

Unix 서버 보안가이드라인

2014. 01



안전행정부 *희망의 새 나라*

Unix 서버 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	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-05
	root 계정 su 제한	하	U-06
	패스워드 최소 길이 설정	중	U-07
	패스워드 최대 사용 기간 설정	중	U-08
	패스워드 최소 사용기간 설정	중	U-09
	불필요한 계정 제거	하	U-10
	관리자 그룹에 최소한의 계정 포함	하	U-11
	계정이 존재하지 않는 GID 금지	하	U-12
	동일한 UID 금지	중	U-13
	사용자 shell 점검	하	U-14
	Session Timeout 설정	하	U-15
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-16
	파일 및 디렉터리 소유자 설정	상	U-17
	/etc/passwd 파일 소유자 및 권한 설정	상	U-18
	/etc/shadow 파일 소유자 및 권한 설정	상	U-19
	/etc/hosts 파일 소유자 및 권한 설정	상	U-20
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-21
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-22
	/etc/services 파일 소유자 및 권한 설정	상	U-23
	SUID,SGID,Stick bit 설정 파일 점검	상	U-24
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-25
	world writable 파일 점검	상	U-26
	/dev에 존재하지 않는 device 파일 점검	상	U-27
	\$HOME/.rhosts, hosts.equiv 사용 금지	상	U-28
	접속 IP 및 포트 제한	상	U-29
	hosts.lpd 파일 소유자 및 권한 설정	하	U-30
	NIS 서비스 비활성화	중	U-31
	UMASK 설정 관리	중	U-32
	홈디렉토리 소유자 및 권한 설정	중	U-33
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-34
	숨겨진 파일 및 디렉토리 검색 및 제거	하	U-35
3. 서비스 관리	finger 서비스 비활성화	상	U-36
	Anonymous FTP 비활성화	상	U-37

	r 계열 서비스 비활성화	상	U-38
	cron 파일 소유자 및 권한설정	상	U-39
	Dos 공격에 취약한 서비스 비활성화	상	U-40
	NFS 서비스 비활성화	상	U-41
	NFS 접근 통제	상	U-42
	automountd 제거	상	U-43
	RPC 서비스 확인	상	U-44
	NIS , NIS+ 점검	상	U-45
	tftp, talk 서비스 비활성화	상	U-46
	Sendmail 버전 점검	상	U-47
	스팸 메일 릴레이 제한	상	U-48
	일반사용자의 Sendmail 실행 방지	상	U-49
	DNS 보안 버전 패치	상	U-50
	DNS Zone Transfer 설정	상	U-51
	Apache 디렉토리 리스팅 제거	상	U-52
	Apache 웹 프로세스 권한 제한	상	U-53
	Apache 상위 디렉토리 접근 금지	상	U-54
	Apache 불필요한 파일 제거	상	U-55
	Apache 링크 사용 금지	상	U-56
	Apache 파일 업로드 및 다운로드 제한	상	U-57
	Apache 웹 서비스 영역의 분리	상	U-58
	ssh 원격접속 허용	중	U-59
	ftp 서비스 확인	하	U-60
	ftp 계정 shell 제한	중	U-61
	Ftpusers 파일 소유자 및 권한 설정	하	U-62
	Ftpusers 파일 설정	중	U-63
	at 파일 소유자 및 권한 설정	중	U-64
	SNMP 서비스 구동 점검	중	U-65
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-66
	로그온 시 경고 메시지 제공	하	U-67
	NFS설정파일접근권한	중	U-68
	expn, vrfy 명령어 제한	중	U-69
	Apache 웹서비스 정보 숨김	중	U-70
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-71
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-72
	정책에 따른 시스템 로깅 설정	하	U-73

UNIX 서버

1. 계정 관리

취약점 항목		1.1. root 계정 원격 접속 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-01	
취약점 개요	*root는 시스템을 관리하는 매우 중요한 계정임. root 계정으로 직접 로그인하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 접속에 대한 관리가 필요함. root 계정의 원격 접속 허용은 공격자에게 더 좋은 기회를 제공할 수 있으므로 root의 원격 접속은 금지하여야 함.					
	*root 계정: 여러 사용자가 사용하는 컴퓨터에서 전체적으로 관리할 수 있는 총괄 권한을 가진 유일한 특별 계정. 유닉스 시스템의 루트(root)는 시스템 관리자인 운용 관리자(Super User)로서 윈도우의 관리자(Administrator)에 해당하며, 사용자 계정을 생성하거나 소프트웨어를 설치하고, 환경 및 설정을 변경하거나 시스템의 동작을 감시 및 제어할 수 있음.					
보안대책						
판단기준	양호: 원격 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우					
	취약: root 직접 접속을 허용하고 원격 서비스를 사용하는 경우					
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	#cat /etc/default/login CONSOLE=/dev/console					
LINUX	#cat /etc/pam.d/login auth required /lib/security/pam_securetty.so #cat /etc/securetty pts/0 ~ pts/x 관련 설정이 존재하지 않음					
AIX	#cat /etc/security/user rlogin = false					
HP-UX	#cat /etc/securetty console					
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS						
1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후						
2. 아래와 같이 주석 제거 또는, 신규 삽입						
(수정 전) #CONSOLE=/dev/console						
(수정 후) CONSOLE=/dev/console						
<pre># If CONSOLE is set, root can only login on that device. # Comment this line out to allow remote login by root. # CONSOLE=/dev/console</pre>						

UNIX 서버

■ LINUX

1. "/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리

2. "/etc/pam.d/login" 파일 수정

(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

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
root	tty1	-	02:34	11:59m	1:37	0.09s	-bash
root	pts/0	-	02:34	11:59m	0.17s	0.17s	/bin/bash
root	pts/1	192.168.100.254	11:11	15.00s	11.02s	10.95s	telnet
root	pts/2	192.168.100.254	08:52	3:28m	0.35s	0.35s	-bash
root	pts/3	192.168.100.254	11:12	23.00s	10.69s	10.63s	telnet
root	pts/4	192.168.100.254	14:05	0.00s	0.40s	0.04s	w
root	pts/5	192.168.100.254	12:50	56:07	0.56s	0.30s	vim .bash_profile

*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

■ AIX

1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후

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 사용하는 명령어

■ HP-UX

1. vi 편집기를 이용하여 "/etc/securetty" 파일을 연 후

2. 아래와 같이 주석 제거 또는, 신규 삽입

(수정 전) #console

(수정 후) console

※ "/etc/securetty" 파일은 디폴트로 존재하지 않으므로 /etc 디렉터리 내에 "securetty" 파일이 존재하지 않는 경우 새로 생성한 후 적용함 (※ vi 편집기를 사용한 파일 생성: 부록 참고)

#vi /etc/securetty

조치 시 영향 일반적으로 영향 없음

UNIX 서버

취약점 항목		1.2. 패스워드 복잡성 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-02
취약점 개요	사용자 계정(root 및 일반 계정 모두 해당) 암호를 유추하기 쉽게 설정할 경우 비인가자의 시스템 접근을 허용하게 하는 위험이 존재함. 여러 문자를 혼합한 8자리 이상의 암호를 사용하게 하여 패스워드 복잡성을 높이면 비인가자에 의해 발생하는 침입 공격 발생률을 낮출 수 있음.				
보안대책					
판단기준	양호: 영문·숫자·특수문자가 혼합된 8자리 이상의 패스워드가 설정된 경우				
	취약: 영문·숫자·특수문자 혼합되지 않은 8자 미만의 패스워드가 설정된 경우				
조치방법	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX		/etc/shadow 파일 내 설정된 패스워드 점검			
AIX		/etc/security/passwd 파일 내 설정된 패스워드 점검			
OS별 점검 파일을 열어 패스워드를 확인 한 후 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
< 부적절한 패스워드 유형 >					
1. 사전에 나오는 단어나 이들의 조합					
2. 길이가 너무 짧거나, NULL(공백)인 패스워드					
3. 키보드 자판의 일련의 나열 (예) abcd, qwert, etc					
4. 사용자 계정 정보에서 유추 가능한 단어들					
(예) 지역명, 부서명, 계정명, 사용자 이름의 이니셜, root, rootroot, root123, admin 등					
< 패스워드 관리 방법 >					
1. 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)					
2. 시스템마다 상이한 패스워드 사용					
3. 패스워드를 기록해 놓을 경우 변형하여 기록					
4. 가급적 자주 패스워드를 변경할 것					
조치 시 영향	패스워드 변경 시 Web, Was, DB연동 구간에서 문제가 발생할 수 있으므로 연동 구간에 미칠 수 있는 영향을 고려하여 적용 필요				

UNIX 서버

취약점 항목		1.3. 계정 잠금 임계값 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-03	
취약점 개요	침입자에 의한 패스워드 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing) 발생 시 암호입력 실패 횟수를 적정하게 제한함으로써 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄일 수 있음.					
	*무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.					
보안대책						
판단기준	양호: 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우					
	취약: 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되지 않은 경우					
조치방법	계정 잠금 임계값을 5 이하로 설정					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	#cat /etc/default/login RETRIES=5 SunOS 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=5					
HP-UX	#cat /tcb/files/auth/system/default u_maxtries#5					
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS						
- SunOS 5.9 이하 버전 -						
1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후						
2. 아래와 같이 수정 또는, 신규 삽입						
(수정 전) #RETRIES=2						
(수정 후) RETRIES=5						
- SunOS 5.9 이상 버전 -						
1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후						

UNIX 서버

- 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 횟수 설정)
(수정 전) #RETRIES=2
(수정 후) RETRIES=5
- vi 편집기를 이용하여 "/etc/security/policy.conf" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 정책사용 설정)
(수정 전) #LOCK_AFTER_RETRIES=NO
(수정 후) LOCK_AFTER_RETRIES=YES

■ LINUX

- vi 편집기를 이용하여 "/etc/pam.d/system-auth" 파일을 연 후
- 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

옵션	설명
no_magic_root	root에게는 패스워드 잠금 설정을 적용하지 않음
deny=5	5회 입력 실패 시 패스워드 잠금
unlock_time	계정 잠금 후 마지막 계정 실패 시간부터 설정된 시간이 지나면 자동 계정 잠금 해제 (단위: 초)
reset	접속 시도 성공 시 실패한 횟수 초기화

■ AIX

- vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입
(수정 전) loginretries = 0
(수정 후) loginretries = 5

■ HP-UX

- vi 편집기를 이용하여 "/tcb/files/auth/system/default" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입
(수정 전) u_maxtries#
(수정 후) u_maxtries#5

※ HP-UX 서버에 계정 잠금 정책 설정을 위해서는 HP-UX 서버가 Trusted Mode로 동작하고 있어야하므로 Trusted Mode로 전환한 후 잠금 정책 적용

조치 시 영향

Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환이 필요함

UNIX 서버

취약점 항목		1.4. 패스워드 파일 보호			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-04
취약점 개요	패스워드 정보를 평문으로 저장하는 경우 정보 유출 피해가 발생할 수 있으므로 패스워드를 암호화하여 보호하여야 함. 쉘도우 패스워드를 사용하여 "/etc/shadow" 파일에 암호화된 패스워드가 저장되도록 하고 특별 권한이 있는 사용자들만 읽을 수 있도록 제한함.				
보안대책					
판단기준	양호: 쉘도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우				
	취약: 쉘도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우				
조치방법	패스워드 암호화 저장·관리 설정 적용				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX	1. /shadow 파일 존재 확인 (일반적으로 /etc디렉터리 내 존재) #ls /etc 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	1. /tcb 디렉터리 존재 확인 2. /etc/passwd 파일 내 두 번째 필드가 "x" 표시되는지 확인				
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX					
1. #pwconv ---> 쉘도우 패스워드 정책 적용 방법 2. #pwunconv ---> 일반 패스워드 정책 적용 방법					
■ AIX					
AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장·관리함					
■ HP-UX					
HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 "/tcb/files/auth" 디렉터리에 계정 이니셜과 계정 이름에 따라 파일로 저장·관리할 수 있으므로 Trusted Mode인지 확인 후 UnTrusted Mode인 경우 모드를 전환함					
1. Trusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행 #/etc/tsconvert 2. UnTrusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행 #/etc/tsconvert -r					
조치 시 영향	Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환 필요				

UNIX 서버

취약점 항목		1.5. root 이외의 UID가 '0' 금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-05
취약점 개요	root(UID=0)와 동일한 *UID(User Identification)를 가진 계정 존재 시 root 권한으로 시스템 접근이 가능하므로 root의 UID를 가진 계정이 존재하지 않도록 확인하여야 함. root뿐만 아니라 사용자 간 UID 중복 시에도 권한 중복으로 인한 사용자 감사 추적이 어렵게 되는 문제가 발생하므로 계정 및 UID 확인이 필요함.				
	*UID(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름.				
보안대책					
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				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, 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 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, HP-UX					
1. usermod 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정					
▪ SunOS, HP-UX의 경우 100 이상					
▪ LINUX의 경우 500 이상					
(예) test 계정의 UID를 2002 로 바꿀 경우					
#usermod -u 2002 test					
※ 각 OS별로 사용자 UID 체계가 달라 시스템 계정 및 일반 사용자 계정이 부여받는 값의 범위에 차이가 있으며, 공통적으로 관리자는 "UID=0"을 부여받음					
■ AIX					
1. chuser 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정					
(예) test 계정의 UID 를 2002 로 바꿀 경우					

UNIX 서버

#chuser id=2002 test

passwd 파일 구조

root:	x:	0:	1:	Super-User:	/:	/usr/bin/ksh
loginID:	x:	UID:	GID:	comment:	home_directory:	login_shell

(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

조치 시 영향 해당 계정에 관리자 권한이 필요하지 않으면 일반적으로 영향 없음

UNIX 서버

취약점 항목	1.6. root 계정 su 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-06
취약점 개요	권한이 없는 일반 사용자가 su 명령을 사용하여 로그인을 시도하고 패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)을 통해 root 권한을 획득할 수 있음. su 명령어 사용이 허용된 사용자만 root 계정으로 접속할 수 있도록 함.				
보안대책					
점검기준	양호: su 명령어를 특정 그룹에 속한 사용자만 사용하도록 제한되어 있는 경우				
	취약: su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우				
조치방법	일반 사용자의 su 명령 사용 제한 1. Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) 2. su 명령어의 그룹을 요청받은 그룹으로 변경 3. su 명령어의 권한 변경(4750) 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				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	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 2. wheel 그룹이 su 명령어를 사용할 수 있는지 설정 여부 확인 [SunOS] #ls -al /usr/bin/su #chgrp security su #chmod 4750 su [AIX] #cat /etc/security/user ---> default의 "sugroups=staff" 설정 확인 /etc/group 에서 staff 그룹에 해당하는 계정만 su 사용 가능 [HP-UX] #vi /etc/default/security ---> SU_ROOT_GROUP=wheel 설정 확인 3. 파일 권한 확인 #ls -l /usr/bin/su -rwsr-x--- /usr/bin/su (파일 권한이 4750인 경우 양호)				

UNIX 서버

OS별 점검 파일 위치 및 점검 방법

LINUX PAM
모듈 이용 시

1. "wheel" 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인
`#cat /etc/group`
`wheel:x:10:root,admin`
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_uid`

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX, HP-UX

1. wheel group 생성 (wheel 그룹이 존재하지 않는 경우)
`#groupadd wheel`
2. su 명령어 그룹 변경
`#chgrp wheel /usr/bin/su`
3. su 명령어 사용권한 변경
`#chmod 4750 /usr/bin/su`
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

1. wheel group 생성(wheel 그룹이 존재하지 않는 경우)
`#mkgroup wheel`
2. su 명령어 그룹 변경
`#chgrp wheel /usr/bin/su`
3. su 명령어 사용권한 변경
`#chmod 4750 /usr/bin/su`
4. wheel 그룹에 su 명령 허용 계정 등록
`#chgroup users=<user_name> wheel`
 (예) `chgroup users=admin wheel`

■ LINUX PAM 모듈을 이용한 설정 방법

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`

UNIX 서버

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 가능
----------------	--

UNIX 서버

취약점 항목		1.7. 패스워드 최소 길이 설정				
대상 OS		SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-07
취약점 개요		패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)을 피하기 위하여 패스워드 최소 길이가 설정되어 있는지 점검함. 패스워드 최소 길이가 설정되어 있지 않거나, 짧게 설정되어 있을 경우 쉽게 유추될 수 있음.				
보안대책						
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				
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS		#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

■ SunOS

1. vi 편집기를 이용하여 “/etc/default/passwd” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입

(수정 전) PASSLENGTH=6

(수정 후) PASSLENGTH=8

■ LINUX

1. vi 편집기를 이용하여 “/etc/login.defs” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입

(수정 전) PASS_MIN_LEN 6

(수정 후) PASS_MIN_LEN 8

■ AIX

1. vi 편집기를 이용하여 “/etc/security/user” 파일을 연 후

2. default: 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) minlen=4

(수정 후) minlen=8

UNIX 서버

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
 (수정 전) MIN_PASSWORD_LENGTH=
 (수정 후) MIN_PASSWORD_LENGTH=8

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.8. 패스워드 최대 사용기간 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-08
취약점 개요	패스워드 최대 사용기간을 설정하지 않은 경우 일정 기간 경과 후에도 유출된 패스워드로 접속이 가능함. 악의적인 사용자로부터 계속적인 접속을 차단하기 위해 패스워드 최대 사용기간을 설정하여 주기적으로 변경할 수 있도록 함.				
보안대책					
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				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#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

■ SunOS

1. vi 편집기를 이용하여 “/etc/default/passwd” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) MAXWEEKS=
(수정 후) MAXWEEKS=12 (단위: 주)

■ LINUX

1. vi 편집기를 이용하여 “/etc/login.defs” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) PASS_MAX_DAYS 99999
(수정 후) PASS_MAX_DAYS 90 (단위: 일)

■ AIX

1. vi 편집기를 이용하여 “/etc/security/user” 파일을 연 후

2. default: 부분을 아래와 같이 수정 또는, 신규 삽입
(수정 전) maxage=0
(수정 후) maxage=12 (단위: 주)

UNIX 서버

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) PASSWORD_MAXDAYS=99999
(수정 후) PASSWORD_MAXDAYS=90 (단위: 일)

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.9. 패스워드 최소 사용기간 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-09	
취약점 개요	패스워드 최소 사용기간을 설정하지 않은 경우 사용자에게 익숙한 패스워드로 변경이 가능하며, 이를 재사용함으로써 패스워드의 정기적인 변경은 무의미해질 수 있음. 이전 암호를 그대로 재사용하는 것을 방지하기 위해 최근 암호 기억 설정을 함께 적용하여 패스워드를 보호함.					
	보안대책					
판단기준	양호: 패스워드 최소 사용기간이 1일(1주)로 설정되어 있는 경우					
	취약: 패스워드 최소 사용기간이 설정되어 있지 않는 경우					
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	#cat /etc/default/passwd MINWEKS=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						
■ SunOS						
1. vi 편집기를 이용하여 "/etc/default/passwd" 파일을 연 후						
2. 아래와 같이 수정 또는, 신규 삽입 (수정 전) MINWEKS= (수정 후) MINWEKS=1 (단위: 주)						
■ LINUX						
1. vi 편집기를 이용하여 "/etc/login.defs" 파일을 연 후						
2. 아래와 같이 수정 또는, 신규 삽입 (수정 전) PASS_MIN_DAYS (수정 후) PASS_MIN_DAYS 1 (단위: 일)						
■ AIX						
1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후						
2. default 부분을 아래와 같이 수정 또는, 신규 삽입 (수정 전) minage=1						

UNIX 서버

(수정 후) minage=1 (단위: 주)

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
 (수정 전) PASSWORD_MINDAYS=
 (수정 후) PASSWORD_MINDAYS=1 (단위: 일)

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.10. 불필요한 계정 제거				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-10	
취약점 개요	OS나 Package 설치 시 Default로 생성되는 계정은 대부분 Default 패스워드를 사용하는 경우가 많으며 패스워드 추측공격에 악용될 수 있으므로 시스템에서 이용하지 않는 "lp, uucp, nuucp" 등의 Default 계정 및 의심스러운 특이한 계정의 존재 유무를 확인 후 삭제함. 또한, 관리되지 않은 불필요한 계정으로 인해 시스템 접속이 가능하므로 퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정은 제거해야 함. 특히, 장기간 패스워드가 변경되지 않은 미사용 계정은 반복적인 패스워드 추측 공격(Password Guessing)이 가능하고 해당 계정 정보의 유출 여부 확인이 어려움.					
보안대책						
판단기준	양호: 불필요한 계정이 존재하지 않는 경우					
	취약: 불필요한 계정이 존재하는 경우					
조치방법	현재 등록된 계정 현황 확인 후 불필요한 계정 삭제					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	1. 미사용 계정 및 의심스러운 계정 존재 여부 확인 (※ "passwd" 파일 구조: 부록 참조) #cat /etc/passwd 2. 사용하지 않는 Default 계정 점검 (lp, uucp, nuucp 계정 존재 확인 예시) #cat /etc/passwd egrep "lp uucp nuucp"					
LOG를 통한 확인	1. 로그인 실패 기록 점검을 통해 미사용 계정 및 의심스러운 계정 확인 #cat /var/adm/loginlog (SunOS, AIX, HP-UX) / #cat /var/log/loginlog (LINUX) #cat /var/adm/authlog (AIX, HP-UX) / #cat /var/log/authlog (SunOS) #cat /var/adm/sulog (SunOS, AIX, HP-UX) / #cat /var/log/sulog (LINUX) ※ 파일의 위치는 버전별 다를 수 있음					

위에 제시한 점검 방법에 의해 불필요한 계정 발견 시 아래의 보안설정방법에 따라 조치함

■ SunOS, LINUX, HP-UX

1. 서버에 등록된 불필요한 사용자 계정 확인

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

1. 서버에 등록된 불필요한 사용자 계정 확인

UNIX 서버

2. rmuser 명령으로 불필요한 사용자 계정 삭제

```
#rmuser <user_name>
```

기본적으로 차단하는 Default 계정 (※ 계정 설명: 부록 참조)

adm, lp, sync, shutdown, halt, news, uucp, operator, games, gopher, nfsnobody, squid 등

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.11. 관리자 그룹에 최소한의 계정 포함				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-11	
취약점 개요	시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근권한이 부여되어 있으므로 최소한의 계정만 등록되어 있어야 함. 해당 그룹 관리가 이루어지지 않으면 허가되지 않은 일반 사용자가 관리자의 권한으로 시스템에 접근할 수 있으며, 파일 수정 및 변경 등의 악의적인 작업으로 인해 시스템 운영에 피해를 줄 수 있음.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, HP-UX		#cat /etc/group (※ "group" 파일 구조: 부록 참조) root:x:0:root				
AIX		#cat /etc/group system:!:0:root				
불필요한 계정이 관리자 그룹에 포함되어 있는 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, HP-UX						
1. vi 편집기를 이용하여 "/etc/group" 파일을 연 후						
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						
1. vi 편집기를 이용하여 "/etc/group" 파일을 연 후						
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	일반적으로 영향 없음					

UNIX 서버

취약점 항목		1.12. 계정이 존재하지 않는 GID 금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-12
취약점 개요	미흡한 계정 그룹 관리로 인해 구성원이 없는 그룹이 존재할 경우 해당 그룹 소유의 파일이 비인가자에게 노출될 위험이 있음. 계정이 존재하지 않는 *GID(Group Identification) 설정을 관리자와 검토 후 제거하여야 함.				
	*GID(Group Identification): 다수의 사용자가 특정 개체를 공유할 수 있게 연계시키는 특정 그룹의 이름으로 주로 계정처리 목적으로 사용되며, 한 사용자는 여러 개의 GID를 가질 수 있음.				
보안대책					
판단기준	양호: 존재하지 않는 계정에 GID 설정을 금지한 경우				
	취약: 존재하지 않은 계정에 GID 설정이 되어있는 경우				
조치방법	구성원이 존재하지 않는 그룹이 있을 경우 관리자와 검토하여 제거				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX, AIX	<pre>#cat /etc/group (※ "group" 파일 구조: 부록 참조) gnats:x:41: shadow:x:42: utmp:x:43: video:x:44:administrador sasl:x:45: plugdev:x:46:haldaemon,administrador,xan,noa staff:x:50: games:x:60: users:x:100: nogroup:x:65534: dhcp:x:101: syslog:x:102: klog:x:103: scanner:x:104:cupsys,hplip,administrador,xan,noa nvram:x:105: messagebus:x:106: ssl-cert:x:107:cupsys</pre>				
LINUX,	<pre>#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 다음과 구조로 구성됨 [그룹명 : 패스워드 : 관리자, 관리자 ... : 멤버, 멤버 ...]</pre>				
구성원이 없는 그룹이 존재하는 경우 아래의 보안설정방법에 따라 그룹을 제거함					
■ SunOS, LINUX, AIX, HP-UX					
#groupdel <group_name>					
※ 구성원이 없거나, 더 이상 사용하지 않는 그룹명 삭제					
조치 시 영향	일반적으로 영향 없음				

UNIX 서버

취약점 항목		1.13. 동일한 UID 금지					
대상 OS		SunOS, LINUX, AIX, HP-UX		위험도	중	Code	U-13
취약점 개요		UNIX 시스템은 모든 사용자 계정에 UID를 부여하여 해당 UID로 사용자 이름, 패스워드, 홈 디렉터리 등과 같은 사용자 정보를 대응시킴. 만약 중복된 UID가 존재할 경우 시스템에서 동일한 사용자로 인식하여 문제가 발생할 수 있으며, 공격자에 의한 개인 정보 및 관련 데이터 유출 발생 시에도 감사 추적이 어렵게 됨.					
보안대책							
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					
보안설정방법							
OS별 점검 파일 위치 및 점검 방법							
SunOS, LINUX, AIX, HP-UX		#cat /etc/passwd (※ "passwd" 파일 구조: 부록 참조) <pre>[root@root root]# cat /etc/passwd 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</pre>					
동일한 UID를 갖는 계정이 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경함							
■ SunOS, 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		일반적으로 영향 없음					

UNIX 서버

취약점 항목		1.14. 사용자 shell 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-14	
취약점 개요	로그인이 필요 없는 계정을 이용해 시스템에 접근하여 사용자의 명령어를 해석하고 악용할 가능성이 있으므로, /bin/false *셸(Shell)을 부여해 로그인을 금지함.					
	*셸(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함.					
보안대책						
판단기준	양호: 로그인에 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되어 있는 경우					
	취약: 로그인에 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되지 않은 경우					
조치방법	로그인에 필요하지 않은 계정에 대해 /bin/false(nologin) 셸 부여					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	<pre>#cat /etc/passwd egrep "^daemon ^bin ^sys ^adm ^listen ^nobody ^nobody4 ^noaccess ^diag ^listen ^operator ^games ^gopher" grep -v "admin"</pre> <pre>games: x: 12: 100: games: /usr/games: /sbin/nologin gopher: x: 13: 30: gopher: /var/gopher: /sbin/nologin ftp: x: 14: 50: FTP User: /var/ftp: /sbin/nologin nobody: x: 99: 99: Nobody: /: /sbin/nologin nfsnobody: x: 65534: 65534: Anonymous NFS User: /var/lib/nfs: /sbin/nologin</pre>					
시스템에 불필요한 계정을 확인한 후 /bin/false(nologin) 셸이 부여되어 있지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 (※ 불필요한 계정은 시스템 용도에 따라 차이가 있음)						
■ SunOS, LINUX, AIX, HP-UX						
1. vi 편집기를 이용하여 "/etc/passwd" 파일을 연 후						
2. 로그인 셸 부분인 계정 맨 마지막에 /bin/false(nologin) 부여 및 변경						
(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

취약점 항목		1.15. Session Timeout 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX		위험도	하	Code	U-15
취약점 개요	계정이 접속된 상태로 방치될 경우 권한이 없는 사용자에게 중요시스템이 노출되어 악의적인 목적으로 사용될 수 있으므로 일정 시간 이후 어떠한 이벤트가 발생하지 않으면 연결을 종료하는 Session Timeout 설정이 필요함.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	#cat /etc/default/login TIMEOUT=600 export TMOUT					
LINUX, AIX, HP-UX	<sh, ksh, bash 사용 시> #cat /etc/profile(.profile) TIMEOUT=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 설정을 변경함

■ SunOS

1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
TIMEOUT=600 (단위: 초)
export TMOUT

■ LINUX, AIX, HP-UX

- sh(born shell), ksh(korn shell), bash(born again shell)을 사용하는 경우 -

1. vi 편집기를 이용하여 "/etc/profile(.profile)" 파일을 연 후

2. 아래와 같이 수정 또는, 추가
TIMEOUT=600 (단위: 초)
export TMOUT

UNIX 서버

- csh 을 사용하는 경우 -

1. vi 편집기를 이용하여 "/etc/csh.login" 또는, "/etc/csh.cshrc" 파일을 연 후
2. 아래와 같이 수정 또는, 추가
set autologout=10 (단위: 분)

조치 시 영향

모니터링 용도로 사용할 경우 해당 계정의 환경변수 파일에만 예외적으로 600초 이상의 시간 입력
(예) root 로 모니터링 할 경우 /.profile, /.bash_profile 등에 600초 이상 입력

UNIX 서버

2. 파일 및 디렉터리 관리

취약점 항목		2.1. root 홈, 패스 디렉터리 권한 및 패스 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-16
취약점 개요	root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 위치하고 있는 명령어가 실행될 수 있음. 즉 "."이 /usr/bin이나 /bin, /sbin 등 명령어들이 위치하고 있는 디렉터리보다 우선하여 위치하고 있을 경우, root 계정의 인가자가 특정 명령을 실행하면, 비인가자가 불법적으로 위치시킨 파일을 실행하여 예기치 않은 결과를 가져올 수 있음. 잘못된 PATH의 우선순위 등이 침해사고에 이용될 수 있으므로 "." 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가리키지 않도록 설정함.				
보안대책					
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 환경변수의 마지막으로 이동 "/etc/profile", root 계정의 환경변수 파일, 일반계정의 환경변수 파일을 순차적으로 검색하여 확인				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	#echo \$PATH /usr/local/sbin:/sbin:/usr/sbin:/bin:/usr/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 설정을 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				
/bin/bash	/etc/profile, \$HOME/.bash_profile				
※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨					

UNIX 서버

■ SunOS, LINUX, AIX, HP-UX

1. vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile)을 연 후

#vi /etc/profile

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

취약점 항목	2.2. 파일 및 디렉터리 소유자 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-17
취약점 개요	소유자가 존재하지 않는 파일 및 디렉터리는 현재 권한이 없는 자(퇴직, 전직, 휴직 등)의 소유였거나, 관리 소홀로 인해 생긴 파일일 가능성이 있음. 만약 중요 파일 및 디렉터리일 경우 문제가 발생할 수 있으므로 관리가 필요함.				
보안대책					
판단기준	양호: 소유자가 존재하지 않은 파일 및 디렉터리가 존재하지 않는 경우				
	취약: 소유자가 존재하지 않은 파일 및 디렉터리가 존재하는 경우				
조치방법	소유자가 존재하지 않은 파일 및 디렉터리 삭제 또는, 소유자 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, AIX	소유자가 nouser, nogroup인 파일이나 디렉터리 검색 #find / -nouser -o -nogroup -xdev -ls 2> /dev/null				
HP-UX	#find / ₩(-nouser -o -nogroup ₩) -xdev -exec ls -al {} ₩; 2> dev/null				
LINUX	#find / -nouser -print #find / -nogroup -print				
소유자가 nouser, nogroup인 파일이나 디렉터리 존재하는 경우 아래의 보안설정방법에 따라 디렉터리 및 파일 삭제 또는, 소유자 및 그룹을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제 #rm <file_name> #rm <directory_name> ※ 삭제할 파일명 또는, 디렉터리명 입력					
2. 필요한 경우 chown 명령으로 소유자 및 그룹 변경 #chown <user_name> <file_name>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.3. /etc/passwd 파일 소유자 및 권한 설정								
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-18				
취약점 개요	"/etc/passwd" 파일은 사용자의 ID, 패스워드(보안상 'x'로 표시), UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 중요 파일로 관리자 이외의 사용자가 "/etc/passwd" 파일에 접근 시 root 권한 획득이 가능하므로 해당 파일의 접근을 제한하여야 함.								
보안대책									
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)								
보안설정방법									
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일></td></tr></table>						OS별 점검 파일 위치 및 점검 방법		SunOS, LINUX, AIX, HP-UX	"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일>
OS별 점검 파일 위치 및 점검 방법									
SunOS, LINUX, AIX, HP-UX	"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일>								
"passwd" 파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 ■ SunOS, LINUX, AIX, HP-UX "/etc/passwd" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644, HP-UX 는 400) #chown root /etc/passwd #chmod 444 /etc/passwd									
조치 시 영향	일반적인 경우 영향 없음								

UNIX 서버

취약점 항목		2.4. /etc/shadow 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-19	
취약점 개요	"/etc/shadow" 파일은 시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리하고 있는 중요 파일로 root 계정을 제외한 모든 사용자의 접근을 제한하여야 함. 해당 파일에 대한 권한 관리가 이루어지지 않을 경우 ID 및 패스워드 정보가 외부로 노출될 수 있는 위험이 존재함.					
보안대책						
판단기준	양호: /etc/shadow 파일의 소유자가 root이고, 권한이 400인 경우					
	취약: /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400이 아닌 경우					
조치방법	"/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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

■ SunOS, LINUX

1. "/etc/shadow" 파일의 소유자 및 권한 확인

#ls -l /etc/shadow

2. "/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)

#chown root /etc/shadow

#chmod 400 /etc/shadow

■ AIX

AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장·관리하므로 해당 디렉터리 권한을 기준에 맞게 설정

1. /etc/security/passwd 디렉터리의 소유자 및 권한 확인

#ls -ld /etc/security/passwd

2. /etc/security/passwd 디렉터리의 소유자 및 권한 변경 (소유자 root, 권한 400)

#chown root /etc/security/passwd

#chmod 400 /etc/security/passwd

UNIX 서버

■ HP-UX

HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 "/tcb/files/auth" 디렉터리에 계정 이니셜과 계정명에 따라 파일로 저장·관리 가능

1. /tcb/files/auth 디렉터리의 소유자 및 권한 확인

```
#ls -ld /tcb/files/auth
```

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

취약점 항목		2.5. /etc/hosts 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-20	
취약점 개요	"/etc/hosts" 파일은 IP 주소와 호스트네임을 매핑 하는데 사용되는 파일이며, 이 파일의 접근권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 되므로 "/etc/hosts" 파일에 대한 접근권한을 제한하고 있는지 점검함.					
보안대책						
판단기준	양호: /etc/hosts 파일의 소유자가 root이고, 권한이 600인 경우					
	취약: /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우					
조치방법	"/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	"# ls -l /etc/hosts rw----- root <hosts 파일>					
"hosts" 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, 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	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		2.6. /etc/(x)inetd.conf 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-21	
취약점 개요	*인터넷 슈퍼데몬 서비스 설정파일인 inetd.conf(xinetd.d) 파일에 대한 접근권한 제한 여부를 점검함. Inetd.conf(xinetd.d)의 접근권한이 잘못 설정되어 있을 경우 비인가자가 악의적인 프로그램을 등록하고 root 권한으로 서비스를 실행시켜 기존 서비스에 영향을 줄 수 있음.					
	*인터넷 슈퍼데몬: 외부 네트워크의 요청이 있을 때 "/etc/inetd.conf"에 등록된 내부 프로그램인 인터넷 서비스들의 데몬을 실행시켜주는 역할을 함.					
보안대책						
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/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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.d 디렉터리 내 모든 파일>					
인터넷 슈퍼데몬 서비스 설정파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, AIX, HP-UX						
"/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)						
#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

취약점 항목		2.7. /etc/syslog.conf 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-22	
취약점 개요	"/etc/syslog.conf" 파일은 시스템 운영 중 발생하는 주요 로그 기록을 설정하는 파일로 관리자 이외의 사용자는 해당 파일을 변경할 수 없도록 하여야 함. 만약, 해당 파일의 접근권한이 적절하지 않을 경우 시스템 로그가 정상적으로 기록되지 않아 침입자의 흔적 또는, 시스템 오류 사항을 정확히 분석할 수 없음.					
보안대책						
판단기준	양호: /etc/syslog.conf 파일의 소유자가 root이고, 권한이 644인 경우					
	취약: /etc/syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644가 아닌 경우					
조치방법	"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	"/etc/syslog.conf" 파일의 소유자 및 권한 확인 #ls -l /etc/syslog.conf rw-r--r-- root <syslog.conf 파일>					
"syslog.conf" 파일의 소유자가 root가 아니거나 파일의 권한이 644가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, AIX, HP-UX						
"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)						
#chown root /etc/syslog.conf						
#chmod 644 /etc/syslog.conf						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		2.8. /etc/services 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-23
취약점 개요	서비스 관리를 위해 사용되는 /etc/services 파일이 일반 사용자에게 의해 접근 및 변경이 가능하면, 정상적인 서비스를 제한하거나 허용되지 않은 서비스를 악의적으로 실행시켜 침해사고를 발생시킬 수 있음. 따라서 소유자 권한 설정을 통해 접근을 제한하여야 함.				
보안대책					
판단기준	양호: /etc/services 파일의 소유자가 root이고, 권한이 644인 경우				
	취약: /etc/services 파일의 소유자가 root가 아니거나, 권한이 644가 아닌 경우				
조치방법	"/etc/services" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, 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 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, 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

취약점 항목		2.9. SUID, SGID, Sticky bit 설정파일 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-24	
취약점 개요	*SUID(Set User-ID)와 *SGID(Set Group-ID)가 설정된 파일은(특히, root 소유의 파일인 경우) 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있으며, 로컬 공격에 많이 이용되므로 보안상 철저한 관리가 필요함. root 소유의 SUID 파일의 경우에는 꼭 필요한 파일을 제외하고는 SUID, SGID 속성을 제거해주고, 잘못 설정되어 보안 위협이 되고 있는지 주기적인 진단 및 관리가 요구됨.					
	*SUID(Set User-ID): 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한을 얻게 됨.					
	*SGID(Set Group-ID): 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 됨.					
보안대책						
판단기준	양호: 주요 파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우					
	취약: 주요 파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우					
조치방법	1. 불필요한 SUID, SGID 파일 제거 2. 아래의 목록 이외에 애플리케이션에서 생성한 파일이나, 사용자가 임의로 생성한 파일 등 의심스럽거나 특이한 파일의 발견 시 SUID 제거 필요					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX		OS별 주요 파일에 대한 SUID/SGID 설정 여부 확인 #ls -all [check_file] awk '{print \$1}' grep -i 's'				
주요 파일에 불필요한 SUID/SGID가 설정된 경우 아래의 보안설정방법에 따라 SUID/SGID를 제거함						
■ SunOS, LINUX, AIX, HP-UX						
1. 제거 방법 #chmod -s <file_name>						
2. 주기적인 감사 방법 #find / -user root -type f ₩(-perm -04000 -o -perm -02000 ₩) -xdev -exec ls -al {} ₩;						
3. 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법 일반 사용자의 Setuid 사용을 제한함 (임의의 그룹만 가능) #/usr/bin/chgrp <group_name> <setuid_file_name> #/usr/bin/chmod 4750 <setuid_file_name>						

UNIX 서버

■ 아래의 표에서 파일명을 확인하여 SUID, SGID를 제거하여야 함

SunOS		
/usr/bin/admintool	/usr/dt/bin/dtprintinfo	/usr/sbin/arp
/usr/bin/at	/usr/dt/bin/sdtcm_convert	/usr/sbin/lpmove
/usr/bin/atq	/usr/lib/fs/ufs/ufsdump	/usr/sbin/prtconf
/usr/bin/atrm	/usr/lib/fs/ufs/ufsrestore	/usr/sbin/sysdef
/usr/bin/lpset	/usr/lib/lp/bin/netpr	/usr/sbin/sparcv7/prtconf
/usr/bin/newgrp	/usr/openwin/bin/ff.core	/usr/sbin/sparcv7/sysdef
/usr/bin/nispasswd	/usr/openwin/bin/kcms_calibrate	/usr/sbin/sparcv9/prtconf
/usr/bin/rdist	/usr/openwin/bin/kcms_configure	/usr/sbin/sparcv9/sysdef
/usr/bin/yppasswd	/usr/openwin/bin/xlock	
/usr/dt/bin/dtappgather	/usr/platform/sun4u/sbin/prtdiag	

LINUX		
/sbin/dump	/usr/bin/lpq-lpd	/usr/bin/newgrp
/sbin/restore	/usr/bin/lpr	/usr/sbin/lpc
/sbin/unix_chkpwd	/usr/bin/lpr-lpd	/usr/sbin/lpc-lpd
/usr/bin/at	/usr/bin/lprm	/usr/sbin/traceroute
/usr/bin/lpq	/usr/bin/lprm-lpd	

AIX		
/usr/dt/bin/dtaction	/usr/dt/bin/dtterm	/usr/bin/X11/xlock
/usr/sbin/mount	/usr/sbin/lchangelv	

HP-UX		
/opt/perf/bin/glance	/usr/dt/bin/dtprintinfo	/usr/sbin/swreg
/opt/perf/bin/gpm	/usr/sbin/arp	/usr/sbin/swremove
/opt/video/lbin/camServer	/usr/sbin/lanadmin	/usr/contrib/bin/traceroute
/usr/bin/at	/usr/sbin/landiag	/usr/dt/bin/dtappgather
/usr/bin/lpalt	/usr/sbin/lpsched	/usr/sbin/swmodify
/usr/bin/mediainit	/usr/sbin/swacl	/usr/sbin/swpackage
/usr/bin/newgrp	/usr/sbin/swconfig	
/usr/bin/rdist	/usr/sbin/swinstall	

조치 시 영향 SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요

UNIX 서버

취약점 항목	2.10. 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-25
취약점 개요	환경변수 파일의 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있으므로 홈 디렉터리 내의 환경변수 파일에 대한 접근 권한(읽기/쓰기/실행)의 적정성을 점검함.				
보안대책					
판단기준	양호: 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되어 있고, 홈 디렉터리 환경변수 파일에 root와 소유자만 쓰기 권한이 부여된 경우				
	취약: 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되지 않고, 홈 디렉터리 환경변수 파일에 root와 소유자 외에 쓰기 권한이 부여된 경우				
조치방법	환경변수 파일의 권한 중 타 사용자 쓰기 권한 제거 (".profile", ".kshrc", ".cshrc", ".bashrc", ".bash_profile", ".login", ".exrc", ".netrc" 등)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		홈 디렉터리 환경변수 파일의 소유자 및 권한 확인 #ls -l <홈 디렉터리 환경변수 파일>			
홈 디렉터리 환경변수 파일의 소유자가 root 또는, 해당 계정으로 설정되어 있는지 확인 후 소유자 이외의 사용자에게 쓰기 권한이 부여되어 있을 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX , HP-UX 1. 소유자 변경 방법 #chown <user_name> <file_name> 2. 일반 사용자 쓰기 권한 제거 방법 #chmod o-w <file_name>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.11. world writable 파일 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-26	
취약점 개요	모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일이 존재할 경우 일반 사용자의 실수 또는, 악의적인 행위로 인해 주요 파일 정보가 노출되거나 시스템 장애를 유발할 수 있음. 만약 의도적으로 변경된 스크립트 파일을 root가 확인하지 않고 실행시켰을 경우 시스템 권한 노출을 비롯해 다양한 보안 위험이 초래될 수 있음.					
보안대책						
판단기준	양호: world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우					
	취약: world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우					
조치방법	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX		world writable 파일 존재 여부 확인 #find / -perm -2 -ls				
“world writable” 파일 존재 시 사용 목적을 확실히 알고 불필요 시 삭제, 필요 시 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, AIX, HP-UX						
1. 일반 사용자 쓰기 권한 제거 방법 #chmod o-w <file_name>						
2. 파일 삭제 방법 #rm -rf <world-writable 파일명>						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		2.12. /dev에 존재하지 않는 device 파일 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-27	
취약점 개요	디바이스가 존재하지 않거나 이름이 잘못 입력된 경우 시스템은 */dev 디렉터리에 계속해서 파일을 생성하여 에러를 발생시킴. 따라서 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하여야 함.					
	* /dev 디렉터리: 논리적 장치 파일을 담고 있는 /dev 디렉터리는 /devices 디렉터리에 있는 물리적 장치 파일에 대한 심볼릭 링크임. 예를 들어 rmt0를 rmt로 잘못 입력한 경우 rmt0 파일이 새로 생성되는 것과 같이 디바이스 이름 입력 오류 시 root 파일 시스템이 에러를 일으킬 때까지 /dev 디렉터리에 계속해서 파일을 생성함.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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 보안설정방법에 따라 제거함						
■ SunOS, LINUX, AIX, HP-UX #find /dev -type f -exec ls -l {} \; 명령으로 확인 후 ※ major, minor number를 가지지 않는 device일 경우 삭제						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		2.13. \$HOME/.rhosts, hosts.equiv 사용 금지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-28	
취약점 개요	*r'command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있을 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 됨. 만약 사용이 불가피한 경우 /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root 또는, 해당 계정으로 설정한 뒤 권한을 600으로 설정하고 해당 파일 설정에 '+' 설정(모든 호스트 허용)이 포함되지 않도록 함. *r'command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음. *NET Backup: 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.					
	보안대책					
판단기준	양호: login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우 1. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우 2. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한이 600 이하인 경우 3. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우					
	취약: login, shell, exec 서비스를 사용하고, 위와 같은 설정이 적용되지 않은 경우					
조치방법	1. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자를 root 또는, 해당 계정으로 변경 2. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한을 600 이하로 변경 3. /etc/hosts.equiv 및 \$HOME/.rhosts 파일에서 "+"를 제거하고 반드시 필요한 호스트 및 계정만 등록 (해당 내역 요청)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	1. 파일 소유자 및 권한 확인 <pre>#ls -al /etc/hosts.equiv #ls -al \$HOME/.rhosts rw----- root <hosts.equiv 파일> rw----- root <\$HOME/.rhosts 파일></pre> 2. 계정 별 '+' 부여 적절성 확인 <pre>#cat /etc/hosts.equiv #cat \$HOME/.rhosts</pre> • /etc/hosts.equiv : 서버 설정 파일 • \$HOME/.rhosts : 개별 사용자의 설정 파일					
"/etc/hosts.equiv 및 \$HOME/.rhosts" 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함						

UNIX 서버

■ SunOS, LINUX, AIX, HP-UX

1. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일의 소유자를 root 또는, 해당 계정으로 변경
 #chown root /etc/hosts.equiv
 #chown <user_name> \$HOME/.rhosts
2. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일의 권한을 600 이하로 변경
 #chmod 600 /etc/hosts.equiv
 #chmod 600 \$HOME/.rhosts
3. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록
 #cat /etc/hosts.equiv (or \$HOME/.rhosts)

+ +	모든 호스트의 모든 계정을 신뢰
+ test	모든 호스트의 test 계정을 신뢰
Web1 +	Web1 호스트의 모든 계정을 신뢰

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		2.14. 접속 IP 및 포트 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-29	
취약점 개요	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고를 방지하기 위하여 TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정함.					
보안대책						
판단기준	양호: /etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근을 허용할 특정 호스트를 등록한 경우					
	취약: 위와 같이 설정되지 않은 경우					
조치방법	/etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근 허용 IP 등록					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX		All deny 적용 확인 및 접근 허용 IP 적절성 확인 #cat /etc/hosts.deny #cat /etc/hosts.allow				
HP-UX		All deny 적용 확인 및 서비스 접근 가능 IP 확인 #cat /var/adm/inetd.sec				

위에 제시한 파일이 존재하지 않거나 All deny 설정이 적용되지 않은 경우 또는, 시스템 접근 제한 IP 설정 필요 시 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX, AIX

1. vi 편집기를 이용하여 “/etc/hosts.deny” 파일을 연 후 (해당 파일이 없을 경우 새로 생성)

2. 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)

(수정 전) 설정 없음

(수정 후) ALL:ALL

3. vi 편집기를 이용하여 “/etc/hosts.allow” 파일을 연 후 (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 >

▪ /etc/hosts.deny --> 시스템 접근을 제한할 IP 설정

▪ /etc/hosts.allow --> 시스템 접근을 허용할 IP 설정

▪ not in either --> 모든 접근 허용

UNIX 서버

■ 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 복사하여 사용함

1. vi 편집기를 이용하여 "/var/adm/inetd.sec" 파일을 연 후 (해당 파일이 없을 경우 새로 생성)
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 접속 불가
----------------	-------------------

UNIX 서버

취약점 항목		2.15. hosts.lpd 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-30	
취약점 개요	* /etc/host.lpd 파일에 일반 사용자가 접근할 수 있다면 이 파일을 가지고 host 파일에 접근하여 공격을 할 수 있으므로 /etc/hosts.lpd 파일의 소유자와 퍼미션 설정을 확인하여야 함.					
	* host.lpd 파일: 로컬 프린트 서비스를 사용할 수 있는 허가된 호스트(사용자) 정보를 담고 있는 파일을 말함. (hostname 또는, IP 주소를 포함하고 있음)					
보안대책						
판단기준	양호: 파일의 소유자가 root이고 Other에 쓰기 권한이 부여되어 있지 않는 경우					
	취약: 파일의 소유자가 root가 아니고 Other에 쓰기 권한이 부여되어 있는 경우					
조치방법	host.lpd 파일의 퍼미션을 확인하여 퍼미션 600, 파일 소유자를 root로 변경					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX		#ls -l /etc/hosts.lpd rw----- root <hosts.lpd 파일>				
"hosts.lpd " 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, AIX, HP-UX						
1. 파일의 퍼미션 변경. #chmod 600 /etc/host.lpd						
2. 소유자를 root로 변경 #chown root /etc/host.lpd						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목	2.16. NIS 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-31
취약점 개요	NIS(Network Information Service) 주 서버는 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 할 수 있으며 사용자들은 패스워드를 한 번만 바꾸어 NIS 영역에 들어 있는 모든 컴퓨터의 정보를 갱신할 수 있음. 하지만 NIS 이용 시 서버 정보 유출 위험이 존재하는 등 보안에 취약함.				
보안대책					
판단기준	양호: 불필요한 NIS 서비스가 비활성화 되어있는 경우				
	취약: 불필요한 NIS 서비스가 활성화 되어있는 경우				
조치방법	NIS 서비스를 사용하지 않는 경우 NIS 서비스 비활성화				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX	NIS 서비스 활성화 여부 확인 #ps -ef grep yp				
불필요한 "NIS" 서비스가 실행중인 경우 아래의 보안설정방법에 따라 비활성화 상태로 변경함					
■ SunOS, LINUX, AIX					
1. NIS 서비스가 불필요하다면 비활성화 상태로 설정 - NIS 서비스 정지: #/usr/lib/netshvc/yp/ypstop - 서비스 확인: #ps -ef grep yp #rm -r /var/yp/blue.org #rm /etc/ethers /etc/netgroup /etc/timezone /etc/bootparams #vi /etc/nsswitch.conf					
2. NIS 설정 삭제					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.17. UMASK 설정 관리			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-32
취약점 개요	시스템 내에서 사용자가 새로 생성하는 파일의 접근권한은 *UMASK 값에 따라 정해짐. 현재 설정된 UMASK는 명령 프롬프트에서 "umask"를 수행하여 확인할 수 있으며 UMASK 값이 "027" 또는, "022"이기를 권장함.				
	UMASK 값 "027"은 "rw-r-----" 접근권한으로 파일이 생성됨. UMASK 값 "022"는 "rw-r--r--" 접근권한으로 파일이 생성됨. 계정의 Start Profile(/etc/profile, /etc/default/login, .cshrc, .kshrc, .bashrc, .login, .profile 등)에 명령을 추가하면, 사용자가 로그인 한 후에도 변경된 UMASK 값을 적용 받게 되며 잘못 설정된 UMASK 값은 잘못된 권한의 파일을 생성시킴. *UMASK: 파일 및 디렉터리 생성 시 기본 퍼미션을 지정해 주는 명령어를 말함.				
보안대책					
판단기준	양호: UMASK 값이 022 이하로 설정된 경우				
	취약: UMASK 값이 022 이하로 설정되지 않은 경우				
조치방법	설정파일에 UMASK 값을 "022"로 설정.				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, AIX, LINUX, HP-UX		#vi /etc/profile UMASK=022			

위에 제시한 UMASK 값이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 적용함

■ SunOS

방법-1. "/etc/profile" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입

umask 022

export umask

방법-2. "/etc/default/login" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입

(수정 전) #UMASK=022

(수정 후) UMASK=022

■ LINUX, HP-UX

1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후

UNIX 서버

2. 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

■ AIX

방법-1. "/etc/profile" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

방법-2. "/etc/security/user" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후
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

취약점 항목		2.18. 홈 디렉터리 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX		위험도	중	Code	U-33
취약점 개요	사용자 홈 디렉터리 내 설정파일이 비인가자에 의해 변조되면 정상적인 사용자 서비스가 제한됨, 해당 홈 디렉터리의 소유자 외 일반 사용자들이 해당 홈 디렉터리를 수정할 수 없도록 제한하고 있는지 점검하여 정상적인 사용자 환경 구성 및 서비스 제공 유무를 확인함.					
보안대책						
판단기준	양호: 홈 디렉터리 소유자가 해당 계정이고, 일반 사용자 쓰기 권한이 제거된 경우					
	취약: 홈 디렉터리 소유자가 해당 계정이 아니고, 일반 사용자 쓰기 권한이 부여된 경우					
조치방법	사용자별 홈 디렉터리 소유주를 해당 계정으로 변경하고, 타사용자의 쓰기 권한 제거 ("/etc/passwd" 파일에서 홈 디렉터리 확인, 진단 보고서에서 조치할 홈 디렉터리 확인)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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 적용된 경우 아래의 보안설정방법에 따라 적용함						
■ SunOS, 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	홈 디렉터리를 업로드 등의 용도로 애플리케이션에서 사용할 수 있기 때문에 권한 변경 시 확인이 필요함					

UNIX 서버

취약점 항목		2.19. 홈 디렉터리로 지정한 디렉터리의 존재 관리				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-34	
취약점 개요	사용자 홈 디렉터리는 사용자가 로그인한 후 작업을 수행하는 디렉터리임. 로그인 후 사용자 홈 디렉터리에 존재하는 사용자 환경 설정파일에 의해 사용자 환경이 구성되며 홈 디렉터리의 부재로 인한 다음의 보안상 문제가 발생할 수 있음. 1. 홈 디렉터리가 존재하지 않는 경우 root 계정이 아닌 일반 사용자의 홈 디렉터리가 /로 되어있을 경우 로그인 시 사용자 현재 디렉터리가 /로 로그인 되므로 관리·보안상 문제가 발생됨. 2. 홈 디렉터리 내에 숨겨진 디렉터리가 존재하는 경우 정당하지 못한 사용자가 파일을 숨길 목적으로 만들어 놓은 것일 수 있음. 3. 홈 디렉터리 내에 시스템 명령의 이름을 가진 불법적인 실행파일이 존재하는 경우 상대경로와 시스템 명령을 입력하여 불법적인 파일이 실행되게 함.					
	보안대책					
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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 보안설정방법에 따라 적용함						
■ SunOS, LINUX, AIX, HP-UX						
1. 홈 디렉터리가 없는 사용자 계정 삭제						
• SunOS, LINUX, HP-UX 설정: #userdel <user_name>						
• AIX 설정: #rmuser <user_name>						
2. 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정						
#vi /etc/passwd						
#test:x:501:501::/home/test:/bin/bash (/home/test=홈 디렉터리)						
#test:x:501:501::/data:/bin/bash (홈 디렉터리 수정 /home/test -> /data)						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		2.20. 숨겨진 파일 및 디렉터리 검색 및 제거			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-35
취약점 개요	불법적으로 생성되었거나 숨겨진 의심스러운 파일로부터 침입자는 정보 습득이 가능하며, 파일을 임의로 변경할 수 있음. [...]으로 시작하는 숨겨진 파일 존재 여부 확인 후 불법적이거나 의심스러운 파일을 삭제함.				
보안대책					
판단기준	양호: 디렉터리 내 숨겨진 파일을 확인하여, 불필요한 파일 삭제를 완료한 경우				
	취약: 디렉터리 내 숨겨진 파일을 확인하지 않고, 불필요한 파일을 방치한 경우				
조치방법	ls -al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭제함				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX,		특정 디렉터리 내 불필요한 파일 점검 #ls -al [디렉터리명]			
특정 디렉터리 내 숨겨진 파일을 확인한 후 불필요한 경우 파일 삭제를 권고함					
■ SunOS, LINUX, AIX, HP-UX					
1. 숨겨진 파일 목록에서 불필요한 파일 삭제					
2. 마지막으로 변경된 시간에 따라, 최근 작업한 파일 확인 시 [-t] 플래그 사용					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

3. 서비스 관리

취약점 항목		3.1. Finger 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-36	
취약점 개요	*Finger(사용자정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있으므로, 사용하지 않는다면 해당 서비스를 중지하여야 함.					
	*Finger(사용자정보 확인 서비스): who 명령어가 현재 사용 중인 사용자들에 대한 간단한 정보만을 보여주는 데 반해 finger 명령은 옵션에 따른 시스템에 등록된 사용자뿐만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌.					
보안대책						
판단기준	양호: Finger 서비스가 비활성화 되어 있는 경우					
	취약: Finger 서비스가 활성화 되어 있는 경우					
조치방법	Finger 서비스 비활성화					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전		#cat /etc/inetd.conf #finger stream tcp nowait bin /usr/sbin/fingerd fingerd 주석처리 확인				
SunOS 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 따라 서비스 중지						
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전						
1. "/etc/inetd.conf" 파일에서 finger 서비스 라인 #처리(주석처리) (수정 전) finger stream tcp nowait bin /usr/sbin/fingerd fingerd (수정 후) #finger stream tcp nowait bin /usr/sbin/fingerd fingerd						
2. inetd 서비스 재시작 #ps -ef grep inetd root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill -HUP [PID]						
■ SunOS 5.10 이상 버전						
inetadm -d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지 #inetadm -d svc:/network/finger:default						
■ LINUX (xinetd일 경우)						
1. vi 편집기를 이용하여 "/etc/xinetd.d/finger" 파일을 연 후						

UNIX 서버

2. 아래와 같이 설정 (Disable = yes 설정)

```

service finger
{
    socket_type      =    stream
    wait             =    no
    user             =    nobody
    server           =    /usr/sbin/in.fingerd
    disable         =    yes
}

```

3. xinetd 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		3.2. Anonymous FTP 비활성화				
대상 OS		SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-37
취약점 개요		*Anonymous FTP(익명 FTP)를 사용할 경우 악의적인 사용자가 시스템에 관한 정보를 획득할 수 있으며 디렉터리에 쓰기 권한이 설정되어 있을 경우 local exploit을 사용하여 다양한 공격이 가능하게 되므로 반드시 필요한 사용자만 접속 할 수 있도록 설정하여 권한 없는 사용자의 FTP 사용을 제한하여야 함. *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.				
보안대책						
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				
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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						
■ SunOS, LINUX, AIX, HP-UX						
1. 일반 FTP - Anonymous FTP 접속 제한 설정 방법						
"/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제						
▪ SunOS, LINUX, HP-UX 설정: #userdel ftp						
▪ AIX 설정: #rmuser ftp						
2. ProFTP - Anonymous FTP 접속 제한 설정 방법						
"/etc/passwd" 파일에서 ftp 계정 삭제						
▪ SunOS, LINUX, HP-UX 설정: #userdel ftp						
▪ AIX 설정: #rmuser ftp						
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

취약점 항목		3.3. r 계열 서비스 비활성화					
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-38		
취약점 개요	*r'command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있는 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 위험이 있음.						
	*r'command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음.						
	*NET Backup: 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.						
보안대책							
점검기준	양호: r 계열 서비스가 비활성화 되어 있는 경우						
	취약: r 계열 서비스가 활성화 되어 있는 경우						
조치방법	NET Backup등 특별한 용도로 사용하지 않는다면 아래의 서비스 중지						
	<table><tr><td>shell(514)</td><td>login(513)</td><td>exec(512)</td></tr></table>					shell(514)	login(513)
shell(514)	login(513)	exec(512)					
보안설정방법							
OS별 점검 파일 위치 및 점검 방법							
SunOS	r'command 서비스 활성화 여부 확인 #svcs -a grep rlogin						
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						
SunOS 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 계열" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지

■ SunOS

1. r 계열 서비스 활성화 여부 확인 후 비활성화 조치

#svcs -a |grep rlogin

#svcadm disable svc:/network/login:rlogin

■ AIX

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)

UNIX 서버

2. /etc/hosts.equiv 파일은 TRUSTED 시스템을 등록
3. .rhosts 파일은 사용자 별로 'r'command를 통해 접근이 가능하도록 설정할 수 있음(\$HOME/.rhosts)

■ HP-UX

1. r 계열 서비스 활성화 여부 확인
vi /etc/inetd.conf
2. r로 시작하는 필드 주석처리 후 재가동
inetd -c

■ SunOS 5.10 이상 버전

1. r'command 관련 데몬 확인

- svc:/network/login:rlogin
- svc:/network/rexec:default
- svc:/network/shell:kshell

2. inetadm -d "중지하고자 하는 데몬" 명령으로 데몬 중지
#inetadm -d svc:/network/login:rlogin
#inetadm -d svc:/network/rexec:default
#inetadm -d svc:/network/shell:kshell

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 rlogin, rsh, rexec 파일을 연 후
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/sbin/in.fingerd
    disable          = yes
}

```

3. xinetd 서비스 재시작
#service xinetd restart

조치 시 영향

rlogin, rshell, rexec 서비스는 backup 등의 용도로 종종 사용되며 /etc/hosts.equiv 또는, 각 홈 디렉터리 밑에 있는 .rhosts 파일에 설정 유무를 확인하여 해당 파일이 존재하지 않거나 해당 파일 내에 설정이 없다면 사용하지 않는 것으로 파악

UNIX 서버

취약점 항목		3.4. cron 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-39	
취약점 개요	*Cron 시스템은 cron.allow 파일과 cron.deny 파일을 통하여 명령어 사용자를 제한할 수 있으며 보안상 해당 파일에 대한 접근제한이 필요함. 만약 cron 접근제한 파일의 권한이 잘못되어 있을 경우 권한을 획득한 사용자가 악의적인 목적으로 임의의 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음.					
	*Cron 시스템: 특정 작업을 정해진 시간에 주기적이고 반복적으로 실행하기 위한 데몬과 그 설정들을 말함.					
보안대책						
판단기준	양호: cron 접근제어 파일 소유자가 root이고, 권한이 640 이하인 경우					
	취약: cron 접근제어 파일 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우					
조치방법	"cron.allow", "cron.deny" 파일 소유자 및 권한 변경 (소유자 root, 권한 640 이하)					
보안설정방법						
OS별 점검 방법						
SunOS, LINUX, AIX, HP-UX,	Cron 관련 파일 권한 확인 #ls -al <cron 접근제어 파일 경로> rw-r----- root <cron 접근제어 파일>					
OS별 점검 파일 위치						
LINUX, AIX, HP-UX	/var/spool/cron/crontabs/*					
SunOS	/etc/crontab, /etc/cron.daily/*, /etc/cron.hourly/*, /etc/cron.monthly/*, /etc/cron.weekly/*, /var/spool/cron/*					
"cron" 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS						
1. "/etc/cron.d/cron.allow" 및 "/etc/cron.d/cron.deny" 파일의 소유자 및 권한 확인						
#ls -l /etc/cron.d/cron.allow						
#ls -l /etc/cron.d/cron.deny						
2. "/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						
■ LINUX						
1. "/etc/cron.allow" 및 "/etc/cron.deny" 파일의 소유자 및 권한 확인						

UNIX 서버

```
#ls -l /etc/cron.allow
```

```
#ls -l /etc/cron.deny
```

2. "/etc/cron.allow" 및 "/etc/cron.deny" 파일의 소유자 및 권한 변경

```
#chown root /etc/cron.allow
```

```
#chmod 640 /etc/cron.allow
```

```
#chown root /etc/cron.deny
```

```
#chmod 640 /etc/cron.deny
```

■ AIX, HP-UX

1. "/var/adm/cron/cron.allow" 및 "/var/adm/cron/cron.deny" 파일의 소유자 및 권한 확인

```
#ls -l /var/adm/cron/cron.allow
```

```
#ls -l /var/adm/cron/cron.deny
```

2. "/var/adm/cron/cron.allow" 및 "/var/adm/cron/cron.deny" 파일의 소유자 및 권한 변경

```
#chown root /var/adm/cron/cron.allow
```

```
#chmod 640 /var/adm/cron/cron.allow
```

```
#chown root /var/adm/cron/cron.deny
```

```
#chmod 640 /var/adm/cron/cron.deny
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.5. DoS 공격에 취약한 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-40	
취약점 개요	*Dos(서비스 거부 공격)에 취약한 echo, discard, daytime, chargen 서비스는 취약점이 많이 발표된 불필요한 서비스들로 해당 서비스 사용을 중지하여야 함. 만약 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 Dos(서비스 거부 공격)의 대상이 될 수 있음.					
	*Dos(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격임. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨.					
보안대책						
점검기준	양호: Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 된 경우					
	취약: Dos 공격에 취약한 echo, discard, daytime, chargen 서비스 활성화 된 경우					
조치방법	echo, discard, daytime, chargen 서비스 비활성화 설정					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	#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					
SunOS 5.10 이상 버전	#inetadm grep enabled egrep "echo discard daytime chargen" 명령으로 기타 서비스 데몬 확인					
아래 제시된 DoS 공격에 취약한 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지						
DoS 공격에 취약한 서비스						
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					
chargen(19)	임의 길이의 문자열을 반환하는 서비스					

UNIX 서버

■ SunOS

1. echo 서비스 비활성화 설정

```
#svcs -a |grep echo
#svcadm disable svc:/network/echo:dgram
#svcadm disable svc:/network/echo:stream
```

2. discard 서비스 비활성화 설정

```
#svcs -a |grep daytime
#svcadm disable svc:/network/daytime:dgram
#svcadm disable svc:/network/daytime:stream
```

3. daytime 서비스 비활성화 설정

```
#svcs -a |grep discard
#svcadm disable svc:/network/discard:dgram
#svcadm disable svc:/network/discard:stream
```

4. chargen 서비스 비활성화 설정

```
#svcs -a |grep chargen
#svcadm disable svc:/network/chargen:dgram
#svcadm disable svc:/network/chargen:stream
```

■ AIX

1. vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
#vi /etc/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
```

■ HP-UX

1. vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
# vi /etc/inetd.conf
```

2. 필드 주석처리 후 재가동

```
# inetd -c
```

■ SunOS 5.10 이상 버전

1. 기타 서비스 데몬 확인

- | | |
|-------------------------------|-------------------------------|
| • svc:/network/echo:dgram | • svc:/network/daytime:dgram |
| • svc:/network/echo:stream | • svc:/network/daytime:stream |
| • svc:/network/discard:dgram | • svc:/network/chargen:dgram |
| • svc:/network/discard:stream | • svc:/network/chargen:stream |

UNIX 서버

2. `inetadm -d "중지하고자 하는 데몬"` 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/echo:stream
```

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 `/etc/xinetd.d/` 디렉터리 내 `echo`, `discard`, `daytime`, `chargen` 파일을 연 후

2. 아래와 같이 설정 (Disable = yes 설정)

```

• /etc/xinetd.d/echo 파일
• /etc/xinetd.d/discard 파일
• /etc/xinetd.d/daytime 파일
• /etc/xinetd.d/chargen 파일

service echo
{
    disable          = yes
    id               = echo-stream
    type             = INTERNAL
    wait             = no
    socket_type      = stream
}
```

3. `xinetd` 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	일반적으로 사용하지 않는 서비스들임
----------------	---------------------

UNIX 서버

취약점 항목	3.6. NFS 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-41
취약점 개요	*NFS(Network File System) 서비스는 root 권한 획득을 가능하게 하는 등 침해사고 위험성이 높으므로 사용하지 않는 경우 중지함.				
	*NFS(Network File System):원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임.				
보안대책					
판단기준	양호: NFS 서비스 관련 데몬이 비활성화 되어 있는 경우				
	취약: 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				
	1. /etc/dfs/dfstab의 모든 공유 제거				
	2. NFS 데몬(nfsd, statd, mountd) 중지				
	3. 시동 스크립트 삭제 또는, 스크립트 이름 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NFS 서비스 데몬 확인 (NFS 동작 SID 확인) #ps -ef grep nfsd root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd				
SunOS 5.10 이상 버전	#inetadm egrep "nfs statd lockd"				
불필요한 "NTFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지					
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전					
NFS 서비스 데몬 중지					
#kill -9 [PID]					
■ SunOS 5.10 이상 버전 설정 방법					
1. NFS 서비스 데몬 확인					
svc:/network/nfs/server:default					
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

취약점 항목		3.7. NFS 접근통제				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-42	
취약점 개요	*NFS(Network File System) 사용 시 허가된 사용자만 접속할 수 있도록 접근제한 설정을 하여야 함. 접근제한 설정이 적절하게 이루어지지 않을 경우 비인가자의 root 권한 획득이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있음.					
	*NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임.					
보안대책						
판단기준	양호: NFS 서비스를 사용하지 않거나, 사용 시 everyone 공유를 제한한 경우					
	취약: NFS 서비스를 사용하고 있고, everyone 공유를 제한하지 않은 경우					
조치방법	사용하지 않는다면 NFS 서비스 중지, 사용할 경우 NFS 설정파일에 everyone 공유 설정 제거					
보안설정방법						
< 서비스 필요 시 >						
불가피하게 NFS 서비스를 사용하여야 하는 경우 NFS 접근제어 파일에 꼭 필요한 공유 디렉터리만 나열하고, everyone으로 시스템이 마운트 되지 않도록 설정						
OS 종류별 NFS 접근제어 파일						
SunOS, HP-UX의 경우		"/etc/dfs/dfstab, /etc/dfs/sharetab 파일				
LINUX, AIX, HP-UX의 경우		"/etc/exports" 파일				
■ /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:client2 /export/home/test						
※ 읽기(ro), 쓰기(rw) 권한에 각각 사용자를 설정하여야 읽기, 쓰기 권한 모두 제한 가능						
■ /etc/exports 설정 예문						
1. everyone으로 시스템 마운트 금지						
#showmount -e hostname 명령어로 확인						
2. /etc/exports 파일에 접근 가능한 호스트명 추가						
(예) /stand host1 host2						
3. NFS 서비스 재구동						
#/etc/exportfs -u						
#/etc/exportfs -a						

UNIX 서버

< 서비스 불필요 시 >

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NFS 서비스 데몬 확인 (NFS 동작 SID 확인) #ps -ef grep nfsd <i>root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd</i>
SunOS 5.10 이상 버전	#inetadm egrep "nfs statd lockd"

불필요한 "NFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

NFS 서비스 데몬 중지

#kill -9 [PID]

■ SunOS 5.10 이상 버전

1. NFS 서비스 데몬 확인

```
svc:/network/nfs/server:default
```

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

취약점 항목		3.8. automountd 제거				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-43	
취약점 개요	*automountd 데몬에는 로컬 공격자가 데몬에 *RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하여 이를 통해 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음.					
	*automountd: 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능을 말함.					
	*RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.					
보안대책						
판단기준	양호: automountd 서비스가 비활성화 되어 있는 경우					
	취약: automountd 서비스가 활성화 되어 있는 경우					
조치방법	automountd 서비스 비활성화					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	automountd 서비스 데몬 확인 (automountd 동작 SID 확인) #ps -ef grep automount root 1131 1 0 Jun 15 ? 32:11 /usr/sbin/automountd					
SunOS 5.10 이상 버전	automountd 서비스 데몬 확인 #svcs -a egrep "autofs"					
"automountd" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지						
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전						
automountd 서비스 데몬 중지 #kill -9 [PID]						
■ SunOS 5.10 이상 버전						
1. autofs 서비스 데몬 확인						
svc:/system/filesystem/autofs:default						
2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지						
#svcadm disable svc:/system/filesystem/autofs:default						
조치 시 영향	NFS 및 *삼바(Samba) 서비스에서 사용 시 automountd 사용 여부 확인이 필요하며, 적용 시 CDROM의 자동 마운트는 이뤄지지 않음 (/etc/auto.*, /etc/auto_* 파일을 확인하여 필요 여부 확인)					
	*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

취약점 항목		3.9. RPC 서비스 확인				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-44	
취약점 개요	*RPC (Remote Procedure Call) 서비스는 분산처리 환경에서 개발을 하는 데 있어 많은 이점을 제공하지만, 아래와 같은 서비스들은 버퍼 오버플로우(Buffer Overflow) 취약성이 다수 존재하여 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 함. rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.yppupdated, rpc.rquotad, kcms_server, cachefs					
	*RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.					
	보안대책					
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)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
LINUX, AIX, HP-UX, SunOS 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]					
SunOS 5.10 이상 버전	RPC 서비스 관련 데몬 확인 #inetadm grep rpc grep enabled egrep "ttldbserver rex rstat rusers spray wall rquota"					
불필요한 "RPC" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지						
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전						
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 (수정 후) #rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd						
2. inetd 서비스 재시작 #ps -ef grep inetd root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill -HUP 141						

UNIX 서버

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내의 불필요한 RPC 서비스 파일을 연 후
2. 아래와 같이 설정 (Disable = yes 설정)

```
service finger
{
    disable          = yes
    socket_type      = stream
    wait            = no

    - 이하 생략 -
}
```

3. xinetd 서비스 재시작
#service xinetd restart

■ SunOS 5.10 이상 버전

1. 불필요한 rpc 서비스 관련 데몬 확인

• svc:/network/rpc/cde-ttdbserver:tcp	• svc:/network/rpc/spray:default
• svc:/network/rpc/rex:default	• svc:/network/rpc/wall:default
• svc:/network/rpc/rstat:default	• svc:/network/fs/rquota:default
• svc:/network/rpc/rusers:default	- 이하 생략 -

2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지
#inetadm -d svc:/network/rpc/rusers:default

UNIX 서버

불필요한 RPC 서비스	
rpc.cmsd	데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용
rusersd	rusers 명령의 조회에 응답
rstatd	커널에서 얻은 성능 통계 리턴
rpc.ttdbserverd	시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램 지원
kcms_server	kodak color management 관련된 api 와 라이브러리들은 데스크탑의 디지털 이미지들의 컬러 퍼포먼스를 컨트롤할 수 있는 Profile를 만들거나 관리하기 위해 사용
rpc.ttdbserverd	RPC 기반의 ToolTalk 데이터베이스 서버 프로그램
Walld	다른 사용자들에게 메시지 발송
rpc.nids	NIS+ server Daemon
rpc.yppupdated	Network Information Services(NIS) 맵 정보 갱신
cachedfsd	Cache 파일 시스템 데몬
sadmind	remote로부터의 시스템 관리
sprayd	지정된 수의 패킷을 호스트에 전송하고 성능 통계를 보고하는 spray 명령에 의해 전송된 패킷 수신
rpc.pcnfsd	PC-NFS (개인용 컴퓨터 네트워크 파일 시스템) 클라이언트에서의 서비스 요청 처리
rexid	원격 시스템용 프로그램 실행
rpc.rquotad	리모트 머신에 NFS mount 되고 있는 파일 시스템에 대해 사용자에게 대한 로컬 머신에서의 할당 제한치를 반환
조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

취약점 항목		3.10. NIS, NIS+ 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-45
취약점 개요	*NIS(Network Information Service)는 중요한 시스템 데이터베이스 파일들을 네트워크를 통하여 공유하며, NIS+는 보안 및 편의 기능들을 추가한 그 후의 버전임. 보안상 취약한 서비스인 NIS, NIS+를 사용하는 경우 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보다 NIS+를 사용하는 것을 권장함. *NIS(Network Information Service) 주 서버는 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 함. 네트워크를 통한 공유로부터 관리자와 사용자들에게 일관성 있는 시스템 환경을 제공함.				
	보안대책				
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				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NIS, NIS+ 서비스 구동 확인 #ps -ef egrep "ypserv ypbind ypxfrd rpc.yppasswdd rpc.yupdated" grep -v "grep" root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv				
SunOS 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				
rpc.yppasswdd	사용자들이 패스워드를 변경하기 위해 사용				
ypxfrd	NIS 마스터 서버에서만 실행되며 고속으로 NIS 맵 전송				
rpc.yupdated	NIS 마스터 서버에서만 실행되며 고속으로 암호화하여 NIS 맵 전송				

UNIX 서버

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

NFS 서비스 데몬 중지

```
#kill -9 [PID]
```

■ SunOS 5.10 이상 버전

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
```

2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#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
```

조치 시 영향	일반적으로 영향 없음
---------	-------------

UNIX 서버

취약점 항목		3.11. tftp, talk 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-46	
취약점 개요	운영체제는 ftp, tftp, telnet, talk 등의 서비스를 포함하고 있으므로 시스템 운영에 필요하지 않는 불필요한 서비스를 제거하여 보안성을 높일 수 있고 해당 불필요한 서비스 취약점 발견으로 인한 피해를 최소화할 수 있음.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	불필요한 서비스 데몬 확인 #ps -ef egrep "tftp talk" root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.tftpd					
LINUX (xinetd)	tftp, talk, ntalk 서비스 활성화 여부 확인 #vi /etc/xinetd.d/tftp #vi /etc/xinetd.d/talk #vi /etc/xinetd.d/ntalk					
SunOS 5.10 이상 버전	서비스 데몬 확인 #inetadm egrep "tftp talk"					

불필요한 "tftp, talk, ntalk" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지

불필요한 서비스 데몬	
tftp(69)	파일 전송을 위한 프로토콜. tftp 프로토콜은 OS에서는 부팅 디스켓이 없는 워크스테이션이나 네트워크 인식 프린터를 위한 설정파일의 다운로드, 설치 프로세스의 시작을 위해 사용
talk(517)	사용자가 시스템에 원격으로 연결하여 다른 시스템에 로그인하고 있는 사용자와 대화 세션을 시작할 수 있음
ntalk(518)	서로 다른 시스템 간에 채팅을 가능하게 하는 서비스

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

불필요한 서비스 데몬 중지

#kill -9 [PID]

UNIX 서버

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk 파일을 연 후
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
}

```

3. xinetd 서비스 재시작
#service xinetd restart

■ SunOS 5.10 이상 버전

1. 불필요한 서비스 데몬 확인

```

svc:/network/tftp:default
svc:/network/talk:default
svc:/network/ntalk:default

```

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	일반적으로 영향 없음
---------	-------------

UNIX 서버

취약점 항목		3.12. Sendmail 버전 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-47	
취약점 개요	Sendmail은 널리 쓰이는 만큼 많은 취약점이 알려져 있어 공격에 목표가 되기 쉬우므로 서버에서 Sendmail을 사용하는 목적을 검토하여 사용할 필요가 없는 경우, 서비스를 제거하는 것이 바람직함. 만일 운영할 필요가 있다면 취약점이 없는 Sendmail 버전을 유지하고 취약점에 대한 패치가 발표되었을 시 빠른 시기에 이를 적용하도록 함. 그렇지 않을 경우 버퍼 오버플로우(Buffer Overflow)의 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있음.					
보안대책						
판단기준	양호: Sendmail 버전이 8.13.8 이상인 경우					
	취약: Sendmail 버전이 8.13.8 이상이 아닌 경우					
조치방법	Sendmail 서비스를 사용하지 않을 경우 서비스 중지, 재부팅 후 다시 시작하지 않도록 시작 스크립트 변경, 사용할 경우 패치 관리 정책을 수립하여 주기적으로 패치 적용 ※ Sendmail 서비스의 경우 8.13.8 이하 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용함					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX	1. Sendmail 서비스 실행 여부 점검 #ps -ef grep sendmail 2. Sendmail 버전 점검 #telnet localhost 25					
"Sendmail" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지 또는, 버전 업그레이드						
■ SunOS, 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

취약점 항목		3.13. 스팸 메일 릴레이 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-48
취약점 개요	*SMTP(Simple Mail Transfer Protocol) 서버의 릴레이 기능을 제한하지 않을 경우 스팸 메일 서버로 악용되거나, 서버의 부하가 증가할 수 있음. 따라서 인증된 사용자에게 메일을 보낼 수 있도록 설정하거나 불필요 시 SMTP 서비스를 중지하여야 함.				
	*SMTP(Simple Mail Transfer Protocol) 서버: 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 SMTP라고 하며, SMTP에 의해 전자 메일을 발신하는 서버(server)를 SMTP 서버라고 함.				
보안대책					
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				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, 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\$W*" grep "Relaying denied" R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"				
AIX	#ps -ef grep sendmail grep -v "grep" #cat /etc/sendmail.cf grep "R\$W*" grep "Relaying denied" R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"				
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
OS 종류별 sendmail.cf 설정파일 위치					
AIX의 경우	"/etc/sendmail.cf" 파일				
SunOS, LINUX, HP-UX의 경우	"/etc/mail/sendmail.cf" 파일				
■ SunOS, LINUX, HP-UX					
1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후					
2. 아래와 같이 주석 제거					
(수정 전) #R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"					
(수정 후) R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"					
3. 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인					
#cat /etc/mail/access					

UNIX 서버

■ AIX

1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후
2. 아래와 같이 주석 제거
 (수정 전) #R\$* \$#error \$@ 5.7.1 \$: "550 Relaying denied"
 (수정 후) R\$* \$#error \$@ 5.7.1 \$: "550 Relaying denied"
3. 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인
 #cat /etc/sendmail.cf

조치 시 영향	릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음
----------------	---------------------------------

UNIX 서버

취약점 항목		3.14. 일반사용자의 Sendmail 실행 방지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-49	
취약점 개요	SMTP 서비스 사용 시 일반 사용자의 q 옵션을 사용한 Sendmail 실행을 방지하여 메일큐 내용과 sendmail 설정을 보거나, 메일큐를 강제로 drop 시킬 수 있는 기능을 막아야 함. 그렇지 않을 경우 비인가자에 의한 SMTP 서비스 오류 발생이 가능함.					
	*SMTP(Simple Mail Transfer Protocol): 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 말함.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, 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				
AIX		#ps -ef grep sendmail grep -v "grep" #grep -v '^ *#' /etc/sendmail.cf grep PrivacyOptions				
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함						
OS 종류별 sendmail.cf 설정파일 위치						
AIX의 경우		"/etc/sendmail.cf" 파일				
SunOS, LINUX, HP-UX의 경우		"/etc/mail/sendmail.cf" 파일				
■ SunOS, LINUX, AIX, HP-UX						
1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후						
2. O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가 (수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn (수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun						
3. Sendmail 서비스 재시작						
조치 시 영향	옵션 적용 시에는 일반적으로 영향 없음					

UNIX 서버

취약점 항목		3.15. DNS 보안 버전 패치				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-50	
취약점 개요	*BIND(Berkeley Internet Name Domain)는 BIND 9.5.0 버전이 나왔으며 이하 버전에서는 많은 취약점이 존재함. BIND 8.x는 BIND의 distribution을 Sendmail의 버전과 일치시키기 위해 사용하는 새로운 버전 번호로 BIND 4의 Production version에 비하여 안정성, 성능, 보안성 등이 향상되었으나, BIND 8.3.4 이하 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재함. *BIND(Berkeley Internet Name Domain): BIND는 BSD 기반의 유닉스 시스템을 위해 설계된 DNS로 서버와 resolver 라이브러리로 구성되어 있음. 네임서버는 클라이언트들이 이름 자원들이나 객체들에 접근하여, 네트워크 내의 다른 객체들과 함께 정보를 공유할 수 있게 해주는 네트워크 서비스로 사실상 컴퓨터 네트워크 내의 객체들을 위한 분산 데이터베이스 시스템.					
	보안대책					
판단기준	양호: DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우 취약: DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우 [취약점이 존재하지 않는 버전] 8.4.6, 8.4.7, 9.2.8-P1, 9.3.4-P1, 9.4.1-P1, 9.5.0a6					
	DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용할 경우 패치 관리 정책을 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 파악하여 주기적인 패치 적용 정책 수립 후 적용					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, LINUX, AIX, HP-UX		DNS 서비스 사용 및 BIND 버전 확인 #ps -ef grep named named -v				
“DNS” 서비스를 사용하지 않는 경우 서비스 중지						
“DNS” 서비스 사용 시 BIND 버전 확인 후 아래의 보안설정방법에 따라 최신 버전으로 업데이트						
■ SunOS, LINUX, AIX, HP-UX						
1. BIND는 거의 모든 버전이 취약한 상태로써 최신 버전으로 업데이트가 요구됨						
2. 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						
• solinger버그 (Denial of Service) : BIND 8.1 이상버전						

UNIX 서버

- 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
 - maxcname bug Denial of service 취약점

※ BIND Vulnerability matrix : <http://www.isc.org/sw/bind/bind-security.php#matrix>

조치 시 영향	패치를 적용 시 시스템 및 서비스 영향 정도를 충분히 고려하여야 함
----------------	---------------------------------------

UNIX 서버

취약점 항목		3.16. DNS Zone Transfer 설정							
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-51				
취약점 개요	DNS Zone Transfer는 Primary Name Server와 Secondary Name Server 간에 Zone 정보를 일관성 있게 유지하기 위하여 사용하는 기능으로 Secondary Name Server로만 Zone 정보를 전송하도록 제한하여야 함. 만약 허가되지 않는 사용자에게 Zone Transfer를 허용할 경우 공격자는 전송받은 Zone 정보를 이용하여 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있음.								
보안대책									
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 DNS설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정								
보안설정방법									
< DNS 서비스를 사용할 경우 > <table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>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"</td></tr></table> "DNS" 서비스 사용 시 위에 제시된 파일의 DNS 설정을 아래의 보안설정방법에 따라 수정함 ■ BIND8 DNS 설정(named.conf) 수정 예 options { allow-transfer {존 파일 전송을 허용하고자 하는 IP;}; ■ BIND4.9 DNS 설정(named.boot) 수정 예 options xfrnets 허용하고자 하는 IP < DNS 서비스를 사용하지 않는 경우 >						OS별 점검 파일 위치 및 점검 방법		SunOS, 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"
OS별 점검 파일 위치 및 점검 방법									
SunOS, 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"								

UNIX 서버

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	DNS 서비스 데몬 확인 (DNS 동작 SID 확인) <pre>#ps -ef grep named</pre> <pre>root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named</pre>
SunOS 5.10 이상 버전	<pre>#svcs -a egrep "dns"</pre>
“DNS” 서비스를 사용하지 않는 경우 서비스 데몬 중지 ■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전 DNS 서비스 데몬 중지 <pre>#kill -9 [PID]</pre> ■ SunOS 5.10 이상 버전 1. DNS 서비스 데몬 확인 <pre>enabled 16:22:31 svc:/network/dns/server:default</pre> 2. svcadm disable “중지하고자 하는 데몬” 명령으로 서비스 데몬 중지 <pre>#svcadm disable svc:/network/dns/server:default</pre>	
조치 시 영향	Zone 파일 전송을 허용할 대상을 정상적으로 등록할 경우 일반적으로 영향 없음

UNIX 서버

취약점 항목		3.17. Apache 디렉터리 리스팅 제거			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-52
취약점 개요	디렉터리 검색은 디렉터리 요청 시 해당 디렉터리에 기본 문서가 존재하지 않을 경우 디렉터리 내 모든 파일의 목록을 보여주는 기능임. 디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 디렉터리 내의 모든 파일에 대한 접근이 가능하여 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일 등 공개되어서는 안 되는 중요 파일 노출이 가능함.				
보안대책					
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)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Indexes 옵션 사용 여부 확인 #vi /[Apache_home]/conf/httpd.conf Options <i>Indexes FollowSymLinks</i>				

위에 제시한 파일에 "Indexes" 옵션이 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경

■ SunOS, LINUX, AIX, HP-UX

1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
#vi /[Apache_home]/conf/httpd.conf

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

(수정 후) Option 지시자에 Indexes 옵션 제거 후 저장

```
<Directory />
  Options FollowSymLinks
  AllowOverride None
  Order allow, deny
  Allow from all

</Directory>
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.18. Apache 웹 프로세스 권한 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-53	
취약점 개요	UNIX 시스템의 경우 Web 서버 데몬이 root 권한으로 운영될 경우 Web Application의 취약점 또는, 버퍼 오버플로우(Buffer Overflow)로 인하여 root 권한을 획득할 수 있으므로 서버 데몬이 root 권한으로 운영되지 않도록 관리하여야 함.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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

■ SunOS, LINUX, AIX, HP-UX

1. 데몬 User & Group 변경

User & Group 부분에 root가 아닌 별도 계정으로 변경

User [root가 아닌 별도 계정명]

Group [root가 아닌 별도 계정명]

3. Apache 서비스 재시작

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		3.19. Apache 상위 디렉터리 접근 금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-54
취약점 개요	상위경로로 이동하는 것이 가능할 경우 하위경로에 접속하여 상위경로로 이동함으로써 해킹을 당할 위험이 있으며, 유니코드 버그(Unicode Bug) 및 서비스 거부 공격에 취약해지기 쉬우므로 "." 와 같은 상위경로로 이동이 가능한 문자사용이 불가능하도록 설정할 것을 권장함. Apache는 특정 디렉터리 내에 존재하는 파일들을 호출할 때 사용자 인증을 수행하도록 설정할 수 있음. 따라서 해당 설정을 이용하여 중요 파일 및 데이터 접근은 허가된 사용자만 가능하도록 제한함.				
보안대책					
판단기준	양호: 상위 디렉터리에 이동제한을 설정한 경우				
	취약: 상위 디렉터리에 이동제한을 설정하지 않은 경우				
조치방법	1. 사용자 인증을 하기 위해서 각 디렉터리 별로 httpd.conf 파일 내 AllowOverride 지시자의 옵션 설정을 변경 (None에서 AuthConfig 또는, All로 변경) 2. 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 3. 사용자 인증 계정 생성: htpasswd -c <인증 파일> <사용자 계정>				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, 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					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
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 </Directory>					
(수정 후) AllowOverride 지시자에 AuthConfig 옵션이 설정되어 있음					

UNIX 서버

```
<Directory "/usr/local/apache2/htdocs">
```

```
    AllowOverride AuthConfig
    Allow from all
```

```
</Directory>
```

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
```

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

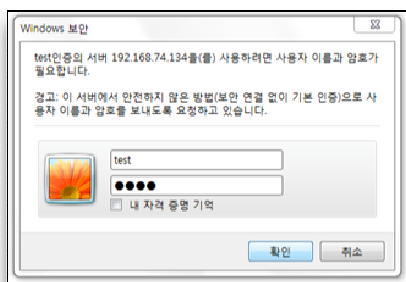
4. 사용자 인증에 사용할 아이디 및 패스워드 생성

```
#htpasswd -c /usr/local/apache/test/.auth test
```

```
New password:
Re-type new password:
Adding password for user test
```

```
[root@localhost apache]#
```

5. 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작
6. 사용자 인증을 설정한 디렉터리 내 파일 호출 화면



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

취약점 항목		3.20. Apache 불필요한 파일 제거								
대상 OS	SunOS, LINUX, AIX, HP-UX		위험도	상	Code	U-55				
취약점 개요	웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 외부 침입자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거하여야 함.									
보안대책										
판단기준	양호: 매뉴얼 파일 및 디렉터리가 제거되어 있는 경우									
	취약: 매뉴얼 파일 및 디렉터리가 제거되지 않은 경우									
조치방법	매뉴얼 파일 및 디렉터리 제거 ("/[Apache_home]/htdocs/manual", "/[Apache_home]/manual" 파일 제거)									
보안설정방법										
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>매뉴얼 및 디렉터리 존재 여부 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual</td></tr></table>							OS별 점검 파일 위치 및 점검 방법		SunOS, LINUX, AIX, HP-UX	매뉴얼 및 디렉터리 존재 여부 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual
OS별 점검 파일 위치 및 점검 방법										
SunOS, LINUX, AIX, HP-UX	매뉴얼 및 디렉터리 존재 여부 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual									
위에 제시한 매뉴얼 파일 및 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 매뉴얼 파일 및 디렉터리 제거 또는, 설정을 변경함										
■ SunOS, LINUX, AIX, HP-UX										
1. #ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거 #rm -rf /[Apache_home]/htdocs/manual #rm -rf /[Apache_home]/manual										
2. #ls 명령어로 정상적인 제거 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual										
조치 시 영향	일반적인 경우 영향 없음									

UNIX 서버

취약점 항목		3.21. Apache 링크 사용금지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-56	
취약점 개요	일부 서버는 *심볼릭 링크(Symbolic link)를 이용하여 기존의 웹 문서 이외의 파일시스템 접근이 가능하도록 하고 있음. 이러한 방법은 편의성을 제공하는 반면, 일반 사용자들도 시스템 중요 파일에 접근할 수 있게 하는 보안 문제를 발생시킴. 가령 시스템 자체의 root 디렉터리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한(nobody)으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 "/etc/passwd" 파일과 같은 민감한 파일을 누구나 열람할 수 있게 됨.					
	*심볼릭 링크(Symbolic link, 소프트 링크): 윈도우 운영체제의 바로가기 아이콘과 비슷함. 링크 생성 시 파일 내용은 존재하지 않으나 사용자가 파일을 요청하면 링크가 가리키고 있는 원본 데이터에서 데이터를 가져와서 전달함. 직접 원본을 가리키지 않고 원본 데이터를 가리키는 포인터를 참조함으로써 원본데이터가 삭제, 이동, 수정이 되면 사용 불가함.					
보안대책						
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 지시자에서 심볼릭 링크를 가능하게 하는 FollowSymLinks 옵션 제거)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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						
■ SunOS, LINUX, AIX, HP-UX						
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf						
2. 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거 (수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음						
<Directory /> Options Indexes FollowSymLinks AllowOverride None Order allow, deny Allow from all </Directory>						

UNIX 서버

(수정 전) Options 지시자에 FollowSymLinks 옵션 제거 후 저장

```
<Directory />
    Options Indexes
    AllowOverride None
    Order allow, deny
    Allow from all

</Directory>
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목	3.22. Apache 파일 업로드 및 다운로드 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-57
취약점 개요	불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드에 의한 서비스 불능상태가 발생할 수 있음. 따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹 서버에 의해 처리되지 못하게 하고, 자동이나 수동으로 파일의 보안성 검토를 수행함.				
보안대책					
판단기준	양호: 파일 업로드 및 다운로드를 제한한 경우				
	취약: 파일 업로드 및 다운로드를 제한하지 않은 경우				
조치방법	파일 업로드 및 다운로드 용량 제한 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 LimitRequestBody 지시자에 파일 사이즈 용량 제한 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, 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					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정					
<Directory /> LimitRequestBody 5000000 (※ "/" 는 모든 파일 사이즈를 5M로 제한하는 설정) </Directory>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.23. Apache 웹 서비스 영역의 분리			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-58
취약점 개요	Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs 디렉터리는 공개되어서는 안 될(또는, 공개될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 변경하여야 함. 또한, 대량의 업로드와 다운로드 시 서비스 불능 상태가 발생할 수 있음.				
보안대책					
판단기준	양호: DocumentRoot를 별도의 디렉터리로 지정한 경우				
	취약: DocumentRoot를 기본 디렉터리로 지정한 경우				
조치방법	DocumentRoot "/usr/local/apache/htdocs"-> DocumentRoot "별도 디렉터리" 로 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	DocumentRoot의 별도 디렉터리 지정 여부 확인 #vi /[Apache_home]/conf/httpd.conf DocumentRoot "/usr/local/apache/htdocs"				
DocumentRoot가 "/usr/local/apache/htdocs"가 아닌 별도의 디렉터리로 지정되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. DocumentRoot 설정 부분에 "/usr/local/apache/htdocs"가 아닌 별도의 디렉터리로 변경					
DocumentRoot "디렉터리"					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.24. ssh 원격접속 허용				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-59	
취약점 개요	Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기 때문에 ID/패스워드 및 중요 정보가 외부로 유출될 위험성이 있음. 따라서 원격 접속 시 사용자와 시스템과의 모든 통신을 암호화하는 *SSH(Secure Shell) 서비스를 사용할 것을 권장함.					
	*SSH(Secure Shell): 공개 키 암호 방식을 사용하여 원격지 시스템에 접근, 암호화된 메시지를 전송하는 시스템을 말함. 암호화된 메시지를 전송함으로써 LAN 상에서 다른 시스템에 로그인할 때 스니퍼에 의해서 도청당하는 것을 막을 수 있음.					
보안대책						
판단기준	양호: 원격 접속 시 SSH 프로토콜을 사용하는 경우					
	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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS		서비스 데몬 실행 여부 확인 # svcs -a grep ssh				
LINUX		서비스 데몬 실행 여부 확인 # ps -ax grep sshd				
서비스 데몬이 실행중인 경우 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치할 것을 권고함						
■ SunOS, LINUX, AIX, HP-UX						
1. 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		3.25. ftp 서비스 확인				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-60	
취약점 개요	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 반드시 필요한 경우를 제외하고는 FTP 서비스 사용을 제한하여야 함.					
보안대책						
판단기준	양호: FTP 서비스가 비활성화 되어 있는 경우					
	취약: FTP 서비스가 활성화 되어 있는 경우					
조치방법	FTP 서비스 중지					
보안설정방법						
FTP 종류별 점검 방법						
SunOS	일반 ftp 서비스 비활성화 여부 확인					
	# vi /etc/inetd.conf					
	proftpd 서비스 데몬 확인 (proftpd 동작 SID 확인)					
	# ps -ef grep proftpd root 3809 3721 0 08:44:40 ? 0:00 /usr/local/proftpd/sbin/proftpd					
LINUX, AIX, HP-UX	vsftpd 서비스 데몬 확인 (vsftpd 동작 SID 확인)					
	# ps -ef grep vsftpd					
	root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd/etc/vsftpd/vsftpd.conf					
	일반 ftp 서비스 비활성화 여부 확인					
LINUX, AIX, HP-UX	# ps -ef grep ftp					
	vsftpd 서비스 데몬 확인 (vsftpd 동작 SID 확인)					
	# ps -ef grep vsftpd					
	root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd					

불필요한 "ftp" 서비스 실행 시 아래의 보안설정방법에 따라 서비스 중지

■ SunOS

< 일반 FTP 서비스 중지 방법 >

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

2. inetd 서비스 재시작

#ps -ef | grep inetd

root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s

#kill -HUP [PID]

■ LINUX, AIX, HP-UX

< vsFTP 서비스 중지 방법 >

1. 서비스 확인

UNIX 서버

```
# ps -ef | grep vsftpd  
2. vsftpd 서비스 데몬 중지  
# service vsftpd stop 또는 /etc/rc.d/init.d/vsftpd stop
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.26. ftp 계정 shell 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-61	
취약점 개요	FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인이 필요하지 않은 기본 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하여야 함. 로그인이 불필요한 기본 계정에 *셸(Shell)을 부여할 경우 공격자에게 해당 계정이 노출되어 시스템 불법 침투가 발생할 수 있음.					
	*셸(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함.					
보안대책						
판단기준	양호: ftp 계정에 /bin/false 쉘이 부여되어 있는 경우					
	취약: ftp 계정에 /bin/false 쉘이 부여되지 않은 경우					
조치방법	ftp 계정에 /bin/false 쉘 부여					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS, 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						
■ SunOS, LINUX, AIX, HP-UX						
1. vi 편집기를 이용하여 "/etc/passwd" 파일을 연 후						
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						
조치 시 영향	일반적인 경우 영향 없음					

UNIX 서버

취약점 항목		3.27. ftpusers 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-62
취약점 개요	FTP 접근제어 설정파일을 관리자가 아닌 일반 사용자들도 접근 및 변경이 가능할 경우 비인가자 FTP 접근을 통해 계정을 등록하고 서버에 접속하여 불법적인 행동을 가능하게 하는 등 침해사고가 발생할 수 있음. FTP 접근제어 설정파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검함.				
보안대책					
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)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, 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				
■ SunOS, LINUX, AIX, HP-UX					
1. “/etc/ftpusers” 파일의 소유자 및 권한 확인 #ls -l /etc/ftpusers					
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					
(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist (ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)					
(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers (ftpusers 파일에 등록된 계정들만 접속이 차단됨)					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.28. ftpusers 파일 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-63	
취약점 개요	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 간단한 스니퍼에 의해서도 아이디 및 패스워드가 노출될 수 있으므로 반드시 필요한 경우를 제외하고는 FTP 서비스 사용을 제한하여야 함. 불가피하게 FTP 서비스를 사용하여야 하는 경우 root 계정의 직접 접속을 제한하여 root 계정의 패스워드 정보가 노출되지 않도록 함.					
	보안대책					
판단기준	양호: FTP 서비스가 비활성화 되어 있거나, 활성화 시 root 계정 접속을 차단한 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)					
보안설정방법						
FTP 종류별 점검 방법						
SunOS, LINUX, AIX, HP-UX	아래 파일에서 ftp에 대한 root 계정으로의 접속 가능 여부 확인 #cat /etc/ftpusers #cat /etc/ftpd/ftpusers #root (주석처리) 또는, root 계정 미등록					
	ProFTP #cat /etc/proftpd.con RootLogin on					
	vsFTP #cat /etc/vsftp/ftpusers #cat /etc/vsftpd.ftpusers #root (주석처리) 또는, root 계정 미등록					
root 계정으로 FTP 접속이 가능하도록 위와 같이 설정된 경우 아래의 보안설정방법에 따라 설정을 변경함						
■ SunOS, LINUX, AIX, HP-UX						
< 일반 FTP 서비스 root 계정 접속 제한 방법 >						
1. vi 편집기를 이용하여 ftpusers 파일을 연 후 ("/etc/ftpusers" 또는, "/etc/ftpd/ftpusers") #vi /etc/ftpusers 또는, /etc/ftpd/ftpusers						
2. ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root						
< ProFTP 서비스 중지 방법>						
1. vi 편집기를 이용하여 proftpd 설정파일("/etc/proftpd.conf")을 연 후 #vi /etc/proftpd.conf						

UNIX 서버

2. proftpd 설정파일 ("/etc/proftpd.conf")에서 RootLogin off 설정

(수정 전) RootLogin on

(수정 후) RootLogin off

< vsFTP 서비스 중지 방법 >

1. vi 편집기를 이용하여 ftpusers 파일을 연 후 ("/etc/vsftp/ftpusers" 또는, "/etc/vsftpd.ftpusers")

#vi /etc/vsftp/ftpusers

2. ftpusers 파일에 root 계정 추가 또는, 주석제거

(수정 전) #root 또는, root 계정 미등록

(수정 후) root

※ vsFTP를 사용할 경우 FTP 접근제어 파일

(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist

(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)

(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers

(ftpusers 파일에 등록된 계정들만 접속이 차단됨)

조치 시 영향	애플리케이션에서 root로 바로 접속하여 ftp를 사용하고 있을 경우 확인 필요
----------------	--

UNIX 서버

취약점 항목		3.29. at 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-64	
취약점 개요	*at 명령어 사용자 제한은 at.allow 파일과 at.deny 파일에서 할 수 있으므로 보안상 해당 파일에 대한 접근제한이 필요함. 만약 at 접근제한 파일의 권한이 잘못되어 있을 경우 권한을 획득한 사용자 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해를 발생할 수 있음.					
	*at 데몬 (일회성 작업 예약): 지정한 시간에 어떠한 작업이 실행될 수 있도록 작업 스케줄을 예약 처리해 주는 기능을 제공함. /etc/at.allow 파일에 등록된 사용자만이 at 명령을 사용할 수 있음.					
보안대책						
판단기준	양호: at 접근제어 파일의 소유자가 root이고, 권한이 640 이하인 경우					
	취약: at 접근제어 파일의 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우					
조치방법	"at.allow", "at.deny" 파일 소유자 및 권한 변경 (소유자 root, 권한 640 이하)					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS	"/etc/cron.d/at.allow", "/etc/cron.d/at.deny" 파일의 소유자 및 권한 확인 #ls -l /etc/cron.d/at.allow #ls -l /etc/cron.d/at.deny rw-r----- root <파일명>					
LINUX	"/etc/at.allow", "/etc/at.deny" 파일의 소유자 및 권한 확인 #ls -l /etc/at.allow #ls -l /etc/at.deny rw-r----- root <파일명>					
AIX, HP-UX	"/var/adm/cron/at.allow", "/var/adm/cron/at.deny" 파일의 소유자 및 권한 확인 #ls -l /var/adm/cron/at.allow #ls -l /var/adm/cron/at.deny rw-r----- root <파일명>					

위에 제시한 파일의 소유자가 root가 아니거나 파일의 권한이 640 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

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

UNIX 서버

■ LINUX

1. "/etc/at.allow" 및 "/etc/at.deny" 파일의 소유자 및 권한 변경

```
# chown root /etc/at.allow
# chmod 640 /etc/at.allow
# chown root /etc/at.deny
# chmod 640 /etc/at.deny
```

■ AIX, HP-UX

1. "/var/adm/cron/at.allow" 및 "/var/adm/cron/at.deny" 파일의 소유자 및 권한 변경

```
# chown root /var/adm/cron/at.allow
# chmod 640 / var/adm/cron/at.allow
# chown root /var/adm/cron/at.deny
# chmod 640 / var/adm/cron/at.deny
```

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		3.30. SNMP 서비스 구동 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-65
취약점 개요	*SNMP(Simple Network Management Protocol)서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스임. SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발생할 수 있으므로 SNMP 서비스를 사용하지 않을 경우 중지시킴.				
	*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.				
보안대책					
판단기준	양호: SNMP 서비스를 사용하지 않는 경우				
	취약: SNMP 서비스를 사용하는 경우				
조치방법	SNMP 서비스를 사용하지 않는 경우 서비스 중지 후 시작 스크립트 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#ps -ef grep snmp 또는 #svcs -a grep snmp				
LINUX, AIX	#ps -ef grep Snmp				
HP-UX	#ps -ef grep snmp				
불필요한 "SNMP" 서비스를 사용하지 않는 경우 중지함					
< 서비스 중지 방법 >					
■ SunOS 5.9 이하					
1. ps -ef grep snmp로 검색하여 위치 확인 후 이름 변경					
2. #/etc/init.d/init.snmpdx stop					
3. #mv /etc/rc3.d/S76snmpdx /etc/rc3.d/_S76snmpdx (rc*/_S**snmpdx 의 *수치는 각각 다름)					
■ SunOS 5.10					
1. "svcs -a grep snmp" 명령으로 데몬 확인					
2. 데몬 활성화 확인					
#ps .ef grep snmp 또는 #svcs -a grep snmp					
online 13:17:34 svc:/application/management/snmpdx:default					
3. "svcadm disable" 명령으로 데몬 중지					
(예) svcadm disable svc:/application/management/snmpdx					
■ LINUX, AIX, HP-UX 설정					
1. ps -ef grep snmp로 검색하여 서비스 중지					

UNIX 서버

2. service snmpd stop

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.31. SNMP 서비스 Community String의 복잡성 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-66	
취약점 개요	*SNMP(Simple Network Management Protocol) 서비스는 시스템 상태를 실시간으로 파악하는 *NMS(Network Management System)를 위하여 UNIX 시스템에서 기본적으로 제공하는 서비스이며 정보를 받기 위해 일종의 패스워드인 Community String을 사용함. *Community String은 Default로 public, private로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 시스템의 주요 정보 및 설정을 파악할 수 있음.					
	*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함. *NMS(Network Management System): 네트워크상의 모든 장비의 중앙 감시 체제를 구축하여 모니터링, 플래닝, 분석을 시행하고 관련 데이터를 보관하여 필요 즉시 활용 가능하게 하는 관리 시스템을 말함. *Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비밀번호인 'Community String'을 사용함.					
보안대책						
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					
보안설정방법						
OS별 점검 파일 위치 및 점검 방법						
SunOS 9 이하 버전		#vi /etc/snmp/conf/snmpd.conf read-community public / write-community private				
SunOS 10 이상 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 get-community-name: public / set-community-name : private				
위의 설정과 같이 디폴트 커뮤니티명인 "public" 또는, "private"을 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함						

UNIX 서버

OS별 snmpd.conf 파일 위치	
SunOS	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /etc/sma/snmp/snmpd.conf" (SunOS 10 버전 일 경우)
LINUX	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf
AIX	SNMP V1 을 사용할 경우: /etc/snmpd.conf SNMP V3 을 사용할 경우: /etc/snmpdv3.conf
HP-UX	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf

※ 일부 정보보호시스템에 따라 또는, 설치 경로에 따라 다를 수 있음

■ SunOS

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

- SunOS9 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>

- SunOS10 이상 버전 -

```
#vi /etc/sma/snmp/snmpd.conf
```

(수정 전) rocommunity public / rwcommunity private

(수정 후) rocommunity <변경 값> / rwcommunity <변경 값>

■ LINUX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
#vi /etc/snmp/snmpd.conf
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)
(수정 전) com2sec notConfigUser default public
(수정 후) com2sec notConfigUser default <변경 값>

■ AIX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
#vi /etc/snmpdv3.conf
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

UNIX 서버

(수정 전) COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0 -

(수정 후) COMMUNITY <변경 값> <변경 값> noAuthNoPriv 0.0.0.0 0.0.0 -

■ HP-UX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후

#vi /etc/snmpd.conf

3. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

(수정 전) get-community-name: public / set-community-name : private

(수정 후) get-community-name: <변경 값> / set-community-name: <변경 값>

조치 시 영향

NMS에서 서버를 모니터링 하는 경우 SNMP를 사용하며, 기타 SNMP를 사용할 경우 Community String 변경 시 통신하고자 하는 Server/Client에 모두 같은 Community String을 사용하여야 함

UNIX 서버

취약점 항목		3.32. 로그인 시 경고 메시지 제공			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-67
취약점 개요	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.				
보안대책					
판단기준	양호: 서버 및 Telnet 서비스에 로그인 메시지가 설정되어 있는 경우				
	취약: 서버 및 Telnet 서비스에 로그인 메시지가 설정되어 있지 않은 경우				
조치방법	Telnet, FTP, SMTP, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	#vi /etc/motd 서버 로그인 메시지 설정 여부 확인				

위에 제시한 파일 내에 로그인 메시지 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 로그인 메시지를 입력함

OS별 점검 파일 위치 및 점검 방법	
SunOS	#vi /etc/default/telnetd BANNER=" WWWnWWWn 'uname -a' 'uname -r' WWWnWWWn "
LINUX	#vi /etc/issue.net CentOS release 5.3 (Final) Kernel Wr on an Wm
AIX	#vi /etc/security/login.cfg default: 설정 없음
HP-UX	#vi /etc/inetd.conf telnet stream tcp nowait root /usr/sbin/telnetd telnetd

위에 제시한 파일 내 Telnet 배너 설정이 위와 같을 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력

#vi /etc/motd

(수정 전) 내용 없음

(수정 후) 로그인 메시지 입력

2. Telnet 배너 설정: vi 편집기로 "/etc/default/telnetd" 파일을 연 후 로그인 메시지 입력

#vi /etc/default/telnetd

(수정 전) BANNER="~~WWWnWWWn~~ 'uname -a' 'uname -r' ~~WWWnWWWn~~"

(수정 후) BANNER="로그온 메시지 입력"

UNIX 서버

■ LINUX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/issue.net" 파일을 연 후 로그인 메시지 입력
#vi /etc/issue.net
(수정 전) CentOS release 5.3 (Final) Kernel Wr on an Wm
(수정 후) 로그인 메시지 입력

■ AIX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/security/login.cfg" 파일을 연 후 로그인 메시지 입력
#vi /etc/security/login.cfg
(수정 전) default: 설정 부분에 herald 설정 없음
(수정 후) default: 설정 부분에 herald="로그인 메시지" 설정 추가

■ HP-UX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 telnet 부분에 로그인 파일 설정
#vi /etc/inetd.conf
(수정 전) telnet stream tcp nowait root /usr/sbin/telnetd telnetd
(수정 후) telnet stream tcp nowait root /usr/sbin/telnetd telnetd -b /etc/issue

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		3.33. NFS 설정파일 접근권한									
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-68						
취약점 개요	*NFS(Network File System) 접근제어 설정파일을 관리자가 아닌 일반 사용자들도 접근 및 변경이 가능하면 이를 통해 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있음. 따라서 NFS 접근제어 설정파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검하여야 함.										
	*NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램.										
보안대책											
판단기준	양호: NFS 접근제어 설정파일의 소유자가 root 이고, 권한이 644 이하인 경우										
	취약: NFS 접근제어 설정파일의 소유자가 root 가 아니거나, 권한이 644 이하가 아닌 경우										
조치방법	NFS 접근제어 설정파일의 소유자 및 권한 변경 (소유자 root, 권한 644)										
보안설정방법											
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS</td><td>#ls -al /etc/dfs/dfstab rw-r--r-- root <nfs 접근제어 파일></td></tr><tr><td>LINUX, AIX, HP-UX</td><td>#ls -al /etc/exports rw-r--r-- root <nfs 접근제어 파일></td></tr></table>						OS별 점검 파일 위치 및 점검 방법		SunOS	#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>
OS별 점검 파일 위치 및 점검 방법											
SunOS	#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											
■ SunOS											
"/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

취약점 항목		3.34. expn, vrfy 명령어 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-69
취약점 개요	*SMTP(Simple Mail Transfer Protocol)는 많은 취약성을 갖고 있어 잠재적인 위험이 존재함. 서버에서 SMTP를 사용하는 목적을 검토하여 사용할 필요가 없는 경우 서비스를 제거해야 하며, SMTP 서비스 운영 시 Sendmail Abuse를 방지하기 위해 Sendmail의 기본적인 서비스인 *VRFY, *EXPN을 막아야 함.				
	*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.				
보안대책					
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 옵션 추가				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX		noexpn, novrfy 옵션 설정 확인 #vi /etc/mail/sendmail.cf O PrivacyOptions=authwarnings			
AIX		#vi /etc/sendmail.cf O PrivacyOptions=authwarnings			
위의 설정과 같이 noexpn, novrfy 옵션이 추가되지 않은 경우 아래의 보안설정방법에 따라 옵션 추가					
<서비스 필요 시>					
■ SunOS, LINUX, HP-UX					
1. vi 편집기를 이용하여 "/etc/mail/sendmail.cf" 파일을 연 후 (단, AIX는 /etc/sendmail.cf) #vi /etc/mail/sendmail.cf					
2. "/etc/mail/sendmail.cf" 파일에 noexpn, novrfy 옵션 추가 (수정 전) O PrivacyOptions=authwarnings (수정 후) O PrivacyOptions=authwarnings, noexpn, novrfy					
3. SMTP 서비스 재시작					
< 서비스 불필요 시>					
■ SunOS, LINUX, HP-UX					
1. 실행중인 서비스 중지 #ps -ef grep sendmail					

UNIX 서버

```
root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections
```

```
#kill -9 [PID]
```

2. 시스템 재시작 시 SMTP 서버가 시작되지 않도록 OS별로 아래와 같이 설정함

■ SunOS, LINUX

1. 위치 확인

```
#ls -al /etc/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail
```

■ AIX

1. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail
```

3. /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

1. 위치 확인

```
#ls -al /sbin/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/_S540sendmail
```

3. /etc/rc.config.d/mailservs 파일에서 SENDMAIL_SERVER 값을 "0"으로 변경 (9.x 이하: /etc/netbsdsrc)
SENDMAIL_SERVER=0

■ SunOS 5.10

1. #svcs -a | grep smtp

2. 데몬 활성화 확인

```
online          13:17:45  svc:/network/smtp:sendmail
```

3. 데몬 중지

```
#svcadm disable [서비스 데몬명]
```

```
(예) #svcadm disable svc:/network/smtp:sendmail
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.35. Apache 웹서비스 정보 숨김			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-70
취약점 개요	에러 페이지, 웹 서버 종류, OS 정보, 사용자 계정 이름 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하여야 함. 불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수집할 수 있음.				
보안대책					
판단기준	양호: ServerTokens 지시자에 Prod 옵션이 설정되어 있는 경우				
	취약: ServerTokens 지시자에 Prod 옵션이 설정되어 있지 않는 경우				
조치방법	헤더에 최소한의 정보를 제한 후 전송 (ServerTokens 지시자에 Prod 옵션 설정)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Prod 옵션 설정 여부 확인 #vi /[Apache_home]/conf/httpd.conf ServerTokens Prod				

"httpd.conf" 파일 내에 ServerTokens 지시자가 위와 같이 "Prod"로 설정되지 않은 경우 아래의 보안설정방법에 따라 옵션 추가

■ SunOS, LINUX, AIX, HP-UX

1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
#vi /[Apache_home]/conf/httpd.conf

2. 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정 (없으면 신규 삽입)

<Directory />
Options Indexes FollowSymLinks
ServerTokens Prod

- 이하생략 -
</Directory>

UNIX 서버

ServerTokens 지시자 옵션		
키워드	제공하는 정보	예문
Prod	웹 서버 종류	Server Apache
Min	Prod 키워드 제공 정보 + 웹 서버 버전	Server Apache/1.3.0
OS	Min 키워드 제공 정보 + 운영체제	Server Apache/1.3.0 (Unix)
Full	OS 키워드 제공 정보 + 설치된 모듈(응용프로그램) 정보	Server Apache/1.3.0 (Unix) PHP/3.0 MyMod/1.2

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

4. 패치 관리

취약점 항목		4.1. 최신 보안패치 및 벤더 권고사항 적용			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-71
취약점 개요	주기적인 패치 적용을 통하여 보안성 및 시스템 안정성을 확보하는 것이 시스템 운용의 중요한 요소임. 서비스 중인 시스템의 경우 패치 적용에 따르는 문제점(현재 운용중인 응용프로그램의 예기치 않은 중지, 패치 자체의 버그 등)과 재부팅의 어려움 등으로 많은 패치를 적용하는 것이 매우 어렵기 때문에 패치 적용 시 많은 부분을 고려하여야 함.				
보안대책					
판단기준	양호: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우				
	취약: 패치 적용 정책을 수립하지 않고 주기적으로 패치관리를 하지 않는 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 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하여 주기적인 패치 적용 정책을 수립하여 적용하여야 함				
보안설정방법					
OS별 점검 방법					
SunOS, LINUX, AIX, HP-UX	패치 적용 정책 수립 여부 및 정책에 따른 패치 적용 여부 확인				

■ SunOS

1. “showrev -p” 로 서버에 적용되어 있는 패치 리스트 확인

2. 아래 2개 패치 사이트 중 하나를 선택 후 접속하여 패치를 찾아 적용

- OS별, 제품별, 보안 관련 그리고 y2k 패치로 분류되어 패치 파일 제공
<http://access1.sun.com/patch.y2k/>
- OS별로 추천되는 패치 파일 제공
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

< 패치 적용의 예 1 >

#mkdir /var/spool/patch

위와 같은 디렉토리를 만들어 Patch 파일을 관리하도록 함

(패치 설치 순서 예): 107403-02: SunOS 5.7: rlmmod & telmod Patch 를 적용하고자 함

#showrev -p | grep 107403

Patch: 107403-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu

UNIX 서버

```
#ls
107403-02.zip
#unzip 107403-02.zip
#patchadd /var/spool/patch/107403-02
erifying sufficient filesystem capacity (dry run method)...
Installing patch packages...
```

Patch number 107403-02 has been successfully installed.
See /var/sadm/patch/107403-02/log for details

Patch packages installed:
SUNWcsu
SUNWcsxu

```
#showrev -p | grep 107403
Patch: 107403-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu
Patch: 107403-02 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu
```

※ 설치 시 주의할 점

1. 패치 적용 후 Rebooting이 필요한 경우가 있으므로 README-Patch-ID 파일 확인 필요
2. 패치 제거 방법: #patchrm Patch-ID 실행

< 패치 적용의 예 2 >

패치 cluster의 이용

패치 cluster란 Sun에서 Recommended 패치와 보안 관련 패치들을 통합하여, 각 시스템 관리자들의 편의를 도모하기 위한 패키지 형태로 제공되는 패치 묶음을 가리킴
이들 패치 cluster는 Sun의 Web 페이지와 ftp 서버에서도 구할 수 있으며, 각각의 패치 cluster들은 아래와 같은 파일명으로 구성됨

```
[version]_Recommended.tar.Z
[version]_Recommended.README
2.5.1_Recommended.tar.Z
2.5.1_Recommended.README
```

위와 같이 각 버전에 따라 Recommended.tar.Z와 같은 바이너리 패치 묶음과 해당 패치 cluster에 대한 주석을 담고 있는 README 파일이 제공되므로 각 시스템의 관리자들은 Sun 사이트에 접속하여 패치 cluster와 README 파일 다운로드 하여 시스템에 설치할 수 있음

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches>

UNIX 서버

< 패치 적용의 예 3 >

Automate patch management tool를 사용하여 현재 시스템에서 업데이트 패치 및 설치될 패치를 분석하여 웹상에서 자동으로 patch list를 다운받아서 설치함
현재 Automate patch management tool을 사용하여 적용될 수 있는 시스템들은 다음과 같음

```
#gunzip -dc pproSunOSx865.9jre2.2.tar.gz | tar xvf -
#zcat pproSunOSSparc5.6jre2.2.tar.Z | tar xvf -
#cd pproSunOSSparc5.9jre2.2
#./setup
```

< 시스템 현황 >

SunOS 2.6 - 9, Sun Cluster, Network Storage, and E10Ks and Star Fires

< Patch management tool download >

<https://sunsolve.sun.com/patchpro/patchpro.html>

■ LINUX

Linux는 서버에 설치된 패치 리스트의 관리가 불가능하므로 rpm 패키지 별 버그가 Fix된 최신 버전 설치가 필요함

Linux는 오픈 되고, 커스터마이징 된 OS이므로 Linux를 구입한 벤더에 따라 rpm 패키지가 다를 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 <package-name>
```

■ AIX

"instfix -iv | grep ML"로 서버에 적용되어 있는 패치 리스트 확인

버전4.3의 경우 아래 사이트에서 다음과 같은 방법으로 패치 버전을 다운받을 수 있고 원하는 레벨의 ML를 찾을 수 있음

※ current를 현재 버전 level로 등록하고, update to를 최신의 대상 패치 버전으로 선택

<http://techsupport.services.ibm.com/server/mlfixes/43/>

UNIX 서버

< 패치 적용의 예 1>

Click on the package name below.

Put the package (a tar.gz file) in /usr/sys/inst.images

Extract the filesets from the package.

```
cd /usr/sys/inst.images
```

```
gzip -d -c 4330910.tar.gz | tar -xvf -
```

Back up your system. 0

Install the package by creating a table of contents for install to use. Then update the install subsystem itself. Run SMIT to complete the installation.

```
inutoc /usr/sys/inst.images
```

```
installp -acgXd /usr/sys/inst.images bos.rte.install
```

```
smit update_all
```

Reboot your system. This maintenance package replaces critical operating system code.

< Security Patch Check 관련 사이트 >

<http://techsupport.services.ibm.com/server/nav?fetch=pm>

■ HP-UX

'swlist -l product'로 서버에 적용된 패치 리스트 확인

HPUX 는 다양한 하드웨어 플랫폼과 O/S로 인해 General 한 Security Patch가 공개되어 있지 않으며, security_patch_check 프로그램(셸 스크립트)을 서버에 설치·실행하여 서버의 취약한 Security Patch 리스트를 얻을 수 있음

security_patch_check는 현재 적용되고 있는 패치 리스트를 분석하는 툴로써, 적용 가능한 패치와 설치되지 않은 패치 정보를 리포트 형식으로 제공하고 보안 패치에 대한 오류 정보를 자동으로 체크하여 알려줌

security_patch_check 프로그램을 사용하기 위해서는 Service Control Manager 도구를 서버에 설치하여야 함 (security_patch_check 사용관련 내용은 '비고' 참조)

< Security Patch Check 관련 사이트 >

http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

< 패치 적용의 예 1>

1. 수작업에 의한 패치 적용

운영자에 의한 패치 적용은 다음과 같은 단계에 의해 수행됨

- 1) <http://support2.itrc.hp.com/service/patch/mainPage.do> 접속
- 2) HPUX 선택하여 해당 페이지 이동
- 3) 해당되는 H/W, OS 선택
- 4) 키워드, Patch-ID, Patch 리스트 옵션을 선택하여 검색

UNIX 서버

- 5) 검색 결과 확인
- 6) 필요한 패치를 선택하여 다운로드 받음
- 7) 패치 간의 dependency를 고려하여 적용할 패치 결정

2. Custom Patch Manager에 의한 패치 적용

CPM(Custom Patch Manager)은 해당 시스템에 적합한 패치를 선택하고 다운로드 받을 수 있도록 하는 툴이며, CPM을 이용하여 환경에서 설정된 일정 기간 간격별로 패치를 자동 적용할 수 있고 dependency 관계나 conflict 관계에 대해 자동 분석된 결과를 얻어 적용할 패치 정보를 확인할 수 있음

CPM을 이용하는 단계는 다음과 같은 단계에 의해 수행됨

- 1) ITRC 웹 사이트 <http://itrc.hp.com>로 이동하여 로그인
- 2) maintenance/support 링크를 클릭한 후 customized patch bundles를 선택
- 3) cpm_collect.sh 스크립트를 다운로드 받아 실행 후 현재 configuration에 대한 정보를 취합
- 4) cpm_collect.sh 스크립트를 실행 후 configuration에 대한 결과를 ITRC 페이지에 업로드
- 5) Perform Patch Analysis를 클릭하여 필요한 candidate patch list를 얻음
- 6) 선택한 패치 간의 conflict가 없는지 점검
- 7) 선택한 패치를 Package 버튼을 선택하여 다운로드 받은 후 패치 설치

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

5. 로그 관리

취약점 항목		5.1. 로그의 정기적 검토 및 보고				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-72	
취약점 개요	로그 정보는 침해사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 정기적인 로그 분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있음.					
보안대책						
판단기준	양호: 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지는 경우					
	취약: 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우					
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정					
보안설정방법						
OS별 점검 방법						
SunOS, LINUX, AIX, HP-UX		로그 분석 계획 수립 여부 및 로그 분석 결과에 대한 점검				

■ SunOS, LINUX, AIX, HP-UX

정기적인 로그 분석을 위하여 아래와 같은 절차 수립

1. 정기적인 로그 검토 및 분석 주기 수립

2. 로그 분석에 대한 결과 보고서 작성

3. 로그 분석 결과보고서 보고 체계 수립

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		5.2. 정책에 따른 시스템 로깅 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-73	
취약점 개요	감사 설정이 구성되어 있지 않거나 보안 정책에 비하여 감사 설정 수준이 낮아 보안 사고가 발생한 경우 원인 파악 및 각종 침해 사실에 대한 확인이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없음.					
보안대책						
판단기준	양호: 로그 기록 정책이 정책에 따라 설정되어 수립되어 있는 경우					
	취약: 로그 기록 정책 미수립, 또는, 정책에 따라 설정되어 있지 않은 경우					
조치방법	로그 기록 정책을 수립하고, 정책에 따라 syslog.conf 파일을 설정					
보안설정방법						
■ SunOS						
1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후						
#vi /etc/syslog.conf						
2. 아래와 같이 수정 또는, 신규 삽입						
<pre>mail.debug /var/log/mail.log *.info /var/log/syslog.log *.alert /var/log/syslog.log *.alert /dev/console *.alert root *.emerg *</pre>						
3. 위와 같이 설정 후 SYSLOG 데몬 재시작						
- SunOS 9 이하 버전 -						
#ps -ef grep syslogd						
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd						
#kill -HUP [PID]						
- SunOS 10 이상 버전 -						
#svcs -a grep system-log						
online 16:23:03 svc:/system/system-log:default						
#svcadm refresh svc:/system/system-log:default						
■ LINUX						
1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후						
#vi /etc/syslog.conf						
2. 아래와 같이 수정 또는, 신규 삽입						

UNIX 서버

```
*.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         *
```

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

1. vi 편집기를 이용하여 “/etc/syslog.conf” 파일을 연 후
#vi /etc/syslog.conf
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
```

3. 위와 같이 설정 후 SYSLOG 데몬 재시작

```
#refresh -s syslogd 또는,
#ps -ef |grep syslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd
#kill -HUP [PID]
```

■ HP-UX

1. vi 편집기를 이용하여 “/etc/syslog.conf” 파일을 연 후
#vi /etc/syslog.conf
2. 아래와 같이 수정 또는, 신규 삽입

```
*.notice       /var/adm/syslog/syslog.log
*.alert        /dev/console
*.emerg        *
```

UNIX 서버

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]

메시지 종류	
메시지	설명
auth	로그인 등의 인증 프로그램 유형이 발생한 메시지
authpriv	개인 인증을 요구하는 프로그램 유형이 발생한 메시지
cron	cron, at 데몬에서 발생한 메시지
daemon	telnet, ftpd 등과 같은 데몬이 발생한 메시지
kern	커널이 발생한 메시지
lpr	프린터 유형의 프로그램이 발생한 메시지
mail	메일 시스템에서 발생한 메시지
news	유즈넷 뉴스 프로그램 유형이 발생한 메시지
syslog	syslog 프로그램 유형이 발생한 메시지
user	사용자 프로세스 관련 메시지
uucp	시스템이 발생한 메시지
local0	여분으로 남겨둔 유형

메시지 우선순위	
메시지	설명
alert	즉각적으로 조치를 취해야 할 상황
crit	급한 상황은 아니지만, 치명적인 시스템 문제 발생 시
deberg	프로그램 실행 시 발생하는 오류 발생 시
emerg	매우 위험한 상황
err	에러 발생 시
info	단순한 프로그램에 대한 정보 메시지
notice	에러가 아닌 알림에 관한 메시지
warning	주의를 요하는 메시지

조치 시 영향	위에 제시한 모든 로그설정을 강제화할 경우, 시스템 퍼포먼스와 로그 저장에 따른 서버 용량 문제가 발생할 수 있으므로 시스템 운영 환경과 특성을 고려하여 적용
---------	--

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.

1. *#cat 파일 경로/파일명* : 파일을 열어 내용을 출력
2. *#cat > 파일 경로/파일명*
 같은 이름의 파일이 없는 경우 -> 파일을 새로 만들고 내용 입력
 같은 이름의 파일이 있는 경우 -> 파일을 덮어쓰고 새로 내용 입력
3. *#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

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

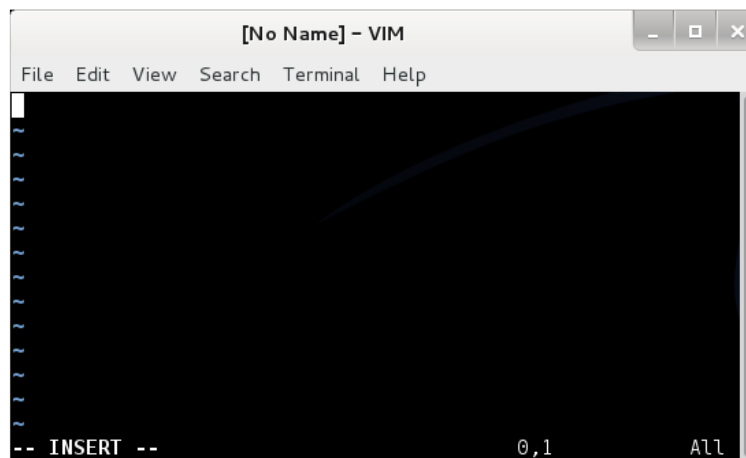
UNIX 서버

02. vi 편집기를 사용하여 파일 내용 수정

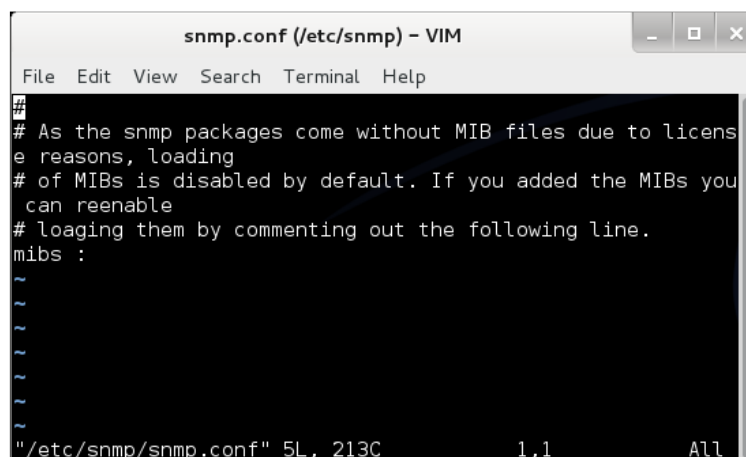
vi 편집기는 윈도우의 메모장처럼 사용되는 유닉스에서 제공하는 표준편집기를 말함.
이미 존재하는 파일을 수정하는 경우 또는, 신규 파일을 만들고자 할 때 vi 명령을 사용함.

#vi <파일 경로/파일명>

vi 명령어를 입력하여 프로그램을 시작하면 일반적으로 명령(normal)모드로 시작되고, 이때 키보드에서 "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)



편집중인 문서 저장 시 ":w"를 입력하고, 수정 완료 후 ":q"를 입력하여 프로그램을 종료함.
파일에 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.

1. 명령모드: 기본 구성 / 텍스트 편집 불가 / 명령어 수행
2. 편집모드: 텍스트 편집만 가능
3. 확장모드: 종료하거나 저장이 가능한 확장 기능 수행

UNIX 서버

03. find 명령어를 사용하여 파일 경로 확인

find 명령어는 원하는 파일을 계속 필터링 하면서 찾아볼 수 있도록 하고, 잘못 수정 된 파일을 추적할 때 유용하게 사용됨. 취약점 진단 시 각 운영체제별로 파일이 존재하는 위치에 차이가 있어 진단 조치 또는, 설정 여부 확인이 어려운 경우가 종종 있는데 find 명령어를 이용하여 파일이 위치한 경로를 쉽게 확인할 수 있음. find 명령어 기본형은 다음과 같음.

```
#find . -name 'pattern'
```

<find 명령어 사용 예시>

01. #find . -name '*.html'

. 은 현재 디렉터리에서 찾을 때, /usr와 같이 특정 위치에서 찾으려면 #find /usr -name '*.html' -name은 파일 이름으로 찾으라는 조건으로 확장자가 .html 로 끝나는 파일만을 검색

02. #find . -type d

디렉터리만 검색

03. #find . -group admin -type l

그룹이 admin이면서 심볼릭 링크만 조회

04. #find . - user icocoa -maxdepth 1 -type d

현재 디렉터리 내에서 소유자가 icocoa이며, 디렉터리인 것만을 검색

05. #find . -name '*.jpg' -o -name '*.html'

-o 옵션은 OR 옵션으로 확장자가 .jpg인 것과 .html인 파일을 검색

06. #find . -atime -2

2일 동안 액세스가 일어나지 않은 파일 검색

07. #find . -atime +3

액세스가 일어난 후 3일된 파일 검색

08. #find . -mtime +7

7일 넘도록 변경되지 않은 파일 검색 (m: modification time)

09. #find . -mmin +30 -maxdepth 1 -type f

현재 디렉터리 내에서 변경이 있은 후 30분 지난 파일 검색(+,- 기호 사용)

10. #find . -name '*.xml' -exec grep -l 'Version' {} \;

현재 디렉터리 내에서 Version이라는 단어가 들어간 .xml 확장자를 가진 파일 검색

11. #find . ! -name '*.jpg'

jpg로 끝나지 않는 파일 검색

12. #find . -newermm test.txt

test.txt 보다 나중에 수정된 파일 검색 (-newermm은 -newer와 동일)

13. #find . -size +100c(+,- 기호 사용)

사이즈가 100바이트 이상인 파일 검색(c: bytes) (-인 경우 100바이트보다 작은 파일 검색)

UNIX 서버

04. /etc/passwd, /etc/shadow, /etc/group 파일 구조

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

■ /etc/passwd

```

root@localhost:/etc
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
games: x: 12: 100: games: /usr/games: /sbin/nologin
gopher: x: 13: 30: gopher: /var/gopher: /sbin/nologin
ftp: x: 14: 50: FTP User: /var/ftp: /sbin/nologin
nobody: x: 99: 99: Nobody: /: /sbin/nologin
dbus: x: 81: 81: System message bus: /: /sbin/nologin
usbmuxd: x: 113: 113: usbmuxd user: /: /sbin/nologin
vcsa: x: 69: 69: virtual console memory owner: /dev: /sbin/nologin
rpc: x: 32: 32: Rpcbind Daemon: /var/cache/rpcbind: /sbin/nologin
rtkit: x: 499: 497: RealtimeKit: /proc: /sbin/nologin
avahi-autoipd: x: 170: 170: Avahi IPv4LL Stack: /var/lib/avahi-autoipd: /sbin/nologin
pulse: x: 498: 496: PulseAudio System Daemon: /var/run/pulse: /sbin/nologin
haldaemon: x: 68: 68: HAL daemon: /: /sbin/nologin
ntp: x: 38: 38: : /etc/ntp: /sbin/nologin
apache: x: 48: 48: Apache: /var/www: /sbin/nologin
saslauth: x: 497: 76: "Saslauthd user": /var/empty/saslauth: /sbin/nologin
postfix: x: 89: 89: : /var/spool/postfix: /sbin/nologin
abrt: x: 173: 173: : /etc/abrt: /sbin/nologin
rpcuser: x: 29: 29: RPC Service User: /var/lib/nfs: /sbin/nologin
nfsnobody: x: 65534: 65534: Anonymous NFS User: /var/lib/nfs: /sbin/nologin
gdm: x: 42: 42: : /var/lib/gdm: /sbin/nologin
sshd: x: 74: 74: Privilege-separated SSH: /var/empty/sshd: /sbin/nologin
tcpdump: x: 72: 72: : /: /sbin/nologin
namegpark: x: 500: 500: namegpark: /home/namegpark: /bin/bash
| root@localhost etc| #

```

namegpark	x	500	500	namegpark	/home/namegpark	/bin/bash
계정명 ^①	패스워드 ^②	UID ^③	GID ^④	계정설명 ^⑤	홈 디렉터리 ^⑥	Shell 정보 ^⑦

- ① 사용자 이름(대부분 ID라고 함)
- 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 연락처 등 기타 정보 입력)
- ⑥ : 사용자 계정 디렉토리(계정 홈 디렉토리)
- ⑦ : 사용자 로그인 셸 (Linux : bash Shell, Unix : Korn Shell 등)


```
root@localhost:/etc# cat /etc/shadow
root:$6$7QkaZvftw.YzVle3$Uv.dfQkeKxnCEklTHyF2oIS7NTObdqOpI5xdDuYmDToD55b.mNlc8Q1
GlKpSc25aoMiCip04bDmDDa6WjT/NN.:15788:0:99999:7:::
bin:!:15628:0:99999:7:::
daemon:!:15628:0:99999:7:::
adm:!:15628:0:99999:7:::
lp:!:15628:0:99999:7:::
sync:!:15628:0:99999:7:::
shutdown:!:15628:0:99999:7:::
halt:!:15628:0:99999:7:::
mail:!:15628:0:99999:7:::
uucp:!:15628:0:99999:7:::
operator:!:15628:0:99999:7:::
games:!:15628:0:99999:7:::
gopher:!:15628:0:99999:7:::
ftp:!:15628:0:99999:7:::
nobody:!:15628:0:99999:7:::
dbus:!!!:15788:!!!!:
usbmuxd:!!!:15788:!!!!:
vcsa:!!!:15788:!!!!:
rpc:!!!:15788:0:99999:7:::
rtkit:!!!:15788:!!!!:
avahi-autoipd:!!!:15788:!!!!:
```

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

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

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

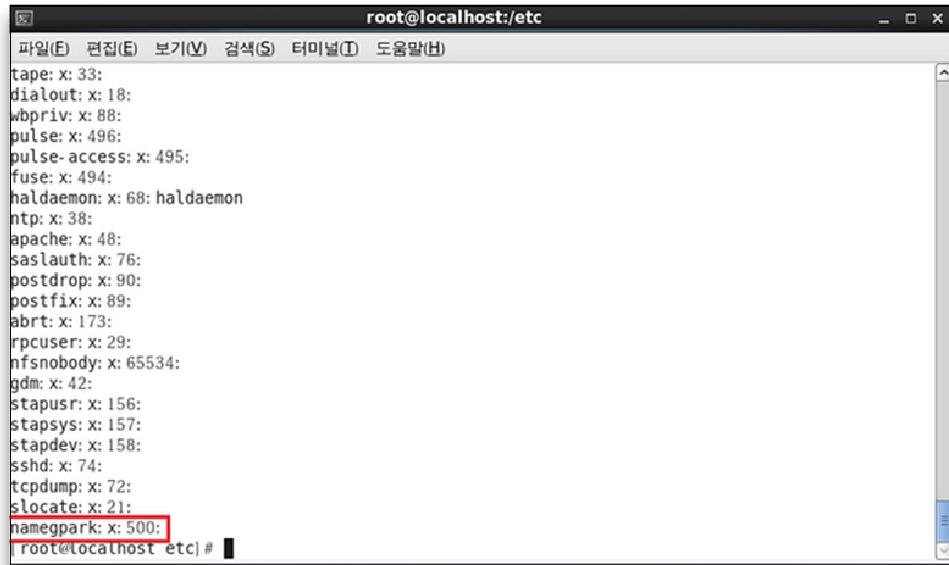
⑦ Inactive : 로그인 접속차단 일 수

⑧ Expire : 로그인 사용을 금지하는 일 수 (월/일/연도)+A1:A44

⑨ Reserved : 사용되지 않음

UNIX 서버

■ /etc/group



```

root@localhost:/etc
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
tape: x: 33:
dialout: x: 18:
wbpriv: x: 88:
pulse: x: 496:
pulse-access: x: 495:
fuse: x: 494:
haldaemon: x: 68: haldaemon
ntp: x: 38:
apache: x: 48:
saslauth: x: 76:
postdrop: x: 90:
postfix: x: 89:
abrt: x: 173:
rpcuser: x: 29:
nfsnobody: x: 65534:
gdm: x: 42:
stapusr: x: 156:
stapsys: x: 157:
stapdev: x: 158:
sshd: x: 74:
tcpdump: x: 72:
slocate: x: 21:
namegpark: x: 500:
root@localhost etc] #
    
```

namegpark	x	500	-
그룹명	패스워드	GID	그룹 구성원

UNIX 서버

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 daemon.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 gopher사이트 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
 - nsd: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
 - 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 셸 계정
 - pcap:x:77:77:/var/arpwatch/sbin/nologin = 패킷 캡처 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 로그인 필요없음.