

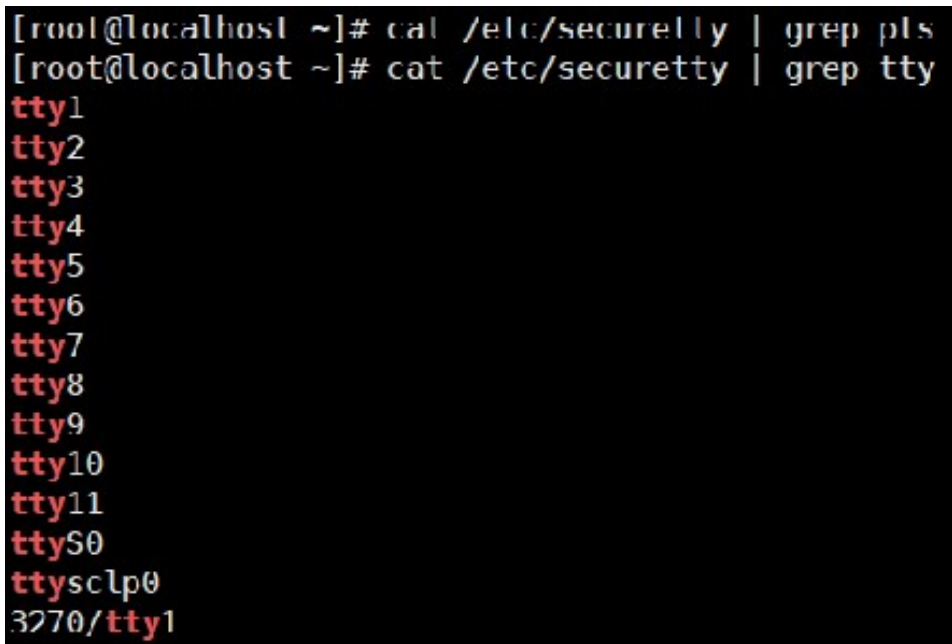
## 2.3. Linux

계정 관리(5개 항목), 파일 및 디렉토리 관리(14개 항목), 서비스 관리(15개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 36개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	U-01	root 계정 원격 접속 제한	상
	U-02	패스워드 복잡성 설정	상
	U-03	계정 잠금 임계값 설정	상
	U-04	패스워드 최대 사용 기간 설정	중
	U-05	패스워드 파일 보호	상
나. 파일 및 디렉토리 관리	U-06	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-07	파일 및 디렉터리 소유자 설정	상
	U-08	/etc/passwd 파일 소유자 및 권한 설정	상
	U-09	/etc/shadow 파일 소유자 및 권한 설정	상
	U-10	/etc/hosts 파일 소유자 및 권한 설정	상
	U-11	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-12	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	U-13	/etc/services 파일 소유자 및 권한 설정	상
	U-14	SUID, SGID, Sticky bit 설정 파일 점검	상
	U-15	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상
	U-16	world writable 파일 점검	상
	U-17	\$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-18	접속 IP 및 포트 제한	상
	U-19	cron 파일 소유자 및 권한 설정	상
다. 서비스 관리	U-20	Finger 서비스 비활성화	상
	U-21	Anonymous FTP 비활성화	상
	U-22	r 계열 서비스 비활성화	상
	U-23	DoS 공격에 취약한 서비스 비활성화	상
	U-24	NFS 서비스 비활성화	상
	U-25	NFS 접근통제	상
	U-26	automountd 제거	상
	U-27	RPC 서비스 확인	상
	U-28	NIS, NIS+ 점검	상
	U-29	tftp, talk 서비스 비활성화	상
	U-30	Sendmail 버전 점검	상
	U-31	스팸 메일 릴레이 제한	상
	U-32	일반사용자의 Sendmail 실행 방지	상
	U-33	DNS 보안 버전 패치	상
	U-34	DNS ZoneTransfer 설정	상
라. 패치 및 로그관리	U-35	최신 보안패치 및 벤더 권고사항 적용	상
	U-36	로그의 정기적 검토 및 보고	상

[표 3] Linux서버 진단 체크리스트

## 가. 계정 관리

진단항목	U-01. root 계정 원격 접속 제한		취약도	상
항목설명	각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 root 원격 접속 차단이 적용되지 않은 시스템의 root 계정 정보를 비인가자가 획득할 경우 시스템 계정 정보 유출, 파일 및 디렉터리 변조 등의 행위 침해사고가 발생할 수 있다.			
진단기준	양호	원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우		
	취약	원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우		
진단방법	<div>■ Telnet</div> <div>1) /etc/securetty 파일에 pts/0 ~ pts/x 관련 설정이 존재하는지 확인</div> <div># cat /etc/securetty</div> <div></div> <div>※ tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함</div> <div>※ pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함</div> <div>■ SSH</div> <div>1) /etc/ssh/sshd_config 파일에서 Root 로그인 설정 확인</div> <div># cat /etc/ssh/sshd_config   grep PermitRootLogin</div>			

	<pre>[root@localhost ~]# cat /etc/ssh/sshd_config   grep PermitRootLogin #PermitRootLogin yes # the setting of "PermitRootLogin without-password".</pre>
조치방법	<ul style="list-style-type: none"> <li>■ Telnet             <ol style="list-style-type: none"> <li>1) "/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리</li> </ol> </li> <li>■ SSH             <ol style="list-style-type: none"> <li>1) vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후                     <pre># vi /etc/ssh/sshd_config</pre> </li> <li>2) 아래와 같이 설정 변경                     <pre>PermitRootLogin no</pre> <pre>#loginGraceTime 2m PermitRootLogin no #StrictModes yes</pre> </li> </ol> </li> </ul>
비고	

진단항목	U-02. 패스워드 복잡성 설정		취약도	상
항목설명	패스워드 복잡성 설정이 되어 있지 않은 사용자 계정 패스워드 존재 시 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 취약한 패스워드가 설정된 사용자 계정의 패스워드를 획득하여 획득한 사용자 계정 정보를 통해 해당 사용자 계정의 시스템에 접근할 수 있는 위험이 존재한다.			
진단기준	양호	영문, 숫자, 특수문자를 조합하여 2종류 조합 시 10자리 이상, 3종류 이상 조합 시 8자리 이상의 패스워드가 설정된 경우(공공기관 9자리 이상)		
	취약	영문, 숫자, 특수문자를 조합하지 않거나 2종류 조합 시 10자리 미만, 3종류 이상 조합 시 8자리 미만의 패스워드가 설정된 경우(공공기관 9자리 미만)		
진단방법	<div>■ Debian 계열</div> <div>1) /etc/pam.d/common-password 파일 또는 /etc/security/pwquality.conf 파일 설정 내용 확인</div> <div># cat /etc/pam.d/common-password 또는</div> <div># cat /etc/security/pwquality.conf</div> <div>■ RHEL 계열</div> <div>1) /etc/pam.d/system-auth 파일 또는 /etc/security/pwquality.conf 파일 설정 내용 확인</div> <div># cat /etc/pam.d/system-auth</div> <div># cat /etc/security/pwquality.conf</div>			
조치방법	<div>■ Debian 계열</div> <div>1) /etc/pam.d/common-password 파일 또는 /etc/security/pwquality.conf 파일 편집</div> <div># vi /etc/pam.d/common-password 또는</div> <div># vi /etc/security/pwquality.conf</div> <div><div>password requisite</div><div>pam_pwquality.so enforce_for_root</div><div>retry=3 minlen=8 dcredit=-1</div><div>ucredit=-1 lcredit=-1 ocredit=-1</div></div> <div>■ RHEL 계열</div> <div>1) /etc/pam.d/system-auth 파일 또는 /etc/security/pwquality.conf 파일 편집</div> <div># vi /etc/pam.d/system-auth 또는</div> <div># vi /etc/security/pwquality.conf</div>			

	<pre>password requisite pam_pwquality.so try_first_pass local_users_only enforce_for_root retry=3 authtok_type= minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1</pre>
<b>비고</b>	<p>lcredit=-1(최소 소문자 요구),  ucredit=-1(최소 대문자 요구),  dcredit=-1(최소 숫자 요구),  ocredit=-1(최소 특수문자 요구),  minlen=8(최소 8자리 이상)  enforce_for_root(root 계정의 경우에도 정책 적용)</p>

진단항목	U-03. 계정 잠금 임계값 설정		취약도	상
항목설명	로그인 실패 임계값이 설정되어 있지 않을 경우 반복되는 로그인 시도에 대한 차단이 이루어지지 않아 각종 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)에 취약하여 비인가자에게 사용자 계정 패스워드를 유출 당할 수 있다.			
진단기준	양호	계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우		
	취약	계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되어 있지 않은 경우		
진단방법	<div>■ Debian 계열</div> <div>1) /etc/pam.d/common-auth 파일에서 임계값 설정 확인</div> <div># cat /etc/pam.d/common-auth</div> <div>■ RHEL 계열</div> <div>1) /etc/pam.d/password-auth 파일에서 임계값 설정 확인</div> <div># cat /etc/pam.d/password-auth</div> <div><pre>[root@localhost ~]# cat /etc/pam.d/password-auth   grep auth # User changes will be destroyed the next time authconfig is run. auth      required      pam_env.so auth      required      pam_tally2.so deny=5 no_magic_root auth      required      pam_faildelay.so delay=2000000 auth      sufficient    pam_unix.so nullok try_first_pass auth      requisite     pam_succeed_if.so uid &gt;= 1000 quiet t_success</pre></div> <div>2) /etc/pam.d/system-auth 파일에서 임계값 설정 확인</div> <div># cat /etc/pam.d/system-auth</div> <div><pre>[root@localhost ~]# cat /etc/pam.d/system-auth   grep account account    required      pam_unix.so account    required      pam_tally2.so deny=5 no_magic_root account    sufficient    pam_localuser.so account    sufficient    pam_succeed_if.so uid &lt; 1000 quiet account    required      pam_permit.so</pre></div>			
조치방법	<div>■ Debian 계열</div> <div>1) /etc/pam.d/common-auth 파일 내 설정 값을 변경</div> <div># vi /etc/pam.d/common-auth</div> <div>auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)</div> <div>■ RHEL 계열</div> <div>1) /etc/pam.d/system-auth 및 /etc/pam.d/password-auth 파일 내 설정 값</div>			

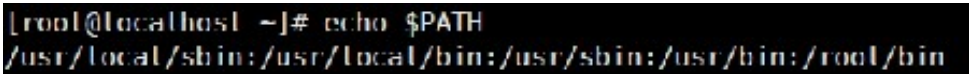
	<p>변경</p> <pre># vi /etc/pam.d/system-auth</pre> <div data-bbox="423 390 1382 430" style="border: 1px solid black; padding: 2px;">auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)</div> <pre># vi /etc/pam.d/password-auth</pre> <div data-bbox="423 491 1382 531" style="border: 1px solid black; padding: 2px;">account required pam_tally2.so deny=5 no_magic_root (두 번째 단락 2번째 줄)</div>
비고	<p>RHEL 계열의 경우, /etc/pam.d/system-auth 파일은 Console 접근, password-auth 파일은 SSH 접근 시 영향 받으므로 2가지 파일 모두 설정해야 함</p>

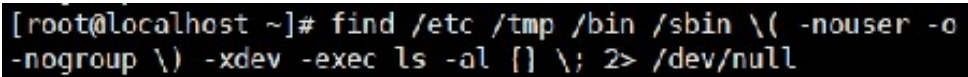
진단항목	U-04. 패스워드 최대 사용 기간 설정		취약도	중		
항목설명	패스워드 최대 사용기간을 설정하지 않은 경우 비인가자의 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 시도할 수 있는 기간 제한이 없으므로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행한 기간에 비례하여 사용자 패스워드가 유출될 수 있는 확률이 증가한다.					
진단기준	양호	패스워드의 최대 사용기간이 90일 이내로 설정되어 있는 경우				
	취약	패스워드의 최대 사용기간이 없거나, 90일 이내로 설정되어 있지 않은 경우				
진단방법	<div>■ /etc/login.defs 파일에서 패스워드 최대 사용 기간의 설정 값 확인</div> <div># cat /etc/login.defs   grep PASS_MAX_DAYS</div> <div><pre>[root@localhost ~]# cat /etc/login.defs   grep PASS_MAX_DAYS #          PASS_MAX_DAYS   Maximum number of days a password may be used. PASS_MAX_DAYS   99999</pre></div>					
조치방법	<div>■ User 생성 시 적용</div> <div># vi /etc/login.defs</div> <div><table><tr><td>PASS_MAX_DAYS</td><td>90</td></tr></table></div> <div><pre>[root@localhost ~]# vi /etc/login.defs [root@localhost ~]# cat /etc/login.defs   grep PASS_MAX_DAYS #          PASS_MAX_DAYS   Maximum number of days a password may be used. PASS_MAX_DAYS   90</pre></div> <div>■ 현재 User의 최대 사용기간 적용</div> <div>chage -M 90 &lt;계정명&gt;</div>				PASS_MAX_DAYS	90
PASS_MAX_DAYS	90					
비고						



진단항목	U-05. 패스워드 파일 보호		취약도	상
항목설명	비인가자에 의해 사용자 계정 패스워드가 평문으로 저장된 파일이 유출될 경우 시스템 사용자 계정 패스워드가 노출될 수 있다.			
진단기준	양호	쉐도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우		
	취약	쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우		
진단방법	<div>■ /etc/shadow 파일 존재 확인</div> <div># ls -l /etc/shadow</div> <div><pre>[root@localhost ~]# ls -l /etc/shadow -----. 1 root root 560 Sep 16 13:06 /etc/shadow</pre></div> <div>■ /etc/passwd 파일 내 두 번째 필드가 "x"표시가 되어 있는지 확인</div> <div># cat /etc/passwd</div> <div><pre>[root@localhost ~]# cat /etc/passwd root:x:0:0:root:/root:/bin/bash</pre></div>			
조치방법	<div>■ 쉐도우 패스워드 정책 적용 방법</div> <div># pwconv</div> <div><pre>[root@localhost ~]# pwconv</pre></div> <div>■ 일반 패스워드 정책 적용 방법</div> <div># pwunconv</div> <div><pre>[root@localhost ~]# pwunconv</pre></div>			
비고				

## 나. 파일 및 디렉토리 관리

진단항목	U-06. root 홈, 패스 디렉터리 권한 및 패스 설정		취약도	상
항목설명	관리자가 명령어(예: ls, mv, cp등)를 수행했을 때 root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면 현재 디렉터리에 명령어와 같은 이름의 악성파일이 실행되어 악의적인 행위가 일어날 수 있다.			
진단기준	양호	PATH 환경변수에 "."이 맨 앞이나 중간에 포함되지 않은 경우		
	취약	PATH 환경변수에 "."이 맨 앞이나 중간에 포함된 경우		
진단방법	<div>■ echo \$PATH 명령어로 현재 설정된 PATH 값 확인</div> <div># echo \$PATH</div> <div></div>			
조치방법	<div>■ vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile)을 연 후</div> <div># vi /etc/profile</div> <div>■ 아래와 같이 수정</div> <div>(수정 전) PATH=.:\$PATH:\$HOME/bin</div> <div>(수정 후) PATH=\$PATH:\$HOME/bin</div>			
비고				

진단항목	U-07. 파일 및 디렉터리 소유자 설정		취약도	상
항목설명	삭제된 소유자의 UID와 동일한 사용자가 해당 파일, 디렉터리에 접근 가능하여 사용자 정보 등 중요 정보가 노출될 위험이 있다.			
진단기준	양호	소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 없는 경우		
	취약	소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 있는 경우		
진단방법	<div>■ 시스템에서 소유자나 그룹이 존재하지 않는 파일 및 디렉터리를 검색</div> <div># find / -nouser -o -nogroup 또는</div> <div># find /etc /tmp /bin /sbin ₩( -nouser -o -nogroup ₩) -xdev -exec ls -al {} ₩; 2&gt; /dev/null</div> <div></div>			
조치방법	<div>■ 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제</div> <div># rm &lt;file_name&gt;</div> <div># rm -rf &lt;directory_name&gt;</div> <div>※ 삭제할 파일명 또는, 디렉터리 명 입력</div> <div>■ 필요한 경우 chown 명령으로 소유자 및 그룹 변경</div> <div># chown &lt;user_name&gt; &lt;file_name&gt;</div>			
비고				

진단항목	U-08. /etc/passwd 파일 소유자 및 권한 설정		취약도	상
항목설명	관리자(root) 외 사용자가 "/etc/passwd" 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능하다.			
진단기준	양호	/etc/passwd 파일의 소유자가 root이고, 권한이 644이하인 경우		
	취약	/etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우		
진단방법	<div>■ /etc/passwd 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/passwd</div> <div><pre>[root@localhost ~]# ls -l /etc/passwd -rw-r--r--. 1 root root 908 Sep 16 13:12 /etc/passwd</pre></div>			
조치방법	<div>■ /etc/passwd 파일의 소유자 및 권한 변경(소유자 root, 권한 644)</div> <div># chown root /etc/passwd</div> <div><pre>[root@localhost ~]# chown root /etc/passwd</pre></div> <div># chmod 644 /etc/passwd</div> <div><pre>[root@localhost ~]# chmod 644 /etc/passwd [root@localhost ~]# ls -l /etc/passwd -rw-r--r--. 1 root root 908 Sep 16 13:12 /etc/passwd</pre></div>			
비고				

진단항목	U-09. /etc/shadow 파일 소유자 및 권한 설정		취약도	상
항목설명	해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있다.			
진단기준	양호	/etc/shadow 파일의 소유자가 root이고, 권한이 400이하인 경우		
	취약	/etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400초과인 경우		
진단방법	<div>■ /etc/shadow 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/shadow</div> <div>[root@localhost ~]# ls -l /etc/shadow</div> <div>-----. 1 root root 560 Sep 16 13:05 /etc/shadow</div>			
조치방법	<div>■ "/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)</div> <div># chown root /etc/shadow</div> <div>[root@localhost ~]# chown root /etc/shadow</div> <div># chmod 400 /etc/shadow</div> <div>[root@localhost ~]# chmod 400 /etc/shadow</div> <div>[root@localhost ~]# ls -l /etc/shadow</div> <div>-r-----. 1 root root 560 Sep 16 13:05 /etc/shadow</div>			
비고				

진단항목	U-10. /etc/hosts 파일 소유자 및 권한 설정		취약도	상
항목설명	hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있다.			
진단기준	양호	/etc/hosts 파일의 소유자가 root이고, 권한이 644 이하인 경우		
	취약	/etc/hosts 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우		
진단방법	<div>■ /etc/hosts 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/hosts</div> <div><pre>[root@localhost ~]# ls -l /etc/hosts</pre><pre>-rw-r--r--. 1 root root 158 Jun  7 2013 /etc/hosts</pre></div>			
조치방법	<div>■ /etc/hosts 파일의 퍼미션을 644로, 소유자를 root로 변경</div> <div># chmod 644 /etc/hosts</div> <div><pre>[root@localhost ~]# chmod 644 /etc/hosts</pre></div> <div># chown root /etc/hosts</div> <div><pre>[root@localhost ~]# chown root /etc/hosts</pre><pre>[root@localhost ~]# ls -l /etc/hosts</pre><pre>-rw-r--r--. 1 root root 158 Jun  7 2013 /etc/hosts</pre></div>			
비고				

진단항목	U-11. /etc/(x)inetd.conf 파일 소유자 및 권한 설정		취약도	상
항목설명	(x)inetd.conf 파일에 비인가자의 쓰기 권한이 부여되어 있을 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있다.			
진단기준	양호	/etc/(x)inetd.conf 파일의 소유자가 root이고, 권한이 644이하인 경우		
	취약	/etc/(x)inetd.conf 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우		
진단방법	<div>■ /etc/(x)inetd.conf 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/(x)inetd.conf</div> <div><pre>[root@localhost ~]# ls -l /etc/xinetd.conf -rw-r--r--. 1 root root 0 Sep 16 13:44 /etc/xinetd.conf</pre></div>			
조치방법	<div>■ /etc/(x)inetd.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</div> <div># chmod 644 /etc/(x)inetd.conf</div> <div><pre>[root@localhost ~]# chmod 644 /etc/xinetd.conf</pre></div> <div># chown root /etc/(x)inetd.conf</div> <div><pre>[root@localhost ~]# chown root /etc/xinetd.conf [root@localhost ~]# ls -l /etc/xinetd.conf -rw-r--r--. 1 root root 0 Sep 16 13:44 /etc/xinetd.conf</pre></div>			
비고				

진단항목	U-12. /etc/(r)syslog.conf 파일 소유자 및 권한 설정		취약도	상
항목설명	(r)syslog.conf 파일의 접근권한이 적절하지 않을 경우, 임의적인 파일 변조로 인해 침입자의 흔적 또는, 시스템 오류 사항을 분석하기 위해 반드시 필요한 시스템 로그가 정상적으로 기록되지 않을 수 있다.			
진단기준	양호	/etc/(r)syslog.conf 파일의 소유자가 root이고, 권한이 644이하인 경우		
	취약	/etc/(r)syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우		
진단방법	<div>■ /etc/(r)syslog.conf 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/(r)syslog.conf</div> <div><pre>[root@localhost ~]# ls -l /etc/rsyslog.conf -rw-r--r--. 1 root root 3232 Nov 28 2019 /etc/rsyslog.conf</pre></div>			
조치방법	<div>■ /etc/(r)syslog.conf 파일의 퍼미션을 644로, 소유자를 root로 변경</div> <div># chmod 644 /etc/(r)syslog.conf</div> <div><pre>[root@localhost ~]# chmod 644 /etc/rsyslog.conf</pre></div> <div># chown root /etc/(r)syslog.conf</div> <div><pre>[root@localhost ~]# chown root /etc/rsyslog.conf [root@localhost ~]# ls -l /etc/rsyslog.conf -rw-r--r--. 1 root root 3232 Nov 28 2019 /etc/rsyslog.conf</pre></div>			
비고	■ root, bin, sys 등 시스템에서 사용하는 계정이 아닌 일반 계정에 소유 권한이 부여되지 않도록 하여야 함			



진단항목	U-13. /etc/services 파일 소유자 및 권한 설정		취약도	상
항목설명	services 파일의 접근권한이 적절하지 않을 경우 비인가 사용자가 운영 포트 번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈하여 악성 서비스를 의도적으로 실행할 수 있다.			
진단기준	양호	/etc/services 파일의 소유자가 root이고, 권한이 644이하인 경우		
	취약	/etc/services 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우		
진단방법	<div>■ /etc/services 파일의 퍼미션과 소유자를 확인</div> <div># ls -l /etc/services</div> <div><pre>[root@localhost ~]# ls -l /etc/services -rw-r--r--. 1 root root 670293 Jun 7 2013 /etc/services</pre></div>			
조치방법	<div>■ /etc/services 파일의 퍼미션을 644로, 소유자를 root로 변경</div> <div># chmod 644 /etc/services</div> <div><pre>[root@localhost ~]# chmod 644 /etc/services</pre></div> <div># chown root /etc/services</div> <div><pre>[root@localhost ~]# chown root /etc/services [root@localhost ~]# ls -l /etc/services -rw-r--r--. 1 root root 670293 Jun 7 2013 /etc/services</pre></div>			
비고				

진단항목	U-14. SUID, SGID, Sticky bit 설정 파일 점검		취약도	상
항목설명	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상 서비스 장애를 발생시킬 수 있다.			
진단기준	양호	주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우		
	취약	주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우		
진단방법	<div>■ 아래와 같은 명령어를 통해 SUID와 SGID 파일을 검색하여 주요 파일의 권한을 확인</div> <div># find / -user root -type f \w( -perm -4000 -o -perm -2000 \w) -exec ls -lg {} \w;</div> <div><pre>[root@localhost ~]# find / -user root -type f \( -perm -4000 -o -perm -2000 \) -exec ls -lg {} \;</pre></div>			
조치방법	<div>■ 제거 방법</div> <div># chmod -s &lt;file_name&gt;</div> <div>■ 주기적인 감사 방법</div> <div># find / -user root -type f \w( -perm -04000 -o -perm -02000 \w) -xdev -exec ls -al {} \w;</div> <div><pre>[root@localhost ~]# find / -user root -type f \( -perm -04000 -o -perm -02000 \) -xdev -exec ls -al {} \;</pre></div> <div>■ 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법(일반 사용자의 Setuid 사용을 제한함, 임의의 그룹만 가능)</div> <div># /usr/bin/chgrp &lt;group_name&gt; &lt;setuid_file_name&gt;</div> <div># /usr/bin/chmod 4750 &lt;setuid_file_name&gt;</div>			
비고	SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요			

진단항목	U-15. 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정		취약도	상
항목설명	홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수 파일을 변조하여 정상 사용중인 사용자의 서비스가 제한될 수 있다.			
진단기준	양호	사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이고 권한이 644로 설정되어 있는 경우		
	취약	사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이 아니거나 권한이 644로 설정되어 있지 않은 경우		
진단방법	<div>■ 사용자 홈 디렉터리 확인</div> <div># cat /etc/passwd   grep /home</div> <div>[root@localhost ~]# cat /etc/passwd   grep /home</div> <div>test:x:1000:1000::/home/test:/bin/bash</div> <div>■ 해당 홈 디렉터리 소유자 및 권한 확인</div> <div># ls -ld &lt;사용자 홈 디렉터리&gt; (홈 디렉터리 소유자 및 권한 확인)</div> <div>[root@localhost ~]# ls -ld /home/test</div> <div>drwxr-xr-x. 2 root root 6 Sep 16 14:23 /home/test</div> <div># ls -al &lt;사용자 홈 디렉터리&gt; (홈 디렉터리 내 환경설정 파일 소유자 및 권한 확인)</div> <div>[root@localhost ~]# ls -al /home/test</div> <div>total 0</div> <div>drwxr-xr-x. 2 root root 77 Sep 16 14:29 .</div> <div>drwxr-xr-x. 3 root root 18 Sep 16 14:23 ..</div> <div>-rw-r--r--. 1 root root 0 Sep 16 14:29 .bash_login</div> <div>-rw-r--r--. 1 root root 0 Sep 16 14:29 .bash_profile</div> <div>-rw-r--r--. 1 root root 0 Sep 16 14:25 .bashrc</div> <div>-rw-r--r--. 1 root root 0 Sep 16 14:25 .profile</div>			
조치방법	<div>■ 소유자 변경 방법</div> <div># chown &lt;user_name&gt; &lt;file_name&gt;</div> <div>[root@localhost ~]# chown root /home/test/.bash_login</div> <div>■ 일반 사용자 쓰기 권한 제거 방법</div> <div># chmod o-w &lt;file_name&gt;</div> <div>[root@localhost ~]# chmod o-w /home/test/.bash_login</div>			
비고				

진단항목	U-16. world writable 파일 점검		취약도	상
항목설명	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 덧붙이거나 지울 수 있게 되어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있다.			
진단기준	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		
진단방법	<div>■ world writable 파일 존재 여부 확인</div> <div># find / -type f -perm -2 -exec ls -l {} \;</div> <div><pre>--w--w--w-. 1 root root 0 Sep 16 12:54 /sys/fs/cgroup/systemd/system.slice/system-getty.slice/getty@tty1.service/cgroup.event_control --w--w--w-. 1 root root 0 Sep 16 12:54 /sys/fs/cgroup/systemd/system.slice/system-getty.slice/cgroup.event_control --w--w--w-. 1 root root 0 Sep 16 12:54 /sys/fs/cgroup/systemd/system.slice/dev-mqueue.mount/cgroup.event_control --w--w--w-. 1 root root 0 Sep 16 12:54 /sys/fs/cgroup/systemd/system.slice/dev-hugepages.mount/cgroup.event_control</pre></div>			
조치방법	<div>■ 일반 사용자 쓰기 권한 제거 방법</div> <div># chmod o-w &lt;file_name&gt;</div> <div><pre>[root@localhost ~]# chmod o-w /sys/fs/cgroup/systemd/system.slice/system-getty.slice/getty@tty1.service/cgroup.event_control</pre></div> <div>■ 파일 삭제 방법</div> <div># rm -rf &lt;world-writable 파일명&gt;</div>			
비고				

진단항목	U-17. \$HOME/.rhosts, hosts.equiv 사용 금지		취약도	상
항목설명	rlogin, rsh 등과 같은 'r' command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템상의 임의의 명령을 수행시킬 수 있으며, 명령어 원격 실행을 통해 중요 정보 유출 및 시스템 장애를 유발시킬 수 있다. 또한 공격자 백도어 등으로도 활용될 수 있다.			
진단기준	양호	login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한이 600 이하인 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우 - /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우		
	취약	login, shell, exec 서비스를 사용하거나, 사용 시 아래와 같은 설정이 적용되어 있지 않은 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한이 600 이하인 경우 - /etc/hosts.equiv 및 \$HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우 - /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우		
진단방법	<ul style="list-style-type: none"><li>■ 파일 소유자 및 권한 확인 # ls -al /etc/hosts.equiv # ls -al \$HOME/.rhosts</li><li>■ 계정 별 '+' 부여 적절성 확인 # cat /etc/hosts.equiv # cat \$HOME/.rhosts</li></ul>			
조치방법	<ul style="list-style-type: none"><li>■ .rhosts, hosts.equiv 파일 미사용 시 1) .rhosts, hosts.equiv 파일 삭제 # rm -f [삭제 할 파일 및 디렉터리 경로] # rm -f \$HOME/.rhosts 또는 or /etc/ hosts.equiv</li><li>■ .rhosts, hosts.equiv 파일 사용 시 1) “/etc/hosts.equiv” 및 “\$HOME/.rhosts” 파일의 소유자를 root 또는, 해당 계정으로 변경 # chown root /etc/hosts.equiv # chown [계정 명] \$HOME/.rhosts 2) “/etc/hosts.equiv” 및 “\$HOME/.rhosts” 파일의 퍼미션을 600 이하로 변경 # chmod 600 /etc/hosts.equiv # chmod 600 \$HOME/.rhosts</li></ul>			

	3) "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록 # vi /etc/hosts.equiv (or \$HOME/.rhosts)
비고	

진단항목	U-18. 접속 IP 및 포트 제한		취약도	상
항목설명	허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있다.			
진단기준	양호	접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정한 경우		
	취약	접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않은 경우		
진단방법	<div>▪ All deny 적용 확인 및 접근 허용 IP 적절성 확인 또는 iptables에서 서버로 접속 하는 IP 설정 확인</div> <div>- /etc/hosts.deny, allow 설정 확인</div> <div># cat /etc/hosts.deny</div> <div><pre>[root@localhost ~]# cat /etc/hosts.deny</pre></div> <div># cat /etc/hosts.allow</div> <div><pre>[root@localhost ~]# cat /etc/hosts.allow</pre></div> <div>- iptables 설정 확인</div> <div># iptables -nL</div> <div><pre>[root@localhost ~]# iptables -nL Chain INPUT (policy ACCEPT) target          prot opt source          destination ACCEPT         all  --  0.0.0.0/0        0.0.0.0/0                ctstate RELATED,ESTABLISHED ACCEPT         all  --  0.0.0.0/0        0.0.0.0/0</pre></div>			
조치방법	<div>▪ vi 편집기를 이용하여 "/etc/hosts.deny" 파일을 연 후</div> <div># vi /etc/hosts.deny</div> <div><pre>[root@localhost ~]# vi /etc/hosts.deny</pre></div> <div>▪ 아래와 같이 수정 또는 추가 (ALL Deny 설정)</div> <div>ALL:ALL</div> <div><pre>[root@localhost ~]# cat /etc/hosts.deny   grep ALL ALL:ALL</pre></div> <div>▪ vi 편집기를 이용하여 "/etc/hosts.allow" 파일을 연 후</div> <div># vi /etc/hosts.allow</div>			

	<pre>[root@localhost ~]# vi /etc/hosts.allow</pre> <ul style="list-style-type: none"> <li>■ 아래와 같이 접속 허용 서비스 및 IP 설정</li> </ul> <pre>sshd : 192.168.0.148, 192.168.0.6 (다른 서비스도 동일한 방식으로 설정)</pre> <pre>[root@localhost ~]# cat /etc/hosts.allow   grep sshd</pre> <pre>sshd : 192.168.88.128</pre> <p>※ TCP Wrapper 접근제어 가능 서비스 SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH</p>
<b>비고</b>	허용되지 않는 IP는 서비스 사용이 불가함



진단항목	U-19. cron 파일 소유자 및 권한 설정		취약도	상
항목설명	root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있다.			
진단기준	양호	/etc/crontab 파일의 소유자가 root이고, 권한이 640이하인 경우		
	취약	/etc/crontab 파일의 소유자가 root가 아니거나, 권한이 640초과인 경우		
진단방법	<div>■ “/etc/cron.allow” 및 “/etc/cron.deny” 파일의 소유자 및 권한 확인</div> <div># ls -l /etc/cron.allow</div> <div><pre>[root@localhost ~]# ls -l /etc/cron.allow</pre><pre>-rw-r--r--. 1 root root 0 Sep 16 15:04 /etc/cron.allow</pre></div> <div># ls -l /etc/cron.deny</div> <div><pre>[root@localhost ~]# ls -l /etc/cron.deny</pre><pre>-rw-----. 1 root root 0 Aug 9 2019 /etc/cron.deny</pre></div>			
조치방법	<div>■ “/etc/cron.allow” 및 “/etc/cron.deny” 파일의 소유자 및 권한 변경</div> <div># chown root /etc/cron.allow</div> <div><pre>[root@localhost ~]# chown root /etc/cron.allow</pre></div> <div># chmod 640 /etc/cron.allow</div> <div><pre>[root@localhost ~]# chmod 640 /etc/cron.allow</pre><pre>[root@localhost ~]# ls -l /etc/cron.allow</pre></div> <div># chown root /etc/cron.deny</div> <div><pre>[root@localhost ~]# chown root /etc/cron.deny</pre></div> <div># chmod 640 /etc/cron.deny</div> <div><pre>[root@localhost ~]# chmod 640 /etc/cron.deny</pre><pre>[root@localhost ~]# ls -l /etc/cron.deny</pre><pre>-rw-r-----. 1 root root 0 Aug 9 2019 /etc/cron.deny</pre></div>			
비고				

## 다. 서비스 관리

진단항목	U-20. Finger 서비스 비활성화		취약도	상
항목설명	비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 한다.			
진단기준	양호	finger 서비스가 비활성화 되어 있는 경우		
	취약	finger 서비스가 활성화 되어 있는 경우		
진단방법	<div><div><div><div>■ xinetd인 경우 /etc/xinetd.d/finger 파일에서 서비스 비활성화 여부 확인</div><div># cat /etc/xinetd.d/finger   grep disable</div><div><pre>[root@localhost ~]# cat /etc/xinetd.d/finger   grep disable</pre><div>disable = no</div></div></div><div><div>■ inetd인 경우 /etc/inetd.conf 파일에서 finger 서비스 라인 #처리(주석처리) 또는 삭제 되어 있는지 확인</div><div># cat /etc/inetd.conf   grep finger</div></div></div></div>			
조치방법	<div><div><div>■ /etc/xinetd.d/finger 파일에서 서비스 비활성화 설정</div><div># vi /etc/xinetd.d/finger</div><div><div>disable = no</div></div></div></div>			
비고				

진단항목	U-21. Anonymous FTP 비활성화		취약도	상			
항목설명	Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 한다.						
진단기준	양호	Anonymous FTP (익명 ftp) 접속을 차단한 경우					
	취약	Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우					
진단방법	<div>■ Default FTP를 사용하는 경우 /etc/passwd 파일에 ftp 계정 존재 여부 확인</div> <div># cat /etc/passwd   grep ftp</div> <div><pre>[root@localhost ~]# cat /etc/passwd   grep ftp ftp:!:14:50:FTP User:/var/ftp:/sbin/nologin</pre></div> <div>■ ProFTP를 사용하는 경우 proftpd.conf 파일에서 &lt;Anonymous ~ ftp&gt; 부분 확인</div> <div>※ UserAlias 항목이 주석처리 되어있거나, 없으면 양호</div> <div># cat etc/proftpd/proftpd.conf</div> <div><table><tr><td>UserAlias</td><td>anonymous ftp</td></tr></table></div> <div>■ vsFTP를 사용하는 경우 vsftpd.conf 파일에서 anonymous_enable 값이 No로 설정되어 있는지 확인</div> <div># cat /etc/vsftpd/vsftpd.conf</div> <div><table><tr><td>anonymous_enable = Yes</td></tr></table></div>				UserAlias	anonymous ftp	anonymous_enable = Yes
	UserAlias	anonymous ftp					
anonymous_enable = Yes							
조치방법	<div>■ 일반 FTP - Anonymous FTP 접속 제한 설정 방법 "/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제</div> <div># userdel ftp</div> <div><pre>[root@localhost ~]# userdel ftp [root@localhost ~]# cat /etc/passwd   grep ftp [root@localhost ~]#</pre></div> <div>■ ProFTP - Anonymous FTP 접속 제한 설정 방법</div> <div>"/etc/passwd" 파일에서 ftp 계정 삭제</div> <div># userdel ftp</div> <div>■ vsFTP - Anonymous FTP 접속 제한 설정 방법</div> <div>vsFTP 설정파일("/etc/vsftpd/vsftpd.conf" 또는, "/etc/vsftpd.conf")에서 anonymous_enable=NO 설정</div>						
비고	Anonymous FTP를 사용하지 않을 경우 영향 없음						

진단항목	U-22. r 계열 서비스 비활성화		취약도	상
항목설명	서비스 포트가 열려있을 경우, 비인가자에 의한 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 될 수 있다.			
진단기준	양호	r 계열 서비스(rlogin, rsh, rexec)가 비활성화 되어 있는 경우		
	취약	r 계열 서비스(rlogin, rsh, rexec)가 활성화 되어 있는 경우		
진단방법	<div>■ xinetd인 경우 rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인</div> <div># cat /etc/xinetd.d/rsh   grep disable</div> <div><pre>[root@localhost ~]# cat /etc/xinetd.d/rsh   grep disable disable = yes</pre></div> <div># cat /etc/xinetd.d/rlogin   grep disable</div> <div><pre>[root@localhost ~]# cat /etc/xinetd.d/rlogin   grep disable disable = yes</pre></div> <div># cat /etc/xinetd.d/rexec   grep disable</div> <div><pre>[root@localhost ~]# cat /etc/xinetd.d/rexec   grep disable disable = yes</pre></div> <div>■ inetd인 경우 rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인</div> <div># cat /etc/inetd.conf   egrep "rsh rlogin rexec" (주석 처리 되어 있으면 비활성화)</div>			
조치방법	<div>■ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 rlogin, rsh, rexec 파일을 연 후</div> <div>■ 아래와 같이 설정 (disable = yes 설정)</div> <div>- /etc/xinetd.d/rlogin 파일</div> <div>- /etc/xinetd.d/rsh 파일</div> <div>- /etc/xinetd.d/rexec 파일</div> <div><pre>service      rlogin { ... disable      = yes }</pre></div>			
비고	<div>■ 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 해당파일 내에 설정이 없다면 사용하지 않는 것으로 파악</div>			

진단항목	U-23. DoS 공격에 취약한 서비스 비활성화		취약도	상
항목설명	해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있다.			
진단기준	양호	Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 된 경우		
	취약	Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 활성화 된 경우		
진단방법	<div><div><div>■ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 서비스 비활성화 여부 확인</div><div># cat /etc/xinetd.d/echo   grep disable</div><div><pre>[root@localhost ~]# cat /etc/xinetd.d/echo   grep disable disable = yes</pre></div><div># cat /etc/xinetd.d/discard   grep disable</div><div><pre>[root@localhost ~]# cat /etc/xinetd.d/discard   grep disable disable = yes</pre></div><div># cat /etc/xinetd.d/daytime   grep disable</div><div><pre>[root@localhost ~]# cat /etc/xinetd.d/daytime   grep disable disable = yes</pre></div><div># cat /etc/xinetd.d/chargen   grep disable</div><div><pre>[root@localhost ~]# cat /etc/xinetd.d/chargen   grep disable disable = yes</pre></div></div><div><div>■ inetd인 경우 /etc/inetd.conf 파일에서 echo, discard, daytime, chargen 서비스 비활성화 여부 확인</div><div># cat /etc/inetd.conf   egrep "echo discard daytime chargen" (주석 처리 되어 있으면 비활성화)</div></div></div>			
조치방법	<div><div>■ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 파일 열기</div><div>■ 아래와 같이 설정 (Disable = yes 설정)</div><div>/etc/xinetd.d/echo 파일(echo-dgram, echo-stream)</div><div>/etc/xinetd.d/discard 파일(discard-dgram, discard-stream)</div><div>/etc/xinetd.d/daytime 파일(daytime-dgram, daytime-stream)</div><div>/etc/xinetd.d/chargen 파일(chargen-dgram, chargen-stream)</div><div>service echo</div></div>			

	<pre>{ disable = yes id      = echo-stream type    = internal wait    = no socket-type = stream }</pre> <ul style="list-style-type: none"><li>■ xinetd 서비스 재시작 # service xinetd restart</li></ul>
비고	

진단항목	U-24. NFS 서비스 비활성화		취약도	상
항목설명	비인가자가 NFS 서비스로 인가되지 않은 시스템이 NFS 시스템 마운트하여 비인가된 시스템 접근 및 파일변조 등의 침해 행위 가능성이 존재한다.			
진단기준	양호	NFS 서비스 관련 데몬이 비활성화 되어 있는 경우		
	취약	NFS 서비스 관련 데몬이 활성화 되어 있는 경우		
진단방법	<div>■ NFS 데몬 구동 여부 확인</div> <div># ps -ef   grep nfsd</div>			
조치방법	<div>■ NFS 데몬(nfsd)을 중지</div> <div># kill -9 [PID]</div>			
비고	<div>■ 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</div>			

진단항목	U-25. NFS 접근통제		취약도	상
항목설명	접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있다.			
진단기준	양호	NFS 서비스 사용 시 everyone 공유를 제한한 경우		
	취약	NFS 서비스 사용 시 everyone 공유를 제한하지 않은 경우		
진단방법	<div>■ everyone으로 시스템이 마운트 되어 있는지 확인</div> <div># showmount -e hostname</div> <div>■ /etc/exports 파일에서 접근 통제 설정 여부 확인</div> <div># cat /etc/exports</div> <div>- 취약한 설정 예 : /var/www/img *(ro,all_squash)</div> <div>- 양호한 설정 예 : /data 172.27.0.0/16(rw,no_root_squash)</div>			
조치방법	<div>■ everyone 마운트 제거</div> <div># umount "파일시스템 이름"</div> <div>■ /etc/exports 파일에서 접근 통제 설정</div> <div># vi /etc/exports</div> <div>(예) /data 172.27.0.0/16(rw,no_root_squash)</div>			
비고	<div>■ 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</div>			



진단항목	U-26. automountd 제거		취약도	상
항목설명	파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있다.			
진단기준	양호	automount 서비스가 비활성화 되어 있는 경우		
	취약	automount 서비스가 활성화 되어 있지 않은 경우		
진단방법	<div>■ automountd 서비스 데몬 확인</div> <pre># ps -ef   grep auto</pre>			
조치방법	<div>■ automountd서비스 데몬 실행 중지</div> <pre># kill -9 [PID]</pre> <div>■ 시스템 재시작 시 automount 가 시작되지 않도록 설정</div> <div>&lt;방법1&gt; 부팅스크립트에서 automountd 제거</div> <pre># chkconfig --level 0123456 autofs off</pre> <div>&lt;방법2&gt; 아래와 같이 파일경로 확인 후 파일명 변경</div> <pre># mv /etc/rc2.d/S28autofs /etc/rc2.d/S28autofs.orig</pre>			
비고	<div>■ 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)</div> <div>※ 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</div>			

진단항목	U-27. RPC 서비스 확인		취약도	상
항목설명	버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 한다.			
진단기준	양호	불필요한 RPC 서비스가 비활성화 되어 있는 경우		
	취약	불필요한 RPC 서비스가 활성화 되어 있는 경우		
진단방법	<div>■ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 RPC 서비스 파일에서 비활성화 여부 확인</div> <div># cat /etc/xinetd.d/rstatd</div> <div>■ inetd인 경우 /etc/inetd.conf 파일에서 불필요한 RPC 서비스 비활성화 여부 확인</div> <div># cat /etc/inetd.conf   grep rpc.cmsd</div>			
조치방법	<div>■ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내의 불필요한 RPC 서비스 파일을 연 후</div> <div>■ 아래와 같이 설정 (disable = yes 설정)</div> <div><pre>service rstatd {     disable      = yes     ... 이하 생략 ... }</pre></div>			
비고				

진단항목	U-28. NIS, NIS+ 점검		취약도	상
항목설명	보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타시스템의 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보다 NIS+를 사용하는 것을 권장한다.			
진단기준	양호	NIS, NIS+ 서비스가 구동 중이지 않을 경우		
	취약	NIS, NIS+ 서비스가 구동 중일 경우		
진단방법	<div>■ NIS, NIS+ 서비스 구동 확인</div> <pre># ps -ef   egrep "ypserv ypbind ypxfrd rpc.yppasswdd rpc.yppupdated"   grep -v "grep"</pre>			
조치방법	<div>■ NFS 서비스 데몬 중지</div> <pre># kill -9 [PID]</pre>			
비고				

진단항목	U-29. tftp, talk 서비스 비활성화		취약도	상
항목설명	사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격자의 공격 시도가 가능하다.			
진단기준	양호	tftp, talk 서비스가 비활성화 되어 있는 경우		
	취약	tftp, talk 서비스가 활성화 되어 있는 경우		
진단방법	<div>■ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk서비스 파일에서 비활성화 여부 확인</div> <div># cat /etc/xinetd.d/tftp</div> <div>■ inetd인 경우 /etc/inetd.conf 파일에서 tftp, talk, ntalk 서비스 비활성화 여부 확인</div> <div># cat /etc/inetd.conf   egrep "tftp talk "</div>			
조치방법	<div>■ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk 파일을 연 후</div> <div>■ 아래와 같이 설정 (disable = yes 설정)</div> <div>- /etc/xinetd.d/tftp 파일</div> <div>- /etc/xinetd.d/talk 파일</div> <div>- /etc/xinetd.d/ntalk 파일</div> <div><pre>service tftp {     ... 생략 ...     disable = yes }</pre></div>			
비고				

진단항목	U-30. Sendmail 버전 점검		취약도	상
항목설명	취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있다.			
진단기준	양호	Sendmail 버전을 정기적으로 점검하고, 최신 버전 패치를 했을 경우		
	취약	Sendmail 버전을 정기적으로 점검하지 않거나, 최신 버전 패치가 되어 있지 않은 경우		
진단방법	<div>■ Sendmail 프로세스 확인</div> <div># ps -ef   grep sendmail</div> <div><pre>[root@localhost ~]# ps -ef   grep sendmail root      9/92   9650  0 16:19 pts/0    00:00:00 grep --col or=auto  sendmail</pre></div> <div>■ Sendmail 버전 확인</div> <div># cat /etc/mail/sendmail.cf   grep DZ</div>			
조치방법	<div>■ Sendmail 서비스 실행 여부 및 버전 점검 후, <a href="http://www.sendmail.org/">http://www.sendmail.org/</a> 또는, 각 OS 벤더사의 보안 패치 설치</div>			
비고	패치를 적용할 경우 시스템 및 서비스의 영향 정도를 충분히 고려하여야 함			

진단항목	U-31. 스팸 메일 릴레이 제한		취약도	상
항목설명	SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있다.			
진단기준	양호	SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우		
	취약	SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우		
진단방법	<div>■ SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인</div> <pre># ps -ef   grep sendmail   grep -v "grep" # cat /etc/mail/sendmail.cf   grep "R\$ W*"   grep "Relaying denied"</pre>			
조치방법	<div>■ vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후</div> <div>■ 아래와 같이 주석 제거</div> <div>(수정 전) #R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"</div> <div>(수정 후) R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"</div> <div>■ 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인</div> <pre># vi /etc/mail/access</pre>			
비고	릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음			

진단항목	U-32. 일반사용자의 Sendmail 실행 방지		취약도	상
항목설명	일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있다.			
진단기준	양호	SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우		
	취약	SMTP 서비스 사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정되지 않은 경우		
진단방법	<div>■ sendmail.cf 파일에서 restrictqrun 옵션 설정 여부 확인</div> <div># cat /etc/mail/sendmail.cf   grep PrivacyOptions</div> <div>○ PrivacyOptions=authwarnings, novrfy, noexpn</div>			
조치방법	<div>■ vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후</div> <div># vi /etc/mail/sendmail.cf</div> <div>■ ○ PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가</div> <div>(수정 전) ○ PrivacyOptions=authwarnings, novrfy, noexpn</div> <div>(수정 후) ○ PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun</div>			
비고				

진단항목	U-33. DNS 보안 버전 패치		취약도	상
항목설명	최신버전 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재한다.			
진단기준	양호	DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우		
	취약	DNS 서비스를 사용하며, 주기적으로 패치를 관리하고 있지 않은 경우		
진단방법	<div>■ DNS 서비스 사용 및 BIND 버전 확인</div> <div># ps -ef   grep named</div> <div># named -v</div>			
조치방법	<div>■ [DNS 서비스를 사용할 경우]</div> <div>1) "DNS" 서비스 사용 시 BIND 버전 확인 후 최신 버전으로 업데이트</div> <div>■ [DNS 서비스를 사용하지 않는 경우]</div> <div>1) 서비스 중지</div> <div># kill -9 [PID]</div>			
비고	패치를 적용 시 시스템 및 서비스 영향 정도를 충분히 고려하여야 함			



진단항목		U-34. DNS ZoneTransfer 설정	취약도	상
항목설명		비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있다.		
진단기준	양호	DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우		
	취약	DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우		
진단방법		<div>■ 설정 파일에서 zone transfer 설정 확인</div> <div># cat /etc/named.conf</div> <div><pre>Options {     allow-transfer{10.10.10.10}; };</pre></div>		
조치방법		<div>■ 특정 서버의 Zone Transfer 지정</div> <div># vi /etc/named.conf</div> <div><pre>Options {     allow-transfer{10.10.10.111; 10.10.10.112}; };</pre></div> <div>■ 특정 도메인의 Zone에 대해서 제한할 경우에는 다음과 같이 설정</div> <div># vi /etc/named.conf</div> <div><pre>zone "xxx.co.kr" {     Type master ;     File "db.xxx.co.kr";     allow-transfer{10.10.10.111; 10.10.10.112}; }</pre></div>		
비고		Zone 파일 전송을 허용할 대상을 정상적으로 등록할 경우 일반적으로 영향 없음		

## 라. 패치 및 로그관리

진단항목	U-35. 최신 보안패치 및 벤더 권고사항 적용		취약도	상
항목설명	최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재한다.			
진단기준	양호	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우		
	취약	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않은 경우		
진단방법	■ 패치 적용 정책 수립 여부 및 정책에 따른 패치 적용 여부 확인			
조치방법	<div>■ LINUX는 서버에 설치된 패치 리스트의 관리가 불가능하므로 rpm 패키지별 버그가 Fix된 최신 버전 설치가 필요함</div> <div>■ LINUX는 오픈되고, 커스터마이징 된 OS이므로 LINUX를 구입한 벤더에 따라 rpm 패키지가 다를 수 있으며, 아래의 사이트는 RedHat LINUX에 대한 버그 Fix 관련 사이트임</div> <div>&lt;Red Hat 일 경우&gt;</div> <div>1) 다음의 사이트에서 해당 버전을 찾음 <a href="http://www.redhat.com/security/updates/">http://www.redhat.com/security/updates/</a> <a href="http://www.redhat.com/security/updates/eol/">http://www.redhat.com/security/updates/eol/</a> (Red Hat LINUX 9 이하 버전)</div> <div>2) 발표된 Update 중 현재 사용 중인 보안 관련 Update 찾아 해당 Update Download</div> <div>3) Update 설치</div> <div># rpm -Uvh &lt;package-name&gt;</div>			
비고				

진단항목	U-36. 로그의 정기적 검토 및 보고		취약도	상
항목설명	로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어렵다.			
진단기준	양호	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지고 있는 경우		
	취약	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우		
진단방법	■ 로그 정책 수립 여부 및 정책에 따른 로그 검토 여부 확인			
조치방법	<div>■ 다음과 같이 로그 파일의 백업에 대한 검토를 해야 함</div> <div>1) su 시도에 관한 로그</div> <div>2). 반복적인 로그인 실패에 관한 로그</div> <div>3) 로그인 거부 메시지에 관한 로그</div> <div>4) 기본적 log 파일의 위치는 /var/adm, /var/log</div> <div>※ 커널과 시스템에 관련된 로그 메시지들은 syslogd와 klogd 두개의 데몬에 의해서 /var/log/messages에 기록하게 됨. 이 파일을 분석함으로써 시스템을 항상 점검 관리해야 함</div>			
비고				