

# 취약점 진단 보고서

## (Cent OS)

2017/01/25 ~ 2017/01/26

이헌진

# 목 차

## 1. 개요

### 1.1 서버 개요

### 1.2 서버취약점 분석 평가 항목

## 2. 취약점 진단

### 2.1 사용자 관리

### 2.2 파일 및 디렉터리 관리

### 2.3 서비스 관리

### 2.4 패치관리

### 2.5 로그관리

## 3. Nessus

# 1. 개요

## 1.1 서버 개요

서버 개요	
서버 OS	Cent OS 5.3
서버 웹	Apache 1.3
DB	mysql
서버 언어	PHP 4.3.9
IP	192.168.222.100

## 1.2 서버취약점 분석 평가 항목

분류	점검항목	항목 중요도	항목 코드	취약점 항목
1. 계정 관리	root 계정 원격 접속 제한	상	U-01	X
	패스워드 복잡성 설정	상	U-02	X
	계정 잠금 임계 값 설정	상	U-03	X
	패스워드 파일 보호	상	U-04	O
	root 이외의 UID가 '0'금지	중	U-05	X
	root 계정 su 제한	하	U-06	X
	패스워드 최소 길이 설정	중	U-07	X
	패스워드 최대 사용 기간 설정	중	U-08	X
	패스워드 최소 사용기간 설정	중	U-09	X
	불필요한 계정 제거	하	U-10	X
	관리자 그룹에 최소한의 계정 포함	하	U-11	O
	계정이 존재하지 않는 GID 금지	하	U-12	O
	동일한 UID 금지	중	U-13	O
	사용자 shell 점검	하	U-14	O
	Session Timeout 점검	하	U-15	X
	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-16	O
	파일 및 디렉터리 소유자 설정	상	U-17	X
	/etc/passwd 파일 소유자 및 권한 설정	상	U-18	O
	/etc/shadow 파일 소유자 및 권한 설정	상	U-19	O

2. 파일 및 디렉터리 관리	/etc/hosts 파일 소유자 및 권한 설정	상	U-20	X
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-21	X
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-22	O
	/etc/services 파일 소유자 및 권한 설정	상	U-23	O
	SUID,SGID,Sticky bit 설정 파일 점검	상	U-24	X
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-25	O
	world writable 파일 점검	상	U-26	X
	/dev에 존재하지 않는 device 파일 점검	상	U-27	O
	\$HOME/.rhosts, hosts.equiv 사용 금지	상	U-28	O
	접속 IP 및 포트 제한	상	U-29	X
	hosts.lpd 파일 소유자 및 권한 설정	하	U-30	O
	NIS 서비스 비활성화	중	U-31	O
	UMASK 설정 관리	중	U-32	O
	홈디렉토리 소유자 및 권한 설정	중	U-33	O
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-34	O
3. 서비스 관리	숨겨진 파일 및 디렉토리 검색 및 제거	하	U-35	O
	finger 서비스 비활성화	상	U-36	O
	Anonymous FTP 비활성화	상	U-37	X
	r 계열 서비스 비활성화	상	U-38	O
	cron 파일 소유자 및 권한 설정	상	U-39	X
	Dos 공격에 취약한 서비스 비활성화	상	U-40	O
	NFS 서비스 비활성화	상	U-41	O
	NFS 접근 통제	상	U-42	O
	automountd 제거	상	U-43	X
	RPC 서비스 확인	상	U-44	O
	NIS, NIS+ 점검	상	U-45	O
	tftp, talk 서비스 비활성화	상	U-46	O
	sendmail 버전 점검	상	U-47	O
	스팸 메일 릴레이 제한	상	U-48	O
	일반사용자의 Sendmail 실행 방지	상	U-49	O
	DNS 보안 버전 패치	상	U-50	O
	DNS Zone Transfer 설정	상	U-51	O
	Apache 디렉토리 리스팅 제거	상	U-52	X
	Apache 웹 프로세스 권한 제한	상	U-53	O
	Apache 상위 디렉토리 접근 금지	상	U-54	O
	Apache 불필요한 파일 제거	상	U-55	O
	Apache 링크 사용 금지	상	U-56	O

	Apache 파일 업로드 및 다운로드 제한	상	U-57	X
	Apache 웹 서비스 영역의 분리	상	U-58	X
	ssh 원격접속 허용	중	U-59	O
	ftp 서비스 확인	하	U-60	O
	ftp 계정 shell 제한	중	U-61	X
	ftputers 파일 소유자 및 권한 설정	하	U-62	O
	ftputers 파일 설정	중	U-63	O
	at 파일 소유자 및 권한 설정	중	U-64	O
	SNMP 서비스 구동 점검	중	U-65	O
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-66	O
	로그온 시 경고 메시지 제공	하	U-67	X
	NFS 설정파일접근권한	중	U-68	O
	expn, vrfy 명령어 제한	중	U-69	O
	Apache 웹서비스의 정보 숨김	중	U-70	X
<b>4. 패치 관리</b>	최신 보안패치 및 벤더 권고 사항 적용	상	U-71	X
<b>5. 로그 관리</b>	로그의 정기적 검토 및 보고	상	U-72	O
	정책에 따른 시스템 로깅 설정	하	U-73	X

## 2. 취약점 진단

### 2.1 사용자 관리

취약점 항목		1.1 root 계정 원격 접속 제한			
대상 OS	Cent OS	위험도	상	Code	U-01
취약점 개요	root는 시스템을 관리하는 매우 중요한 계정임. root 계정으로 직접 로그인 하도록 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.				
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				
보안 설정 방법					
1. "/etc/ssh/sshd_config"에서 PermitRootLogin의 주석을 제거하고 no로 접근 차단					
<div><div><pre>#LoginGraceTime 2m #PermitRootLogin yes #StrictModes yes #MaxAuthTries 6</pre></div><div><pre>#LoginGraceTime 2m PermitRootLogin no #StrictModes yes #MaxAuthTries 6</pre></div></div>					
그림 1 PermitRootLogin 수정					
조치 시 영향	일반적인 경우 영향 없음				

취약점 항목	1.2 패스워드 복잡성 설정 1.3 계정 잠금 임계값 설정				
대상 OS	Cent OS	위험도	상	Code	U-02 U-03

<b>취약점 개요</b>	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.
<b>보안대책</b>	
<b>판단기준</b>	<b>양호</b> : 영문·숫자·특수문자가 혼합된 8자리 이상의 패스워드가 설정된 경우
	<b>취약</b> : 영문·숫자·특수문자가 혼합되지 않은 8자 미만의 패스워드가 설정된 경우
<b>조치방법</b>	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정
<b>보안 설정 방법</b>	
<b>OS별 점검 파일 위치 및 점검 방법</b>	
<b>Sun OS, LINUX, HP-UX</b>	/etc/shadow 파일 내 설정된 패스워드 점검
<b>AIX</b>	/etc/security/passwd 파일 내 설정된 패스워드 점검
<p><b>&lt;부적절한 패스워드 유형&gt;</b></p> <ol style="list-style-type: none"> <li>1. 사전에 나오는 단어나 이들의 조합</li> <li>2. 길이가 너무 짧거나, NULL(공백)인 패스워드</li> <li>3. 키보드 자판의 일련의 나열 (예) abcd, qwer, etc</li> <li>4. 사용자 계정 정보에서 유추 가능한 단어들 (예) 지역명, 부서명, 계정명, 사용자 이름의 이니셜, root ... 등</li> </ol>	
<p><b>&lt;패스워드 관리 방법&gt;</b></p> <ol style="list-style-type: none"> <li>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 8자 리 이상의 길이로 구성 <ul style="list-style-type: none"> <li>가. 영문대문자(26개)</li> <li>나. 영문소문자(26개)</li> <li>다. 숫자(10개)</li> <li>라. 특수문자(32개)</li> </ul> </li> <li>2. 시스템마다 상이한 패스워드 사용</li> <li>3. 패스워드를 기록해 놓을 경우 변형하여 기록</li> <li>4. 가급적 자주 패스워드를 변경할 것</li> </ol>	

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      sufficient     pam_unix.so nullok try_first_pass
auth      requisite      pam_succeed_if.so uid >= 500 quiet
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient     pam_succeed_if.so uid < 500 quiet
account    required      pam_permit.so

password   requisite      pam_cracklib.so try_first_pass retry=3
password   sufficient     pam_unix.so md5 shadow nullok try_first_pass use_authn
password   required      pam_deny.so

session    optional      pam_keyinit.so revoke
session    required      pam_limits.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet
session    use_uid
session    required      pam_unix.so

```

그림 2 /etc/pam.d/system-auth

- password requisite 부분을 수정을 해서 패스워드 복잡성을 수정

```

account    required      pam_unix.so
account    sufficient     pam_succeed_if.so uid < 500 quiet
account    required      pam_permit.so

password   requisite      pam_cracklib.so try_first_pass retry=3 minlen=8 ucred
t=-1 dcredit=-1 ocredit=-1 lcredit=-1
password   sufficient     pam_unix.so md5 shadow nullok try_first_pass use_authn
password   required      pam_deny.so

```

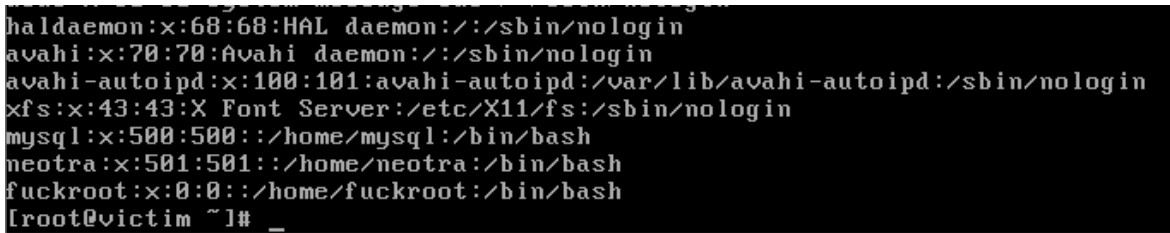
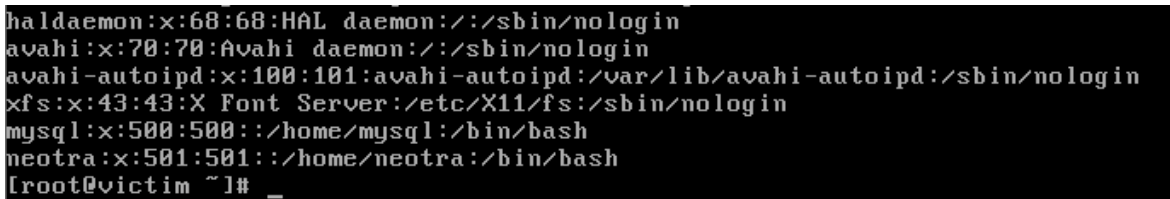
그림 3 /etc/pam.d/system-auth

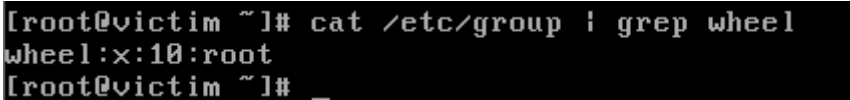
- “password requisite pam\_cracklib.so try\_firsh\_pass retry=3 minlen=8 ucredit=-1 dcredit=-1 ocredit=-1 lcredit=-1” 로 변경

retry=N	패스워드 입력 실패 시 재시도 횟수
minlen=N	크레디트를 더한 패스워드 최소 길이
dcredit=N	숫자에 주어지는 크레딧 값, 기본 1
ucredit=N	영어 대문자에 주어지는 크레딧 값
lcredit=N	영어 소문자에 주어지는 크레딧 값
ocredit=N	숫자, 영대문자/소문자를 제외한 기타 문자
각항목에서 -1 값을 주면 해당하는 문자를 반드시 포함 시켜야 함	

조치 시 영향	패스워드 변경 시 Web, Was, DB연동 구간에서 문제가 발생할 수 있으므로 연동 구간에 미칠 수 있는 영향을 고려하여 적용 필요
---------	----------------------------------------------------------------------------



취약점 항목		1.5 root 이외의 UID가 '0' 금지			
대상 OS	Cent OS	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.				
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				
보안 설정 방법					
1. "/etc/passwd" 에 UID가 0인 계정 확인					
					
그림 4 fuckroot					
2. fuckroot가 UID가 0이므로 fuckroot 계정 제거 – userdel fuckroot					
					
그림 5 fuckroot 제거					
조치 시 영향	해당 계정에 관리자 권한이 필요하지 않으면 일반적으로 영향 없음				

취약점 항목	1.6 root 계정 su 제한				
대상 OS	Cent OS	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					
판단기준	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 요청 받은 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				
보안 설정 방법					
1. "wheel" 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인  #cat /etc/group   grep wheel    그림 6 /etc/group					
2. 허용 그룹(su 명령어 사용 그룹) 설정 여부 확인  #cat /etc/pam.d/su					

```
#%PAM-1.0
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            include         system-auth
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         optional        pam_xauth.so
```

그림 7 /etc/pam.d/su

3. "auth required pam\_wheel.so use\_uid" 의 주석을 제거

```
# Uncomment the following line to require a user to be in the "wheel" group.
auth            required        pam_wheel.so use_uid
auth            include         system-auth
```

그림 8 /etc/pam.d/su

4. usermod -G wheel heonjin

5. cat /etc/group | grep wheel

```
[root@victim ~]# cat /etc/group | grep wheel
wheel:x:10:root,heonjin
```

그림 9 /etc/group

6. chmod 4755 /bin/su

chgrp wheel /bin/su

```
[root@victim ~]# ls -al /bin/su
-rwxr-xr-x 1 root wheel 23960 Jan 21 2009 /bin/su
[root@victim ~]# _
```

그림 10 /bin/su 옵션변경

7. wheel 그룹에 있는 계정 제외하고 su 접근 차단

```
[lee@victim ~]$ su
Password:
su: incorrect password
[lee@victim ~]$ _
```

그림 11 su 접근 차단

조치 시 영향	그룹에 추가된 계정들은 모든 Session 종료 후 재로그인 시 su 명령어 사용 가능
---------	--------------------------------------------------

취약점 항목	1.7 패스워드 최소 길이 설정				
	1.8 패스워드 최대 길이 설정				
	1.9 패스워드 최소 사용기간 설정				
	대상 OS	Cent OS	위험도	중	Code
					U-07 U-08 U-09
취약점 개요	<p>-패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격&gt;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.</p>				
	<p>-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.</p>				
	<p>-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.</p>				
보안대책					
판단기준	<p><b>양호 :</b></p> <ul style="list-style-type: none"><li>- 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우</li><li>- 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있는 경우</li><li>- 패스워드 최소 사용기간이 1일(1주)로 설정되어 있는 경우</li></ul>				
	<p><b>취약 :</b></p> <ul style="list-style-type: none"><li>- 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우</li><li>- 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있지 않는 경우</li><li>- 패스워드 최소 사용기간이 설정되어 있지 않는 경우</li></ul>				
조치방법	<ul style="list-style-type: none"><li>- 패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정</li><li>- 패스워드 정책 설정파일을 수정하여 패스워드 최대 사용기간을 90일(12주)로 설정</li><li>- 패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정</li></ul>				
	보안 설정 방법				

1. vi 편집기를 이용하여 “/etc/login.defs” 파일 편집

```
PASS_MAX_DAYS    99999
PASS_MIN_DAYS    0
PASS_MIN_LEN     5
PASS_WARN_AGE    7
```

그림 12 /etc/login.defs

2. “PASS\_MIN\_LEN”를 8이상으로 변경

“PASS\_MAX\_DAYS”를 90일(12주) 이하로 변경

“PASS\_MIN\_DAYS”를 1로 변경

```
PASS_MAX_DAYS    90
PASS_MIN_DAYS    1
PASS_MIN_LEN     8
PASS_WARN_AGE    7
```

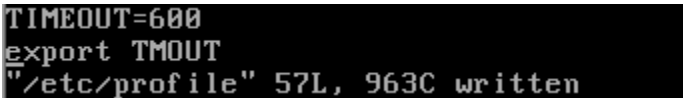
그림 13 /etc/login.defs

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

취약점 항목	1.10 불필요한 계정 제거				
대상 OS	Cent OS	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				

보안 설정 방법	
<p>1. "cat /etc/passwd"로 서버에 등록된 불필요한 사용자 계정 확인</p> <pre>mysql:x:500:500::/home/mysql:/bin/bash neotra:x:501:501::/home/neotra:/bin/bash heonjin:x:502:502::/home/heonjin:/bin/bash lee:x:503:503::/home/lee:/bin/bash [root@victim ~]#</pre> <p>그림 14 /etc/passwd</p> <p>2. userdel 명령으로 불필요한 사용자 계정 삭제</p> <pre>[root@victim ~]# userdel neotra [root@victim ~]# tail -n 4 /etc/passwd xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin mysql:x:500:500::/home/mysql:/bin/bash heonjin:x:502:502::/home/heonjin:/bin/bash lee:x:503:503::/home/lee:/bin/bash [root@victim ~]#</pre> <p>그림 15 /etc/passwd</p> <p>3. 사용하지 않는 default 계정 점검</p> <pre>[root@victim ~]# cat /etc/passwd   grep lp lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin [root@victim ~]# cat /etc/passwd   grep uucp uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin [root@victim ~]# cat /etc/passwd   grep nuucp [root@victim ~]#</pre> <p>그림 16 default 계정 점검</p>	
조치 시 영향	일반적으로 영향 없음

취약점 항목	1.15 Session Timeout 설정				
대상 OS	Cent OS	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 않는 경우
조치방법	600초(10분) 동안 입력이 없을 경우 접속된 Session을 끊도록 설정
보안 설정 방법	
1. Linux, AIX, HP-UX - "vi /etc/profile(.profile)" 명령 실행 - 아래와 같이 수정 또는 추가 TIMEOUT=600 (단위:초) export TMOUT 	
그림 17 /etc/profile	
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

## 2.2 파일 및 디렉터리 관리

취약점 항목	2.2 파일 및 디렉터리 소유자 설정				
대상 OS	Cent OS	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				
보안 설정 방법					

1. find / -nouser -print

find / -nogroup -print

소유자가 nouser, nogroup인 파일이나 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 디렉터리 및 파일 삭제 또는, 소유자 및 그룹을 변경함

```

/usr/local/apache/icons/world2.gif
/usr/bin/pstree
/usr/bin/top
/usr/bin/dir
/usr/bin/find
/usr/bin/md5sum
/home/neotra
/home/neotra/.bashrc
/home/neotra/.bash_logout
/home/neotra/.mozilla
/home/neotra/.mozilla/extensions
/home/neotra/.mozilla/plugins
/home/neotra/.viminfo
/home/neotra/.bash_history
/home/neotra/.bash_profile
/bin/netstat
/bin/ps
/bin/ls
find: /proc/9154/task/9154/fd/4: No such file or directory
find: /proc/9154/fd/4: No such file or directory
/var/spool/mail/neotra
[root@victim ~]# find / -nouser -print_

```

그림 18 find 명령어

2. 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제

#rm <file\_name>

#rm <directory\_name>

※ 삭제할 파일명 또는 디렉터리명 입력

3. 필요한 경우 chown 명령으로 소유자 및 그룹 변경

#chown <user\_name> <file\_name>

조치 시 영향

일반적인 경우 영향 없음

취약점 항목	2.5 /etc/hosts 파일 소유자 및 권한 설정				
	2.6. /etc/(x)inetd.conf 파일 소유자 및 권한 설정				
대상 OS	Cent OS	위험도	상	Code	U-20 U-21
취약점 개요	<p>- "/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.</p>				



	<ul style="list-style-type: none"> <li>- 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.</li> </ul>
<b>보안대책</b>	
<b>판단기준</b>	<b>양호 :</b> <ul style="list-style-type: none"> <li>- /etc/hosts 파일의 소유자가 root이고, 권한이 600인 경우</li> <li>- /etc/inetd.conf 파일의 소유자가 root이고, 권한이 600인 경우</li> </ul>
	<b>취약 :</b> <ul style="list-style-type: none"> <li>- /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우</li> <li>- /etc/inetd.conf 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우</li> </ul>
<b>조치방법</b>	<ul style="list-style-type: none"> <li>- "/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)</li> <li>- "/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)</li> </ul>
<b>보안 설정 방법</b>	
1. "ls -l /etc/hosts"로 권한 확인 <pre>[root@victim ~]# ls -al /etc/hosts -rw-r--r--  1 root    root      194 May  3  2009 /etc/hosts</pre>	
<p style="text-align: center;"><b>그림 19 /etc/hosts</b></p> <p>"ls -l /etc/xinetd.d/*"로 권한 확인</p> <pre>[root@victim ~]# ls -al /etc/xinetd.d/* -rw-r--r--  1 root    root      523 Mar 17  2007 /etc/xinetd.d/cvs -rw-r--r--  1 root    root      323 Sep  9  2004 /etc/xinetd.d/eklogin -rw-r--r--  1 root    root      347 Sep  6  2005 /etc/xinetd.d/ekrb5-telnet -rw-r--r--  1 root    root      326 Sep  9  2004 /etc/xinetd.d/gssftp -rw-r--r--  1 root    root      310 Sep  9  2004 /etc/xinetd.d/klogin -rw-r--r--  1 root    root      323 Sep  9  2004 /etc/xinetd.d/krb5-telnet -rw-r--r--  1 root    root      308 Sep  9  2004 /etc/xinetd.d/kshell -rw-r--r--  1 root    root      317 Jan  6  2007 /etc/xinetd.d/rsync</pre>	
<p style="text-align: center;"><b>그림 20 /etc/xinetd.d</b></p>	
2. 소유자는 root, 권한은 600으로 변경 <pre>[root@victim ~]# chmod 600 /etc/hosts [root@victim ~]# ls -al /etc/hosts -rw-----  1 root    root      194 May  3  2009 /etc/hosts</pre>	
<p style="text-align: center;"><b>그림 21 /etc/hosts</b></p>	

```

[root@victim ~]# chmod -R 600 /etc/xinetd.d
[root@victim ~]# ls -al /etc/xinetd.d/*
-rw----- 1 root root 523 Mar 17 2007 /etc/xinetd.d/cvs
-rw----- 1 root root 323 Sep 9 2004 /etc/xinetd.d/eklogin
-rw----- 1 root root 347 Sep 6 2005 /etc/xinetd.d/ekrb5-telnet
-rw----- 1 root root 326 Sep 9 2004 /etc/xinetd.d/gssftp
-rw----- 1 root root 310 Sep 9 2004 /etc/xinetd.d/klogin
-rw----- 1 root root 323 Sep 9 2004 /etc/xinetd.d/krb5-telnet
-rw----- 1 root root 308 Sep 9 2004 /etc/xinetd.d/kshell
-rw----- 1 root root 317 Jan 6 2007 /etc/xinetd.d/rsync

```

그림 22 /etc/xinetd.d

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

취약점 항목	2.9 SUID, SGID, Sticky bit 설정파일 점검				
대상 OS	Cent OS	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.				
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 파일을 발견 시 SUID 제거 필요				
보안 설정 방법					

1. 아래의 표에서 파일명을 확인하여 SUID, SGID을 제거하여야 함

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	

- "find / -user root -perm +4000" 으로 SUID 파일 조회



그림 23 SUID

- "/usr/bin/at"과 "usr/bin/newgrp" 발견

2. SUID가 필요없는 파일 SUID 제거

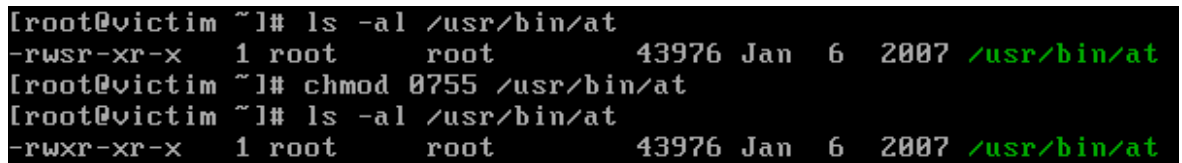


그림 24 SUID 제거

- "chmod 0755 /usr/bin/at"
- "chmod 0755 /usr/bin/newgrp"
- 위 명령으로 SUID 제거

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

취약점 항목	2.11 world writable 파일 점검				
대상 OS	Cent OS	위험도	상	Code	U-26

<b>취약점 개요</b>	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.
<b>보안대책</b>	
<b>판단기준</b>	<b>양호</b> : world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우
	<b>취약</b> : world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우
<b>조치방법</b>	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거
<b>보안 설정 방법</b>	
1. world writeable 파일 존재 여부 확인 - find / -perm 2 -ls <div data-bbox="378 1008 1208 1411" data-label="Text"> <pre> 1420230684  0 -rw-rw-rw-  1 root    root          0 Jan  5 19:43 /proc/216 71/attr/keycreate 1420230685  0 -rw-rw-rw-  1 root    root          0 Jan  5 19:43 /proc/216 71/attr/sockcreate 1178532    1 lrwxrwxrwx  1 root    root          10 May  3 2009 /var/mail -&gt; spool/mail 1178500    4 drwxrwxrwt  2 root    root        4096 May  3 2009 /var/tmp 1178731    0 srwxrwxrwx  1 avahi   avahi         0 Jan  5 18:03 /var/run/ava hi-daemon/socket 1178707    0 srw-rw-rw-  1 root    root          0 Jan  5 18:03 /var/run/acp id.socket 1178694    0 srwxrwxrwx  1 root    root          0 Jan  5 18:03 /var/run/dbu s/system_bus_socket 1178711    0 srwxrwxrwx  1 root    root          0 Jan  5 18:03 /var/run/cup s/cups.sock 1178702    0 srwxrwxrwx  1 root    root          0 Jan  5 18:03 /var/run/pcs ed.comm 1178593    0 srwxrwxrwx  1 root    root          0 Jan  5 18:03 /var/run/set rans/.setrans-unix 1178660    4 drwxrwxrwt  2 root    root        4096 May 25 2008 /var/cache/c oolkey [root@victim ~]# </pre> </div>	
<b>그림 25 world writable</b>	
2. 일반 사용자 쓰기 권한 제거 - chmod o-w <file_name>	
3. 파일 삭제 - rm -rf <world-writable 파일명>	
<b>조치 시 영향</b>	일반적인 경우 영향 없음

취약점 항목	2.14 접속 IP 및 포트 제한				
대상 OS	Cent OS	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				
보안 설정 방법					
1. "cat /etc/hosts.deny"					
"cat /etc/hosts.allow" 접근 허용 IP 설정을 확인					
<pre>[root@victim dev]# cat /etc/hosts.allow ## ## hosts.allow   This file describes the names of the hosts which are ##               allowed to use the local INET services, as decided ##               by the '/usr/sbin/tcpd' server. ## [root@victim dev]# cat /etc/hosts.deny ## ## hosts.deny    This file describes the names of the hosts which are ##               *not* allowed to use the local INET services, as decided ##               by the '/usr/sbin/tcpd' server. ## ## The portmap line is redundant, but it is left to remind you that ## the new secure portmap uses hosts.deny and hosts.allow.  In particular ## you should know that NFS uses portmap!</pre>					
그림 26 접근 허용 IP 설정					
- 설정이 전부 안되어 있음					
2. "/etc/hosts.allow" 와 "/etc/hosts.deny" 옵션 변경					

```

[root@victim ~]# cat /etc/hosts.allow
#
# hosts.allow  This file describes the names of the hosts which are
#              allowed to use the local INET services, as decided
#              by the '/usr/sbin/tcpd' server.
#
sshd : 127.0.0.1
[root@victim ~]# cat /etc/hosts.deny
#
# hosts.deny   This file describes the names of the hosts which are
#              *not* allowed to use the local INET services, as decided
#              by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.  In particular
# you should know that NFS uses portmap!
#
ALL:ALL
[root@victim ~]#

```

그림 27 접근 허용 IP 설정

조치 시 영향	허용되지 않은 IP는 접속 불가
---------	-------------------

## 2.3 서비스 관리

취약점 항목	3.2 Anonymous FTP 비활성화				
대상 OS	Cent OS	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.				
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				
보안 설정 방법					

1. /etc/passwd 파일에 ftp 계정 존재 여부 확인

- cat /etc/passwd | grep ftp

```
[root@victim ~]# cat /etc/passwd | grep ftp
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

그림 28 ftp 계정 존재 확인

2. 일반 FTP – Anonymous FTP 접속 제한 설정 방법

"/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제

```
[root@victim ~]# cat /etc/passwd | grep ftp
[root@victim ~]# _
```

그림 29 ftp 계정 삭제 확인

조치 시 영향	Anonymous FTP를 사용하지 않을 경우 영향 없음
---------	---------------------------------

취약점 항목	3.4 cron 파일 소유자 및 권한 설정				
대상 OS	Cent OS	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.				
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)				
보안 설정 방법					

1. /var/spool/cron/crontab/\*

- "cron" 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

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

```
[root@victim ~]# cd /etc/cron
cron.d/      cron.deny    cron.monthly/ cron.weekly/
cron.daily/  cron.hourly/ crontab
```

그림 30 /etc/cron\*

- "/etc/cron.allow"는 존재 하지 않아서 "touch /etc/cron.allow"로 파일 생성

```
[root@victim ~]# ls -al /etc | grep cron*
-rw-r--r-- 1 root root      298 Mar 28 2007 anacrontab
-rw-r--r-- 1 root root         0 Jan  5 21:42 cron.allow
drwx----- 2 root root    4096 Feb 27 2009 cron.d
drwxr-xr-x 2 root root    4096 May  3 2009 cron.daily
-rw-r--r-- 1 root root         0 May  3 2009 cron.deny
drwxr-xr-x 2 root root    4096 Jan  6 2007 cron.hourly
drwxr-xr-x 2 root root    4096 May  3 2009 cron.monthly
drwxr-xr-x 2 root root    4096 May  3 2009 cron.weekly
-rw-r--r-- 1 root root      400 May  3 2009 crontab
```

그림 31 /etc/cron\*

- 권한이 640이하가 아니라서 권한 변경

3. "chmod 640 /etc/cron.allow /etc/cron.deny" 로 권한 변경

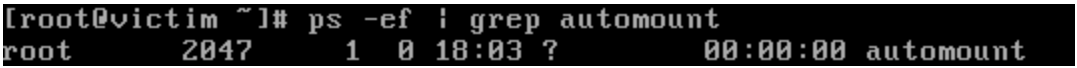
```
[root@victim ~]# chmod 640 /etc/cron.allow /etc/cron.deny
[root@victim ~]# ls -al /etc | grep cron*
-rw-r--r-- 1 root root      298 Mar 28 2007 anacrontab
-rw-r----- 1 root root         0 Jan  5 21:42 cron.allow
drwx----- 2 root root    4096 Feb 27 2009 cron.d
drwxr-xr-x 2 root root    4096 May  3 2009 cron.daily
-rw-r----- 1 root root         0 May  3 2009 cron.deny
drwxr-xr-x 2 root root    4096 Jan  6 2007 cron.hourly
drwxr-xr-x 2 root root    4096 May  3 2009 cron.monthly
drwxr-xr-x 2 root root    4096 May  3 2009 cron.weekly
-rw-r----- 1 root root      400 May  3 2009 crontab
```

그림 32 /etc/cron\*

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

취약점 항목	3.6 automountd 제거				
대상 OS	Cent OS	위험도	상	Code	U-43



<b>취약점 개요</b>	automountd 데몬 에는 로컬 공격자가 데몬에 *RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하여 이를 통해 파일 시스템의 마운트 옵션을 변경하여 root권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음.
<b>보안대책</b>	
<b>판단기준</b>	<b>양호</b> : automountd 서비스가 비활성화 되어 있는 경우
	<b>취약</b> : automountd 서비스가 활성화 되어 있는 경우
<b>조치방법</b>	automountd 서비스 비활성화
<b>보안 설정 방법</b>	
1. ps -ef   grep automount  <p style="text-align: center;"><b>그림 33 automount 확인</b></p> 2. automountd 서비스 데몬 중지 - kill -9 2047	
<b>조치시 영향</b>	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)

취약점 항목	3.17 Apache 디렉터리 리스팅 제거				
대상 OS	Cent OS	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				

	<b>취약</b> : 디렉터리 검색 기능을 사용하는 경우
<b>조치방법</b>	디렉터리 검색 기능 제거 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시자 에서 Indexes 옵션 제거)
<b>보안 설정 방법</b>	
1. Indexes 옵션 사용 여부 확인 - "vi /usr/local/apache/conf/httpd.conf"에 Indexes 옵션 확인 <div data-bbox="343 591 1243 828" data-label="Text"> <pre>&lt;Directory "/usr/local/apache/htdocs"&gt; # # This may also be "None", "All", or any combination of "Indexes", # "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews". # # Note that "MultiViews" must be named *explicitly* --- "Options All" # doesn't give it to you. # Options Indexes FollowSymLinks MultiViews</pre> </div> <p style="text-align: center;"><b>그림 34 /usr/local/apache/conf/httpd.conf</b></p>	
2. Indexes 제거 <div data-bbox="320 992 1265 1247" data-label="Text"> <pre>&lt;Directory "/usr/local/apache/htdocs"&gt; # # This may also be "None", "All", or any combination of "Indexes", # "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews". # # Note that "MultiViews" must be named *explicitly* --- "Options All" # doesn't give it to you. # Options FollowSymLinks MultiViews</pre> </div> <p style="text-align: center;"><b>그림 35 /usr/local/apache/conf/httpd.conf</b></p>	
<b>조치 시 영향</b>	일반적인 경우 영향 없음

취약점 항목	3.21 Apache 링크 사용금지				
대상 OS	Cent OS	위험도	상	Code	U-57
<b>취약점 개요</b>	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.
<b>보안대책</b>	
<b>판단기준</b>	<b>양호</b> : 심볼릭 링크, aliases 사용을 제한한 경우
	<b>취약</b> : 심볼릭 링크, aliases 사용을 제한하지 않은 경우
<b>조치방법</b>	심볼릭 링크, aliases 사용 제한 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시자에서 심볼릭 링크를 가능하게 하는 FollowSymLinks 옵션 제거)
<b>보안 설정 방법</b>	
1. “vi /usr/local/apache/conf/httpd.conf”에 FollowSymLinks 확인 <div data-bbox="542 846 1046 983" data-label="Text"> <pre>&lt;Directory /&gt;     Options FollowSymLinks     AllowOverride None &lt;/Directory&gt;</pre> </div> <p style="text-align: center;"><b>그림 36 FollowSymLinks</b></p> 2. FollowSymLinks 제거 <div data-bbox="568 1149 1021 1283" data-label="Text"> <pre>&lt;Directory /&gt;     Options_     AllowOverride None &lt;/Directory&gt;</pre> </div> <p style="text-align: center;"><b>그림 37 FollowSymLinks</b></p>	
<b>조치 시 영향</b>	일반적인 경우 영향 없음

취약점 항목	3.23 Apache 웹 서비스 영역의 분리				
대상 OS	Cent OS	위험도	상	Code	U-58
<b>취약점 개요</b>	Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs디렉터리는 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
보안 설정 방법	
<p>1. "vi /usr/local/apache/conf/httpd.conf"에 접속 해서 DocumentRoot 디렉토리 확인</p> <pre>DocumentRoot "/usr/local/apache/htdocs"</pre> <p>그림 38 DocumentRoot</p> <p>- 확인결과 기본설정 "/usr/local/apache/htdocs"으로 변경해 줘야 함.</p> <p>2. 별도의 디렉터리로 변경</p> <pre>DocumentRoot "/usr/local/apache/heonjin"</pre> <p>그림 39 DocumentRoot</p>	
조치 시 영향	일반적인 경우 영향 없음

취약점 항목	3.26 ftp 계정 shell 제한				
대상 OS	Cent OS	위험도	중	Code	U-61
취약점 개요	FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인 필요하지 않은 기본 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하여야 함. 로그인이 불필요한 기본 계정에 쉘(Shell)을 부여할 경우 공격자에게 해당 계정이 노출되어 시스템 불법 침투가 발생할 수 있음.				
보안대책					
판단기준	양호 : ftp 계정에 /bin/false 쉘이 부여되어 있는 경우				
	취약 : ftp 계정에 /bin/false 쉘이 부여되어 있는 경우				
조치방법	ftp 계정에 /bin/false 쉘 부여				
보안 설정 방법					

### 1. ftp 계정에 대한 /bin/false 부여 확인

"cat /etc/passwd | grep ftp"

```
[root@victim ~]# cat /etc/passwd | grep ftp
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

그림 40 /etc/passwd

- ftp 셸이 "/sbin/nologin"으로 됨

### 2. vi 편집기로 "vi /etc/passwd"

- "/bin/false"로 변경

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

취약점 항목		3.32 로그인 시 경고 메시지 제공			
대상 OS	Cent OS	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				
보안 설정 방법					
1. "vi /etc/motd" (수정 전) 내용 없음 (수정 후) 로그인 메시지 입력 <div>Hello Heonjin</div> 그림 41 /etc/motd					
2. Telnet 배너 설정 : "vi /etc/issue.net" 파일에 로그인 메시지 입력					

```
Who are you?
Hacking?? Fuck
I see you!!!
```

그림 42 /etc/issue.net

```
[root@victim ~]# ssh root@127.0.0.1
root@127.0.0.1's password:
Last login: Fri Jan 6 15:07:38 2017 from victim
Hello Heonjin
```

그림 43 접속 모습

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

취약점 항목	3.35 Apache 웹 서비스 정보 숨김				
대상 OS	Cent OS	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)				
보안 설정 방법					
1. "vi /usr/local/apache/conf/httpd.conf" - ServerTokens Prod 설정이 되어 있는지 확인					
<pre>&lt;Directory /&gt;     Options FollowSymLinks     AllowOverride None &lt;/Directory&gt;</pre>					
그림 44 ServerTokens					

2. ServerTokens가 없으므로 추가

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    ServerTokens Prod
</Directory>
```

그림 45 ServerTokens

- 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정

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

## 2.4 패치 관리

취약점 항목	4.1 최신 보안패치 및 벤더 권고사항 적용				
대상 OS	Cent OS	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 OS관리자 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				
보안 설정 방법					

- 리눅스는 서버에 설치된 패치 리스트의 관리가 불가능하므로 패키지 별 버그가 Fix된 최신 버전 설치가 필요함.
- 리눅스의 최신 버전이 나올 시 최신버전으로 업데이트가 필요함.

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

## 2.5 로그 관리

취약점 항목		5.2 정책에 따른 시스템 로깅 설정			
대상 OS	Cent OS	위험도	하	Code	U-73
취약점 개요	감사 설정이 구성되어 있지 않거나 보안 정책에 비하여 감사 설정 수준이 낮아 보안사고가 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				
보안 설정 방법					
1. "vi /etc/syslog.conf" 파일 편집					
<div><pre>*.info;mail.none;authpriv.none;cron.none    /var/log/messages # The authpriv file has restricted access. authpriv.*    /var/log/secure # Log all the mail messages in one place. mail.*    -/var/log/maillog # Log cron stuff cron.*    /var/log/cron # Everybody gets emergency messages *.emerg    *</pre></div>					
그림 46 /etc/syslog.conf					
2. 아래와 같이 수정 또는, 신규 삽입					
<div><ul style="list-style-type: none"><li>- *.info;mail.none;authpriv.none;cron.none /var/log/messages</li><li>- authpriv.* /var/log/secure</li><li>- mail.* /var/log/maillog</li><li>- cron.* /var/log/cron</li></ul></div>					



- \*.alert /dev/console
- \*.emerg \*

```

*.info;mail.none;authpriv.none;cron.none    /var/log/messages

# The authpriv file has restricted access.
authpriv.*    /var/log/secure

# Log all the mail messages in one place.
mail.*    -/var/log/maillog

# Log cron stuff
cron.*    /var/log/cron

*.alert    /dev/console

# Everybody gets emergency messages
*.emerg    *

```

그림 47 /etc/syslog.conf

### 3. 설정 후 syslog 데몬 재시작

- "ps -ef | grep syslogd"
- "kill -HUP [PID]"
- "service syslog restart"

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

### 3. Nessus

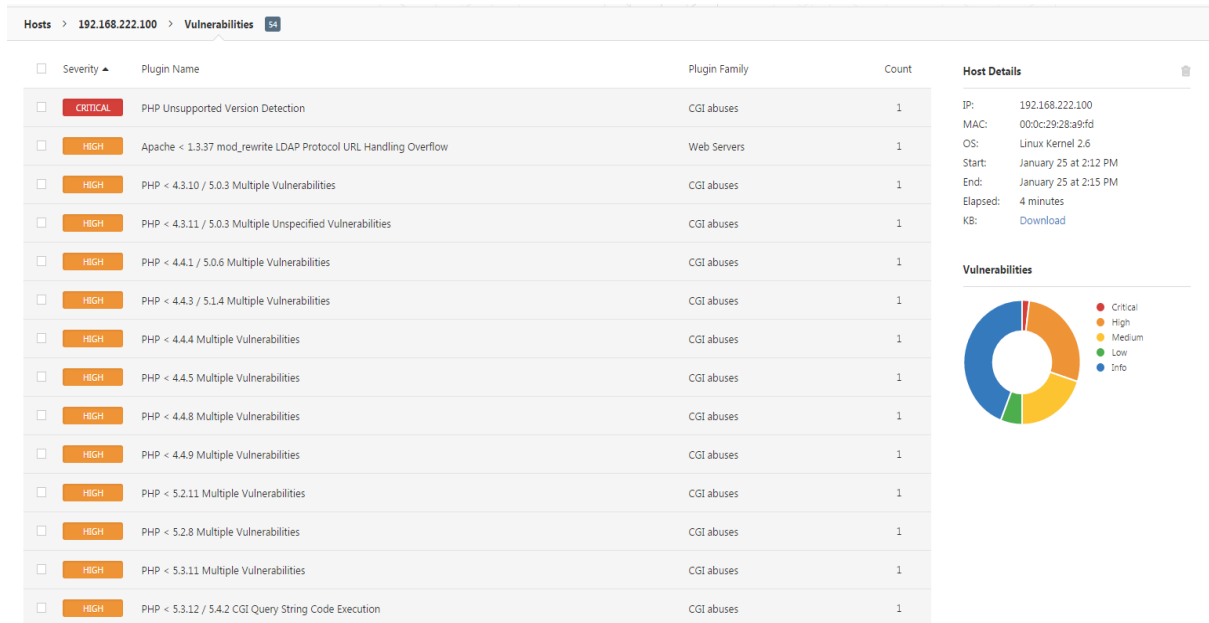


그림 48 NESSUS

- PHP 4.3.9 버전을 사용하고 있음
- PHP 버전이 낮아서 많은 취약점을 가지고 있음