 하여 네트워크  장비를 관리하는데 사용되는 서비스 |
| SMTP(25) | 인터넷에서 메일을 보내기 위해 사용되는 서비스 |

|  |  |
| --- | --- |
| U-23 (상) | 3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화 |
| ※ 일반적으로 사용하지 않는 서비스인 echo, discard, daytime, chargen 비활성화 방법   * SOLARIS   Step 1) echo 서비스 비활성화 설정  #svcs -a |grep echo  #svcadm disable svc:/network/echo:dgrm #svcadm disable svc:/network/echo:stream  Step 2) discard 서비스 비활성화 설정  #svcs -a |grep daytime  #svcadm disable svc:/network/daytime:dgram #svcadm disable svc:/network/daytime:stream  Step 3) daytime 서비스 비활성화 설정  #svcs -a |grep discard  #svcadm disable svc:/network/discard:dgram #svcadm disable svc:/network/discard:stream  Step 4) chargen 서비스 비활성화 설정  #svcs -a |grep chargen  #svcadm disable svc:/network/chargen:dgram #svcadm disable svc:/network/chargen:stream   * AIX   Step 1) vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리  #vi /etc/inetd.conf  <inetd.conf>  #echo stream tcp nowait root internal #discard stream tcp nowait root internal #chargen stream tcp nowait root internal #daytime stream tcp nowait root internal | |

UNIX 서버

|  |  |
| --- | --- |
| U-23 (상) | 3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화 |
| #echo dgram udp wait root internal #discard dgram udp wait root internal #chargen dgram udp wait root internal #daytime dgram udp wait root internal  Step 2) 필드 주석처리 후 재가동  #refresh -s inetd   * HP-UX   Step 1) vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리  #vi /etc/inetd.conf  <inetd.conf>  #daytime stream udp6 nowait root internal #daytime dgram udp6 nowait root internal #echo stream tcp6 nowait root internal #echo dgram udp6 nowait root internal #discard stream tcp6 nowait root internal #discard dgram udp6 nowait root internal #chargen stream tcp6 nowait root internal #chargen dgram udp6 nowait root internal  Step 2) 필드 주석처리 후 재가동  # inetd -c   * SOLARIS 5.10 이상 버전   Step 1) 기타 서비스 데몬 확인  #inetadm | grep echo  enabled online svc:/network/echo:dgram enabled online svc:/network/echo:stream #inetadm | grep daytime  enabled online svc:/network/daytime:dgram enabled online svc:/network/daytime:stream #inetadm | grep discard  enabled online svc:/network/discard:dgram enabled online svc:/network/discard:stream #inetadm | grep chargen  enabled online svc:/network/chargen:dgram  enabled online svc:/network/chargen:stream | |

UNIX 서버



|  |  |
| --- | --- |
| U-23 (상) | 3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화 |
| Step 2) inetadm –d “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #inetadm -d svc:/network/echo:stream   * LINUX (xinetd일 경우)   Step 1) vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 echo, discard, daytime, chargen 파 일 열기  Step 2) 아래와 같이 설정 (Disable = yes 설정)   * + /etc/xinetd.d/echo 파일(echo-dgram, echo-stream)   + /etc/xinetd.d/discard 파일(discard-dgram, discard-stream)   + /etc/xinetd.d/daytime 파일(daytime-dgram, daytime-stream)   + /etc/xinetd.d/chargen 파일(chargen-dgram, chargen-stream)   service echo  {  disable = yes  id = echo-stream  type = internal  wait = no  socket\_type = stream  }  Step 3) xinetd 서비스 재시작  #service xinetd restart | |
| 조치 시  영향 | echo, discard, daytime, chargen는 일반적으로 사용하지 않는 서비스들임 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX,  HP-UX, SOLARIS 5.9  이하 버전 | NFS 서비스 데몬 확인 (NFS 동작 SID 확인)  #ps -ef | egrep "nfs|statd|lockd"  root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd |
| SOLARIS 5.10  이상 버전 | #inetadm | egrep “nfs|statd|lockd” |
| 불필요한 "NFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬  중지 | |

|  |  |
| --- | --- |
| U-24 (상) | 3. 서비스 관리 > 3.6 NFS 서비스 비활성화 |
| 취약점 개요 | |
| 점검내용 | * 불필요한 NFS 서비스 사용여부 점검 |
| 점검목적 | * NFS(Network File System) 서비스는 한 서버의 파일을 많은 서비스 서버들 이 공유하여 사용할 때 많이 이용되는 서비스이지만 이를 이용한 침해사고 위험성이 높으므로 사용하지 않는 경우 중지함 |
| 보안위협 | * NFS 서비스는 서버의 디스크를 클라이언트와 공유하는 서비스로 적정한 보 안설정이 적용되어 있지 않다면 불필요한 파일 공유로 인한 유출위험이 있음 |
| 참고 | ※ NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마  치 로컬 파일시스템처럼 사용할 수 있는 프로그램임  ※ NFS 서비스 사용은 원칙적으로 금지되어 있지만 불가피하게 필요한 경우 U-25(상) 항 목을 참조하여 통제해야함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요한 NFS 서비스 관련 데몬이 비활성화 되어 있는 경우 |
| 취약 : 불필요한 NFS 서비스 관련 데몬이 활성화 되어 있는 경우 |
| 조치방법 | 사용하지 않는다면 NFS 서비스 중지  아래의 방법으로 NFS 서비스를 제거한 후 시스템 부팅 시, 스크립트 실행 방지 가능   * /etc/dfs/dfstab(또는 /etx/exports)의 모든 공유 제거 * NFS 데몬(nfsd, statd, mountd) 중지 * 시동 스크립트 삭제 또는, 스크립트 이름 변경 |
| 점검 및 조치 사례 | |
| * LINUX, AIX, SOLARIS 5.9 이하 버전   Step 1) NFS 서비스 데몬 중지 | |

UNIX 서버



|  |  |
| --- | --- |
| U-24 (상) | 3. 서비스 관리 > 3.6 NFS 서비스 비활성화 |
| #kill -9 [PID]  Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경 1.. 위치 확인  #ls -al /etc/rc.d/rc\*.d/\* | grep nfs  2. 이름 변경  #mv /etc/rc.d/rc2.d/S60nfs /etc/rc.d/rc2.d/\_S60nfs   * HP-UX   Step 1) NFS 서비스 데몬 중지  #kill -9 [PID]  Step 2) /etc/rc.config.d/nfsconf 파일 설정 수정 #vi /etc/rc.config.d/nfsconf (수정 전) NFS\_SERVER=1  (수정 후) NFS\_SERVER=0   * SOLARIS 5.10 이상 버전 설정 방법   Step 1) NFS 서비스 데몬 확인  svc:/network/nfs/server:default  Step 2) inetadm –d “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #inetadm -d svc:/network/nfs/server:default | |
| 조치 시 영향 | 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 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 NFS 접근제어 파일 | |
| SOLARIS,  HP-UX | “/etc/dfs/dfstab, /etc/dfs/sharetab 파일 |
| LINUX, AIX,  HP-UX | "/etc/exports" 파일 |
| 불가피하게 NFS 서비스를 사용하여야 하는 경우 NFS 접근제어 파일에 꼭 필요한 공유 디렉터리만 나열하고, everyone으로 시스템이 마운트 되지 않도록 설정 | |

|  |  |
| --- | --- |
| U-25 (상) | 3. 서비스 관리 > 3.7 NFS 접근 통제 |
| 취약점 개요 | |
| 점검내용 | * NFS(Network File System) 사용 시 허가된 사용자만 접속할 수 있도록 접근 제한 설정 적용 여부 점검 |
| 점검목적 | * 접근권한이 없는 비인가자의 접근을 통제함 |
| 보안위협 | * 접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파 일을 변조하거나 유출할 위험이 있음 |
| 참고 | ※ NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마  치 로컬 파일시스템처럼 사용할 수 있는 프로그램임  ※ NFS 서비스 사용 금지가 원칙이나 불가피하게 사용이 필요한 경우 NFS v2, v3은 평문 으로 전송되는 취약점이 있기 때문에 암호화 되는 v4를 사용하는 것을 권고함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요한 NFS 서비스를 사용하지 않거나, 불가피하게 사용 시 everyone 공유를 제한한 경우 |
| 취약 : 불필요한 NFS 서비스를 사용하고 있고, everyone 공유를 제한하지 않은 경우 |
| 조치방법 | 사용하지 않는다면 NFS 서비스 중지, 사용할 경우 NFS 설정파일에 everyone 공유 설정 제거 |
| 점검 및 조치 사례 | |
| * /etc/dfs/dfstab 설정 예문   rw=client, ro=client 형식으로 접속 허용 client 지정   * + 사용자의 읽기, 쓰기 권한 접속 허용: share -F nfs -o rw, ro /export/home/test   + 사용자의 권한 접속 제한: share -F nfs -o rw=client1:client2, ro=client1:c   lient2 /export/home/test  ※ 읽기(ro), 쓰기(rw) 권한에 각각 사용자를 설정하여야 읽기, 쓰기 권한 모두 제한 가능 | |

UNIX 서버



|  |  |
| --- | --- |
| U-25 (상) | 3. 서비스 관리 > 3.7 NFS 접근 통제 |
| * /etc/exports 설정 예문   Step 1) /etc/exports 파일에 접근 가능한 호스트명 추가 (예) /stand host1(또는 IP주소) host2  Step 1) 접속시 인증 및 클라이언트 권한 nobody 설정  # vi /etc/export  # /stand host1 (root\_squash)  ※ () 옵션에 인증되지 않은 엑세스를 허용하는 “insecure" 구문 설정 금지 Step 3. NFS 서비스 재구동  #/etc/exportfs –u #/etc/exportfs –a | |
| 조치 시 영향 | 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 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX, HP-UX, SOLARIS 5.9  이하 버전 | automountd 서비스 데몬 확인 (automountd 동작 SID 확인)  #ps -ef | grep automount(or autofs)  root 1131 1 0 jun 15 ? 32:11 /usr/sbin/automountd |
| SOLARIS 5.10  이상 버전 | automount 서비스 데몬 확인  #svcs -a | grep "autofs" |
| "automount" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중  지 | |

|  |  |
| --- | --- |
| U-26 (상) | 3. 서비스 관리 > 3.8 automountd 제거 |
| 취약점 개요 | |
| 점검내용 | * automountd 서비스 데몬의 실행 여부 점검 |
| 점검목적 | * 로컬 공격자가 automountd 데몬에 RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하기 때문에 해당 서비스가 실행중일 경우 서비스를 중 지시키기 위함 |
| 보안위협 | * 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음 |
| 참고 | ※ automountd: 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능을 말함  ※ RPC(Remote Procedure Call): 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : automountd 서비스가 비활성화 되어 있는 경우 |
| 취약 : automountd 서비스가 활성화 되어 있는 경우 |
| 조치방법 | automountd 서비스 비활성화 |
| 점검 및 조치 사례 | |
| * LINUX, AIX, SOLARIS 5.9 이하 버전   Step 1) automountd 서비스 데몬 중지  #kill -9 [PID]  Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경 1.. 위치 확인  #ls -al /etc/rc.d/rc\*.d/\* | grep automount(or autofs)  2. 이름 변경 | |

UNIX 서버



|  |  |
| --- | --- |
| U-26 (상) | 3. 서비스 관리 > 3.8 automountd 제거 |
| #mv /etc/rc.d/rc2.d/S28automountd /etc/rc.d/rc2.d/\_S28automountd   * HP-UX   Step 1) automount 서비스 데몬 중지  #kill -9 [PID]  Step 2) /etc/rc.config.d/nfsconf 파일 설정 수정 #vi /etc/rc.config.d/nfsconf (수정 전) AUTOFS=1  (수정 후) AUTOFS=0   * SOLARIS 5.10 이상 버전   Step 1) autofs 서비스 데몬 확인  svc:/system/filesystem/autofs:default  Step 2) svcadm disable “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #svcadm disable svc:/system/filesystem/autofs:default | |
|  | NFS 및 삼바(Samba) 서비스에서 사용 시 automountd 사용 여부 확인이 필요 |
|  | 하며, 적용 시 CDROM의 자동 마운트는 이뤄지지 않음 (/etc/auto.\*, |
| 조치 시 | /etc/auto\_\* 파일을 확인하여 필요 여부 확인) |
| 영향 |  |
|  | ※ 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 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX, HP-UX, SOLARIS 5.9  이하 버전 | 불필요한 RPC 서비스 비활성화 여부 확인  #cat /etc/inetd.conf |
| LINUX(xinetd) | “/etc/xinetd.d" 디렉터리 내 서비스별 파일 비활성화 여부 확인  #vi /etc/xinetd.d/[서비스별 파일명] |
| SOLARIS 5.10  이상 버전 | RPC 서비스 관련 데몬 확인  #inetadm | grep rpc | grep enabled | egrep "ttdbserver|rex  |rstart|rusers|spray|wall|rquota" |
| 불필요한 “RPC" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지 | |

|  |  |
| --- | --- |
| U-27 (상) | 3. 서비스 관리 > 3.9 RPC 서비스 확인 |
| 취약점 개요 | |
| 점검내용 | * 불필요한 RPC 서비스의 실행 여부 점검 |
| 점검목적 | * 다양한 취약성(버퍼 오버플로우, Dos, 원격실행 등)이 존재하는 RPC 서비스 를 점검하여 해당 서비스를 비활성화 하도록 함 |
| 보안위협 | * 버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있 으므로 서비스를 중지하여야 함 |
| 참고 | ※ RPC(Remote Procedure Call): 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜  ※ 불필요한 RPC 서비스: rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.ypupdated, rpc.rquotad, kcms\_server, cachefsd (※ 각 서비스 설명은 부록 참조) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요한 RPC 서비스가 비활성화 되어 있는 경우 |
| 취약 : 불필요한 RPC 서비스가 활성화 되어 있는 경우 |
| 조치방법 | 일반적으로 사용하지 않는 RPC 서비스들을 inetd.conf 파일에서 주석 처리한 후 inetd 재구동 (진단 보고서에 발견된 RPC 서비스 조치) |
| 점검 및 조치 사례 | |
| * LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전   Step 1) “/etc/inetd.conf” 파일에서 해당 라인 #처리(주석처리)  (수정 전) rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd | |

UNIX 서버



|  |  |
| --- | --- |
| U-27 (상) | 3. 서비스 관리 > 3.9 RPC 서비스 확인 |
| (수정 후) #rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd  Step 2) inetd 서비스 재시작  #ps -ef | grep inetd  root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s  #kill -HUP 141   * LINUX (xinetd일 경우)   Step 1) vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내의 불필요한 RPC 서비스 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)  service finger  {  disable = yes  socket\_type = stream  wait = no  - 이하 생략 -  }  Step 3) xinetd 서비스 재시작  #service xinetd restart   * SOLARIS 5.10 이상 버전   Step 1) 불필요한 rpc 서비스 관련 데몬 확인   * + svc:/network/rpc/cde-ttdbserver:tcp   + svc:/network/rpc/rex:default   + svc:/network/rpc/rstat:default   + svc:/network/rpc/rusers:default   + svc:/network/rpc/spray:default   + svc:/network/rpc/wall:default   + svc:/network/fs/rquota:default   - 이하 생략 -  Step 2) svcadm disable “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #inetadm –d svc:/network/rpc/rusers:default | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX, HP-UX, SOLARIS 5.9  이하 버전 | NIS, NIS+ 서비스 구동 확인  #ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd  |rpc.ypupdated”  root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv |
| SOLARIS 5.10  이상 버전 | 서비스 데몬 구동 여부 확인  #svcs -a | grep nis |
| 불필요한 “NIS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬  중지 | |

|  |  |
| --- | --- |
| NIS 관련 서비스 데몬 | |
| ypserv | master와 slave 서버에서 실행되며 클라이언트로부터의 ypbind  요청에 응답 |
| ypbind | 모든 NIS 시스템에서 실행되며 클라이언트와 서버를 바인딩하고  초기화함 |

|  |  |
| --- | --- |
| U-28 (상) | 3. 서비스 관리 > 3.10 NIS, NIS+ 점검 |
| 취약점 개요 | |
| 점검내용 | * 안전하지 않은 NIS 서비스의 비활성화, 안전한 NIS+ 서비스의 활성화 여부 점검 |
| 점검목적 | * 안전하지 않은 NIS 서비스를 비활성화 하고 안전한 NIS+ 서비스를 활성화 하여 시스템 보안수준을 향상하고자 함 |
| 보안위협 | * 보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타시스템의 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보 다 NIS+를 사용하는 것을 권장함 |
| 참고 | ※ NIS 주 서버는 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네 트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 함. 네트워크를 통한 공유로부터 관리자와 사용자들에게 일관성 있는 시스템 환경을 제공함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : NIS 서비스가 비활성화 되어 있거나, 필요 시 NIS+를 사용하는 경우 |
| 취약 : NIS 서비스가 활성화 되어 있는 경우 |
| 조치방법 | NIS 관련 서비스 비활성화 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| rpc.yppasswdd | 사용자들이 패스워드를 변경하기 위해 사용 |
| ypxfrd | NIS 마스터 서버에서만 실행되며 고속으로 NIS 맵 전송 |
| rpc.ypupdated | NIS 마스터 서버에서만 실행되며 고속으로 암호화하여 NIS 맵  전송 |

|  |  |
| --- | --- |
| U-28 (상) | 3. 서비스 관리 > 3.10 NIS, NIS+ 점검 |
| * LINUX, AIX, SOLARIS 5.9 이하 버전   Step 1) NFS 서비스 데몬 중지  #kill -9 [PID]  Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경 1.. 위치 확인  #ls -al /etc/rc.d/rc\*.d/\* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd  | rpc.ypupdated”  2. 이름 변경  #mv /etc/rc.d/rc2.d/S73ypbind /etc/rc.d/rc2.d/\_S73ypbind   * HP-UX   Step 1) NFS 서비스 데몬 중지  #kill -9 [PID]  Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경   * + 위치 확인   #ls -al /etc/rc.d/rc\*.d/\* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd  | rpc.ypupdated”   * + /etc/rc.config.d/namesvrs 파일에서 NIS\_MASTER\_SERVER, NIS\_SLAVE\_SERVER, NIS\_CLI ENT 값을 0으로 설정   NIS\_MASTER\_SERVER=0 NIS\_SLAVE\_SERVER=0 NIS\_CLIENT\_SERVER=0   * SOLARIS 5.10 이상 버전   Step 1) NIS 관련 서비스 데몬 확인  online 16:44:06 svc:/network/nis/client:default  online 16:44:07 svc:/network/nis/passwd:default  online 16:44:07 svc:/network/nis/server:default  online 16:44:07 svc:/network/nis/update:default  online 16:44:07 svc:/network/nis/xfr:default  Step 2) svcadm disable “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지 | |

UNIX 서버

|  |  |
| --- | --- |
| U-28 (상) | 3. 서비스 관리 > 3.10 NIS, NIS+ 점검 |
| #svcadm disable svc:/network/nis/server:default #svcadm disable svc:/network/nis/client:default #svcadm disable svc:/network/nis/passwd:default #svcadm disable svc:/network/nis/update:default #svcadm disable svc:/network/nis/xfr:default  ※ NIS 사용이 반드시 필요 시 NIS+ 사용 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX, HP-UX, SOLARIS 5.9  이하 버전 | 불필요한 서비스 데몬 확인  #cat /etc/inetd.conf | grep “tftp|talk|ntalk"  tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n |
| LINUX(xinetd) | tftp, talk, ntalk 서비스 활성화 여부 확인  #vi /etc/xinetd.d/tftp  #vi /etc/xinetd.d/talk #vi /etc/xinetd.d/ntalk |
| SOLARIS 5.10  이상 버전 | 서비스 데몬 확인  #inetadm | egrep “tftp|talk” |
| 불필요한 “tftp, talk ntalk" 서비스가 활성화된 경우 아래의 보안설정방법에 따라  서비스 데몬 중지 | |

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| tftp(69) | 파일 전송을 위한 프로토콜로서 FTP서비스 보다 구조가 단순하며  적은 양의 데이트를 보낼 때 사용됨, 주로 원격의 부팅파일을 불러오거나 설치 프로세스를 시작하기 위한 초기 데이터 호출  용도로 사용. 서비스 사용시 인증절차가 없어 보안에 취약함. |
| talk(517) | 사용자가 시스템에 원격으로 연결하여 다른 시스템에 로그인하고 |

|  |  |
| --- | --- |
| U-29 (상) | 3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화 |
| 취약점 개요 | |
| 점검내용 | * tftp, talk 등의 서비스를 사용하지 않거나 취약점이 발표된 서비스의 활 성화 여부 점검 |
| 점검목적 | * 안전하지 않거나 불필요한 서비스를 제거함으로써 시스템 보안성 및 리소스 의 효율적 운용 |
| 보안위협 | * 사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격 시도 가능 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : tftp, talk, ntalk 서비스가 비활성화 되어 있는 경우 |
| 취약 : tftp, talk, ntalk 서비스가 활성화 되어 있는 경우 |
| 조치방법 | 시스템 운영에 불필요한 서비스(tftp, talk, ntalk) 비활성화 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 있는 사용자와 대화 세션을 시작할 수 있음 | | | | | | | |
| ntalk(518) | 서로 | 다른 | 시스템 | 간에 | 채팅을 | 가능하게 | 하는 | 서비스 |

|  |  |
| --- | --- |
| U-29 (상) | 3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화 |
| * LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전   Step 1) vi 편집기를 이용하여 "/etc/inetd.conf" 파일 열기  #vi /etc/inetd.conf  Step 2) tftp, talk, ntalk 서비스 주석 처리  #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  Step 3) inetd 데몬 재시작 AIX) #refresh -s inetd HP-UX) #inetd -c  LINUIX, SOLARIS) #kill -HUP [inetd pid]   * LINUX (xinetd일 경우)   Step 1) vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 tftp, talk, ntalk 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)   * + /etc/xinetd.d/tftp 파일   + /etc/xinetd.d/talk 파일   + /etc/xinetd.d/ntalk 파일   service tftp  {  socket\_type = dgram  protocol = udp  wait = yes  user = root  server = /usr/sbin/in.tftpd  server\_args = -s /tftpboot  disable = yes  }  Step 3) xinetd 서비스 재시작  #service xinetd restart | |

UNIX 서버



|  |  |
| --- | --- |
| U-29 (상) | 3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화 |
| * SOLARIS 5.10 이상 버전   Step 1) 불필요한 서비스 데몬 확인  svc:/network/tftp:default svc:/network/talk:default svc:/network/ntalk:default  Step 2) inetadm –d “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #inetadm -d svc:/network/tftp:default #inetadm -d svc:/network/talk:default  #inetadm -d svc:/network/ntalk:default | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | * Sendmail 서비스 실행 여부 점검   #ps -ef | grep sendmail   * Sendmail 버전 점검   #telnet localhost 25 |
| "Sendmail" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지 또  는, 버전 업그레이드 | |

|  |  |
| --- | --- |
| U-30 (상) | 3. 서비스 관리 > 3.12 Sendmail 버전 점검 |
| 취약점 개요 | |
| 점검내용 | * 취약한 버전의 Sendmail 서비스 이용 여부 점검 |
| 점검목적 | * Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무 점검 으로 최적화된 Sendmail 서비스의 운영 |
| 보안위협 | * 취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있음 |
| 참고 | ※ Sendmail 서비스의 경우 최신버전(2016.01 기준 8.15.2) 이하 대부분의 버전에서 취약 점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영 향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : Sendmail 버전이 최신버전인 경우 |
| 취약 : Sendmail 버전이 최신버전이 아닌 경우 |
| 조치방법 | Sendmail 서비스를 사용하지 않을 경우 서비스 중지, 재부팅 후 다시 시작하지 않도록 시작 스크립트 변경, 사용할 경우 패치 관리 정책을 수립하여 주기적으 로 패치 적용 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Sendmail 서비스 실행 여부 및 버전 점검 후, <http://www.sendmail.org/>또는, 각 OS 벤더사의 보안 패치 설치 | |
| 조치 시  영향 | 패치를 적용할 경우 시스템 및 서비스의 영향 정도를 충분히 고려하여야 함 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인  #ps -ef | grep sendmail | grep -v "grep"  #cat /etc/mail/sendmail.cf | grep "R$\\*" | grep "Relaying denied"  R$\* $#error $@ 5.7.1 $: "550 Relaying denied" | | | | | | |
| "SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보  안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| sendmail.cf 설정파일 위치 | |
| SOLARIS,  LINUX, AIX,  HP-UX | "/etc/mail/sendmail.cf" |
| ※ sendmail 버전에 따라 /etc/sendmail.cf 존재함 | |

|  |  |
| --- | --- |
| U-31 (상) | 3. 서비스 관리 > 3.13 스팸 메일 릴레이 제한 |
| 취약점 개요 | |
| 점검내용 | * SMTP 서버의 릴레이 기능 제한 여부 점검 |
| 점검목적 | * 스팸 메일 서버로의 악용방지 및 서버 과부하의 방지를 위함 |
| 보안위협 | * SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가 진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있음 |
| 참고 | ※ SMTP(Simple Mail Transfer Protocol) 서버: 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 SMTP라고 하며, SMTP에 의해 전자 메일을 발신 하는 서버(server)를 SMTP 서버라고 함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우 |
| 취약 : SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우 |
| 조치방법 | Sendmail 서비스를 사용하지 않을 경우 서비스 중지  사용할 경우 릴레이 방지 설정 또는, 릴레이 대상 접근 제어 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, HP-UX, AIX   Step 1) vi 편집기를 이용하여 sendmail.cf 설정파일 열기 Step 2) 아래와 같이 주석 제거  (수정 전) #R$\* $#error $@ 5.7.1 $: "550 Relaying denied" | |

UNIX 서버

|  |  |
| --- | --- |
| U-31 (상) | 3. 서비스 관리 > 3.13 스팸 메일 릴레이 제한 |
| (수정 후) R$\* $#error $@ 5.7.1 $: "550 Relaying denied"  Step 3) 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인 (없을 시 파일생성)  #cat /etc/mail/access  예)  localhost.localdomain RELAY localhost RELAY  127.0.0.1 RELAY  spam.com REJECT  Step 4) 수정을 했거나 생성했을 경우 DB 파일 생성  #makemap hash /etc/mail/access.db < /etc/mail/access | |
| 조치 시  영향 | 릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | SMTP 서비스 사용 여부 및 restrictqrun 옵션 확인  #ps -ef | grep sendmail | grep -v "grep"  #grep -v '^ \*#' /etc/mail/sendmail.cf | grep PrivacyOptions |
| "SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보 안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-32 (상) | 3. 서비스 관리 > 3.14 일반사용자의 Sendmail 실행 방지 |
| 취약점 개요 | |
| 점검내용 | * SMTP 서비스 사용 시 일반사용자의 q 옵션 제한 여부 점검 |
| 점검목적 | * 일반사용자의 q 옵션을 제한하여 Sendmail 설정 및 메일큐를 강제적으로 drop 시킬 수 없게 하여 비인가자에 의한 SMTP 서비스 오류 방지 |
| 보안위협 | * 일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐 를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시 킬 수 있음 |
| 참고 | ※ SMTP(Simple Mail Transfer Protocol): 인터넷상에서 전자우편(E-mail)을 전송할 때 이 용하게 되는 표준 통신 규약을 말함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우 |
| 취약 : SMTP 서비스 사용 및 일반 사용자의 Sendmail 실행 방지가 설정되어 있지 않은 경우 |
| 조치방법 | Sendmail 서비스를 사용하지 않을 경우 서비스 중지  Sendmail 서비스를 사용 시 sendmail.cf 설정파일에 restrictqrun 옵션 추가 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 sendmail.cf 설정파일 열기  Step 2) O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가  (수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn  (수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun  Step 3. Sendmail 서비스 재시작 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 위치 및 | | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | DNS 서비스 #ps -ef | named -v | 사용  grep | 및 BIND  named | 버전 | 확인 | |
| "DNS" 서비스를 사용하지 않는 경우 서비스 중지  "DNS" 서비스 사용 시 BIND 버전 확인 후 아래의 보안설정방법에 따라 최신 버전  으로 업데이트 | | | | | | |

|  |  |
| --- | --- |
| U-33 (상) | 3. 서비스 관리 > 3.15 DNS 보안 버전 패치 |
| 취약점 개요 | |
| 점검내용 | * BIND 최신버전 사용 유무 및 주기적 보안 패치 여부 점검 |
| 점검목적 | * 취약점이 발표되지 않은 BIND 버전의 사용을 목적으로 함 |
| 보안위협 | * 최신버전(2016.01 기준 9.10.3-P2) 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재함 |
| 참고 | ※ BIND(Berkeley Internet Name Domain): BIND는 BSD 기반의 유닉스 시스템을 위해 설 계된 DNS로 서버와 resolver 라이브러리로 구성되어 있음. 네임서버는 클라이언트들이 이름 자원들이나 객체들에 접근하여, 네트워크 내의 다른 객체들과 함께 정보를 공유 할 수 있게 해주는 네트워크 서비스로 사실상 컴퓨터 네트워크 내의 객체들을 위한 분 산 데이터베이스 시스템임 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우 |
| 취약 : DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우 |
| 조치방법 | DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용할 경우 패치 관리 정책 을 수립하여 주기적으로 패치 적용  ※ DNS 서비스의 경우 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악 하여 주기적인 패치 적용 정책 수립 후 적용 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX * BIND는 거의 모든 버전이 취약한 상태로서 최신 버전으로 업데이트가 요구됨 * 다음은 구체적인 BIND 취약점들이며, 취약점 관련 버전을 사용하는 시스템에서는 버전 업그레이드를 하여야 함   + Inverse Query 취약점 (Buffer Overflow) : BIND 4.9.7이전 버전과 BIND 8.1.2 이전 버전   + NXT버그 (buffer overflow) : BIND 8.2, 8.2 p1, 8.2.1버전 | |

UNIX 서버



|  |  |
| --- | --- |
| U-33 (상) | 3. 서비스 관리 > 3.15 DNS 보안 버전 패치 |
| * solinger버그 (Denial of Service) : BIND 8.1 이상버전 * fdmax 버그 (Denial of Service) : BIND 8.1 이상버전 * Remote Execution of Code(Buffer Overflow) : BIND 4.9.5 to 4.9.10, 8.1, 8.2 to 8.2.6,   8.3.0 to 8.3.3 버전   * Multiple Denial of Service: BIND 8.3.0 - 8.3.3, 8.2 - 8.2.6 버전 * LIBRESOLV: buffer overrun(Buffer Overflow) : BIND 4.9.2 to 4.9.10 버전 * OpenSSL (buffer overflow) : BIND 9.1, BIND 9.2 if built with OpenSSL(configure   --with-openssl)   * libbind (buffer overflow) : BIND 4.9.11, 8.2.7, 8.3.4, 9.2.2 이외의 모든 버전 * DoS internal consistency check (Denial of Service) : BIND 9 ~ 9.2.0 버전 * tsig bug (Access possible) : BIND 8.2 ~ 8.2.3 버전 * complain bug (Stack corruption, possible remote access) : BIND 4.9.x 거의 모든 버전 * zxfr bug (Denial of service) : BIND 8.2.2, 8.2.2 patchlevels 1 through 6 버전 * sigdiv0 bug (Denial of service) : BIND 8.2, 8.2 patchlevel 1, 8.2.2 버전 * srv bug(Denial of service): BIND 8.2, 8.2 patchlevel 1, 8.2.1, 8.2.2, 8.2.2 patchlevels 1-6 버전 * nxt bug (Access possible) : BIND 8.2, 8.2 patchlevel 1, 8.2.1 버전 * BIND 4.9.8 이전 버전, 8.2.3 이전 버전과 관련된 취약점   + TSIG 핸들링 버퍼오버플로우 취약점   + nslookupComplain() 버퍼오버플로우 취약점   + nslookupComplain() input validation 취약점   + information leak 취약점   + sig bug Denial of service 취약점   + naptr bug Denial of service 취약점   + maxdname bug enial of service 취약점   ※ Bind 최신버전 다운로드 사이트 <http://www.isc.org/downloads/>  ※ 각 버전에 대한 취약점 정보 사이트   * BIND 8 Vulnerability matrix :   https://kb.isc.org/article/AA-00959/0/BIND-8-Security-Vulnerability-Matrix.html   * BIND 9 Vulnerability matrix :   https://kb.isc.org/article/AA-00913/74/BIND-9-Security-Vulnerability-Matrix.html | |
| 조치 시  영향 | 패치를 적용 시 시스템 및 서비스 영향 정도를 충분히 고려하여야 함 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | DNS 서비스 사용 시 /etc/named.conf 파일의 allow-transfer 및 xfrnets 확인  #ps -ef | grep named | grep -v "grep"  #cat /etc/named.conf | grep 'allow-transfer' #cat /etc/named.boot | grep "xfrnets" | | | | | | |
| "DNS" 서비스 사용 시 위에 제시된 파일의 DNS 설정을 아래의 보안설정방법에 따라 수정함 | | | | | | | |

|  |  |
| --- | --- |
| U-34 (상) | 3. 서비스 관리 > 3.16 DNS Zone Transfer 설정 |
| 취약점 개요 | |
| 점검내용 | * Secondary Name Server로만 Zone 정보 전송 제한 여부 점검 |
| 점검목적 | * 허가되지 않는 사용자에게 Zone Transfer를 제한함으로써 호스트 정보, 시스 템 정보 등 정보 유출의 방지를 목적으로 함 |
| 보안위협 | * 비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스 템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있음 |
| 참고 | ※ DNS Zone Transfer는 Primary Name Server와 Secondary Name Server 간에 Zone 정 보를 일관성 있게 유지하기 위하여 사용하는 기능 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우 |
| 취약 : DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우 |
| 조치방법 | DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용한다면 DNS 설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정 |
| 점검 및 조치 사례 | |
| < DNS 서비스를 사용할 경우 >   * BIND8 DNS 설정(named.conf) 수정 예   Options {  allow-transfer (존 파일 전송을 허용하고자 하는 IP;);  }; | |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| LINUX, AIX,  HP-UX, SOLARIS 5.9  이하 버전 | DNS 서비스 데몬 확인 (DNS 동작 SID 확인)  #ps -ef | grep named  root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named |
| SOLARIS 5.10  이상 버전 | #svcs -a | egrep “dns” |
| “DNS” 서비스를 사용하지 않는 경우 서비스 데몬 중지 | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-34 (상) | 3. 서비스 관리 > 3.16 DNS Zone Transfer 설정 | | | | | | | | | | |
| * BIND4.9 DNS 설정(named.conf) 수정 예   Options  xfrnets 허용하고자 하는 IP  < DNS 서비스를 사용하지 않는 경우 >   * LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전   DNS 서비스 데몬 중지 #kill -9 [PID]   * SOLARIS 5.10 이상 버전   Step 1) DNS 서비스 데몬 확인  enabled 16:22:31 svc:/network/dns/server:default  Step 2) svcadm disable “중지하고자 하는 데몬“ 명령으로 서비스 데몬 중지  #svcadm disable svc:/network/dns/server:default | | | | | | | | | | | |
| 조치 시  영향 | Zone | 파일 | 전송을 | 허용할 | 대상을 | 정상적으로 | 등록할 | 경우 | 일반적으로 | 영향 | 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | Indexes 옵션 사용 여부 확인  #vi /[Apache\_home]/conf/httpd.conf  Options Indexes FollowSymLinks | | | | | | |
| 위에 제시한 파일에 "Indexes" 옵션이 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경 | | | | | | | |

|  |  |
| --- | --- |
| U-35 (상) | 3. 서비스 관리 > 3.17 웹서비스 디렉토리 리스팅 제거 |
| 취약점 개요 | |
| 점검내용 | * 디렉터리 검색 기능의 활성화 여부 점검 |
| 점검목적 | * 외부에서 디렉터리 내의 모든 파일에 대한 접근 및 열람을 제한함을 목적으 로 함 |
| 보안위협 | * 디렉터리 검색 기능이 활성화 되어 있을 경우, 사용자에게 디렉터리내 파일 이 표시되어 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일, 공 개되어서는 안되는 파일 등이 노출 가능함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 디렉터리 검색 기능을 사용하지 않는 경우 |
| 취약 : 디렉터리 검색 기능을 사용하는 경우 |
| 조치방법 | 디렉터리 검색 기능 제거 (/[Apache\_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시자에서 Indexes 옵션 제거) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일 열기  #vi /[Apache\_home]/conf/httpd.conf  Step 2) 설정된 모든 디렉터리의 Options 지시자에서 Indexes 옵션 제거 (수정 전) Option 지시자에 Indexes 옵션이 설정되어 있음  <Directory />  Options Indexes FollowSymLinks AllowOverride None  Order allow, deny Allow from all  </Directory> | |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-35 (상) | 3. | | 서비스 관리 | | > | 3.17 | 웹서비스 | 디렉토리 | 리스팅 | 제거 |
| (수정 후) Option 지시자에 Indexes 삭제 또는 -Indexes 변경 후 저장  <Directory />  Options Indexes 삭제 (또는 -Indexes) AllowOverride None  Order allow, deny Allow from all  </Directory> | | | | | | | | | | |
| 조치 시  영향 | 일반적인 | 경우 | 영향 | 없음 | | | | | | |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | Apache 데몬 구동 권한(User 및 Group) 확인  #vi /[Apache\_home]/conf/httpd.conf User [root가 아닌 별도 계정명]  Group [root가 아닌 별도 계정명] |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-36 (상) | 3. 서비스 관리 > 3.18 웹서비스 웹 프로세스 권한 제한 |
| 취약점 개요 | |
| 점검내용 | * Apache 데몬이 root 권한으로 구동되는지 여부 점검 |
| 점검목적 | * Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 구동함으로   써 침해사고 발생 시 피해범위 확산 방지를 목적으로 함 |
| 보안위협 | * 웹서비스 데몬을 root 권한으로 실행시 웹서비스가 파일을 생성, 수정하는 과정에서 웹서비스에 해당하지 않는 파일도 root 권한에 의해 쓰기가 가능 하며 해킹 발생시 root 권한이 노출 될 수 있음 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : Apache 데몬이 root 권한으로 구동되지 않는 경우 |
| 취약 : Apache 데몬이 root 권한으로 구동되는 경우 |
| 조치방법 | Apache 데몬을 root 가 아닌 별도 계정으로 구동 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 데몬 User & Group 변경  User & Group 부분에 root가 아닌 별도 계정으로 변경  ※ 웹서비스 실행 계정은 로그인이 불가능하도록 쉘 제한 필수  User [root가 아닌 별도 계정명] Group [root가 아닌 별도 계정명]  Step 2) Apache 서비스 재시작 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | AllowOverride 지시자 Authconfig 옵션 확인 #vi /[Apache\_home]/conf/httpd.conf AllowOverride None | | | | | | |
| "AllowOverride" 옵션이 “None”으로 설정된 경우 아래의 보안설정방법에 따라 옵션  설정 변경 | | | | | | | |

|  |  |
| --- | --- |
| U-37 (상) | 3. 서비스 관리 > 3.19 웹서비스 상위 디렉토리 접근 금지 |
| 취약점 개요 | |
| 점검내용 | * “..” 와 같은 문자 사용 등으로 상위 경로로 이동이 가능한지 여부 점검 |
| 점검목적 | * 상위 경로 이동 명령으로 비인가자의 특정 디렉터리에 대한 접근 및 열람을 제한하여 중요 파일 및 데이터 보호를 목적으로 함 |
| 보안위협 | * 상위 경로로 이동하는 것이 가능할 경우 접근하고자 하는 디렉터리의 하위 경로에 접속하여 상위경로로 이동함으로써 악의적인 목적을 가진 사용자의 접근이 가능함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 상위 디렉터리에 이동제한을 설정한 경우 |
| 취약 : 상위 디렉터리에 이동제한을 설정하지 않은 경우 |
| 조치방법 | Step 1) 사용자 인증을 하기 위해서 각 디렉터리 별로 httpd.conf 파일 내 AllowOverride 지시자의 옵션 설정을 변경 (None에서 AuthConfig 또 는, All로 변경)  Step 2) 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성  Step 3) 사용자 인증 계정 생성: htpasswd -c <인증 파일> <사용자 계정> |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일 열기  #vi /[Apache\_home]/conf/httpd.conf  Step 2) 설정된 모든 디렉터리의 AllowOverride 지시자에서 AuthConfig 옵션 설정  (수정 전) AllowOverride 지시자에 None 옵션이 설정되어 있음  <Directory “/usr/local/apache2/htdocs”> AllowOverride None  Allow from all | |

UNIX 서버

|  |  |
| --- | --- |
| 지시자 | 설명 |
| AuthName | 인증 영역(웹 브라우저의 인증 창에 표시되는 문구) |
| AuthType | 인증 형태(Basic 또는, Digest) |
| AuthUserFile | 사용자 정보(아이디 및 패스워드) 저장 파일 위치 |
| AuthGroupFile | 그룹 파일의 위치(옵션) |
| Require | 접근을 허용할 사용자 또는, 그룹 정의 |

|  |  |
| --- | --- |
| U-37 (상) | 3. 서비스 관리 > 3.19 웹서비스 상위 디렉토리 접근 금지 |
| </Directory>  (수정 후) AllowOverride 지시자에 AuthConfig 옵션이 설정되어 있음  <Directory “/usr/local/apache2/htdocs”> AllowOverride AuthConfig  Allow from all  </Directory>  Step 3) 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 (아래 내용 삽입)  AuthName "디렉터리 사용자 인증" AuthType Basic  AuthUserFile /usr/local/apache/test/.auth Require valid-user  Step 4) 사용자 인증에 사용할 아이디 및 패스워드 생성  htpasswd -c /usr/local/apache/test/.auth test New password:  Re-type new password:  Adding password for user test [root@localhost apache]#  Step 5) 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작 | |
| 조치 시 영향 | 해당 설정이 적용된 디렉터리 내 파일들은 아이디/패스워드 인증절차 없이는 접속이 불가능하며, 대외 서비스인 경우 해당 디렉터리에 대한 외부자의 접근 필요성을 검토 후 적용하여야 함 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | 불필요한 파일 및 디렉터리 존재 여부 확인 #ls -ld /[Apache\_home]/htdocs/manual #ls -ld /[Apache\_home]/manual | | | | | | |
| 위에 제시한 불필요한 파일 및 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 불필요한 파일 및 디렉터리 제거 또는, 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-38 (상) | 3. 서비스 관리 > 3.20 웹서비스 불필요한 파일 제거 |
| 취약점 개요 | |
| 점검내용 | * Apache 설치 시 기본으로 생성되는 불필요한 파일의 삭제 여부 점검 |
| 점검목적 | * Apache 설치 시 디폴트로 설치되는 불필요한 파일을 제거함을 목적으로 함. |
| 보안위협 | * Apache 설치 시 htdocs 디렉터리 내에 매뉴얼 파일은 시스템 관련정보를   노출하거나 해킹에 악용될 수 있음 |
| 참고 | ※ 불필요한 파일: 샘플 파일, 매뉴얼 파일, 임시 파일, 테스트 파일, 백업 파일 등 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되어 있는 경우 |
| 취약 : 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되지 않은 경우 |
| 조치방법 | 불필요한 파일 및 디렉터리 제거  (“/[Apache\_home]/htdocs/manual”, “/[Apache\_home]/manual” 파일 제거 등) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) #ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거  #rm -rf /[Apache\_home]/htdocs/manual #rm -rf /[Apache\_home]/manual  Step 2) #ls 명령어로 정상적인 제거 확인  #ls -ld /[Apache\_home]/htdocs/manual #ls –ld /[Apache\_home]/manual  Step 3) 추가적으로 웹서비스 운영에 불필요한 파일이나 디렉터리가 있을 시 제거 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | Options 지시자 FollowSymLinks 옵션 제거 여부 확인 #vi /[Apache\_home]/conf/httpd.conf Options Indexes FollowSymLinks | | | | | | |
| 위에 제시한 옵션이 적용되어 있는 경우 아래의 보안설정방법에 따라 옵션을 제거함 | | | | | | | |

|  |  |
| --- | --- |
| U-39 (상) | 3. 서비스 관리 > 3.21 웹서비스 링크 사용금지 |
| 취약점 개요 | |
| 점검내용 | * 심볼릭 링크, aliases 사용 제한 여부 점검 |
| 점검목적 | * 무분별한 심볼릭 링크, aliases 사용제한으로 시스템 권한의 탈취 방지를 목   적으로 함 |
| 보안위협 | * 웹 루트 폴더(DocumentRoot)에 root 디렉터리(/)를 링크하는 파일이 있으며 디렉터리 인덱싱 기능이 차단되어 있어도 root 디렉터리 열람이 가능함 |
| 참고 | ※ 심볼릭 링크(Symbolic link, 소프트 링크): 윈도우 운영체제의 바로가기 아이콘과 비슷 함. 링크 생성 시 파일 내용은 존재하지 않으나 사용자가 파일을 요청하면 링크가 가 리키고 있는 원본 데이터에서 데이터를 가져와서 전달함. 직접 원본을 가리키지 않고 원본 데이터를 가리키는 포인터를 참조함으로써 원본데이터가 삭제, 이동, 수정이 되면 사용 불가함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 심볼릭 링크, aliases 사용을 제한한 경우 |
| 취약 : 심볼릭 링크, aliases 사용을 제한하지 않은 경우 |
| 조치방법 | 심볼릭 링크, aliases 사용 제한  (/[Apache\_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시 자에서 심볼릭 링크를 가능하게 하는 FollowSymLinks 옵션 제거) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일 열기  #vi /[Apache\_home]/conf/httpd.conf  Step 2) 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거 (수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음  <Directory />  Options Indexes FollowSymLinks | |

UNIX 서버



|  |  |
| --- | --- |
| U-39 (상) | 3. 서비스 관리 > 3.21 웹서비스 링크 사용금지 |
| AllowOverride None Order allow, deny Allow from all  </Directory>  (수정 후) Options 지시자에 FollowSymLinks 삭제 또는 -FollowSymLinks 변경 후 저장  <Directory />  Options FollowSymLinks 삭제 또는 -FollowSymLinks  AllowOverride None Order allow, deny Allow from all  </Directory> | |
| 조치 시 영향 | 심볼릭 링크를 이용하여 웹페이지가 구성되어 있는 경우 해당 서비스가 실행되 지 않을 수 있음. 웹서버의 DocumentRoot 폴더 내에 심볼릭 링크가 설정된 파 일 검토 필요 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | LimitRequestBody 파일 사이즈 용량 제한 설정 여부 확인 #vi /[Apache\_home]/conf/httpd.conf LimitRequestBody 5000000  (※ 업로드 및 다운로드 파일이 5M를 넘지 않도록 설정 권고함) |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-40 (상) | 3. 서비스 관리 > 3.22 웹서비스 파일 업로드 및 다운로드 제한 |
| 취약점 개요 | |
| 점검내용 | * 파일 업로드 및 다운로드의 사이즈 제한 여부 점검 |
| 점검목적 | * 기반시설 특성상 원칙적으로 파일 업로드 및 다운로드를 금지하고 있지만 불가피하게 필요시 용량 사이즈를 제한함으로써 불필요한 업로드와 다운로 드를 방지해 서버의 과부하 예방 및 자원을 효율적으로 관리하기 위함 |
| 보안위협 | * 악의적 목적을 가진 사용자가 반복 업로드 및 웹 쉘 공격 등으로 시스템 권 한을 탈취하거나 대용량 파일의 반복 업로드로 서버자원을 고갈시키는 공격 의 위험이 있음 |
| 참고 | ※ 불필요한 업로드와 다운로드: 내부 정책에 맞지 않는 업로드와 다운로드를 말함. 예를 들어 5Mb 이상의 대용량 파일이나 확장자를 화이트 리스트 방식으로 제한함을 말함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 파일 업로드 및 다운로드를 제한한 경우 |
| 취약 : 파일 업로드 및 다운로드를 제한하지 않은 경우 |
| 조치방법 | 1. 파일 업로드 및 다운로드 용량 제한 (/[Apache\_home]/conf/httpd.conf 파일 에 설정된 모든 디렉터리의 LimitRequestBody 지시자에 파일 사이즈 용량 제한 설정) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일 열기  #vi /[Apache\_home]/conf/httpd.conf | |

UNIX 서버



|  |  |
| --- | --- |
| U-40 (상) | 3. 서비스 관리 > 3.22 웹서비스 파일 업로드 및 다운로드 제한 |
| Step 2) 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정  예)  <Directory />  LimitRequestBody 5000000 (※ “/” 는 모든 파일 사이즈를 5M로 제한하는 설 정 단위:byte)  </Directory> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | DocumentRoot의 별도 디렉터리 지정 여부 확인  #vi /[Apache\_home]/conf/httpd.conf DocumentRoot "/usr/local/apache/htdocs" 또는 DocumentRoot "/usr/local/apache2/htdocs" 또는  DocumentRoot "/var/www/html" | | | | | | |
| DocumentRoot가 별도의 디렉터리로 지정되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-41 (상) | 3. 서비스 관리 > 3.23 웹서비스 영역의 분리 |
| 취약점 개요 | |
| 점검내용 | * 웹 서버의 루트 디렉터리와 OS의 루트 디렉터리를 다르게 지정하였는지 점검 |
| 점검목적 | * 웹 서비스 영역과 시스템 영역을 분리시켜서 웹 서비스의 침해가 시스템 영 역으로 확장될 가능성을 최소화하기 위함 |
| 보안위협 | * 웹 서버의 루트 디렉터리와 OS의 루트 디렉터리를 다르게 지정하지 않았을 경우, 비인가자가 웹 서비스를 통해 해킹이 성공할 경우 시스템 영역까지 접 근이 가능하여 피해가 확장될 수 있음 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : DocumentRoot를 별도의 디렉터리로 지정한 경우 |
| 취약 : DocumentRoot를 기본 디렉터리로 지정한 경우 |
| 조치방법 | DocumentRoot "/usr/local/apache/htdocs”, "/usr/local/apache2/htdocs", "/var/www/html"와 같이 기본경로일 경우 -> etc, bin, sbin, usr 등 시스템 중요 디렉터리 외에 설치(예 : /www 와 같이 별도의 디렉터리를 생성하여 설치, 운영) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일 열기  #vi /[Apache\_home]/conf/httpd.conf  Step 2) DocumentRoot 설정 부분에 “/usr/local/apache/htdocs”, "/usr/local/apache2/htdocs", "/var/www/html" 셋 중 하나가 아닌 별도의 디렉터리로 변경  DocumentRoot "디렉터리" | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 점검 방법 | | | | | | | | | | | | |
| SOLARIS,  LINUX, AIX,  HP-UX | 패치 | 적용 | 정책 | 수립 | 여부 | 및 | 정책에 | 따른 | 패치 | 적용 | 여부 | 확인 |

|  |  |
| --- | --- |
| U-42 (상) | 4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용 |
| 취약점 개요 | |
| 점검내용 | * 시스템에서 최신 패치가 적용되어 있는지 점검 |
| 점검목적 | * 주기적인 패치 적용을 통하여 보안성 및 시스템 안정성을 확보함 |
| 보안위협 | * 최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자 에 의해 시스템 침해사고 발생 가능성이 존재함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 패치 적용 정책을 수립하여 주기적으로 패치관리를 하고 있으며, 패치 관련 내용을 확인하고 적용했을 경우 |
| 취약 : 패치 적용 정책을 수립하지 않고 주기적으로 패치관리를 하지 않거나 패 치 관련 내용을 확인하지 않고 적용하지 않았을 경우 |
| 조치방법 | O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 파악하여 OS 관리자 및 벤더에서 적용함  ※ OS 패치의 경우 지속적으로 취약점이 발표되고 있기 때문에 O/S 관리자, 서비스 개발 자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하여 주기적인 패치 적용 정책 을 수립하여 적용하여야 함 |
| 점검 및 조치 사례 | |
| * SOLARIS * “showrev –p” 서버에 적용되어 있는 패치 리스트 확인 * 아래 사이트에 접속하여 패치를 찾아 적용 https://support.oracle.com * 패치를 검색하는 방법 * Patches & Updates(패치 및 업데이트) 탭을 클릭 * Patch Search(패치 검색) 섹션에서 Product or the Family (Advanced Search)(제품 또는 제   품군(고급 검색)) 옵션을 클릭   * 제품으로 Solaris Operating System(Solaris 운영 체제)을 선택 * 릴리스로 Solaris xx Operating System(Solaris xx 운영 체제)을 선택 | |

UNIX 서버

|  |  |
| --- | --- |
| U-42 (상) | 4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용 |
| * 유형으로 Patch(패치) 또는 Patchset(패치 세트) 또는 둘 다 선택 * Search(검색)을 클릭 후 파일 다운로드   < 패치 적용 방법 >  MOS(My Oracle Support) 웹 사이트에서 패치 파일(119784-17.zip)을 다운로드 했다고 가정 Step 1) 슈퍼유저가 되어야 함.  Step 2) 패치 파일을 임시 디렉터리에 복사  #cp /<patch download location>/119784-17.zip /tmp  Step 3) 패치 파일의 압축 풀기.  #cd /tmp  #unzip 119784-17.zip  Step 4) 패치를 적용  #patchadd 119784-17  Step 5) (옵션)패치가 적용되었는지 확인  #patchadd –p | grep 119784-17  ※ 패치 시 주의점  patchadd -M 명령이 개선되어 더 이상 정확한 설치 순서로 패치ID를 지정할 필요가 없고 디 렉터리의 모든 패치가 시스템에 설치 됨   * LINUX   LINUX는 서버에 설치된 패치 리스트의 관리가 불가능하므로 rpm 패키지 별 버그가 Fix된 최 신 버전 설치가 필요함  LINUX는 오픈되고, 커스터마이징 된 OS이므로 LINUX를 구입한 벤더에 따라 rpm 패키지가 다 를 수 있으며, 아래의 사이트는 RedHat LINUX에 대한 버그 Fix 관련 사이트임  <Red Hat 일 경우>  Step 1) 다음의 사이트에서 해당 버전을 찾음 <http://www.redhat.com/security/updates/> <http://www.redhat.com/security/updates/eol/>(Red Hat LINUX 9 이하 버전)  Step 2) 발표된 Update 중 현재 사용 중인 보안 관련 Update 찾아 해당 Update Download Step 3) Update 설치  #rpm –Uvh <pakage-name>   * AIX * “oslevel –s, instfix-i |grep ML, instfix –i |grep ML, instfix –i |grep SP”로 서버에 적용되어 있는 패치 리스트 확인 * 아래 사이트에 접속하여 패치를 찾아 적용 | |

UNIX 서버



|  |  |
| --- | --- |
| U-42 (상) | 4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용 |
| <http://techsupport.services.ibm.com/server/mlfixes/43/>  < 패치 적용 방법>  Step 1) 패치를 다운로드 후 서버에 파일 업로드 한 뒤 “installp”를 이용하여 OS패치 설치  #smitty installp  Step 2) install Software 선택 후 INPUT device / directory for software에서 패치파일 업로드 한 경로 입력  Step 3) SOFTWARE to install 항목은 all-latest 선택  Step 4) PREVIEW only? (install operation will NOT occur) 항목을 yes로 설정할 경우 실제 설 치가 아닌 사전 설치가 진행되고 문제 발생 시 Failed 결과값 출력함  Step 5) COMMIT software updates? 항목을 no로 설정할 경우 Apply설치가 진행되고 향후 이 전버전의 OS Patch 단계로 롤백이 가능. YES로 설정 시 롤백 불가  Step 6) ACCEPT new license agreements? 항목은 YES로 설정해야만 설치 진  ※ 패치 시 문제가 발생한 경우 Apply 설치에 한해 기본버전으로 재설정 가능 Apply, commit 된 패키지 확인은 “lslpp –l”로 확인 가능  # smitty install\_reject   * SOFTWARE name 항목에서 Apply설치된 OS Patch를 선택 * Preview 항목을 Yes로 설정 * 소프트웨어 제거에 문제가 없는지 확인 후 진행 * HP-UX * ‘swlist –l product’로 서버에 적용된 패치 리스트 확인 * 아래 사이트에 접속하여 패치를 찾아 적용(ID, password가 필요함) <http://h20565.www2.hp.com/portal/site/hpsc/> * 패치를 검색하는 방법 * 유지보수 및 지원 (hp 제품) 에서 “개별패치”를 선택 * patch database main에서 원하는 패치 database를 선택(여기서 firmware 부분 선택) * search for patches 에서 원하는 항목을 선택(여기서 CPU 선택) * 검색할 키워드에서 원하는 항목을 선택 후 search 클릭 * most recently에서 체크박스에 체크하고 add to selected patch list 버튼 클릭 * selected patch list가 나오면 패치의 체크박스 선택 후 download patch 버튼 클릭 후 다운 로드   - 설치되는 방법을 보고 싶다면 패치이름의 링크 클릭  < 패치 적용 방법 >  Step 1) patch 파일을 /tmp 밑에 다운로드 받음  - 파일명을 patch\_10으로 가정 | |

UNIX 서버

|  |  |
| --- | --- |
| U-42 (상) | 4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용 |
| Step 2) HP-UX에서 shell archive를 품  #sh patch\_10  - patch\_10.depot와 patch\_10.text가 생성됨 Step 3) patch\_10.depot 설치  #swinstall –s /tmp/patch\_10.depot (경로는 절대경로를 써야함)  #swinstall ?x autoreboot=true ?x patch\_match\_target=true \ -s /tmp/patch\_10.depot | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 점검 방법 | | | | | | | | | | | |
| SOLARIS,  LINUX, AIX,  HP-UX | 로그 | 분석 | 계획 | 수립 | 여부 | 및 | 로그 | 분석 | 결과에 | 따른 | 점검 |

|  |  |
| --- | --- |
| U-43 (상) | 5. 로그 관리 > 5.1 로그의 정기적 검토 및 보고 |
| 취약점 개요 | |
| 점검내용 | * 로그의 정기적 검토 및 보고 여부 점검 |
| 점검목적 | * 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부 를 파악하기 위함 |
| 보안위협 | * 로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락 될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움 |
| 참고 | ※ 시스템 접속 기록, 계정 관리 로그 등 U-73(하) 점검 항목에서 설정한 보안 로그를 포 함하여 응용 프로그램, 시스템 로그 기록에 대하여 주기적인 검토 및 보고가 필요함  ※ 관련 점검 항목 : A-85(하), U-73(하) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기 적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우 |
| 취약 : 위 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조  치가 이루어 지지 않는 경우 |
| 조치방법 | 로그 기록 검토 및 분석을 시행하여 리포트를 작성하고 정기적으로 보고함 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   정기적인 로그 분석을 위하여 아래와 같은 절차 수립 Step 1) 정기적인 로그 검토 및 분석 주기 수립   * + utmp, wtmp ,btmp 등의 로그를 확인하여 마지막 로그인 시간, 접속 IP, 실패한 이력 등을 확인하여 계정 탈취 공격 및 시스템 해킹 여부를 검토   + sulog를 확인하여 허용된 계정 외에 su 명령어를 통해 권한상승을 시도하였는지 검토   + xferlog를 확인하여 비인가자의 ftp 접근 여부를 검토 Step 2) 로그 분석에 대한 결과 보고서 작성   Step 3) 로그 분석 결과보고서 보고 체계 수립 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | #cat /etc/passwd (※ “passwd” 파일 구조: 부록 참조) root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin  “/etc/passwd” 파일 내 UID 확인 (세 번째 필드 값)  root 이외의 계정이 “UID=0”인 경우 0이 아닌 적절한 UID 부여 |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-44 (중) | 1. 계정관리 > 1.5 root 이외의 UID가 ‘0’ 금지 |
| 취약점 개요 | |
| 점검내용 | * 사용자 계정 정보가 저장된 파일(예 /etc/passwd)에 root(UID=0) 계정과 동 일한 UID(User Identification)를 가진 계정이 존재하는지 점검 |
| 점검목적 | * root 계정과 동일한 UID가 존재하는지 점검하여 root권한이 일반 사용자 계 정이나 비인가자의 접근 위협에 안전하게 보호되고 있는지 확인하기 위함 |
| 보안위협 | * root 계정과 동일 UID가 설정되어 있는 일반사용자 계정도 root 권한을 부 여받아 관리자가 실행 할 수 있는 모든 작업이 가능함(서비스 시작, 중지, 재부팅, root 권한 파일 편집 등) * root와 동일한 UID를 사용하므로 사용자 감사 추적 시 어려움이 발생함 |
| 참고 | ※ UID(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자 신을 대표하기 위해 쓰는 이름 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : root 계정과 동일한 UID를 갖는 계정이 존재하지 않는 경우 |
| 취약 : root 계정과 동일한 UID를 갖는 계정이 존재하는 경우 |
| 조치방법 | UID가 0인 계정 존재 시 변경할 UID를 확인 후 다른 UID로 변경 및 불필요 시 삭제, 계정이 사용 중이면 명령어로 조치가 안 되므로 /etc/passwd 파일 설정 변경 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, HP-UX   Step 1) usermod 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정   * + SOLARIS, HP-UX의 경우 100 이상 | |

UNIX 서버



|  |  |  |
| --- | --- | --- |
| passwd 파일 구조 | | |
| 계정명 UID값 GID값 홈디렉터리 위치  ↧ ↧ ↧ ↧  Test : x : 500 : 500 : Gen-User : /hom e/test : /usr/bin/bash | |  |
|  | ↥ ↥ ↥  패스워드 설명(comment) 지정된 쉘 |
| (예) root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin  위의 예는 /etc/passwd 파일의 내용으로 “:”을 사용하여 필드를 구분함  세 번째 필드(UID)가 “0”인 경우 슈퍼유저 권한을 갖으며, “0”이외의 계정은 일반  계정으로 볼 수 있음 | | |

|  |  |
| --- | --- |
| U-44 (중) | 1. 계정관리 > 1.5 root 이외의 UID가 ‘0’ 금지 |
| * LINUX의 경우 500 이상   (예) test 계정의 UID를 100 로 바꿀 경우  #usermod –u 100 test  ※ 각 OS별로 사용자 UID 체계가 상이하여 시스템 계정 및 일반 사용자 계정이 부여받는 값 의 범위에 차이가 있으며, 공통적으로 관리자는 "UID=0"을 부여받음   * AIX   Step 1) chuser 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정 (예) test 계정의 UID 를 100 로 바꿀 경우  #chuser id=100 test | |
| 조치 시  영향 | 해당 계정에 관리자 권한이 필요하지 않으면 일반적으로 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | Step 1) “wheel” 그룹 (su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인  #cat /etc/group (※ “group” 파일 구조: 부록 참조)  wheel:x:10:root,admin  Step 2) wheel 그룹이 su 명령어를 사용할 수 있는지 설정 여부 확인  [SOLARIS] #ls –al /usr/bin/su  #chgrp security su |

|  |  |
| --- | --- |
| U-45 (하) | 1. 계정관리 > 1.6 root 계정 su 제한 |
| 취약점 개요 | |
| 점검내용 | * su 명령어 사용을 허용하는 사용자를 지정한 그룹이 설정되어 있는지 점검 |
| 점검목적 | * su 관련 그룹만 su 명령어 사용 권한이 부여되어 있는지 점검하여 su 그룹 에 포함되지 않은 일반 사용자의 su 명령 사용을 원천적으로 차단하는지 확 인하기 위함 |
| 보안위협 | * 무분별한 사용자 변경으로 타 사용자 소유의 파일을 변경 할 수 있으며 root 계정으로 변경하는 경우 관리자 권한을 획득 할 수 있음 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : su 명령어를 특정 그룹에 속한 사용자만 사용하도록 제한되어 있는 경우  ※ 일반사용자 계정 없이 root 계정만 사용하는 경우 su 명령어 사용제한 불필요 |
| 취약 : su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 |
| 조치방법 | 일반 사용자의 su 명령 사용 제한  Step 1) Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) Step 2) su 명령어의 그룹을 su 명령어 허용할 그룹으로 변경 Step 3) su 명령어의 권한 변경(4750)  Step 4) su 명령어 사용이 필요한 계정을 새로 생성한 그룹에 추가(추가할 계정 요청)  ※ LINUX의 경우, PAM(Pluggable Authentication Module)을 이용한 설정 가능  PAM(Pluggable Authentication Module): 사용자를 인증하고 그 사용자의 서비스에 대한 액세스를 제어하는 모듈화 된 방법을 말하며, PAM은 관리자가 응용프로그램들의 사용자 인증 방법을 선택할 수 있도록 해줌 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
|  | #chmod 4750 su  [AIX] #cat /etc/security/user ---> default의 “sugroup=staff” 설정 확인  [HP-UX] #vi /etc/default/security --->  SU\_ROOT\_GROUP=wheel 설정 확인 Step 3) 파일 권한 확인  #ls –l /usr/bin/su  -rwsr-x--- /usr/bin/su  (파일 권한이 4750인 경우 양호) |
| LINUX PAM  모듈 이용 시 | Step 1) “wheel” 그룹 (su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인  #cat /etc/group  wheel:x:10:root,admin  Step 2) 허용 그룹 (su 명령어 사용 그룹) 설정 여부 확인  #cat /etc/pam.d/su  auth required /lib/security/pam\_wheel.so debug group=wheel 또는, auth required  /lib/security/$ISA/pam\_wheel.so use\_id |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-45 (하) | 1. 계정관리 > 1.6 root 계정 su 제한 |
| * SOLARIS, LINUX, HP-UX   Step 1) wheel group 생성 (wheel 그룹이 존재하지 않는 경우)  #groupadd wheel  Step 2) su 명령어 그룹 변경  #chgrp wheel /usr/bin/su  Step 3) su 명령어 사용권한 변경  #chmod 4750 /usr/bin/su  Step 4) wheel 그룹에 su 명령 허용 계정 등록  #usermod –G wheel <user\_name>  또는, 직접 /etc/group 파일을 수정하여 필요한 계정 등록  wheel:x:10: -> wheel:x:10:root,admin   * AIX   Step 1) wheel group 생성(wheel 그룹이 존재하지 않는 경우)  #mkgroup wheel | |

UNIX 서버

|  |  |
| --- | --- |
| U-45 (하) | 1. 계정관리 > 1.6 root 계정 su 제한 |
| Step 2) su 명령어 그룹 변경  #chgrp wheel /usr/bin/su  Step 3) su 명령어 사용권한 변경  #chmod 4750 /usr/bin/su  Step 4) wheel 그룹에 su 명령 허용 계정 등록 #chgroup users=<user\_name> wheel (예) chgroup users=admin wheel   * LINUX PAM 모듈을 이용한 설정 방법   Step 1) “/etc/pam.d/su” 파일을 아래와 같이 설정(주석제거)  auth sufficient /lib/security/pam\_rootok.so  auth required /lib/security/pam\_wheel.so debug group=wheel 또는,  auth sufficient /lib/security/$ISA/pam\_rootok.so  auth required /lib/security/$ISA/pam\_wheel.so use\_uid  Step 2) wheel 그룹에 su 명령어를 사용할 사용자 추가  #usermod –G wheel <user\_name>  또는, 직접 “/etc/group” 파일을 수정하여 필요한 계정 추가  wheel:x:10: -> wheel:x:10:root,admin | |
| 조치 시 영향 | 그룹에 추가된 계정들은 모든 Session 종료 후 재로그인 시 su 명령어 사용 가 능 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | #cat /etc/default/passwd PASSLENGTH=8 |
| LINUX | #cat /etc/login.defs PASS\_MIN\_LEN 8 |
| AIX | #cat /etc/security/user minlen=8 |
| HP-UX | #cat /etc/default/security MIN\_PASSWORD\_LENGTH=8 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-46 (중) | 1. 계정관리 > 1.7 패스워드 최소 길이 설정 |
| 취약점 개요 | |
| 점검내용 | * 시스템 정책에 패스워드 최소(8자 이상) 길이 설정이 적용되어 있는 점검 |
| 점검목적 | * 패스워드 최소 길이 설정이 적용되어 있는지 점검하여 짧은(8자 미만) 패스 워드 길이로 발생하는 취약점을 이용한 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비(사용자 패스워드 유출)가 되어 있는지 확인하기 위함 |
| 보안위협 | * 패스워드 문자열이 짧은 경우 유추가 가능 할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크렉이 가능함 |
| 참고 | ※ 패스워드 최소길이를 8자리 이상으로 설정하여도 특수문자, 대소문자, 숫자를 혼합하여 사용하여함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우 |
| 취약 : 패스워드 최소 길이가 8자 미만으로 설정되어 있는 경우 |
| 조치방법 | 패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS   Step 1) vi 편집기를 이용하여 “/etc/default/passwd” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASSLENGTH=6  (수정 후) PASSLENGTH=8( 8 이상권장) | |

UNIX 서버

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-46 (중) | 1. | | | 계정관리 | > | 1.7 | 패스워드 | 최소 | 길이 | 설정 |
| * LINUX   Step 1) vi 편집기를 이용하여 “/etc/login.defs” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASS\_MIN\_LEN 6  (수정 후) PASS\_MIN\_LEN 8( 8 이상권장)   * AIX   Step 1.) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) default: 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) minlen=4  (수정 후) minlen=8( 8 이상권장)   * HP-UX   Step 1) vi 편집기를 이용하여 “/etc/default/security” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) MIN\_PASSWORD\_LENGTH=  (수정 후) MIN\_PASSWORD\_LENGTH=8( 8 이상권장) | | | | | | | | | | |
| 조치 시  영향 | 일반적인 | 경우 | 영향 | 없음 | | | | | | |



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | #cat /etc/default/passwd PASSLENGTH=8 |
| LINUX | #cat /etc/login.defs PASS\_MIN\_LEN 8 |
| AIX | #cat /etc/security/user minlen=8 |
| HP-UX | #cat /etc/default/security MIN\_PASSWORD\_LENGTH=8 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| * SOLARIS   Step 1) vi 편집기를 이용하여 “/etc/default/passwd” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASSLENGTH=6  (수정 후) PASSLENGTH=8   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/login.defs” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASS\_MIN\_LEN 6  (수정 후) PASS\_MIN\_LEN 8   * AIX   Step 1.) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) default: 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) minlen=4  (수정 후) minlen=8   * HP-UX   Step 1) vi 편집기를 이용하여 “/etc/default/security” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) MIN\_PASSWORD\_LENGTH=  (수정 후) MIN\_PASSWORD\_LENGTH=8 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | #cat /etc/default/passwd MAXWEEKS=12 |
| LINUX | #cat /etc/login.defs PASS\_MAX\_DAYS 90 |
| AIX | #cat /etc/security/user maxage=12 |
| HP-UX | #cat /etc/default/security PASSWORD\_MAXDAYS=90 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-47 (중) | 1. 계정관리 > 1.8 패스워드 최대 사용기간 설정 |
| 취약점 개요 | |
| 점검내용 | * 시스템 정책에 패스워드 최대(90일 이하) 사용기간 설정이 적용되어 있는지 점검 |
| 점검목적 | * 패스워드 최대 사용 기간 설정이 적용되어 있는지 점검하여 시스템 정책에 서 사용자 계정의 장기간 패스워드 사용을 방지하고 있는지 확인하기 위함 |
| 보안위협 | * 패스워드 최대 사용기간을 설정하지 않은 경우 비인가자의 각종 공격(무작 위 대입 공격, 사전 대입 공격 등)을 시도할 수 있는 기간 제한이 없으므로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행한 기간에 비례하 여 사용자 패스워드가 유출될 수 있는 확률이 증가함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있는 경우 |
| 취약 : 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있지 않는 경우 |
| 조치방법 | 패스워드 정책 설정파일을 수정하여 패스워드 최대 사용기간을 90일(12주)로 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS   Step 1) vi 편집기를 이용하여 “/etc/default/passwd” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입 | |

UNIX 서버



|  |  |
| --- | --- |
| U-47 (중) | 1. 계정관리 > 1.8 패스워드 최대 사용기간 설정 |
| (수정 전) MAXWEEKS=  (수정 후) MAXWEEKS=12 (단위: 주)   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/login.defs” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASS\_MAX\_DAYS 99999  (수정 후) PASS\_MAX\_DAYS 90 (단위: 일)   * AIX   Step 1) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) default: 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) maxage=0  (수정 후) maxage=12 (단위: 주)   * HP-UX   Step 1) vi 편집기를 이용하여 “/etc/default/security” 파일 열기 Step 2.) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASSWORD\_MAXDAYS=99999  (수정 후) PASSWORD\_MAXDAYS=90 (단위: 일) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS | #cat /etc/default/passwd MINWEEKS=1 |
| LINUX | #cat /etc/login.defs PASS\_MIN\_DAYS 1 |
| AIX | #cat /etc/security/user minage=1 |
| HP-UX | #cat /etc/default/security PASSWORD\_MINDAYS=1 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-48 (중) | 1. 계정관리 > 1.9 패스워드 최소 사용기간 설정 |
| 취약점 개요 | |
| 점검내용 | * 시스템 정책에 패스워드 최소 사용기간 설정이 적용되어 있는지 점검 |
| 점검목적 | * 사용자가 자주 패스워드를 변경할 수 없도록 하고 관련 설정(최근 암호 기 억)과 함께 시스템에 적용하여 패스워드 변경 전에 사용했던 패스워드를 재 사용 할 수 없도록 방지하는지 확인하기 위함 |
| 보안위협 | * ※ 최소 사용기간이 설정되어 있지 않아 반복적으로 즉시 변경이 가능한 경 우 이전 패스워드 기억 횟수를 설정하여도 반복적으로 즉시 변경하여 이전 패스워드로 설정이 가능함 |
| 참고 | ※ 최근 암호 기억: 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만드는 것을 방지하는 설정. 예를 들어 값 1은 마지막 암호만 기억한다는 의미이며 값 5는 이전 암호 5개를 기억한다는 의미임 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 패스워드 최소 사용기간이 1일 이상 설정되어 있는 경우 |
| 취약 : 패스워드 최소 사용기간이 설정되어 있지 않는 경우 |
| 조치방법 | 패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS   Step 1) vi 편집기를 이용하여 “/etc/default/passwd” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입 | |

UNIX 서버



|  |  |
| --- | --- |
| U-48 (중) | 1. 계정관리 > 1.9 패스워드 최소 사용기간 설정 |
| (수정 전) MINWEEKS=  (수정 후) MINWEEKS=1 (단위: 주)   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/login.defs” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASS\_MIN\_DAYS  (수정 후) PASS\_MIN\_DAYS 1 (단위: 일)   * AIX   Step 1) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) default 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) minage=  (수정 후) minage=1 (단위: 주)   * HP-UX   Step 1) vi 편집기를 이용하여 “/etc/default/security” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) PASSWORD\_MINDAYS=  (수정 후) PASSWORD\_MINDAYS=1 (단위: 일) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | Step 1) 미사용 계정 및 의심스러운 계정 존재 여부 확인 (※ “passwd” 파일 구조: 부록 참조)  #cat /etc/passwd  Step 2) 사용하지 않는 Default 계정 점검 (lp, uucp, nuucp 계정 존재 확인 예시)  #cat /etc/passwd | egrep “lp|uucp|nuucp” | | | | | | |
| LOG를 통한 확인 | Step 1) 최근 로그인하지 않은 계정 및 의심스러운 계정 확인  #cat /var/adm/wtmp (SOLARIS, AIX, HP-UX)  #cat /var/log/wtmp (LINUX)  #cat /var/adm/authlog (AIX, HP-UX)  #cat /var/log/authlog (SOLARIS)  #cat /var/adm/sulog (SOLARIS, AIX, HP-UX)  #cat /var/log/sulog (LINUX)  ※ 파일의 위치는 버전마다 다를 수 있음 | | | | | | |
| 위에 제시한 점검 방법에 의해 불필요한 계정 발견 시 아래의 보안설정방법에 따  라 조치함 | | | | | | | |

|  |  |
| --- | --- |
| U-49 (하) | 1. 계정관리 > 1.10 불필요한 계정 제거 |
| 취약점 개요 | |
| 점검내용 | * 시스템 계정 중 불필요한 계정(퇴직, 전직, 휴직 등의 이유로 사용하지 않는 계정 및 장기적으로 사용하지 않는 계정 등)이 존재하는지 점검 |
| 점검목적 | * 불필요한 계정이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 대비하는지 확인하기 위함 |
| 보안위협 | * 로그인이 가능하고 현재 사용하지 않는 불필요한 계정은 사용중인 계정보다 상대적으로 관리가 취약하여 공격자의 목표가 되어 계정이 탈취될 수 있음   ※ 퇴직, 전직, 휴직 등의 사유발생시 즉시 권한을 회수 |
| 참고 | ※ Default 계정: OS나 Package 설치 시 기본적으로 생성되는 계정(예 lp, uucp, nuucp 등)  ※ 불필요한 default 계정 삭제 시 업무 영향도 파악 후 삭제 권고 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요한 계정이 존재하지 않는 경우 |
| 취약 : 불필요한 계정이 존재하는 경우 |
| 조치방법 | 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| U-49 (하) | 1. 계정관리 > 1.10 불필요한 계정 제거 |
| * SOLARIS, LINUX, HP-UX   Step 1) 서버에 등록된 불필요한 사용자 계정 확인 Step 2) userdel 명령으로 불필요한 사용자 계정 삭제  #userdel <user\_name>  ※ /etc/passwd 파일에서 계정 앞에 #을 삽입하여도 주석처리가 되지 않으므로 조치 시에는 반드시 계정을 삭제하도록 권고함   * AIX   Step 1) 서버에 등록된 불필요한 사용자 계정 확인 Step 2) rmuser 명령으로 불필요한 사용자 계정 삭제  #rmuser <user\_name> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, HP-UX | #cat /etc/group (※ “group” 파일 구조: 부록 참조)  root:x:0:root | | | | | | |
| AIX | #cat /etc/group system:!:0:root | | | | | | |
| 관리자 용도 외의 계정이 root 그룹에 포함되어 있는 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-50 (하) | 1. 계정관리 > 1.11 관리자 그룹에 최소한의 계정 포함 |
| 취약점 개요 | |
| 점검내용 | * 시스템 관리자 그룹에 최소한(root 계정과 시스템 관리에 허용된 계정)의 계 정만 존재하는지 점검 |
| 점검목적 | * 관리자 그룹에 최소한의 계정만 존재하는지 점검하여 불필요하게 권한이 남   용되고 있는지 확인하기 위함 |
| 보안위협 | * 시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근 권한이 부여되어 있으므로 해당 관리자 그룹에 속한 계정이 비인가자에게 유출될 경우 관리자 권한으로 시스템에 접근하여 계정 정보 유출, 환경설정 파일 및 디렉터리 변조 등의 위협이 존재함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 관리자 그룹에 불필요한 계정이 등록되어 있지 않은 경우 |
| 취약 : 관리자 그룹에 불필요한 계정이 등록되어 있는 경우 |
| 조치방법 | 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, HP-UX   Step 1) vi 편집기를 이용하여 “/etc/group” 파일 열기 Step 2) root 그룹에 등록된 불필요한 계정 삭제  (예) root 그룹에 등록된 불필요한 test 계정 삭제 (수정 전) root:x:0:root,test  (수정 후) root:x:0:root   * AIX   Step 1) vi 편집기를 이용하여 “/etc/group” 파일 열기 | |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U-50 (하) | 1. | | 계정관리 > | | 1.11 | 관리자 | 그룹에 | 최소한의 | 계정 | 포함 |
| Step 2) system 그룹에 등록된 불필요한 계정 삭제  (예) system 그룹에 등록된 불필요한 test 계정 삭제 (수정 전) system:!:0:root,test  (수정 후) system:!:0:root | | | | | | | | | | |
| 조치 시  영향 | 일반적인 | 경우 | 영향 | 없음 | | | | | | |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS,  LINUX,  HP-UX, AIX | #cat /etc/group (※ “group” 파일 구조: 부록 참조)  #cat /etc/passwd | | | | | | |
| LINUX | #cat /etc/gshadow  \*gshadow 파일: “shadow” 파일에 사용자 계정의 암호가 저장되어 있는 것처럼 시스템 내 존재하는 그룹의 암호 정보 저장 파일로 그룹 관리자 및 구성원 설정 가능  “gshadow” 파일 내 필드는 다음 같은 구조로 구성됨  [그룹명 : 패스워드 : 관리자, 관리자, … : 멤버, 멤버 … ] | | | | | | |
| 계정이 존재하지 않고 시스템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용에 사용되지 않는 그룹 등의 경우 아래의 보안설정 방법에 따라  그룹을 제거함 | | | | | | | |

|  |  |
| --- | --- |
| U-51 (하) | 1. 계정관리 > 1.12 계정이 존재하지 않는 GID 금지 |
| 취약점 개요 | |
| 점검내용 | * 그룹(예 /etc/group) 설정 파일에 불필요한 그룹(계정이 존재하지 않고 시스 템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용 에 사용되지 않는 그룹 등)이 존재하는지 점검 |
| 점검목적 | * 시스템에 불필요한 그룹이 존재하는지 점검하여 불필요한 그룹의 소유권으 로 설정되어 있는 파일의 노출에 의해 발생할 수 있는 위험에 대한 대비가 되어 있는지 확인하기 위함 |
| 보안위협 | * 계정이 존재하지 않는 그룹은 현재 사용되고 있는 그룹이 아닌 불필요한 그 룹으로 삭제 조치가 필요함. |
| 참고 | ※ GID(Group Identification): 다수의 사용자가 특정 개체를 공유할 수 있게 연계시키는 특정 그룹의 이름으로 주로 계정처리 목적으로 사용되며, 한 사용자는 여러 개의 GID 를 가질 수 있음.  ※ /etc/group 파일과 /etc/passwd 파일을 비교하여 점검하기를 권고함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 시스템 관리나 운용에 불필요한 그룹이 삭제 되어있는 경우 |
| 취약 : 시스템 관리나 운용에 불필요한 그룹이 존재할 경우 |
| 조치방법 | 불필요한 그룹이 있을 경우 관리자와 검토하여 제거 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| U-51 (하) | 1. 계정관리 > 1.12 계정이 존재하지 않는 GID 금지 |
| * SOLARIS, LINUX, AIX, HP-UX   #groupdel <group\_name>  ※ 해당 그룹 삭제시 그룹권한으로 존재하는 파일이 존재하는지 확인이 필요하며 사용자가 없 는 그룹이라 하더라도 추후 권한 할당을 위해 그룹을 먼저 생성하였을 가능성도 존재하므로 무분별한 삭제는 권장하지 않으며 신규 생성된 그룹(GID 500 이상)을 중점적으로 점검 권고 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX,  HP-UX, AIX | #cat /etc/passwd (※ “passwd” 파일 구조: 부록 참조) | | | | | | |
| 동일한 UID를 갖는 계정이 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-52 (중) | 1. 계정관리 > 1.13 동일한 UID 금지 |
| 취약점 개요 | |
| 점검내용 | * /etc/passwd 파일 내 UID가 동일한 사용자 계정 존재 여부 점검 |
| 점검목적 | * UID가 동일한 사용자 계정을 점검함으로써 타 사용자 계정 소유의 파일 및 디 렉터리로의 악의적 접근 예방 및 침해사고 시 명확한 감사추적을 목적으로 함 |
| 보안위협 | * 중복된 UID가 존재할 경우 시스템은 동일한 사용자로 인식하여 소유자의 권 한이 중복되어 불필요한 권한이 부여되며 시스템 로그를 이용한 감사 추적 시 사용자가 구분되지 않음 (권한 할당은 그룹권한을 이용하여 운영) |
| 참고 | ※ UID(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자 신을 대표하기 위해 사용되는 식별 번호  ※ 패스워드 파일 ~~수정 변경 및 신규 사용자 추가 시 UID가 동일한 계정이 존재하는지 확인 해야 함(계정생성, UID 변경은 passwd 파일을 직접 편집 금지, 명령어를 이용하여 수정)~~ |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 동일한 UID로 설정된 사용자 계정이 존재하지 않는 경우 |
| 취약 : 동일한 UID로 설정된 사용자 계정이 존재하는 경우 |
| 조치방법 | 동일한 UID로 설정된 사용자 계정의 UID를 서로 다른 값으로 변경 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, HP-UX   usermod 명령으로 동일한 UID로 설정된 사용자 계정의 UID 변경  #usermod –u <변경할 UID값> <user\_name>   * AIX   chuser 명령으로 동일한 UID로 설정된 사용자 계정의 UID 변경  #chuser id=<변경할 UID값> <user\_name> | |
| 조치 시 영향 | 운영목적으로 동일한 UID 값을 부여하였다면 해당 계정이 사용하고 있는 파일 및 디렉터리를 검토하여 권한이 삭제되어도 서비스 영향이 없는지 확인 필요 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX,  HP-UX, AIX | #cat /etc/passwd | egrep “^daemon|^bin|^sys|^adm|^listen|^nobody|^nobody4|^  noaccess|^diag|^operator|^games|^gopher” | grep –v  “admin” |
| 시스템에 불필요한 계정을 확인한 후 /bin/false(nologin) 쉘이 부여되어 있지 않은 경 우 아래의 보안설정방법에 따라 설정을 변경함  (※ 불필요한 계정은 시스템 용도에 따라 차이가 있음) | |

|  |  |
| --- | --- |
| U-53 (하) | 1. 계정관리 > 1.14 사용자 shell 점검 |
| 취약점 개요 | |
| 점검내용 | * 로그인이 불필요한 계정(adm, sys, daemon 등)에 쉘 부여 여부 점검 |
| 점검목적 | * 로그인이 불필요한 계정에 쉘 설정을 제거하여, 로그인이 필요하지 않은 계 정을 통한 시스템 명령어를 실행하지 못하게 하기 위함 |
| 보안위협 | * ~~로그인이 불필요한 계정은 일반적으로 OS 설치 시 기본적으로 생성되는 계 정으로 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 이용하여 시스템 에 명령어를 실행 할 수 있음~~ |
| 참고 | ※ 쉘(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사 용자의 명령어를 이해하고 실행함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin) 쉘이 부여되어 있는 경우 |
| 취약 : 로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin) 쉘이 부여되지 않은 경우 |
| 조치방법 | 로그인이 필요하지 않은 계정에 대해 /bin/false(/sbin/nologin) 쉘 부여 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 “/etc/passwd” 파일 열기  Step 2) 로그인 쉘 부분인 계정 맨 마지막에 /bin/false(/sbin/nologin) 부여 및 변경 | |

UNIX 서버

|  |  |
| --- | --- |
| U-53 (하) | 1. 계정관리 > 1.14 사용자 shell 점검 |
| (수정 전) daemon:x:1:1::/:/sbin/ksh  (수정 후) daemon:x:1:1::/:/bin/false 또는, daemon:x:1:1::/:/sbin/nologin  일반적으로 로그인이 불필요한 계정 (※ 계정 설명: 부록 참조)  daemon, bin, sys, adm, listen, nobody, nobody4, noaccess, diag, listen, operator, games, gopher 등 일반적으로 UID 100 이하 60000 이상의 시스템 계정 해당 | |
| 조치 시 영향 | 일반적인 경우 영향 없음  모호한 경우 “/etc/shadow” 파일에서 해당 계정에 패스워드 존재 여부로 확인 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | <sh, ksh, bash 사용 시>  #cat /etc/profile(.profile)  TMOUT=600  export TMOUT  <csh 사용 시>  #cat /etc/csh.login 또는, #cat /etc/csh.cshrc  set autologout=10 |
| 위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설 정을 변경함 | |

|  |  |
| --- | --- |
| U-54 (하) | 1. 계정관리 > 1.15 Session Timeout 설정 |
| 취약점 개요 | |
| 점검내용 | * 사용자 쉘에 대한 환경설정 파일에서 session timeout 설정 여부 점검 |
| 점검목적 | * 사용자의 고의 또는 실수로 시스템에 계정이 접속된 상태로 방치됨을 차단 하기 위함 |
| 보안위협 | * Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 불필요한 내부 정보의 노출 위험이 존재함 |
| 참고 | ※ session: 프로세스들 사이에 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식 한 이후부터 통신을 마칠 때까지의 시간 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : Session Timeout이 600초(10분) 이하로 설정되어 있는 경우 |
| 취약 : Session Timeout이 600초(10분) 이하로 설정되지 않은 경우 |
| 조치방법 | 600초(10분) 동안 입력이 없을 경우 접속된 Session을 끊도록 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   - sh(born shell), ksh(korn shell), bash(born again shell)을 사용하는 경우 - Step 1) vi 편집기를 이용하여 “/etc/profile(.profile)” 파일 열기  Step 2) 아래와 같이 수정 또는, 추가  TMOUT=600 (단위: 초)  export TMOUT | |

UNIX 서버

|  |  |
| --- | --- |
| U-54 (하) | 1. 계정관리 > 1.15 Session Timeout 설정 |
| - csh 을 사용하는 경우 -  Step 1) vi 편집기를 이용하여 “/etc/csh.login” 또는, “/etc/csh.cshrc” 파일 열기 Step 2) 아래와 같이 수정 또는, 추가  set autologout=10 (단위: 분) | |
| 조치 시 영향 | 모니터링 용도일 경우 세션 타임 설정 시 모니터링 업무가 불가 할 수 있으므 로 예외처리 필요 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX, HP-UX | #ls –l /etc/hosts.lpd  rw------- root <hosts.lpd 파일> | | | | | | |
| “hosts.lpd” 파일이 존재하고 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-55 (하) | 2. 파일 및 디렉토리 관리 > 2.15 hosts.lpd 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * /etc/hosts.lpd 파일의 삭제 및 권한 적절성 점검 |
| 점검목적 | * 비인가자의 임의적인 hosts.lpd 변조를 막기 위해 hosts.lpd 파일 삭제 또는 소유자 및 권한 관리를 해야 함 |
| 보안위협 | * hosts.lpd 파일의 접근권한이 적절하지 않을 경우 비인가자가 /etc/hosts.lpd 파일을 수정하여 허용된 사용자의 서비스를 방해할 수 있으며, 호스트 정보 를 획득 할 수 있음 |
| 참고 | ※ hosts.lpd 파일: 로컬 프린트 서비스를 사용할 수 있는 허가된 호스트(사용자) 정보를 담고 있는 파일 (hostname 또는, IP 주소를 포함하고 있음) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : hosts.lpd 파일이 삭제되어 있거나 불가피하게 hosts.lpd 파일을 사용할 시 파일의 소유자가 root이고 권한이 600인 경우 |
| 취약 : hosts.lpd 파일이 삭제되어 있지 않거나 파일의 소유자가 root가 아니고 권한이 600이 아닌 경우 |
| 조치방법 | hosts.lpd 파일을 삭제하거나 hosts.lpd 파일의 퍼미션을 확인하여 퍼미션 600, 파일 소유자를 root로 변경 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) hosts.lpd 파일 삭제  #rm –rf /etc/hosts.lpd  Step 2) 파일의 퍼미션 변경 (hosts.lpd 파일이 필요시)  #chmod 600 /etc/hosts.lpd  Step 3) 소유자를 root로 변경 (hosts.lpd 파일이 필요시)  #chown root /etc/hosts.lpd | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS,  LINUX, AIX,  HP-UX | #vi /etc/profile UMASK=022 | | | | | | |
| 위에 제시한 UMASK 값이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법  에 따라 적용함 | | | | | | | |

|  |  |
| --- | --- |
| U-56 (중) | 2. 파일 및 디렉토리 관리 > 2.17 UMASK 설정 관리 |
| 취약점 개요 | |
| 점검내용 | * 시스템 UMASK 값이 022 이상인지 점검 |
| 점검목적 | * 잘못 설정된 UMASK 값으로 인해 신규 파일에 대한 과도한 권한 부여되는   것을 방지하기 위함 |
| 보안위협 | * 잘못된 UMASK 값으로 인해 파일 및 디렉터리 생성시 과도하게 퍼미션이 부여 될 수 있음 |
| 참고 | * 시스템 내에서 사용자가 새로 생성하는 파일의 접근권한은 UMASK 값에 따 라 정해지며, 계정의 Start Profile 에 명령을 추가하면 사용자가 로그인 한 후에도 변경된 UMASK 값을 적용받게 됨   ※ Start Profile: /etc/profile, /etc/default/login, .cshrc, .kshrc, .bashrc, .login, .profile 등  ※ umask: 파일 및 디렉터리 생성 시 기본 퍼미션을 지정해 주는 명령어 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : UMASK 값이 022 이상으로 설정된 경우 |
| 취약 : UMASK 값이 022 이상으로 설정되지 않은 경우 |
| 조치방법 | 설정파일에 UMASK 값을 “022”로 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS   방법-1. “/etc/profile” 파일을 이용한 UMASK 설정 변경 Step 1) vi 편집기를 이용하여 “/etc/profile” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  umask 022 export umask  방법-2. “/etc/default/login” 파일을 이용한 UMASK 설정 변경  Step 1) vi 편집기를 이용하여 “/etc/default/login” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  (수정 전) #UMASK=022 | |

UNIX 서버



|  |  |
| --- | --- |
| U-56 (중) | 2. 파일 및 디렉토리 관리 > 2.17 UMASK 설정 관리 |
| (수정 후) UMASK=022   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/profile” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  umask 022 export umask   * HP-UX   방법-1. “/etc/profile” 파일을 이용한 UMASK 설정 변경 Step 1) vi 편집기를 이용하여 “/etc/profile” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  umask 022 export umask  방법-2. "/etc/defualt/security" 파일을 이용한 UMASK 설정 변경  Step 1) vi 편집기를 이용하여 “/etc/defualt/security” 파일 열기 Step 2) default 설정 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) # UMASK=022 (수정 후) UMASK=022   * AIX   방법-1. “/etc/profile” 파일을 이용한 UMASK 설정 변경 Step 1) vi 편집기를 이용하여 “/etc/profile” 파일 열기 Step 2) 아래와 같이 수정 또는, 신규 삽입  umask 022 export umask  방법-2. “/etc/security/user” 파일을 이용한 UMASK 설정 변경  Step 1) vi 편집기를 이용하여 “/etc/security/user” 파일 열기 Step 2) default 설정 부분을 아래와 같이 수정 또는, 신규 삽입  (수정 전) umask = (수정 후) umask = 022 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | "/etc/passwd" 파일에서 사용자별 홈 디렉터리 확인 후 소유자 및 권한 확인  #cat /etc/passwd  #ls -ald <user-home-directory> |
| "/etc/passwd" 파일 내 존재하는 모든 사용자 계정이 적절한 홈 디렉터리를 갖는지  확인함. 홈 디렉터리 소유자가 해당 계정이 아니거나, 부적절한 권한 설정이 적용  된 경우 아래의 보안설정방법에 따라 적용함 | |

|  |  |
| --- | --- |
| U-57 (중) | 2. 파일 및 디렉토리 관리 > 2.18 홈디렉토리 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * 홈 디렉터리의 소유자 외 타사용자가 해당 홈 디렉터리를 수정할 수 없도록 제한하는지 점검 |
| 점검목적 | * 사용자 홈 디렉터리 내 설정파일이 비인가자에 의한 변조를 방지함 |
| 보안위협 | * 홈 디렉터리 내 설정파일 변조 시 정상적인 서비스 이용이 제한될 우려가 존재함 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 홈 디렉터리 소유자가 해당 계정이고, 타 사용자 쓰기 권한이 제거된 경우 |
| 취약 : 홈 디렉터리 소유자가 해당 계정이 아니고, 타 사용자 쓰기 권한이 부여된 경우 |
| 조치방법 | 사용자별 홈 디렉터리 소유주를 해당 계정으로 변경하고, 타사용자의 쓰기 권한 제거  (“/etc/passwd” 파일에서 홈 디렉터리 확인, 사용자 홈 디렉터리 외 개별적으로 만들어 사용하는 사용자 디렉터리 존재여부 확인하여 점검) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   “/etc/passwd” 파일의 소유자 및 권한 변경  #chown <user\_name> <user\_home\_directory>  #chmod o-w <user\_home\_directory> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS, LINUX, AIX,  HP-UX | 사용자 계정 별 홈 디렉터리 지정 여부 확인  # cat /etc/passwd | | | | | | |
| "/etc/passwd" 파일 내 존재하는 모든 사용자 계정이 적절한 홈 디렉터리를 갖는지  확인한 후 홈 디렉터리가 존재하지 않는 계정이 발견된 경우 아래의 보안설정방법  에 따라 적용함 | | | | | | | |

|  |  |
| --- | --- |
| U-58 (중) | 2. 파일 및 디렉토리 관리 > 2.19 홈디렉토리로 지정한 디렉토리의 존재 관리 |
| 취약점 개요 | |
| 점검내용 | * 사용자 계정과 홈 디렉터리의 일치 여부를 점검 |
| 점검목적 | * /home 이외 사용자의 홈 디렉터리 존재 여부를 점검하여 비인가자가 시스 템 명령어의 무단 사용을 방지하기 위함 |
| 보안위협 | * passwd 파일에 설정된 홈디렉터리가 존재하지 않는 경우, 해당 계정으로 로 그인시 홈디렉터리가 루트 디렉터리(“/“)로 할당되어 접근이 가능함 |
| 참고 | ※ 홈디렉터리: 사용자가 로그인한 후 작업을 수행하는 디렉터리  ※ 일반 사용자의 홈 디렉터리 위치: /home/user명 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 홈 디렉터리가 존재하지 않는 계정이 발견되지 않는 경우 |
| 취약 : 홈 디렉터리가 존재하지 않는 계정이 발견된 경우 |
| 조치방법 | 홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는, 계정 삭제 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 홈 디렉터리가 없는 사용자 계정 삭제   * + SOLARIS, LINUX, HP-UX 설정: #userdel <user\_name>   + AIX 설정: #rmuser <user\_name>   Step 2) 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정  #vi /etc/passwd  #test:x:501:501::/:/bin/bash (홈 디렉터리가 /로 설정 된 경우) #test:x:501:501::/home/test:/bin/bash (홈 디렉터리 수정 / -> /home/test) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
|  | 특정 디렉터리 내 불필요한 파일 점검 |
| SOLARIS, | #ls -al [디렉터리명] |
| LINUX, AIX, | 전체 숨김 디렉터리 및 숨김 파일 점검 |
| HP-UX | #find / -type f –name ".\*" (파일 점검) |
|  | #find / -type d -name ".\*" (디렉터리 점검) |
| 특정 디렉터리 내 숨겨진 파일을 확인한 후 불필요한 경우 파일 삭제를 권고함 | |

|  |  |
| --- | --- |
| U-59 (하) | 2. 파일 및 디렉토리 관리 > 2.20 숨겨진 파일 및 디렉토리 검색 및 제거 |
| 취약점 개요 | |
| 점검내용 | * 숨김 파일 및 디렉터리 내 의심스러운 파일 존재 여부 점검 |
| 점검목적 | * 숨겨진 파일 및 디렉터리 중 의심스러운 내용은 정상 사용자가 아닌 공격자 에 의해 생성되었을 가능성이 높음으로 이를 발견하여 제거함 |
| 보안위협 | * 공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변 경 등을 할 수 있음 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 불필요하거나 의심스러운 숨겨진 파일 및 디렉터리를 삭제한 경우 |
| 취약 : 불필요하거나 의심스러운 숨겨진 파일 및 디렉터리를 방치한 경우 |
| 조치방법 | ls –al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭  제함 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) 숨겨진 파일 목록에서 불필요한 파일 삭제  Step 2) 마지막으로 변경된 시간에 따라, 최근 작업한 파일 확인 시 [-t] 플래그 사용 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| U-60 (중) | 3. 서비스 관리 > 3.24 ssh 원격접속 허용 |
| 취약점 개요 | |
| 점검내용 | * 원격 접속 시 SSH 프로토콜을 사용하는지 점검 |
| 점검목적 | * 비교적 안전한 SSH 프로토콜을 사용함으로써 스니핑 등 아이디/패스워드의   누출의 방지를 목적으로 함 |
| 보안위협 | * 원격 접속 시 Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기   때문에 아이디/패스워드 및 중요 정보가 외부로 유출될 위험성이 있음 |
| 참고 | ※ SSH 사용 시 TCP/22번 포트를 기본 포트로 사용하기 때문에 공격자가 기본 포트를 통하여 공격을 시도할 수 있으므로 기본 포트를 변경하여 사용하는 것을 권고함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 원격 접속 시 SSH 프로토콜을 사용하는 경우  ※ ssh, telnet이 동시에 설치되어 있는 경우 취약한 것으로 평가됨 |
| 취약 : 원격 접속 시 Telnet, FTP 등 안전하지 않은 프로토콜을 사용하는 경우 |
| 조치방법 | Telnet, FTP 등 안전하지 않은 서비스 사용을 중지하고, SSH 설치 및 사용 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) SSH 서비스 활성화 명령어 실행  ∎ SOLARIS  <SOLARIS 5.9 이하 버전>  #/etc/init.d/sshd start  <SOLARIS 5.10 이상 버전>  #svcadm enable ssh   * LINUX   #service start sshd 또는, #service start ssh   * AIX   #startsrc -s sshd   * HP-UX   #/sbin/init.d/secsh start  Step 2) SSH 설치가 필요할 경우 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서 버에 설치 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| FTP 종류별 점검 방법 | |
| SOLARIS, AIX, HP-UX | 일반 ftp 서비스 비활성화 여부 확인  #vi /etc/inetd.conf |
| proftpd 서비스 데몬 확인 (proftpd 동직 SID 확인)  #ps -ef | grep proftpd  root 3809 3721 0 08:44:40 ? 0:00  /usr/local/proftpd/sbin/proftpd |
| vsftpd 서비스 데몬 확인 (vsftpd 동작 SID 확인)  #ps -ef | grep vsftpd  root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd/et c/vsftpd/vsftpd.conf |
| LINUX | 일반 ftp 서비스 비활성화 여부 확인  #ps -ef | grep ftp |
| vsftpd 또는 ProFTP 서비스 데몬 확인(vsftpd, proftpd 동작 SID  확인)  #ps -ef | egrep "vsftpd|proftp"  root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd |
| 불필요한 "ftp" 서비스 실행 시 아래의 보안설정방법에 따라 서비스 중지 | |

|  |  |
| --- | --- |
| U-61 (하) | 3. 서비스 관리 > 3.25 ftp 서비스 확인 |
| 취약점 개요 | |
| 점검내용 | * FTP 서비스가 활성화 되어있는지 점검 |
| 점검목적 | * 취약한 서비스인 FTP서비스를 가급적 제한함을 목적으로 함 |
| 보안위협 | * FTP 서비스는 통신구간이 평문으로 전송되어 계정정보(아이디, 패스워드) 및 전송 데이터의 스니핑이 가능함 |
| 참고 | ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용 해야 하는 경우 SFTP 사용을 권고함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : FTP 서비스가 비활성화 되어 있는 경우 |
| 취약 : FTP 서비스가 활성화 되어 있는 경우 |
| 조치방법 | FTP 서비스 중지 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버



|  |  |
| --- | --- |
| U-61 (하) | 3. 서비스 관리 > 3.25 ftp 서비스 확인 |
| * SOLARIS, AIX, HP-UX   < 일반 FTP 서비스 중지 방법 >  Step 1) “/etc/inetd.conf” 파일에서 ftp 서비스 라인 #처리(주석처리)  (수정 전) ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a (수정 후) #ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a  Step 2) inetd 서비스 재시작  #ps -ef | grep inetd  root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill –HUP [PID]  <SOLARIS 5.10 이상 버전>  # svcs | grep ftp  online 12:51:49 svc:/network/ftp:default # svcadm disable svc:/network/ftp:default   * SOLARIS, LINUX, AIX, HP-UX   < vsFTP, ProFTP 서비스 중지 방법 ＞  Step 1) 서비스 확인  # ps –ef | egrep "vsftpd|proftpd"  Step 2) vsftpd 또는 ProFTP 서비스 데몬 중지  # service vsftpd(proftp) stop 또는 /etc/rc.d/init.d/vsftpd(proftp) stop 또는 kill -9 [PID] | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | ftp 계정에 대한 /bin/false 부여 확인 #cat /etc/passwd ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash |
| "passwd" 파일 내 로그인 쉘 설정이 “/bin/false"가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-62 (중) | 3. 서비스 관리 > 3.26 ftp 계정 shell 제한 |
| 취약점 개요 | |
| 점검내용 | * ftp 기본 계정에 쉘 설정 여부 점검 |
| 점검목적 | * FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인이 필요하지 않은 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하기 위함 |
| 보안위협 | * 불필요한 기본 계정에 쉘(Shell)을 부여할 경우, 공격자에게 해당 계정이 노 출되어 ftp 기본 계정으로 시스템 접근하여 공격이 가능해짐 |
| 참고 | ※ 쉘(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사 용자의 명령어를 이해하고 실행함  ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용 해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함  ※ 관련 점검 항목 : U-64(하), U-65(중) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : ftp 계정에 /bin/false 쉘이 부여되어 있는 경우 |
| 취약 : ftp 계정에 /bin/false 쉘이 부여되어 있지 않은 경우 |
| 조치방법 | ftp 계정에 /bin/false 쉘 부여 |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 “/etc/passwd” 파일 열기  Step 2) ftp 계정의 로그인 쉘 부분인 계정 맨 마지막에 /bin/false 부여 및 변경 (수정 전) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash  (수정 후) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/bin/false Step 3) # usermod –s /bin/false [계정ID] 부여로 변경 가능  \* Step 2 로 적용이 되지 않을경우는 Step3의 usermod 명령어를 사용하여 쉘 변경 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | ftpusers 파일에 대한 일반사용자 쓰기권한 확인  #ls -al /etc/ftpusers  #ls -al /etc/ftpd/ftpusers  rw-r----- root <ftpusers 파일> |
| “ftpusers" 파일의 소유자가 root가 아니거나 파일의 권한이 640 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| FTP 종류 별 ftpusers 파일 위치 | |
| 기본 FTP | /etc/ftpusers 또는, /etc/ftpd/ftpusers |
| ProFTP | /etc/ftpusers 또는, /etc/ftpd/ftpusers |
| vsFTP | /etc/vsftpd/ftpusers, /etc/vsftpd/user\_list 또는,  /etc/vsftpd.ftpusers, /etc/vsftpd.user\_list |

|  |  |
| --- | --- |
| U-63 (하) | 3. 서비스 관리 > 3.27 ftpusers 파일 소유자 및 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * FTP 접근제어 설정파일에 관리자 외 비인가자들이 수정 제한 여부 점검 |
| 점검목적 | * 비인가자들의 ftp 접속을 차단하기 위해 ftpusers 파일 소유자 및 권한을 관 리해야함 |
| 보안위협 | * ftpusers 파일에 인가되지 않은 사용자를 등록하여 해당 계정을 이용, 불법 적인 FTP 서비스에 접근이 가능함 |
| 참고 | ※ ftpusers 파일: FTP 접근제어 설정파일로써 해당 파일에 등록된 계정은 ftp에 접속할 수 없음  ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용 해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함  ※ 관련 점검 항목 : U-63(중), U-65(중) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : ftpusers 파일의 소유자가 root이고, 권한이 640 이하인 경우 |
| 취약 : ftpusers 파일의 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우 |
| 조치방법 | FTP 접근제어 파일의 소유자 및 권한 변경 (소유자 root, 권한 640 이하) |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버

|  |  |
| --- | --- |
| U-63 (하) | 3. 서비스 관리 > 3.27 ftpusers 파일 소유자 및 권한 설정 |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) “/etc/ftpusers” 파일의 소유자 및 권한 확인  #ls -l /etc/ftpusers  Step 2) “/etc/ftpusers” 파일의 소유자 및 권한 변경 (소유자 root, 권한 640)  #chown root /etc/ftpusers #chmod 640 /etc/ftpusers  ※ vsFTP를 사용할 경우 FTP 접근제어 파일   * vsftpd.conf 파일에서 userlist\_enable=YES인 경우: vsftpd.ftpusers, vsftpd.user\_list 또는 ftpusers, user\_list 파일의 소유자 및 권한 확인 후 변경   (ftpusers, user\_list 파일에 등록된 모든 계정의 접속이 차단됨)   * vsftpd.conf 파일에서 userlist\_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers   또는 ftpusers 파일의 소유자 및 권한 확인 후 변경 (ftpusers 파일에 등록된 계정들만 접속이 차단됨) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| FTP 종류별 점검 방법 | |
|  | 아래 파일에서 ftp에 대한 root 계정으로의 접속 가능 여부 확인 |
|  | #cat /etc/ftpusers |
|  | #cat /etc/ftpd/ftpusers |
|  | #root (주석처리) 또는, root 계정 미등록 |
|  | ProFTP |
| SOLARIS, | #cat /etc/proftpd.conf |
| LINUX, | RootLogin on |
|  |
| AIX, HP-UX | vsFTP |
|  | #cat /etc/vsftp/ftpusers |
|  | #cat /etc/vsftp/user\_list |
|  | 또는 |
|  | #cat /etc/vsftpd.ftpusers |
|  | #cat /etc/vsftpd.user\_list |
|  | #root (주석처리) 또는, root 계정 미등록 |
| root 계정으로 FTP 접속이 가능하도록 위와 같이 설정된 경우 아래의 | |

|  |  |
| --- | --- |
| U-64 (중) | 3. 서비스 관리 > 3.28 ftpusers 파일 설정(FTP 서비스 root 계정 접근제한) |
| 취약점 개요 | |
| 점검내용 | * FTP 서비스를 사용할 경우 ftpusers 파일 root 계정이 포함 여부 점검 |
| 점검목적 | * root의 FTP 직접 접속을 방지하여 root 패스워드 정보를 노출되지 않도록 하기 위함 |
| 보안위협 | * FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑 에 의해서 관리자 계정의 아이디 및 패스워드가 노출될 수 있음 |
| 참고 | ※ 스니핑: 컴퓨터 네트워크상에 흘러 다니는 트래픽을 도청하는 행위  ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용 해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함  ※ 관련 점검 항목 : U-63(중), U-64(하) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : FTP 서비스가 비활성화 되어 있거나, 활성화 시 root 계정 접속을 차단 한 경우 |
| 취약 : FTP 서비스가 활성화 되어 있고, root 계정 접속을 허용한 경우 |
| 조치방법 | FTP 접속 시 root 계정으로 직접 접속 할 수 없도록 설정파일 수정 (접속 차단 계정을 등록하는 ftpusers 파일에 root 계정 추가) |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버

|  |  |
| --- | --- |
| U-64 (중) | 3. 서비스 관리 > 3.28 ftpusers 파일 설정(FTP 서비스 root 계정 접근제한) |
| 보안설정방법에 따라 설정을 변경함   * SOLARIS, LINUX, AIX, HP-UX   < 일반 FTP 서비스 root 계정 접속 제한 방법 >  Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/ftpusers” 또는 “/etc/ftpd/ftpusers”)  #vi /etc/ftpusers 또는 /etc/ftpd/ftpusers  Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root  < ProFTP 서비스 ROOT 접속 차단 >  Step 1) vi 편집기를 이용하여 proftpd 설정파일(“/etc/proftpd.conf”) 열기  #vi /etc/proftpd.conf  Step 2) proftpd 설정파일 (“/etc/proftpd.conf”)에서 RootLogin off 설정  (수정 전) RootLogin on (수정 후) RootLogin off  Step 3) ProFTP 서비스 재시작  < vsFTP 서비스 ROOT 접속 차단 >  Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/vsftp/ftpusers” 또는, “/etc/vsftpd.ftpus ers”)  #vi /etc/vsftp/ftpusers  Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root  Step 3) vsFTP 서비스 재시작  ※ vsFTP를 사용할 경우 FTP 접근제어 파일   * + vsftpd.conf 파일에서 userlist\_enable=YES인 경우: vsftpd.ftpusers, vsftpd.user\_list 또는 ftpusers, user\_list   (ftpusers, user\_list 파일에 등록된 모든 계정의 접속이 차단됨)   * + vsftpd.conf 파일에서 userlist\_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers   또는 ftpusers  (ftpusers 파일에 등록된 계정들만 접속이 차단됨) | |
| 조치 시  영향 | 애플리케이션에서 root로 바로 접속하여 ftp를 사용하고 있을 경우 확인 필요 |

UNIX 서버



|  |  |  |
| --- | --- | --- |
| OS별 점검 파일 위치 | | |
| SOLARIS | /etc/cron.d/ | at.allow <- at 명령어 허용 사용자  at.deny <- at 명령어 차단 사용자 |
| LINUX | /etc/ |
| AIX, HP-UX | /var/adm/cron/ |
| "cron" 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을  변경함 | | |

|  |  |
| --- | --- |
| U-65 (중) | 3. 서비스 관리 > 3.29 at 서비스 권한 설정 |
| 취약점 개요 | |
| 점검내용 | * 관리자(root)만 at.allow파일과 at.deny 파일을 제어할 수 있는지 점검 |
| 점검목적 | * 관리자외 at 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목   적으로 함 |
| 보안위협 | * root 외 일반사용자에게도 at 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음 |
| 참고 | ※ at 데몬 (일회성 작업 예약): 지정한 시간에 어떠한 작업이 실행될 수 있도록 작업 스 케줄을 예약 처리해 주는 기능을 제공함. /etc/at.allow 파일에 등록된 사용자만이 at 명령을 사용할 수 있음  ※ 기반시설 시스템에서 at 데몬의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해 야 하는 경우 소유자 및 권한 설정 등의 보안 조치를 반드시 적용하여야 함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : at 명령어 일반사용자 금지 및 at 관련 파일 640 이하인 경우 |
| 취약 : at 명령어 일반사용자 사용가능하거나, at 관련 파일 640 이상인 경우 |
| 조치방법 | crontab 명령어 750 이하, cron 관련 파일 소유자 및 권한 변경(소유자 root, 권한 640 이하) |
| 점검 및 조치 사례 | |
| * 공통설정   Step 1) at 명령어 일반사용자 권한 삭제 (at 명령어 위치는 OS별 다를수 있음)  ※ at 명령어는 SUID가 설정되어 있으므로 SUID 설정 제거  # ls -l /usr/bin/at  # chmod 4750 /usr/bin/at  Step 2) cron 관련 설정파일 소유자 및 권한 설정 | |

UNIX 서버

|  |  |
| --- | --- |
| 운영체제 | 관련 설정파일 위치 |
| SOLARIS | /etc/cron.d/at.deny |
| LINUX | /etc/at.deny |
| AIX, HP-UX | /var/adm/cron/at.deny |

|  |  |
| --- | --- |
| U-65 (중) | 3. 서비스 관리 > 3.29 at 서비스 권한 설정 |
| # chown root <at 관련 파일> # chmod 640 <at 관련 파일>   * at 명령어를 일반사용자에게 허용하는 경우   Step 1) “/etc/cron.d/at.allow” 및 “/etc/cron.d/at.deny” 파일의 소유자 및 권한 변경  #chown root /etc/cron.d/at.allow #chmod 640 /etc/cron.d/at.allow #chown root /etc/cron.d/at.deny #chmod 640 /etc/cron.d/at.deny  Step 2) “/etc/cron.d/at.allow” 및 “/etc/cron.d/at.deny” 파일에 사용자 등록  # cat /etc/at.allow (at 명령어 사용을 허용하는 사용자 등록)  # cat /etc/at.deny (at 명령어 사용을 차단하는 사용자 등록) | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | | | | | | | | | | | |
| SOLARIS | #ps | -ef | | | grep | snmp | 또는 | #svcs | -a | | | grep | snmp |
| LINUX, AIX,  HP-UX | #ps | -ef | | | grep | snmp |  |  |  |  |  |  |
| 불필요한 “SNMP" 서비스를 사용하지 않는 경우 중지함 | | | | | | | | | | | |

|  |  |
| --- | --- |
| U-66 (중) | 3. 서비스 관리 > 3.30 SNMP 서비스 구동 점검 |
| 취약점 개요 | |
| 점검내용 | * SNMP 서비스 활성화 여부 점검 |
| 점검목적 | * 불필요한 SNMP 서비스 활성화로 인해 필요 이상의 정보가 노출되는 것을 막기 위해 SNMP 서비스를 중지해야함 |
| 보안위협 | * SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발 생할 수 있음 |
| 참고 | ※ SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트 에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토 콜을 의미함  ※ 기반시설 시스템에서 SNMP 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 기본 Comunity String 변경, 네트워크 모니터링 등의 보안 조치를 반 드시 적용하여야 함  ※ 관련 점검 항: U-68(중) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : SNMP 서비스를 사용하지 않는 경우 |
| 취약 : SNMP 서비스를 사용하는 경우 |
| 조치방법 | SNMP 서비스를 사용하지 않는 경우 서비스 중지 후 시작 스크립트 변경 |
| 점검 및 조치 사례 | |
| < 서비스 중지 방법 >   * SOLARIS 5.9 이하   Step 1) ps -ef | grep snmp로 검색하여 위치 확인 후 이름 변경 Step 2) #/etc/init.d/init.snmpdx stop  Step 3) #mv /etc/rc3.d/S76snmpdx /etc/rc3.d/\_S76snmpdx (rc\*/\_S\*\*snmpdx 의  \*수치는 각각 다름)   * SOLARIS 5.10   Step 1) svcs -a | grep snmp 명령으로 데몬 확인 | |

UNIX 서버

|  |  |
| --- | --- |
| U-66 (중) | 3. 서비스 관리 > 3.30 SNMP 서비스 구동 점검 |
| Step 2) 데몬 활성화 확인  #ps ef | grep snmp 또는 #svcs -a | grep snmp  Step 3. svcadm disable 명령으로 데몬 중지  (예) svcadm disable svc:/application/management/snmpdx  svcadm disable svs:/application/management/dmi:default   * LINUX, AIX, HP-UX 설정   Step 1) ps –ef | grep snmp로 검색  root 2028 1 0 Nov 24 ? 0:00 /usr/sbin/snmpdm  Step 2) snmp 사용하지 않을 시 서비스 중지  <LINUX>  #service snmpd stop  <AIX>  Step 1) #kill -9 [PID]  Step 2) vi /etc/rc.tcpip 실행하여 다음 라인 #처리(주석처리) (수정 전) start /usr/sbin/snmpd "$src\_running" (수정 후) #start /usr/sbin/snmpd "$src\_running"  <HP-UX>  Step 1) #kill -9 [PID] 또는 /sbin/SnmpAgtStart.d/S560SnmpMaster stop  Step 2) mv /sbin/SnmpAgtStart.d/S560SnmpMaster/sbin/SnmpAgtStart.d/\_S560Sn  mpMaster | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS  9이하 버전 | #vi /etc/snmp/conf/snmpd.conf  read-community public / write-community private |
| SOLARIS  10이상 버전 | #vi /etc/sma/snmp/snmpd.conf rocommunity public / rwcommunity private |
| LINUX | #vi /etc/snmp/snmpd.conf  com2sec notConfigUser default public |
| AIX | #vi /etc/snmpdv3.conf  COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0 - |
| HP-UX | #vi /etc/snmpd.conf |

|  |  |
| --- | --- |
| U-67 (중) | 3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정 |
| 취약점 개요 | |
| 점검내용 | * SNMP Community String 복잡성 설정 여부 점검 |
| 점검목적 | * Community String 기본 설정인 Public, Private는 공개된 내용으로 공격자가 이를 이용하여 SNMP 서비스를 통해 시스템 정보를 얻을 수 있기 때문에 Community String을 유추하지 못하도록 설정해야함 |
| 보안위협 | * Community String은 Default로 public, private로 설정된 경우가 많으며, 이 를 변경하지 않으면 이 String을 악용하여 환경설정 파일 열람 및 수정을 통 한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 Dos공격까지 다양 한 형태의 공격이 가능함 |
| 참고 | ※ NMS(Network Management System): 네트워크상의 모든 장비의 중앙 감시 체제를 구 축하여 모니터링, 플래닝, 분석을 시행하고 관련 데이터를 보관하여 필요 즉시 활용 가능하게 하는 관리 시스템을 말함  ※ Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비  밀번호인 'Community String'을 사용함  ※ 기반시설 시스템에서 SNMP 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 기본 Comunity String 변경, 네트워크 모니터링 등의 보안 조치를 반 드시 적용하여야 함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX |
| 판단기준 | 양호 : SNMP Community 이름이 public, private 이 아닌 경우 |
| 취약 : SNMP Community 이름이 public, private 인 경우 |
| 조치방법 | snmpd.conf 파일에서 커뮤니티명을 확인한 후 디폴트 커뮤니티명인 “public, private”를 추측하기 어려운 커뮤니티명으로 변경 |
| 점검 및 조치 사례 | |
|  | |

UNIX 서버

|  |  |
| --- | --- |
|  | get-community-name: public / set-community-name: private |
| 위의 설정과 같이 디폴트 커뮤니티명인 “public" 또는, ”private"을 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함 | |

|  |  |
| --- | --- |
| U-67 (중) | 3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정 |
| * SOLARIS   Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기  Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)  <SOLARIS9 이하 버전>  #vi /etc/snmp/conf/snmpd.conf  (수정 전) read-community public / write-community private (수정 후) read-community <변경 값> / write-community <변경 값>  <SOLARIS10 이상 버전>  #vi /etc/sma/snmp/snmpd.conf  (수정 전) rocommunity public / rwcommunity private (수정 후) rocommunity <변경 값> / rwcommunity <변경 값>  Step 3) 서비스 재구동  <SOLARIS9 이하 버전>  # ps –ef | grep snmp # kill –HUP [PID]  <SOLARIS10 이상 버전>  # svcs –a | grep snmpdx  # svcadm disable svc:/application/management/snmpdx:default  # svcadm enable svc:/application/management/snmpdx:default   * LINUX   Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기  #vi /etc/snmp/snmpd.conf  Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)  (수정 전) com2sec notConfigUser default public (수정 후) com2sec notConfigUser default <변경 값>  Step 3) 서비스 재구동  # service snmpd rstart   * AIX   Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기  #vi /etc/snmpdv3.conf  Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)  (수정 전) COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0 - | |

UNIX 서버



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| U-67 (중) | 3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정 | | | |
| (수정 후) COMMUNITY <변경 값> <변경 값> noAuthNoPriv 0.0.0.0 0.0.0 -  Step 3) 서비스 재구동  # ps –ef | grep snmp # kill –HUP [PID]   * HP-UX   Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기  #vi /etc/snmpd.conf  Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)  (수정 전) get-community-name: public / set-commnunity-name : private  (수정 후) get-community-name: <변경 값> / set-commnunity-name: <변경 값>  Step 3) 서비스 재구동  # ps –ef | grep snmp # kill –HUP [PID] | | | | |
| 조치 시 영향 | Community String 수정 시 Server/Client에 모두 변경하지 않을 시 통신 장애가 일어날 수 있음 | 같은 | Community | String으로 |

UNIX 서버

|  |  |
| --- | --- |
| U-68 (하) | 3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공 |
| 취약점 개요 | |
| 점검내용 | * 서버 및 서비스에 로그온 시 불필요한 정보 차단 설정 및 불법적인 사용에 대한 경고 메시지 출력 여부 점검 |
| 점검목적 | * 비인가자들에게 서버에 대한 불필요한 정보를 제공하지 않고, 서버 접속 시 관계자만 접속해야 한다는 경각심을 심어 주기위해 경고 메시지 설정이 필 요함 |
| 보안위협 | * 로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음 |
| 참고 | ※ 로그온 시 경고 메시지는 공격자의 활동을 주시하고 있다는 생각을 상기시킴으로써  간접적으로 공격 피해를 감소시키는 효과를 줄 수 있음 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : 서버 및 Telnet, FTP, SMTP, DNS 서비스에 로그온 메시지가 설정되어 있는 경우 |
| 취약 : 서버 및 Telnet, FTP, SMTP, DNS 서비스에 로그온 메시지가 설정되어 있지 않은 경우 |
| 조치방법 | Telnet, FTP, SMTP, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬  재시작 |
| 점검 및 조치 사례 | |
| * SOLARIS   Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력  #vi /etc/motd  경고 메시지 입력  Step 2) Telnet 배너 설정: vi 편집기로 "/etc/default/telnetd" 파일을 연 후 로그온 메시지 입력  #vi /etc/default/telnetd BANNER="WARNING:Authorized use only" or BANNER=""  Step 3) FTP 배너 설정: vi 편집기로 "/etc/default/ftpd" 파일을 연 후 로그인 메시지 입력  #vi /etc/default/ftpd  BANNER="WARNING:Authorized use only" or BANNER=""  Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입력  #vi /etc/mail/sendmail.cf  O Smtp GreetingMessage="경고 메시지 입력"  Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력  #vi /etc/named.conf | |

UNIX 서버



|  |  |
| --- | --- |
| U-68 (하) | 3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공 |
| 경고 메시지 입력   * LINUX   Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력  #vi /etc/motd  경고 메시지 입력  Step 2) Telnet 배너 설정: vi 편집기로 "/etc/issue.net" 파일을 연 후 로그온 메시지 입력  #vi /etc/issue.net  경고 메시지 입력  Step 3) FTP 배너 설정: vi 편집기로 "/etc/vsftpd/vsftpd.conf" 파일을 연 후 로그인 메시지 입  력  #vi /etc/vsftpd/vsftpd.conf ftpd\_banner="경고 메시지 입력"  Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입  력  #vi /etc/mail/sendmail.cf  O Smtp GreetingMessage="경고 메시지 입력"  Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력  #vi /etc/named.conf  경고 메시지 입력   * AIX   Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력  #vi /etc/motd  경고 메시지 입력  Step 2) Telnet 배너 설정: vi 편집기로 "/etc/security/login.cfg" 파일을 연 후 로그온 메시지 입력  #vi /etc/security/lgoin.cfg  default: 라인 끝부분에 herald=”경고 메시지” 설정 추가 Step 3) FTP 배너 설정  #dspcat -g /usr/lib/nls/msg/en\_US/ftpd.cat > /tmp/ftpd.msg  #vi /tmp/ftpd.msg의 내용중 "(%s) FTP server (%s) ready." 삭제 후 경고 메시 지 입력  #gencat /tmp/ftpd.cat /tmp/ftpd.msg  #cp -p /tmp/ftpd.cat /usr/lib/nls/msg/en\_US/ftpd.cat  Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입력  #vi /etc/mail/sendmail.cf  #SMTP initial login message (old $e marco) O SmtpGreetingMessage="경고 메시지 입력"  Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력 | |

UNIX 서버

|  |  |
| --- | --- |
| U-68 (하) | 3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공 |
| #vi /etc/named.conf  경고 메시지 입력   * HP-UX   Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력  #vi /etc/motd  경고 메시지 입력  Step 2) Telnet 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 telnet 부분에 로그인 파 일 설정  #telnet stream tcp6 nowait root /usr/lbin/telnetd telnetd –b /etc/issue  (/etc/issue 파일은 banner가 작성되어 있는 파일)  (-b : 뒤에 따라오는 banner 파일을 사용하겠다는 옵션)  #vi /etc/issue  경고 메시지 입력  Step 3) FTP 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 다음 내용 추가  #vi /etc/inetd.conf  ftp stream tcp nowait root /usr/lbin/ftpd ftpd -a /etc/ftpd/ftpaccess  (-a : 뒤에 따라오는 설정파일을 사용하겠다는 옵션)  ※ hostname제거  <wu-ftpd v2.4 미만인 경우>  #vi /etc/ftpd/ftpaccess suppresshostname yes (hostname 숨김) suppressversion yes (version 정보 숨김)  banner /etc/ftpd/ftp\_banner(ftp 배너가 작성된 파일)  <we-ftpd v2.4 이상인 경우>  #vi /etc/ftpd/ftpaccess  greeting terse (hostname 및 version 정보 숨김)  </etc/ftpd/ftpaccess 파일이 없을 경우>  #cp /usr/newconfig/etc/ftpd/examples/ftpaccess /etc/ftpd/ftpaccess  Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 메시지 입력  #vi /etc/mail/sendmail.cf  SMTP initial login message (old $e marco) O SmtpGreetingMessage="경고 메시지 입력"  Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 메시지 입력  #vi /etc/named.conf  경고 메시지 입력 | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OS별 | | 점검 | 파일 | 위치 | 및 | 점검 | 방법 |
| SOLARIS | #ls -al /etc/dfs/dfstab  rw-r--r-- root <nfs 접근제어 파일> | | | | | | |
| LINUX, AIX,  HP-UX | #ls -al /etc/exports  rw-r--r-- root <nfs 접근제어 파일> | | | | | | |
| "NFS" 접근제어 설정파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가  아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 | | | | | | | |

|  |  |
| --- | --- |
| U-69 (중) | 3. 서비스 관리 > 3.33 NFS 설정파일 접근권한 |
| 취약점 개요 | |
| 점검내용 | * NFS 접근제어 설정파일에 대한 비인가자들의 수정 제한 여부 점검 |
| 점검목적 | * 비인가자에 의한 불법적인 외부 시스템 마운트를 차단하기 위해 NFS 접근 제어 파일의 소유자 및 파일 권한을 설정 |
| 보안위협 | * NFS 접근제어 설정파일에 대한 권한 관리가 이루어지지 않을 시 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있음 |
| 참고 | ※ NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마  치 로컬 파일시스템처럼 사용할 수 있는 프로그램  ※ 관련 점검 항목 : U-24(상), U-25(상) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : NFS 접근제어 설정파일의 소유자가 root 이고, 권한이 644 이하인 경우 |
| 취약 : NFS 접근제어 설정파일의 소유자가 root 가 아니거나, 권한이 644 이하 가 아닌 경우 |
| 조치방법 | NFS 접근제어 설정파일의 소유자가 root 가 아니거나, 권한이 644 이하가 아닌 경우 |
| 점검 및 조치 사례 | |
| * SOLARIS   “/etc/dfs/dfstab” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)  #chown root /etc/dfs/dfstab #chmod 644 /etc/dfs/dfstab   * LINUX, AIX, HP-UX   “/etc/exports” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)  #chown root /etc/exports  #chmod 644 /etc/exports | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, HP-UX | noexpn, novrfy 옵션 설정 확인  #vi /etc/mail/sendmail.cf  O PrivacyOptions= (noexpn, novrfy 또는 goaway 옵션 설정 여부) |
| AIX | #vi /etc/sendmail.cf  O PrivacyOptions=(noexpn, novrfy 또는 goaway 옵션 설정 여부) |
| ※ goaway 옵션 : authwarnings, noexpn, novrfy, noverb, needmailhelo, needexpnhelo, needvrfyhelo, nobodyreturn 통합하는 단축 옵션 | |

|  |  |
| --- | --- |
| U-70 (중) | 3. 서비스 관리 > 3.34 expn, vrfy 명령어 제한 |
| 취약점 개요 | |
| 점검내용 | * SMTP 서비스 사용 시 vrfy, expn 명령어 사용 금지 설정 여부 점검 |
| 점검목적 | * SMTP 서비스의 expn, vrfy 명령을 통한 정보 유출을 막기 위하여 두 명령어 를 사용하지 못하게 옵션을 설정해야함 |
| 보안위협 | * VRFY, EXPN 명령어를 통하여 특정 사용자 계정의 존재유무를 알 수 있고, 사용자의 정보를 외부로 유출 할 수 있음 |
| 참고 | ※ SMTP(Simple Mail Transfer Protocol) 서버: 인터넷상에서 전자우편(E-mail)을 전송할  때 이용하게 되는 표준 통신 규약을 말함  ※ VRFY: SMTP 클라이언트가 SMTP 서버에 특정 아이디에 대한 메일이 있는지 검증하기 위해 보내는 명령어를 말함  ※ EXPN(메일링 리스트 확장): 메일 전송 시 포워딩하기 위한 명령어를 말함 |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, LINUX, AIX, HP-UX 등 |
| 판단기준 | 양호 : SMTP 서비스 미사용 또는, noexpn, novrfy 옵션이 설정되어 있는 경우 |
| 취약 : SMTP 서비스를 사용하고, noexpn, novrfy 옵션이 설정되어 있지 않는 경우 |
| 조치방법 | SMTP 서비스 설정파일에 noexpn, novrfy 또는 goaway 옵션 추가 |
| 점검 및 조치 사례 | |
| <서비스 필요 시>   * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 “/etc/mail/sendmail.cf” 파일을 연 후 (단, AIX는 /etc/sendmail.cf)  #vi /etc/mail/sendmail.cf  Step 2) “/etc/mail/sendmail.cf” 파일에 noexpn, novrfy 옵션 추가 | |

UNIX 서버



|  |  |
| --- | --- |
| U-70 (중) | 3. 서비스 관리 > 3.34 expn, vrfy 명령어 제한 |
| (수정 전) O PrivacyOptions=authwarnings  (수정 후) O PrivacyOptions=authwarnings, noexpn, novrfy 또는 goaway  Step 3) SMTP 서비스 재시작  < 서비스 불필요 시>   * SOLARIS, LINUX, HP-UX   Step 1) 실행중인 서비스 중지  #ps –ef | grep sendmail  root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections  #kill -9 [PID]  Step 2) 시스템 재시작 시 SMTP 서버가 시작되지 않도록 OS별로 아래와 같이 설정함   * SOLARIS, LINUX   + 위치 확인   #ls –al /etc/rc\*.d/\* | grep sendmail   * + 이름 변경   #mv /etc/rc2.d/S88sendmail /etc/rc2.d/\_S88sendmail   * AIX   + 위치 확인   #ls –al /etc/rc.d/rc\*.d/\* | grep sendmail   * + 이름 변경   #mv /etc/rc2.d/S88sendmail /etc/rc2.d/\_S88sendmail   * + /etc/rc.tcpip 파일에서 아래 내용 #처리(주석 처리)   (수정 전) start /usr/lib/sendmail "$src\_running" "-bd -q${qpi}" (수정 후) #start /usr/lib/sendmail "$src\_running" "-bd -q${qpi}"   * HP-UX   + 위치 확인   #ls –al /sbin/rc\*.d/\* | grep sendmail   * + 이름 변경   #mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/\_S540sendmail   * + /etc/rc.config.d/mailservs 파일에서 SENDMAIL\_SERVER 값을 “0”으로 변경 (9.x 이하:   /etc/netbsdsrc)  SENDMAIL\_SERVER=0   * SOLARIS 5.10   + #svcs -a | grep smtp   + 데몬 활성화 확인   online 13:17:45 svc:/network/smtp:sendmail   * + 데몬 중지   #svcadm disable [서비스 데몬명]  (예) #svcadm disable svc:/network/smtp:sendmail | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| OS별 점검 파일 위치 및 점검 방법 | |
| SOLARIS, LINUX, AIX, HP-UX | ServerTokens, ServerSignature 옵션 설정 여부 확인  # vi /[Apache\_Home]/conf/httpd.conf ServerTokens Prod  ServerSignature off  “httpd.conf” 파일 내에 ServerTokens, ServerSignature 지시자가 위와 같이 설정되어 있지 않은 경우 아래의 보안설정방법에 따라 옵션 추가 |

|  |  |
| --- | --- |
| U-71 (중) | 3. 서비스 관리 > 3.35 Apache 웹 서비스 정보 숨김 |
| 취약점 개요 | |
| 점검내용 | * 웹페이지에서 오류 발생 시 출력되는 메시지 내용 점검 |
| 점검목적 | * HTTP 헤더, 에러페이지에서 웹 서버 버전 및 종류, OS 정보 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위함 |
| 보안위협 | * 불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수 집할 수 있음 |
| 참고 | - |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : ServerTokens Prod, ServerSignature Off로 설정되어있는 경우 |
| 취약 : ServerTokens Prod, ServerSignature Off로 설정되어있지 않은 경우 |
| 조치방법 | 헤더에 최소한의 정보를 제한 후 전송 (ServerTokens 지시자에 Prod 옵션, ServerSignature 지시자에 Off 옵션 설정) |
| 점검 및 조치 사례 | |
| * SOLARIS, LINUX, AIX, HP-UX   Step 1) vi 편집기를 이용하여 /[Apache\_home]/conf/httpd.conf 파일을 연 후  #vi /[Apache\_home]/conf/httpd.conf  Step 2) 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정 및 ServerSignature Off 지시자에 Off 옵션 설정 (없으면 신규 삽입)  <Directory />  Options Indexes FollowSymlinks ServerTokens Prod ServerSignature Off | |

UNIX 서버



|  |  |  |
| --- | --- | --- |
| ServerTokens 지시자 옵션 | | |
| 키워드 | 제공하는 정보 | 예문 |
| Prod | 웹 서버 종류 | Apache |
| Min | 웹 서버 버전 | Apache/2.2.3 |
| OS | 웹 서버 버전 + 운영체제 | Apache/2.2.3 (CentOS) (기본값) |
| Full | 웹 서버의 모든 정보 | Apache/2.2.3 (CentOS) DAV/2  PHP/5.16 |

|  |  |
| --- | --- |
| U-71 (중) | 3. 서비스 관리 > 3.35 Apache 웹 서비스 정보 숨김 |
| - 이하 생략-  </Directory> | |
| 조치 시  영향 | 일반적인 경우 영향 없음 |

UNIX 서버

|  |  |
| --- | --- |
| U-72 (하) | 5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정 |
| 취약점 개요 | |
| 점검내용 | * 내부 정책에 따른 시스템 로깅 설정 적용 여부 점검 |
| 점검목적 | * 보안 사고 발생 시 원인 파악 및 각종 침해 사실에 대한 확인을 하기 위함 |
| 보안위협 | * 로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한   충분한 증거로 사용할 수 없음 |
| 참고 | * 감사 설정이 너무 높으면 보안 로그에 불필요한 항목이 많이 기록되므로 매우 중요한 항목과 혼동할 수 있으며 시스템 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요 구 사항과 조직의 정책에 따라 필요한 로그를 남기도록 설정하여야 함   ※ 관련 점검 항목 : A-20(상), A-85(상) |
| 점검대상 및 판단기준 | |
| 대상 | * SOLARIS, Linux, AIX, HP-UX 등 |
| 판단기준 | 양호 : 로그 기록 정책이 정책에 따라 설정되어 수립되어 있으며 보안정책에 따  라 로그를 남기고 있을 경우 |
| 취약 : 로그 기록 정책 미수립 또는, 정책에 따라 설정되어 있지 않거나 보안정 책에 따라 로그를 남기고 있지 않을 경우 |
| 조치방법 | 로그 기록 정책을 수립하고, 정책에 따라 syslog.conf 파일을 설정 |
| 점검 및 조치 사례 | |
| * SOLARIS   Step 1) vi 편집기를 이용하여 “/etc/syslog.conf” 파일 열기  #vi /etc/syslog.conf  Step 2) 아래와 같이 수정 또는, 신규 삽입  mail.debug /var/log/mail.log  \*.info /var/log/syslog.log  \*.alert /var/log/syslog.log  \*.alert /dev/console  \*.alert root  \*.emerg \*  Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작  < SOLARIS 9 이하 버전 >  #ps –ef | grep syslogd  root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd #kill –HUP [PID]  < SOLARIS 10 이상 버전 > | |

UNIX 서버



|  |  |
| --- | --- |
| U-72 (하) | 5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정 |
| #svcs -a | grep system-log  online 16:23:03 svc:/system/system-log:default #svcadm disable svc:/system/system-log:default #svcadm enable svc:/system/system-log:default   * LINUX   Step 1) vi 편집기를 이용하여 “/etc/syslog.conf” 파일 열기  #vi /etc/syslog.conf  ※ CentOS 6.x 이상 버전의 로그파일명: rsyslog.conf  Step 2) 아래와 같이 수정 또는, 신규 삽입  \*.info;mail.none;authpriv.none;cron.none /var/log/messages authpriv.\* /var/log/secure  mail.\* /var/log/maillog  cron.\* /var/log/cron  \*.alert /dev/console  \*.emerg \*  Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작  #ps –ef | grep syslogd  root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd #kill –HUP [PID]   * AIX   Step 1) vi 편집기를 이용하여 “/etc/syslog.conf” 파일 열기  #vi /etc/syslog.conf  Step 2) 아래와 같이 수정 또는, 신규 삽입  \*.emerg \*  \*.alert /dev/console  \*.alert /var/adm/alert.log  \*.err /var/adm/error.log  mail.info /var/adm/mail.log  auth.info /var/adm/auth.log  daemon.info /var/adm/daemon.log  \*.emerg;\*.alert;\*.crit;\*.err;\*.warning;\*.notice;\*.info /var/adm/messages  Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작  #refresh –s syslogd 또는, #ps –ef |grep syslogd | |

UNIX 서버

|  |  |  |
| --- | --- | --- |
| 구분 | 왼쪽 필드 | 오른쪽 필드 |
| 형식 | A.B | C |
| 예시 | mail.debug;cron.crit;auth.info | /var/log/syslog.log |
| 설명 | A서비스 데몬의 B 로그레벨 이상 | C 형식으로 로그를 남김 |

|  |  |
| --- | --- |
| 서비스 데몬 종류 | |
| 메시지 | 설명 |
| auth | 로그인 등의 인증 프로그램 유형이 발생한 메시지 |
| authpriv | 개인 인증을 요구하는 프로그램 유형이 발생한 메시지 |

|  |  |
| --- | --- |
| U-72 (하) | 5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정 |
| root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd #kill –HUP [PID]   * HP-UX   Step 1) vi 편집기를 이용하여 “/etc/syslog.conf” 파일 열기  #vi /etc/syslog.conf  Step 2) 아래와 같이 수정 또는, 신규 삽입  \*.notice /var/adm/syslog/syslog.log  \*.alert /dev/console  \*.emerg \*  Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작 #/sbin/init.d/syslogd start 또는, #ps –ef |grep syslogd  root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd #kill –HUP [PID]   * Syslog.conf 파일 형식   [오른쪽 필드의 로그 형식 종류]   * + var/log/syslog.log -> 해당 파일에 로그를 기록   + dev/console -> 모니터 화면과 같은 지정된 콘솔로 메시지 출력   + user -> 지정된 사용자의 화면에 메시지 출력   + \* -> 현재 로그인되어 있는 모든 사용자의 화면에 메시지 출력   5. @192.168.0.1 -> 지정된 호스트로 로그 전송 | |

UNIX 서버



|  |  |
| --- | --- |
| 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 | | |
| 등급 | 메시지 | 설명 |
| 4 (높음) | Emergency [emerg] | 매우 위험한 상황 |
| 3 | Alert [alert] | 즉각적으로 조치를 취해야 할 상황 |
| 2 | Critical [crit] | 하드웨어 등의 심각한 오류가 발생화 상황 |
| 1 | Error [err] | 에러 발생 시 |
| 0 | Warnnig [warning] | 주의를 요하는 메시지 |
| -1 | Notice [notice] | 에러가 아닌 알림에 관한 메시지 |
| -2 | Information [info] | 단순한 프로그램에 대한 정보 메시지 |
| -3 (낮음) | Debug [debug] | 프로그램 실행 오류 발생 시 |

|  |  |
| --- | --- |
| U-72 (하) | 5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정 |
|  | |
| 조치 시 영향 | 위에 제시한 모든 로그를 설정할 경우, 시스템 퍼포먼스와 로그 저장에 따른 서 버 용량 부족 문제가 발생할 수 있으므로 시스템 운영환경과 특성을 고려하여 적용 |

UNIX 서버

|  |  |
| --- | --- |
| | more | 많은 내용 출력 시 사용하는 옵션  “Enter”를 누르면 한 줄씩, “SpaceBar”를 누르면 한  화면씩 더 보여줌 |
| | grep [Word] | 특정 단어가 포함된 줄만 출력하는 명령어  [Word]에 특정 단어를 입력하여 호출 |
| | nl | 파일의 내용이 총 몇 줄인지 출력하는 명령어 |
| | head | 파일의 앞부분 10줄만 출력하는 명령어 |
| | tail | 파일의 뒷부분 10줄만 출력하는 명령어 |

|  |
| --- |
| 부 록 |
| 01. cat 명령어로 파일 내용 확인 |
| cat 명령어는 텍스트 파일 내용 출력, 쓰기, 복사 시 사용하며 주로 텍스트 파일 내용을 표준 출력장치로 출력하여 확인하는 경우 사용됨. 명령어 입력 방법은 다음과 같음   * *#cat* 파일 경로*/*파일명 : 파일을 열어 내용을 출력 * *#cat >* 파일 경로*/*파일명   같은 이름의 파일이 없는 경우 -> 파일을 새로 만들고 내용 입력 같은 이름의 파일이 있는 경우 -> 파일을 덮어쓰고 새로 내용 입력   * *#cat >>* 파일 경로*/*파일명   같은 이름의 파일이 없는 경우 -> 파일을 새로 만들고 내용 입력  같은 이름의 파일이 있는 경우 -> 기존 파일의 내용 밑에 이어서 입력  ※ 덧붙여 사용할 수 있는 명령어 |
| 02. vi 편집기를 사용하여 파일 내용 수정 |
| vi 편집기는 윈도우의 메모장처럼 사용되는 유닉스에서 제공하는 표준편집기를 말함. 이미 존 재하는 파일을 수정하는 경우 또는, 신규 파일을 만들고자 할 때 vi 명령을 사용함  #vi <파일 경로/파일명>  vi 명령어를 입력하여 프로그램을 시작하면 일반적으로 명령(normal)모드로 시작되고, 이때 키 보드에서“I” 키를 누르게 되면 편집(insert)모드로 바뀌어 “Esc” 키를 누를 때까지 문서 작성을 할 수 있음. (편집모드에서는 아래 화면과 같이 “--INSERT--”를 확인할 수 있음) |

UNIX 서버



|  |
| --- |
| 부 록 |
| 편집중인 문서 저장 시 “:w"를 입력하고, 수정 완료 후 ”:q"를 입력하여 프로그램을 종료함. 파 일에 쓰기 권한이 없을 때 'readonly‘ option qis set (use ! to override)라는 메시지가 출력이 되면서 저장이 안 되는 경우가 있는데 이때는 강제 옵션인 "!“를 추가로 붙여서 문제를 해결함  ※ vi 편집기는 아래의 “3가지 모드”로 구성됨   * 명령모드: 기본 구성 / 텍스트 편집 불가 / 명령어 수행 * 편집모드: 텍스트 편집만 가능 * 확장모드: 종료하거나 저장이 가능한 확장 기능 수행 |
| 03. find 명령어를 사용하여 파일 경로 확인 |
| find 명령어는 원하는 파일을 계속 필터링 하면서 찾아볼 수 있도록 하고, 잘못 수정 된 파일 을 추적할 때 유용하게 사용됨. 취약점 진단 시 각 운영체제별로 파일이 존재하는 위치에 차 이가 있어 진단 조치 또는, 설정 여부 확인이 어려운 경우가 종종 있는데 find 명령어를 이용 하여 파일이 위치한 경로를 쉽게 확인할 수 있음. find 명령어 기본형은 다음과 같음  *#find . -name 'pattern’*  <find 명령어 사용 예시> |

UNIX 서버

|  |  |
| --- | --- |
| 파일 | 속 성 |
| /etc/passwd | 사용자 ID, Shell등 사용자 계정 정보 저장 |
| /etc/shadow | root 또는, 사용자 계정의 암호 저장 |
| /etc/group | 각 그룹 목록에 대한 정보 저장 |

|  |
| --- |
| 부 록 |
| * #find . -name '\*.html'   . 은 현재 디렉터리에서 찾음, /usr와 같이 특정 위치에서 찾으려면 #find /usr –name '\*.html’  -name은 파일 이름으로 찾으라는 조건으로 확장자가 .html 로 끝나는 파일만을 검색   * #find . -type d   디렉터리만 검색   * #find . -group admin -type l   그룹이 admin이면서 심볼릭 링크만 조회   * #find . - user icocoa -maxdepth 1 -type d   현재 디렉터리 내에서 소유자가 icocoa이며, 디렉터리인 것만을 검색   * #find . -name '\*.jpg' -o -name '\*.html'   -o 옵션은 OR 옵션으로 확장자가 .jpg인 것과 .html인 파일을 검색   * #find . -atime -2   2일 동안 액세스가 일어나지 않은 파일 검색   * #find . -atime +3   액세스가 일어난 후 3일된 파일 검색   * #find . -mtime +7   7일 넘도록 변경되지 않은 파일 검색 (m: modification time)   * #find . -mmin +30 -maxdepth 1 -type f   현재 디렉터리 내에서 변경이 있은 후 30분 지난 파일 검색(+,- 기호 사용)   * #find . -name '\*.xml' -exec grep -l 'Version' { } \;   현재 디렉터리 내에서 Version이라는 단어가 들어간 .xml 확장자를 가진 파일 검색   * #find . \! -name "\*.jpg"   .jpg로 끝나지 않는 파일 검색   * #find . -newermm test.txt   test.txt 보다 나중에 수정된 파일 검색 (-newermm은 -newer와 동일)   * #find . -size +100c(+,- 기호 사용)   사이즈가 100바이트 이상인 파일 검색(c: bytes) (-인 경우 100바이트보다 작은 파일 검색) |
| 04. /etc/passwd, /etc/shadow, /etc/group 파일 구조 |
|  |

UNIX 서버



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| namegpark | x | 500 | 500 | namegpark | /home/namegpark | /bin/bash |
| 계정명① | 패스워드② | UID③ | GID④ | 계정설명⑤ | 홈 디렉터리⑥ | Shell 정보⑦ |

|  |
| --- |
| 부 록 |
| **□** /etc/passwd  ① 사용자 이름(대부분 ID라고함)  ② 사용자 비밀번호(X로 되어 있는 것은 /etc/shadow 에 암호화된 형태로 저장되어 있음)  ③ 사용자 UID(Unix의 모든 정보는 수치값으로 저장되어 있음 (root -> 0(GID))  ④ 사용자 소속 그룹 GID(리눅스의 모든 정보는 수치값으로 저장 되어 있음 root -> 0(GID))  ⑤ 사용자 정보(이름이나 연락처등 기타 정보 입력)  ⑥ 사용자 계정 디렉터리(계정 홈 디렉터리)  ⑦ 사용자 로그인 쉘 (Linux : bash Shell, Unix : Korn Shell 등) |

UNIX 서버

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| root | $6$7~ | 15788 | 0 | 99999 | 7 |
| 계정명 | 패스워드 | 암호  생성일자 | 변경가능  최소시간 | 유효기간 | 경고일수 |

|  |
| --- |
| 부 록 |
| * /etc/shadow   ex)Root : $1$Fz4q1GjE$G/EskZPyPdMo9.cNhRKSY.:14806: 0 : 99999 : 7 : : :  ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨  각 필드의 구분자는 콜론(:)이며, 각 필드는 아래의 의미를 가지고 있다.  ① Login Name : 사용자 계정  ② Encrypted : 패스워드를 암호화시킨 값  ③ Last Changed : 1970년부터 1월 1일부터 패스워드가 수정된 날짜의 일수를 계산  ④ Minimum : 패스워드가 변경되기 전 최소사용기간(일수)  ⑤ Maximum : 패스워드 변경 전 최대사용기간(일수)  ⑥ Warn : 패스워드 사용 만기일 전에 경고 메시지를 제공하는 일수  ⑦ Inactive : 로그인 접속차단 일 수  ⑧ Expire : 로그인 사용을 금지하는 일 수 (월/일/연도)+A1:A44  ⑨ Reserved : 사용되지 않음 |

UNIX 서버



|  |  |  |  |
| --- | --- | --- | --- |
| namegpark | x | 500 | - |
| 그룹명 | 패스워드 | GID | 그룹구성원 |

|  |
| --- |
| 부 록 |
| * /etc/group |
| 05. 계정 설명 |
| ⦁  ⦁lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin = 로컬 프린트 서버  ⦁sync:x:5:0:sync:/sbin:/bin/sync = 원격지 서버 동기화  ⦁shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown = soft 시스템 종료  ⦁halt:x:7:0:halt:/sbin:/sbin/halt = 강제 시스템 종료  ⦁mail:x:8:12:mail:/var/spool/mail:/sbin/nologin = 메일 서비스 계정  ⦁news:x:9:13:news:/etc/news:/sbin/nologin  ⦁uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin = 유닉스 시스템 간 파일을 복사 프로토콜  operator:x:11:0:operator:/root:/sbin/nologin = 설정에 따라 다르지만 /etc/syslog.conf 에 대해서  d⦁aemon.err operator라고 표기되어 있다면 데몬 관련 에러를 operator 계정을 이용해 출력하라는 의미임  ⦁games:x:12:100:games:/usr/games:/sbin/nologin  gopher:x:13:30:gopher:/var/gopher:/sbin/nologin = 웹(www)이 나오기 전 대표적인 서비스 중 하나로  g⦁opher사이트 접속 후 잘 정리된 메뉴를 이용해서 웹 서핑을 즐기도록 한 서비스  ⦁ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin = ftp 사용 시 필요  ⦁squid:x:23:23::/var/spool/squid:/sbin/nologin = 프록시 서버  ⦁named:x:25:25:Named:/var/named:/sbin/nologin = 네임서비스 데몬 계정  ⦁mysql:x:27:27::/home/mysql:/bin/bash = mysql 서비스 시작 시 사용하는 계정  ⦁nscd:x:28:28:NSCD Daemon:/:/sbin/nologin = 네임서비스에 대한 캐시 기능 제공  ⦁rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin = 원격 호출 관련 데몬 |

UNIX 서버

|  |  |
| --- | --- |
| SOLARIS | |
| /usr/bin/admintool | System Administration Tools |
| /usr/bin/at | 지정된 시간에 실행할 작업을 입력하고, 대기 목록을 확 인하고, 제거하는 명령어 |
| /usr/bin/atq | Daemons  현재 대기중인 작업 목록 확인 |
| /usr/bin/atrm | Daemons  현재 대기중인 작업제거 |
| /usr/bin/lpset | 프린터와 관련된 장치, 디렉터리를 접근하는 명령어로 EG ID 를 변경 |
| /usr/bin/newgrp | 현재 세션의 사용자 그룹 변경  (지정한 그룹의 쉘로 환경이 바로 변경) |
| /usr/bin/nispasswd | RPC DAEMON  NIS+passwd 테이블 패스워드 변경 |

|  |
| --- |
| 부 록 |
| ⦁  ⦁netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash = 네트워크 오류 파일 저장 서비스  ⦁rpm:x:37:37::/var/lib/rpm:/sbin/nologin = 레드햇 패키지 매니저  ⦁ntp:x:38:38::/etc/ntp:/sbin/nologin = 컴퓨터 간 시간 동기화 Network Time Protocol  ⦁gdm:x:42:42::/var/gdm:/sbin/nologin = x-window 사용  ⦁xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin = X윈도우 폰트서버  ⦁mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin = 메일 큐  ⦁apache:x:48:48:Apache:/var/www:/sbin/nologin = httpd 사용  ⦁smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin = root가 아닌 smmsp로 메일 발송  pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin = System  ⦁Center Operation Manager가 이기종 환경 관리를 위해 Cross-Platform Extension 제공  ⦁webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin = 웹 로그 분석 프로그램  ⦁haldaemon:x:68:68:HAL daemon:/:/sbin/nologin = 디바이스 장치 인식 데몬  ⦁vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin = 가상메모리 생성 시 계정  ⦁sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin = 보안 쉘 계정  ⦁pcap:x:77:77::/var/arpwatch:/sbin/nologin = 패킷 캡쳐 관련 라이브러리 계정  ⦁dbus:x:81:81:System message bus:/:/sbin/nologin = 시스템 메시지  ⦁ident:x:98:98::/home/ident:/sbin/nologin = inetd에서 구동되는 데몬  ⦁nobody:x:99:99:Nobody:/:/sbin/nologin = 익명 연결 (웹 서비스 등 누구나 연결 가능한 서비스 사용 시)  nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  ※ UID 100이하 또는 60000이상의 계정들은 시스템 계정으로 로그인이 필요없음 |
| 06. 불필요한 SUID/SGID 목록 설명 |
|  |

UNIX 서버



|  |  |
| --- | --- |
| /usr/bin/rdist | 원격 서버로 동기화, 복사, 백업 수행 |
| /usr/bin/yppasswd |  |
| /usr/dt/bin/dtappgather | 사용자 세션을 시작하는 것과 연관된 명령어로 사용 가능 한 응용프로그램 모으는 명령어 |
| /usr/dt/bin/dtprintinfo | 데스크탑에 프린터 추가할 때 사용하는 명령어 |
| /usr/dt/bin/sdtcm\_convert | 캘린더 도구로서 데이터 형식을 변환하거나 캘린더의 불 필요한 부분을 제거하는데 사용 |
| /usr/lib/fs/ufs/ufsdump | Backup/Restore |
| /usr/lib/fs/ufs/ufsrestore | Backup/Restore |
| /usr/lib/lp/bin/netpr | lpsched 데몬, LP 프린트 서비스와 PostScript 필터들에 의해 사용되는 바이너리 파일들, 기본 프린터 인터페이스 프로그램들과 연관 |
| /usr/openwin/bin/ff.core |  |
| /usr/openwin/bin/kcms\_cali brate | /tmp 디렉터리에 kp\_kcms\_sys.sem 이라는 임시 파일을 /t mp에 존재하는지 검사하지 않고 무조건 생성하는 프로그램 |
| /usr/openwin/bin/kcms\_con  figure |  |
| /usr/openwin/bin/xlock | X 터미널을 잠그기 위한 프로그램 |
| /usr/platform/sun4u/sbin/prtdiag | 시스템 하드웨어 사항과 시스템의 하드웨어적 실패 부분 조회 |
| /usr/sbin/arp | 네트워크 관련 명령어 |
| /usr/sbin/lpmove | 다른 프린터와 print request 를 이동할 수 있는 명령어 |
| /usr/sbin/prtconf | 현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록 을 장치 트리를 사용해서 보여주는 명령어 |
| /usr/sbin/sysdef | 유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어 |
| /usr/sbin/sparcv7/prtconf | 현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록 을 장치 트리를 사용해서 보여주는 명령어 |
| /usr/sbin/sparcv7/sysdef | 유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어 |
| /usr/sbin/sparcv9/prtconf | 현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록 을 장치 트리를 사용해서 보여주는 명령어 |

|  |
| --- |
| 부 록 |
|  |

UNIX 서버

|  |  |
| --- | --- |
| /usr/sbin/sparcv9/sysdef | 유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어 |
| LINUX | |
| /sbin/dump | Backup/Restore |
| /sbin/restore | Backup/Restore |
| /sbin/unix\_chkpwd | 사용자의 암호가 읽을 수 없는 장소에 보관되는 경우 사 용자의 암호를 검사해주는 프로그램. 이 프로그램을 호출 한 사용자의 암호를 검사해주는 역할만 함 |
| /usr/bin/at | 지정된 시간에 실행할 작업을 입력하고, 대기 목록을 확 인하고, 제거하는 명령어 |
| /usr/bin/lpq | 라인프린터 작업 큐 조회 명령어 |
| /usr/bin/lpq-lpd | DAEMON |
| /usr/bin/lpr | 콘솔환경에서 명시된 파일을 인쇄할 때 사용 |
| /usr/bin/lpr-lpd | DAEMON |
| /usr/bin/lprm | lpq 명령어로 볼 수 있는 작업 큐를 살펴보고 해당하는 작업을 취소하거나 작업 번호를 지정하여 작업 번호에 해 당하는 큐를 삭제. |
| /usr/bin/lprm-lpd | DAEMON |
| /usr/bin/newgrp | 현재 세션의 사용자 그룹 변경(지정한 그룹의 쉘로 환경 이 바로 변경) |
| /usr/sbin/lpc | 커맨드 기반의 프린터 제어 |
| /usr/sbin/lpc-lpd | DAEMON |
| /usr/sbin/traceroute | 네트워크 경로 출력 |
| AIX | |
| /usr/dt/bin/dtaction | 지정된 인수로 CDE 작업을 호출 |
| /usr/sbin/mount | 파일시스템을 지정된 위치에서 사용 가능하도록 연결 |
| /usr/dt/bin/dtterm | 데스크탑 기본 터미널 에뮬레이터 |
| /usr/sbin/lchangelv | 논리적 볼륨과 연관되는 명령어 |
| /usr/bin/X11/xlock | X 터미널을 잠그기 위한 프로그램 |

|  |
| --- |
| 부 록 |
|  |

UNIX 서버



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HP-UX | | | | |
| /opt/perf/bin/glance | 성능 모니터링 툴(CUI) | | | |
| /opt/perf/bin/gpm | 성능 모니터링 툴(GUI) | | | |
| /opt/video/lbin/camServer |  | | | |
| /usr/bin/at | Daemons  지정된 시간에 실행할 작업을 확인하고, 제거하는 명령어 | 입력하고, | 대기 | 목록을 |
| /usr/bin/lpalt | 프린터 및 인쇄 요청의 우선 순위 변경 | | | |
| /usr/bin/mediainit | 디스크 포맷 명령어로 읽기, 쓰기 테스트를 수행하여 디 스크 무결성을 검증하고 손상된 블럭이 발견될 경우 수정 | | | |
| /usr/bin/newgrp | 현재 세션의 사용자 그룹 변경(지정한 그룹의 쉘로 환경 이 바로 변경) | | | |
| /usr/bin/rdist | 원격 서버로 동기화, 복사, 백업 수행 | | | |
| /usr/dt/bin/dtprintinfo | 데스크탑에 프린터 추가할 때 사용하는 명령어 | | | |
| /usr/sbin/arp | 네트워크 관련 명령어 | | | |
| /usr/sbin/lanadmin | 네트워크 관련 명령어 | | | |
| /usr/sbin/landiag | 네트워크 하드웨어 이상을 진단하는 명령어 | | | |
| /usr/sbin/lpsched | LP 요청 스케줄러의 데이터를 표시 | | | |
| /usr/sbin/swacl | 소프트웨어 생산품 접근 통제 명령어 | | | |
| /usr/sbin/swconfig | 시스템에 설치된 소프트웨어를 configure 하는 명령어 | | | |
| /usr/sbin/swinstall | 시스템에 소프트웨어를 설치하거나 업데이트 하는 명령어 | | | |
| /usr/sbin/swreg | 특정 서버에 등록하는 명령어 | | | |
| /usr/sbin/swremove | 시스템에 설치되어 있는 소프트웨어를 제거 | | | |
| /usr/contrib/bin/traceroute | 네트워크 경로 출력 | | | |
| /usr/dt/bin/dtappgather | 사용자 세션을 시작하는 것과 연관된 명령어로 사용 가능 한 응용프로그램 모으는 명령어 | | | |
| /usr/sbin/swmodify | 소프트웨어 패키지 내역 변경 명령어 | | | |
| /usr/sbin/swpackage | 소프트웨어 패키지 시 사용하는 명령어 | | | |

|  |
| --- |
| 부 록 |
|  |

UNIX 서버

|  |
| --- |
| 부 록 |
| 07. RPC 서비스 종류 |
| ⦁  rpc.statd : 시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램을 지원하는 도구로 클  ⦁ 라이언트와 서버의 상태를 모니터링 하는 데몬  ⦁rpc.ttdbserverd : ToolTalk 애플리케이션간의 통신을 관리하는 데몬  ⦁sadmind : 원격에서 시스템을 관리하거나 모니터링하기 쉽게 도와주는 데몬  ⦁rpc.ypupdated : nis process 변경된 정보를 변경해주는 데몬  ⦁rusersd : 현재 네트워크에 있는 사용자 리스트를 리턴해주는 데몬  ⦁walld : 메시지를 네트워크의 모든 사용자에게 전송하는 요청을 처리하는 데몬  ⦁sprayd : 지정된 수의 패킷을 호스트에 전송하고 성능 통계를 보고하는 데몬  ⦁rstatd : CPU와 가상메모리 사용통계, 네트워크 가동시간, 하드디스크에 대한 정보를 제공하는 데몬  ⦁rpc.nisd : NIS+의 서비스를 제공하는 데몬  ⦁rexd : 원격 사용자가 서버에서 명령어를 실행하도록 하는 데몬  rpc.pcnfsd : PC-NFS(개인용 컴퓨터 네트워크 파일 시스템) 클라이언트에서의 서비스 요청을 처리하는   * 데몬   rpc.cmsd : 데이터베이스 관리 데몬으로 open Windows의 Calender Manager와 CDE의 Calender에서   * 사용   ⦁rpc.rquotad : 원격 쿼터 데몬으로 NFS 서버의 파일 시스템을 마운트한 로컬 유저의 쿼터를 넘겨줌  kcms\_server : 데스크탑 컴퓨터 및 관련 주변 기기에 디지털 컬러 이미지의 색상 성능을 제어 할 수 있   * 는 코닥 색상 관리 시스템을 원격에서 접근할 수 있게 해주는 데몬   cachefsd : 캐시 파일 시스템 데몬. nfs나 cdrom 같은 저속의 장치를 디스크로부터 캐싱하여 성능을 증가시킴 |