Linux 취약점 점검

구분	코드	진단 항목	등급	상세 진단 결과	보안수준	위험현황	개선대책
계정관리	U-01	root 계정 원격 접속 제한	상	원격 터미널 서비스 사용 시 root 직접 접속을 허용되어 있음 [현황] permitrootlogins yes	취약	root 계정을 탈취하여 외부에서 원격으로 이용한 시스템 장악 및 각종 공격으로 인한 root 계정 사용 불가 위협	vi 편집기를 이용하여 "/etc/ssh/sshd_config"파일에 아래와 같이 주석 제거 또는, 신규 삽입 (수정 전) #PermitRootLogin Yes (수정 후) PermitRootLogin No
	U-02	패스워드 복잡성 설정	상	패스워드 최소길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정되지 않음 [현황] minlen = 1, dcredit = 1, ucredit = 1, lcredit = 1, ocredit = 1	취약	패스워드를 사회공학적인 유추가 가능할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크랙이 가능함	패스워드 복잡성 설정 파일 확인 #/etc/security/pwquality.conf파일 내용을 내부 정책에 맞도록 편집 (수정 전) minlen = 1, dcredit = 1, ucredit = 1, lcredit = 1, ocredit = 1 (수정 후) minled = 8, dcredit = -1, ucredit = -1, lcredit = -1, ocredit = -1
	U-03	계정 잠금 임계값 설정	상	계정 잠금 임계값이 10회 이하의 값으로 설정되지 않음 [현황] auth required pam_tally2.so deny=50	취약	패스워드 탈취 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)의 인증 요청에 대해 설정된 패스워드와 일치 할 때 까지 지속적으로 응답하여 해당 계정의 패스워드가 유출 될 수 있음	vi 편집기를 이용하여 "etc/pam.d/system-auth" 파일 내용을 내부 정책에 맞도록 편집 (수정 전) auth required pam_tally2.so deny=50 (수정 후) auth required pam_tally2.so deny=10
	U-04	패스워드 파일 보호	상	패스워드를 암호화하여 저장 [현황] root:x:0:0:root:/root:/bin/bash	양호		
	U-44	root 이외의 UID가 '0' 금지	중	root 계정과 동일한 UID를 갖는 계정이 존재하지 않음	양호		
	U-45	root 계정 su 제한	하	su 명령어를 모든 사용자가 사용하도록 설정되어 있음 [현황] wheel:x:10 [현황] #auth required pam_wheel.so use_uid	취약	무분별한 사용자 변경으로 타 사용자 소유의 파일을 변경 할 수 있으며 root 계정으로 변경하는 경우 관리자 권한을 획득 할 수 있음	"/etc/pam.d/su" 파일을 아래와 같이 설정 (수정 전) #auth required pam_wheel.so use_uid (수정 후) auth required pam_wheel.so use_uid wheel 그룹에 su 명령어를 사용할 사용자 추가 (수정 전) wheel:x:10 (수정 후) wheel:x:10:root,admin
	U-46	패스워드 최소 길이 설정	중	패스워드 최소 길이가 8자 이상으로 설정되지 않음 [현황] PASS_MIN_LEN 5	취약	패스워드 문자열이 짧은 경우 유추가 가능 할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크랙이 가능함	vi 편집기를 이용하여 "/etc/login.defs" 파일을 아래와 같이 설정 (수정 전) PASS_MIN_LEN 5 (수정 후) PASS_MIN_LEN 8
	U-47	패스워드 최대 사용 기간 설정	중	패스워드 최대 사용기간이 90일 이하로 설정되지 않음 [현황] PASS_MAX_DAYS 99999	취약	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 증가함	vi 편집기를 이용하여 "/etc/login.defs" 파일을 아래와 같이 설정 (수정 전) PASS_MAX_DAYS 99999 (수정 후) PASS_MAX_DAYS 90
	U-48	패스워드 최소 사용기간 설정	중	패스워드 최소 사용기간이 1일 이상 설정되지 않음 [현황] PASS_MIN_DAYS 0	취약	최소 사용기간이 설정되어 있지 않아 반복적으로 즉시 변경이 가능한 경우 이전 패스워드 기억 횟수를 설정하여도 반복적으로 즉시 변경하여 이전 패스워드로 설정이 가능함	vi 편집기를 이용하여 "/etc/login.defs" 파일을 아래와 같이 설정 (수정 전) PASS_MIN_DAYS 0 (수정 후) PASS_MIN_DAYS 1
	U-49	불필요한 계정 제거	하	불필요한 계정이 존재 [현황] TestUser:x:1001:1001::/home/TestUser:/bin/bash TestUser2:x:1002:1002::/home/TestUser2:/bin/bash	취약	로그인이 가능하고 현재 사용하지 않는 불필요한 계정은 사용중인 계정보다 상대적으로 관리가 취약하여 공격자의 목표가 되어 계정 탈취될 수 있음	userdel 명령으로 불필요한 사용자 계정 삭제 (수정 후) #userdel <TestUser> (수정 후) #userdel <TestUser2>
	U-50	관리자 그룹에 최소한의 계정 포함	하	관리자 그룹에 불필요한 계정이 존재 [현황] root:x:0:TestUser	취약	시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근 권한이 부여되어 있으므로 해당 관리자 그룹에 속한 계정이 비인가자에게 유출될 경우 관리자 권한으로 시스템에 접근하여 계정 정보 유출, 환경 설정 파일 및 디렉토 변조 등의 위협이 존재함	vi 편집기를 이용하여 "/etc/group 파일에 불필요한 계정 삭제 (수정 전) root:x:0:TestUser (수정 후) root:x:0:
	U-51	계정이 존재하지 않는 GID 금지	하	시스템 관리나 운용에 불필요한 그룹이 존재 [현황] TestUser:!:: TestUser2:!::	취약	불필요한 그룹의 소유권으로 설정되어 있는 파일의 노출에 의한 위협이 존재함	groupdel 명령으로 불필요한 그룹 삭제 (수정 후) #gropdel <TestUser> (수정 후) #gropdel <TestUser2> ※ 그룹 삭제시 그룹권한으로 존재하는 파일이 존재하는지 확인이 필요하며 추후 권한 할당을 위해 그룹을 먼저 생성하였을 가능성도 존재하므로 무분별한 삭제는 권장하지 않으며 신규 생성된 그룹을 중점적으로 점검 권고
	U-52	동일한 UID 금지	중	동일한 UID로 설정된 사용자 계정이 존재하지 않음	양호		

		U-53	사용자 shell 점검	하	로그인이 필요하지 않은 계정에 /bin/false(nologin) 쉘이 부여되지 않음 [현황] TestUser:x:1001:1001::/home/TestUser:/bin/bash TestUser2:x:1002:1002::/home/TestUser2:/bin/bash	**취약**	로그인이 불필요한 계정은 일반적으로 OS 설치 시 기본적으로 생성되는 계정으로 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 이용하여 시스템에 명령어를 실행 할 수 있음	vi 편집기를 이용하여 "/etc/passwd"파일에 로그인 쉘 부분인 계정 맨 마지막에 /bin/false 부여 및 변경 (수정 전) TestUser:x:1001:1001::/home/TestUser:/bin/bash (수정 전) TestUser2:x:1002:1002::/home/TestUser2:/bin/bash (수정 후) TestUser:x:1001:1001::/home/TestUser:/bin/false (수정 후) TestUser2:x:1002:1002::/home/TestUser2:/bin/false
		U-54	Session Timeout 설정	하	Session Timeout이 600초 이하로 설정되지 않음 [현황] TMOUT=9999	**취약**	Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 불필요한 내부 정보의 노출 위험이 존재함	sh, ksh, bash : vi 편집기를 이용하여 "etc/profile" 파일을 아래와 같이 수정 (수정 전) TMOUT=9999 (수정 후) TMOUT=600
	파일 및 디렉토리 관리	U-05	root 홈, 패스 디렉토리 권한 및 패스 설정	상	- PATH: … → 없음 → 양호- 홈 권한: drwx------ → 양호 …	**양호**		
		U-06	파일 및 디렉터리 소유자 설정	상	- 소유자 없는 파일 : 2건 설정 내용 : /home/TestUser/test1 /home/TestUser/test2 - 그룹 없는 파일 : 0건	**취약**	UID/GID 충돌 시 비인가 사용자가 파일 소유자로 가장하여 조작 가능성 존재	소유자가 존재하지 않는 파일 및 디렉터리 삭제 또는, 소유자 변경
		U-07	/etc/passwd 파일 소유자 및 권한 설정	상	소유자: root, 권한: 644	**양호**	-	-
		U-08	/etc/shadow 파일 소유자 및 권한 설정	상	소유자: root, 권한: 000 (정상)	**양호**	-	-
		U-09	/etc/hosts 파일 소유자 및 권한 설정	상	소유자 root (적절함), 권한 644 (600 이상)	**취약**	hosts 파일에 비인가자 쓰기 권한이 부여되어 정상적인 DNS를 우회하는 파밍(Pharming) 공격에 악용될 수 있음.	/etc/hosts 파일의 권한을 600이하으로 설정
		U-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	- /etc/inetd.conf 파일 없음 - /etc/xinetd.conf 소유자: root, 권한: 644	**취약**	/etc/inetd.conf: 파일 없어 보안 점검 불가, 상(x)inetd 설정 파일에 비인가자 쓰기 권한이 부여되어 있음으로, 서비스 변조나 악성 서비스 등록을 통해 시스템이 악용될 수 있음.	/etc/inetd.conf 또는 /etc/xinetd.conf 파일이 필요한 경우 복원하거나 재설치, "/etc/(x)inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
		U-11	/etc/syslog.conf 파일 소유자 및 권한 설정	상	소유자 root (적절함), 권한 644 (640 초과)	**취약**	syslog.conf 파일에 비인가자에게 쓰기 권한이 부여되어 있어, 로그 설정을 조작해 서비스 변조나 악성 로그 유입 등 보안 위협이 발생할 수 있음.	/etc/rsyslog.conf 파일의 권한을 640 이하로 설정
		U-12	/etc/services 파일 소유자 및 권한 설정	상	소유자 TestUser (부적절), 권한 666 (644 초과)	**취약**	/etc/services 파일 소유자 및 권한이 부적절하게 설정되어 있어, 비인가 사용자가 포트 번호를 변경하거나 허용되지 않은 포트를 열어 악성 서비스를 실행할 수 있음.	"/etc/ services" 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권한 644 이하)
		U-13	SUID, SGID, Sticky bit 설정 파일 점검	상	- 파일 경로 : /usr/bin/passwd 권한 : -rwsr-xr-x. SUID 상태 : 설정됨 SGID 상태 : 없음 - 파일 경로 : /usr/bin/sudo 권한 : ---s--x--x. SUID 상태 : 설정됨 SGID 상태 : 없음 - 파일 경로 : /usr/bin/chage 권한 : -rwsr-xr-x. SUID 상태 : 설정됨 SGID 상태 : 없음	**취약**	SUID 파일 권한이 설정되어 있어, 이를 통해 root 권한 획득이 가능함.	권한이 설정되어 있는 불필요한 SUID의 해당 권한을 제거
		U-14	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	- 사용자: TestUser > 환경파일: .bash_profile - 소유자: wins - 권한 : 644 - 진단 : 취약 (소유자가 사용자 또는 root 아님)	**취약**	파일 소유자가 본인도 아니고 root도 아니어서 권한 및 무결성 관리가 불안정함	파일 권한은 644 유지 (소유자 읽기/쓰기, 그룹 및 기타는 읽기만 가능), .bash_profile 파일 소유자를 해당 사용자(TestUser) 또는 root로 변경
		U-15	world writable 파일 점검	상	* 전체 world writable 파일 수 : 3 건 * 중요 시스템 경로 내 존재 파일 수 : 1 건 * 전체 world writable 파일 목록 및 확인 여부: - /etc/services : 아니오 (설정 이유 미확인) - /home/TestUser/test4 : 아니오 (설정 이유 미확인) - /home/TestUser/test5 : 아니오 (설정 이유 미확인)	**취약**	설정 이유 확인이 되지 않는 world writable이 설정되어 있어, 일반사용 자 및 비인가된 사용자가 해당 파일을 임의로 수정, 삭제가 가능함	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거할 것. 해당 권한이 꼭 필요한 경우, 설정 이유를 명확히 문서화하고 권한을 엄격히 관리할 것.
		U-16	/dev에 존재하지 않는 device 파일 점검	상	- dev 파일 점검 여부 : X - 비정상 device 파일 제거 상태 : 미점검 - 세부 사항 : - /dev 디렉터리에 일반 파일이 존재하지 않아 점검이 수행되지 않음.	**취약**	dev 에 대한 파일 점검이 이행되지 않아, 공격자는 루트킷 설정 파일을 /dev에 실제 장치 파일처럼 위장해 관리자 탐지를 회피할 수 있음	/dev 디렉터리 내 파일들을 주기적으로 점검하여, 실제 장치 파일이 아닌 일반 파일이나 의심스러운 파일이 있는지 확인할 것
		U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상	login, shell, exec 서비스가 사용 중이지 않아 .rhosts 관련 취약점 위험이 낮음.	**양호**		

	U-18	접속 IP 및 포트 제한	상	- TCP Wrapper 상태 : ALL:ALL 없음, 접근 IP 없음 설정 내용 : (없음) - iptables 상태 : 포트/IP 제한 있음 설정 내용: -A IN_public_allow -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT - IPFilter 상태 : ipf 명령어 없음 설정 내용 : (없음)	**양호**		
	U-55	hosts.lpd 파일 소유자 및 권한 설정	하	/etc/hosts.lpd 파일이 존재하지 않음	**양호**	-	-
	U-56	UMASK 설정 관리	중	UMASK 값이 낮음 (현재: 002)	**취약**	새로 생성되는 파일/디렉토리에 그룹과 다른 사용자에게 쓰기 권한까지 허용 불필요한 권한 노출로 파일 변조, 정보 유출, 권한 남용 위험	설정파일에 UMASK 값을 “022”로 설정
	U-57	홈디렉토리 소유자 및 권한 설정	중	- 사용자: wins > 홈 디렉토리: /home/wins > 실제 소유자: wins - 사용자: TestUser > 홈 디렉토리: /home/TestUser > 실제 소유자: wins - 사용자: TestUser2 > 홈 디렉토리: /home/TestUser2(존재하지 않음) - 사용자: nfsnobody > 홈 디렉토리: /var/lib/nfs > 실제 소유자: root	**취약**	소유자 불일치 및 타 사용자 쓰기 권한 있음, 타 사용자가 설정 파일을 변조할 수 있음 /home/TestUser2 : 홈 디렉토리가 존재하지 않아, 악성 디렉토리/파일 생성 및 악용 가능	사용자별 홈 디렉터리 소유주를 해당 계정으로 변경 타사용자의 쓰기 권한 제거 “/etc/passwd” 파일에서 홈 디렉터리 확인, 사용자 홈 디렉터리 외 개별적으로 만들어 사용하는 사용자 디렉터리 존재여부 확인 및 점검 홈 디렉토리가 없을 경우 : 홈 디렉토리 생성, 소유자 및 그룹 설정, 적절한 권한 부여 (본인만 접근 가능) 실시할 것
	U-58	홈디렉토리로 지정한 디렉토리의 존재 관리	중	"- 사용자: TestUser2 > 홈 디렉토리: /home/TestUser2" > 홈 디렉토리: /home/TestUser2(존재하지 않음)	**취약**	홈 디렉토리 존재하지 않아, 로그인 시 루트 디렉터리(/)로 접근 가능성 존재 /home/TestUser2 : 홈 디렉토리가 존재하지 않아, 악성 디렉토리/파일 생성 및 악용 가능	홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는, 계정 삭제
	U-59	숨겨진 파일 및 디렉토리 검색 및 제거	하	- 의심 항목 발견: /boot/.vmlinuz-3.10.0-327.36.1.el7.x86_64.hmac - 의심 항목 발견: /usr/lib64/.libgcrypt.so.11.hmac - 의심 항목 발견: /usr/lib64/.libhogweed.so.2.5.hmac - 의심 항목 발견: /usr/lib64/.libnettle.so.4.7.hmac - 의심 항목 발견: /usr/lib64/.libgnutls.so.28.41.0.hmac - 의심 항목 발견: /usr/lib64/.libcrypto.so.1.0.2k.hmac - 의심 항목 발견: /usr/lib64/.libssl.so.1.0.2k.hmac	**취약**	숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음	ls –al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭제함

	U-19	Finger 서비스 비활성화	상	현재 finger 서비스가 아래와 같이 활성화 상태임을 확인:
				service finger
				{
				socket_type = stream
				protocol = tcp
				wait = no
				user = nobody
				server = /usr/sbin/in.fingerd
				disable = no
				}
					취약	비인가자가 finger 서비스를 통해 사용자 정보를 조회할 경우, 이를 바탕으로 패스워드 공격이 이루어져 시스템 권한 탈취의 위험이 존재합니다. 따라서 사용하지 않는 finger 서비스는 반드시 중지하여야 함	vi 편집기를 이용하여 /etc/xinetd.d/finger 파일을 열고, finger 서비스를 비활성화
							service finger
							{
							socket_type = stream
							protocol = tcp
							wait = no
							user = nobody
							server = /usr/sbin/in.fingerd
							disable = yes
							}
							disable = yes로 설정하여 finger 서비스가 중지되도록 변경.

	U-20	Anonymous FTP 비활성화	상	설정 파일: /etc/vsftpd.conf 설정 내용: anonymous_enable=yes → 익명(anonymous) FTP 접속이 허용되어 있음	**취약**	익명 FTP 접속 시 anonymous 계정으로 로그인 가능 만약 익명 접속 디렉터리에 쓰기 권한(write permission) 이 설정되어 있다면, 악의적인 사용자가 해당 권한을 이용해 로컬 익스플로잇(local exploit) 등으로 시스템을 공격할 수 있음	일반 FTP - 익명 FTP 계정 삭제 /etc/passwd 파일에서 ftp 또는 anonymous 계정 삭제 userdel ftp ProFTP - 익명 FTP 접속 제한 설정 conf/proftpd.conf 파일 내 익명 FTP 관련 설정 주석 처리 <Anonymous ~ftp> # User ftp Group ftp # UserAlias anonymous ftp ... </Anonymous> vsFTP - 익명 FTP 접속 제한 설정 설정파일 위치: /etc/vsftpd/vsftpd.conf 또는 /etc/vsftpd.conf anonymous_enable=NO 설정 변경 후 서비스 재시작 필요: systemctl restart vsftpd

	U-21	r 계열 서비스 비활성화	상	r-command(rsh, rlogin, rexec) 서비스 활성화 확인 및 보안 위험성
				/etc/xinetd.d/ 디렉터리 내 rexec, rlogin, rsh 서비스 설정 파일에서 모두 disable = no로 설정되어 있음이 확인됨.
				
				각각의 서비스는 다음과 같이 root 권한으로 동작하며, 인증 없이 원격 접속이 가능함.
				service exec {
				disable = no
				user = root
				server = /usr/sbin/in.rexecd
				...
				}
				service login {
				disable = no
				user = root
				server = /usr/sbin/in.rlogind
				...
				}
				service shell {
				disable = no
				user = root
				server = /usr/sbin/in.rshd
				...
				}
					취약	rsh, rlogin, rexec 등의 r-command 서비스가 활성화되어 있어 원격에서 인증 절차 없이 터미널 접속 및 쉘 명령어 실행이 가능한 상태임.
						
						이로 인해 외부 공격자가 시스템에 무단 접근하거나 권한 상승 공격을 수행할 위험이 존재함.
							/etc/xinetd.d/rexec, /etc/xinetd.d/rlogin, /etc/xinetd.d/rsh 설정 파일 내 disable 값을 no에서 yes로 변경하여 서비스를 비활성화함.
							service exec
							{
							disable = yes
							...
							}
							
							service login
							{
							disable = yes
							...
							}
							
							service shell
							{
							disable = yes
							...
							}
							이를 통해 인증 없이 원격 접속 및 명령어 실행이 가능한 r-command 서비스를 중지하여 보안 취약점을 제거함.

	U-22	cron 파일 소유자 및 권한 설정	상	rontab 및 관련 파일 권한 설정 점검 /etc/cron.daily, /etc/cron.hourly, /etc/cron.monthly, /etc/cron.weekly 디렉터리 권한이 drwxr-xr-x로 설정되어 있어 일반 사용자도 읽기 및 실행 권한을 보유함. /etc/crontab 파일은 -rw-r--r-- 권한으로 일반 사용자도 읽기 가능함. /var/spool/cron/ 또는 /var/spool/cron/crontabs/ 디렉터리는 생성되어 있지 않음. /etc/cron.deny 파일이 -rw------- (600) 권한이어야 하나 현재 0바이트 파일로 존재함. alloy(crontab 허용 사용자 파일) 파일은 생성되어 있지 않음.	**취약**	Crontab 명령어 권한 부여에 따른 위험성 root 외 일반 사용자에게 crontab 명령어 사용 권한을 부여할 경우, 고의 또는 실수로 인해 불법적이거나 악의적인 예약 작업이 실행될 가능성이 있음. 이로 인해 시스템 자원 과다 사용, 보안 취약점 노출, 시스템 장애 등 피해가 발생할 위험이 존재함.	Crontab 명령어 및 관련 파일 권한 설정 권고 crontab 명령어 파일 권한 권한을 750 이하로 설정 일반 사용자의 실행 제한 및 root와 같은 관리자만 사용 가능하도록 제한 cron 관련 파일 소유자 및 권한 소유자는 root로 설정 권한은 640 이하로 제한하여 읽기 권한을 최소화 불필요한 사용자 접근 차단 및 보안 강화 목적 chmod 750 /usr/bin/crontab chown root:root /etc/crontab /etc/cron.d/* /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly chmod 640 /etc/crontab /etc/cron.d/* /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly

U-23	DoS 공격에 취약한 서비스 비활성화	상	/etc/xinetd.d/ 내 echo, discard, daytime, chargen 관련 서비스 파일에 대해 cat 명령어로 확인한 결과, disable = no (또는 0)로 설정되어 활성화된 상태임을 확인함.
			
			ps -ef | grep [포트번호] 명령어로 주요 서비스 상태 점검 결과:
			
			NTP(123) : 비활성화
			
			DNS(53) : 비활성화
			
			SNMP(161,162) : 비활성화
			
			SMTP(25) : 활성화
				취약	시스템 정보 유출: echo, discard, daytime, chargen 서비스는 불필요한 응답을 제공해 공격자에게 시스템 상태나 네트워크 구성을 알릴 수 있음
					
					DoS (서비스 거부) 공격: 이들 서비스를 악용해 증폭 공격, 반사 공격을 실행할 수 있어 시스템 자원 고갈 및 서비스 장애를 초래할 수 있음
						echo, discard, daytime, chargen, SMTP 등의 서비스는 inet_interfaces = none 으로 설정하여 비활성화함으로써 외부 네트워크 접근을 차단함.
						
						NTP, DNS, SNMP, SMTP 서비스는 사용 여부에 따라 활성화 또는 비활성화 관리함.
						
						SMTP 서비스가 현재 미사용 상태임에도 활성화 되어 있으므로, 아래와 같이 비활성화 조치함:
						vi /etc/postfix/main.cf
						# inet_interfaces 값을 loopback-only로 변경하여 외부 접속 제한
						inet_interfaces = loopback-only
						이를 통해 불필요한 외부 서비스 노출을 줄이고 시스템 보안을 강화함.

U-24	NFS 서비스 비활성화	상	ps -ef | grep nfs 명령어를 통해 불필요하게 실행 중인 NFS 서비스 프로세스를 확인함. 현재 여러 NFS 데몬(nfsd, nfsd4, nfsd4_callbacks 등)이 동작 중이며, 서비스 불필요 시 비활성화가 필요함.	**취약**	NFS 서비스는 서버의 디스크를 클라이언트와 공유하는 기능으로, 적절한 보안 설정이 적용되지 않을 경우 불필요한 파일이 외부에 공유되어 중요 정보 유출 위험이 존재함. 따라서 공유 대상 및 접근 권한 설정을 철저히 관리해야 함.	/etc/dfs/dfstab (또는 /etc/exports) 파일 내 모든 공유 설정을 제거하여 공유가 없도록 조치함. /etc/dfs/dfstab 파일이 존재하지 않아 현재 공유 설정이 없음을 확인함. NFS 관련 데몬(nfsd, statd, mountd)을 종료함. kill -9 [PID] 명령어를 사용해 해당 프로세스를 강제 종료함.
U-25	NFS 접근통제	상	아래 명령어를 통해 NFS 서비스가 활성화되어 있음을 확인하였음. [root@vbox ~]# ps -ef | grep nfs root 1519 2 0 09:31 ? 00:00:00 [nfsd4] root 1520 2 0 09:31 ? 00:00:00 [nfsd4_callbacks] root 1599 2 0 09:31 ? 00:00:00 [nfsd] root 1601 2 0 09:31 ? 00:00:00 [nfsd] ... NFS 접근 제어 설정 파일인 /etc/exports가 존재하며, 내용 확인 결과 비활성화 상태임을 아래 명령어를 통해 확인함. [root@vbox ~]# ls -l /etc/exports -rw-r--r--. 1 root root 0 6월 7 2013 /etc/exports [root@vbox ~]# exportfs -v (출력 없음 또는 비활성화 상태)	**취약**	접근 제한 설정이 적절하지 않을 경우, 인증 절차 없이 비인가자가 디렉터리나 파일에 접근할 수 있으며, 원격에서 해당 공유 시스템을 마운트하여 중요 파일을 변조하거나 유출할 위험이 존재함.	NFS 서비스가 활성화되어 있으며, 사용자 제한 설정이 되어 있지 않아 다음과 같이 제한 설정을 추가함. 접근 가능한 호스트 설정 /stand host1 host2 클라이언트 권한 제한 옵션(root_squash) 설정 /stand 192.168.0.10(rw,root_squash) 설정 변경 후에는 아래 명령어로 적용 및 해제를 수행함. # exportfs -u # exportfs -r
U-26	automountd 제거	상	automount 서비스가 시스템에서 활성화되어 정상적으로 동작 중임을 확인함. [root@vbox ~]# ps -ef | grep automount root 1463 1 0 09:31 ? 00:00:00 /usr/sbin/automount --systemd-service --dont-check-daemon	**취약**	자동 마운트(automount) 서비스 취약점 automount 서비스가 활성화되어 있을 경우, 해당 파일 시스템의 마운트 옵션을 변경하여 공격자가 root 권한을 획득할 수 있음. 특히 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령어를 실행할 위험이 존재함.	automountd 서비스 데몬을 중지하여 서비스를 비활성화 # kill -9 [PID] 아래 명령어를 통해 자동 시작 스크립트가 없는지 확인 # ls -al /etc/rc.d/rc*.d/* | grep automount (또는 autofs)
U-27	RPC 서비스 확인	상	내부 etc/xinetd.d 내부 파일에 RPC와 관련된 설정 파일 확인 명령어 사용 grep -i 'disable' /etc/xinetd.d/* | grep -Ei 'rusers|rstat|rexec|walld|spray|quotad|statd' | grep -v yes 아래와 같이 일부 r-서비스가 disable = no 로 설정되어 활성화 상태임을 확인 /etc/xinetd.d/rexec: disable = no /etc/xinetd.d/rlogin: disable = no /etc/xinetd.d/rsh: disable = no	**취약**	버퍼 오버플로우(Buffer Overflow): 입력값 검증 부재로 인해 악의적인 코드 실행 가능 DoS 공격(서비스 거부): 비정상 입력을 통해 시스템 자원을 고갈시켜 서비스 마비 유도 원격 코드 실행(Remote Code Execution): 인증 우회 또는 조작을 통한 공격자 명령 실행 가능	/etc/xinetd.d 디렉터리 내 RPC 관련 서비스 설정 파일(rexec, rlogin, rsh)을 확인한 결과, 각 파일의 disable 항목을 yes로 설정하여 해당 서비스를 비활성화해야함
U-28	NIS, NIS+ 점검	상	ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated" ypserv, ypbind, ypxfrd, rpc.yppasswdd, rpc.ypupdated 등의 NIS 관련 프로세스가 현재 실행되고 있지 않음	**양호**		

	서비스 관리	U-29	tftp, talk 서비스 비활성화	상	ps -ef 명령어를 통해 다음과 같이 tftp, talk, ntalk 서비스의 실행 상태를 확인함:
					[root@vbox xinetd.d]# ps -ef | grep tftp
					[root@vbox xinetd.d]# ps -ef | grep talk
					[root@vbox xinetd.d]# ps -ef | grep ntalk
					tftp, talk: 실행 중인 프로세스 없음
					ntalk: /etc/xinetd.d/ntalk 설정 파일 존재하며, 설정 내용 중 disable = no로 서비스가 활성화되어 있음
					service ntalk
					{
					socket_type = dgram
					protocol = udp
					wait = yes
					user = nobody
					server = /usr/sbin/in.talkd
					disable = no
					}
						취약	talk, ntalk, tftp 등은 과거 시스템 간 메시지 송수신이나 파일 전송을 위해 사용되던 서비스이며, 암호화되지 않은 통신 및 인증 부재 등의 보안 취약점이 존재함. 현재 대부분 시스템에서는 사용하지 않으므로, 서비스를 유지할 경우 보안 위협에 노출될 수 있음.	/etc/xinetd.d/ntalk 파일 내 disable = no → disable = yes 로 변경
								xinetd 재시작:
								systemctl restart xinetd
								이후 상태 확인:
								ps -ef | grep ntalk
								서비스 비활성화 및 삭제를 원할 경우:
								yum remove talk-server talk

		U-30	Sendmail 버전 점검	상	Sendmail 사용 여부 및 버전 확인 시스템에서 Sendmail 서비스가 실행 중임을 다음 명령어로 확인함: ps -ef | grep sendmail 실행 결과: root 1576 1 0 09:31 ? 00:00:00 sendmail: accepting connections smmsp 1739 1 0 09:31 ? 00:00:00 sendmail: Queue runner@01:00:00 for /var/spool/clientmqueue Sendmail의 설치 및 실행 버전 확인을 위해 다음 명령어를 수행: 실행 결과: Version 8.14.7 Compiled with: DNSMAP HESIOD HES_GETMAILHOST LDAPMAP LOG MAP_REGEX MATCHGECOS MILTER MIME7TO8 MIME8TO7 NAMED_BIND NETINET NETINET6 NETUNIX NEWDB NIS PIPELINING SASLv2 SCANF SOCKETMAP STARTTLS TCPWRAPPERS USERDB USE_LDAP_INIT Sendmail 버전이 최신버전이 아니라고 판단	**취약**	현재 사용 중인 Sendmail 8.14.7 버전은 오래된 버전으로, 과거에 버퍼 오버플로우(Buffer Overflow) 등의 보안 취약점이 다수 발견된 바 있음. 이러한 취약점을 악용할 경우 다음과 같은 보안 위협이 발생할 수 있음: 시스템 권한 획득: 공격자가 루트 권한을 포함한 시스템 권한을 탈취할 수 있음 중요 정보 유출: 메일 서버를 통해 전송되는 개인정보, 인증정보 등 주요 정보가 유출될 수 있음 서비스 거부 공격(DoS): 메일 서비스의 비정상 종료를 유도하여 서비스 가용성에 영향을 줄 수 있음	Sendmail 최신 버전으로의 패치 또는 불필요 시 서비스 비활성화 조치가 필요함.
		U-31	스팸 메일 릴레이 제한	상	SMTP 서비스 사용 여부를 확인하기 위해 다음 명령어를 수행한 결과, sendmail 프로세스가 정상적으로 실행 중임을 확인함. [root@vbox xinetd.d]# ps -ef | grep sendmail | grep -v "grep" root 1576 1 0 09:31 ? 00:00:00 sendmail: accepting connections smmsp 1739 1 0 09:31 ? 00:00:00 sendmail: Queue runner@01:00:00 for /var/spool/clientmqueue 또한, 일반 사용자의 Sendmail 실행 방지를 위해 PrivacyOptions 설정을 확인한 결과 아래와 같이 novrfy, noexpn 옵션이 설정되어 있음. [root@vbox xinetd.d]# grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions O PrivacyOptions=authwarnings,novrfy,noexpn, restrictqrun	**양호**		
		U-32	일반사용자의 Sendmail 실행 방지	상	SMTP 서비스 사용 여부 확인 [root@vbox xinetd.d]# ps -ef | grep sendmail | grep -v "grep" root 1576 1 0 09:31 ? 00:00:00 sendmail: accepting connections smmsp 1739 1 0 09:31 ? 00:00:00 sendmail: Queue runner@01:00:00 for /var/spool/clientmqueue 일반 사용자 Sendmail 실행 방지를 다음과 같이 PraivacyOptions 옵션에서 확인할 수 있다. [root@vbox xinetd.d]# grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions O PrivacyOptions=authwarnings,novrfy,noexpn, restrictqrun	**양호**		

	U-33	DNS 보안 버전 패치	상	DNS 서비스 비활성화 확인 및 바인드 사용 하지 않음. [root@vbox xinetd.d]# ps -ef | grep anmed root 12397 2453 0 11:27 pts/0 00:00:00 grep --color=auto anmed [root@vbox xinetd.d]# named -v -bash: named: command not found 따라서 DNS 서비스는 비활성화 상태이며, BIND 서비스는 사용하지 않고 있음.	**양호**		
	U-34	DNS Zone Transfer 설정	상	DNS 서비스 비활성화 및 바인드 미사용 확인 [root@vbox xinetd.d]# ps -ef | grep named | grep -v "grep" [root@vbox xinetd.d]# ps -ef | grep 53 root 653 1 0 09:31 ? 00:00:00 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid root 2453 2445 0 09:36 pts/0 00:00:00 -bash root 12678 2453 0 13:39 pts/0 00:00:00 ps -ef root 12679 2453 0 13:39 pts/0 00:00:00 grep --color=auto 53	**양호**		
	U-35	웹서비스 디렉토리 리스팅 제거	상	vi 편집기를 이용하여 /etc/httpd/conf/httpd.conf 설정 파일을 확인한 결과, <Directory "/var/www/html"> 설정에서 디렉터리 인덱싱 기능(Options Indexes)이 활성화되어 있음을 확인함. <Directory "/var/www/html"> Options Indexes FollowSymLinks AllowOverride None Require all granted </Directory> 디렉터리 인덱싱이 활성화된 경우, 해당 디렉터리에 인덱스 파일이 존재하지 않을 시 파일 목록이 사용자에게 노출되어 웹 서버 구조 및 중요 파일이 외부에 공개될 위험이 있으므로 보안상 주의가 필요함.	**취약**	디렉터리 검색 기능이 활성화되어 있을 경우, 사용자는 해당 디렉터리 내 모든 파일 목록을 확인할 수 있으며, 이로 인해 웹 서버 구조가 노출될 뿐만 아니라 백업 파일, 소스 코드 등 공개되어서는 안 되는 민감한 정보가 노출될 위험이 존재함.	디렉터리 검색 기능을 제거하기 위해 /[Apache_home]/conf/httpd.conf 파일 내 모든 디렉터리 설정의 Options 지시자에서 Indexes 옵션을 삭제하거나 -Indexes로 변경함. 예시 설정: <Directory /> Options -Indexes AllowOverride None Order allow,deny Allow from all </Directory> 이를 통해 디렉터리 인덱싱 기능이 비활성화되어 파일 목록 노출 위험을 차단함.
	U-36	웹서비스 웹 프로세스 권한 제한	상	아파치 서버 프로세스 상태를 확인한 결과, 마스터 프로세스는 root 권한으로 1개가 실행 중이며, 자식 프로세스들은 apache 사용자 권한으로 동작하는 것을 확인함. [root@vbox httpd]# ps -ef | grep httpd root 1262 1 0 09:31 ? 00:00:04 /usr/sbin/httpd -DFOREGROUND apache 1680 1262 0 09:31 ? 00:00:00 /usr/sbin/httpd -DFOREGROUND apache 1681 1262 0 09:31 ? 00:00:00 /usr/sbin/httpd -DFOREGROUND apache 1682 1262 0 09:31 ? 00:00:00 /usr/sbin/httpd -DFOREGROUND apache 1686 1262 0 09:31 ? 00:00:00 /usr/sbin/httpd -DFOREGROUND apache 1690 1262 0 09:31 ? 00:00:00 /usr/sbin/httpd -DFOREGROUND 또한, Apache 설정 파일(/etc/httpd/conf/httpd.conf)에서 User와 Group 항목이 apache로 지정되어 있음을 확인함. [root@vbox httpd]# grep -E '^User|^Group' /etc/httpd/conf/httpd.conf User apache Group apache 이는 Apache 서버가 root 권한의 마스터 프로세스 하에 비특권 사용자 apache로 실행되어, 보안상 권한 분리가 적절히 이루어지고 있음을 의미함.	**양호**		

U-37	웹서비스 상위 디렉토리 접근 금지	상	vi 편집기를 통해 /etc/httpd/conf/httpd.conf 아파치 설정 파일을 확인한 결과, <Directory /> 설정에서 AllowOverride none이 설정되어 있음이 확인됨. <Directory /> AllowOverride none Require all denied </Directory>	**취약**	모든 접근을 차단하는 설정으로 인해 인증되지 않은 사용자는 물론, 인증된 사용자도 해당 디렉터리에 접근할 수 없게 되어 정상적인 서비스 이용에 제한이 발생할 수 있음.	Apache 설정 파일(/etc/httpd/conf/httpd.conf)의 <Directory /> 설정에서 AllowOverride None을 AllowOverride AuthConfig으로 변경하여, 디렉터리 단위의 사용자 인증 설정을 허용하도록 수정함. 이후, 아래와 같은 내용으로 .htaccess 파일을 생성하여 기본 인증을 적용함: AuthName "디렉터리 사용자 인증" AuthType Basic AuthUserFile /usr/local/apache/test/.auth Require valid-user 사용자 인증에 필요한 아이디 및 비밀번호는 다음 명령어로 생성하여 적용함: htpasswd -c /usr/local/apache/test/.auth test New password: Re-type new password: Adding password for user test 이를 통해 해당 디렉터리 접근 시 인증이 요구되도록 설정하여 보안성을 강화함.
U-38	웹서비스 불필요한 파일 제거	상	아래 명령어를 통해 /etc/httpd/conf.d/ 내에 manual 관련 파일 또는 설정이 존재하지 않음을 확인함. [root@vbox etc]# grep -i manual /etc/httpd/conf.d/*.conf [root@vbox etc]# 판단: 불필요한 manual 관련 파일 및 설정이 제거되어 있어 양호한 상태임.	**양호**		
U-39	웹서비스 링크 사용금지	상	httpd.conf 설정 파일에서 <Directory /> 항목이 아래와 같이 설정되어 있음: <Directory /> AllowOverride none Require all denied </Directory> 해당 설정은 서버의 루트 디렉토리에 대해 .htaccess 파일 등의 설정 적용을 허용하지 않으며, 모든 접근을 기본적으로 차단하여 보안성을 강화함.	**취약**	웹 루트 디렉터리(DocumentRoot)에 시스템 루트 디렉터리(/)를 심볼릭 링크한 파일이 존재하며, 디렉터리 인덱싱 기능이 차단되어 있더라도 해당 링크를 통해 루트 디렉터리의 파일 구조를 열람할 수 있는 보안 취약점이 존재함.	심볼릭 링크 및 Aliases 사용을 제한하기 위해 httpd.conf 파일의 <Directory /> 설정을 다음과 같이 수정하여 적용함: <Directory /> Options -FollowSymLinks AllowOverride None Order allow,deny Allow from all </Directory> FollowSymLinks 옵션을 비활성화하여 웹 루트 경로 내 심볼릭 링크를 통한 시스템 디렉터리 접근을 차단함으로써, 정보 유출 및 시스템 침해 가능성을 낮춤.
U-40	웹서비스 파일 업로드 및 다운로드 제한	상	웹 서버에서 파일 업로드 및 다운로드에 대한 제한이 설정되어 있지 않아, 악의적인 파일 업로드 또는 중요 파일의 무단 다운로드 등의 보안 위협이 존재함.	**취약**	악의적인 사용자가 웹 쉘 파일을 반복적으로 업로드하거나 대용량 파일을 무단으로 업로드할 경우, 시스템 권한 탈취 및 서버 자원 고갈 등의 보안 위협이 발생할 수 있음.	vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일에 다음과 같이 설정하여 업로드 가능한 파일의 크기를 제한함: (수정 후) <Directory /> LimitRequestBody 5000000 </Directory> 해당 설정을 통해 업로드 가능한 파일의 최대 크기를 약 5MB로 제한하여, 대용량 파일 업로드로 인한 자원 고갈 및 악의적 파일 업로드 시도를 방지함.
U-41	웹 서비스 영역의 분리	상	DocumentRoot가 별도의 전용 디렉토리로 지정되어 있지 않음. DocumentRoot가 기본값인 /var/www/html로 설정되어 있음.	**취약**	웹 서버의 루트 디렉토리와 운영체제의 루트 디렉토리가 동일하게 설정된 경우, 비인가자가 웹 서비스를 통해 침투 시 시스템 주요 영역까지 접근할 위험이 있으며, 이로 인해 심각한 피해가 발생할 수 있음.	vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일의 DocumentRoot 설정을 다음과 같이 변경함: (수정 전) DocumentRoot "/var/www/html" (수정 후) DocumentRoot를 /usr/local/apache/htdocs, /usr/local/apache2/htdocs, /var/www/html을 제외한 별도의 디렉토리로 변경하여 웹 루트 디렉토리를 운영체제 기본 디렉토리와 분리함.
U-60	ssh 원격접속 허용	중	원격 접속 시 안전하지 않은 프로토콜이 사용되고 있음. 보안이 강화된 ssh와 함께 보안 취약점이 있는 telnet이 동시에 설치되어 있음	**취약**	원격 접속 시 Telnet, FTP 등 암호화되지 않은 프로토콜을 사용하여 아이디, 패스워드 및 중요 정보가 외부로 유출될 위험이 존재함.	yum remove telnet-server, dnf remove telnet telnet-server 명령어를 사용하여 Telnet 클라이언트와 서버 패키지를 삭제함. (수정 전) rpm -qa | grep telnet 명령어 실행 시, telnet-server-0.17-66.el7.x86_64, telnet-0.17-66.el7.x86_64 패키지가 확인됨. (수정 후) 동일 명령어 실행 시, 관련 패키지가 출력되지 않음.
U-61	ftp 서비스 확인	하	FTP 서비스가 활성화되어 있음. root 계정이 PID 1268로 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf 프로세스를 실행 중임 (10:28 기준).	**취약**	FTP 서비스는 통신 구간이 암호화되지 않은 평문으로 전송되어, 계정 정보(아이디, 패스워드) 및 데이터가 네트워크상에서 스니핑될 위험이 존재함.	FTP 서비스를 중지하기 위해 service vsftpd stop, service proftpd stop 명령어를 실행함. (수정 전) ps –ef | egrep "vsftpd|proftpd" 명령어 실행 시, root 1268 1 0 10:28 ? 00:00:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf 프로세스가 확인됨. (수정 후) 동일 명령어 실행 시, 관련 프로세스가 출력되지 않음.

		U-62	ftp 계정 shell 제한	중	FTP 계정에 /bin/false 쉘이 부여되어 있지 않음. ftp 계정의 로그인 쉘이 /sbin/nologin으로 설정되어 있음	**취약**	불필요한 기본 계정에 쉘이 부여될 경우, 공격자가 해당 계정을 이용해 FTP 기본 계정으로 시스템에 접근하여 공격할 위험이 존재함.	vi 편집기를 이용하여 /etc/passwd 파일의 FTP 계정 쉘을 아래와 같이 변경함: (수정 전) ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin (수정 후) ftp:x:14:50:FTP User:/var/ftp:/bin/false
		U-63	Ftpusers 파일 소유자 및 권한 설정	하	vsftpd 파일의 소유자가 root이며, 파일 권한이 640 이하로 설정되어 있음.	**양호**		
		U-64	Ftpusers 파일 설정	중	FTP 서비스가 활성화되어 있으나, root 계정의 접속은 차단되어 있음.	**양호**		
		U-65	at 파일 소유자 및 권한 설정	중	at 명령어가 일반 사용자도 사용할 수 있는 상태이며, 관련 파일의 권한이 640 이상으로 설정되어 있음. /usr/bin/at 파일의 권한은 -rwsr-xr-x로 설정되어 있으며, 소유자는 root, 그룹은 root임	**취약**	root 외 일반 사용자도 at 명령어를 사용할 수 있을 경우, 고의 또는 실수로 불법적인 예약 작업 실행을 통해 시스템에 피해가 발생할 위험이 존재함.	sudo touch /etc/at.allow 명령어로 /etc/at.allow 파일을 생성하고, 빈 내용으로 초기화합니다. sudo sh -c "echo '*' >> /etc/at.deny" 명령어를 사용하여 모든 일반 사용자의 at 명령어 사용을 차단합니다. sudo chown root /etc/at.allow /etc/at.deny 명령어로 두 파일의 소유자를 root로 설정하고, sudo chmod 640 /etc/at.allow /etc/at.deny 명령어로 파일 권한을 640 이하로 제한하여 비인가 사용자의 접근을 방지합니다.
		U-66	SNMP 서비스 구동 점검	중	SNMP 서비스가 활성화되어 있음.	**취약**	SNMP 서비스가 활성화됨에 따라 시스템의 주요 정보가 유출되거나 정보의 불법 수정이 발생할 위험이 존재함.	SNMP 서비스를 사용하지 않는 경우, 서비스를 중지하고 자동 시작 스크립트에서 해당 서비스를 비활성화해야 함.
		U-67	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	SNMP Community 이름이 기본값인 public으로 설정되어 있음. 기본 커뮤니티 이름 사용은 보안 취약점을 초래할 수 있으며, 무단 접근 및 정보 유출 위험이 존재함	**취약**	Community String이 기본값인 public 또는 private로 설정된 경우가 많으며, 이를 변경하지 않으면 공격자가 해당 문자열을 악용하여 환경설정 파일 열람 및 수정, 정보 수집, 관리자 권한 획득, DoS 공격 등 다양한 형태의 공격을 수행할 수 있음.	snmpd.conf 파일에서 커뮤니티명을 확인하고, 기본값인 public 및 private 커뮤니티명을 추측하기 어려운 값으로 변경해야 함.
		U-68	로그온 시 경고 메시지 제공	하	서버 및 Telnet, FTP, SMTP, DNS 서비스에 로그온 메시지가 설정되어 있지 않음	**취약**	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	Telnet, FTP, SMTP, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작
		U-69	NFS 설정 파일 접근 권한	중	NFS 접근제어 설정파일에 대한 비인가자의 수정 제한 여부를 점검함. 설정파일의 소유자가 root이며, 파일 권한이 644 이하로 설정되어 있을 경우 비인가자의 수정이 제한되어 있는 것으로 판단됨.	**양호**		
		U-70	expn, vrfy 명령어 제한	중	SMTP 서비스가 실행 중이며, PrivacyOptions=noexpn, novrfy 설정이 적용되어 있음. 해당 설정은 SMTP 서버가 EXPN 및 VRFY 명령어에 대한 응답을 제한하여, 불필요한 사용자 정보 노출을 방지함으로써 보안 강화에 기여함.	**양호**		
		U-71	Apache 웹서비스 정보 숨김	중	ServerTokens Prod 및 ServerSignature Off 설정이 적용되어 있지 않음. 이로 인해 웹 서버의 상세 정보(Apache 버전, 운영 체제 등)가 HTTP 응답 헤더나 오류 페이지를 통해 외부에 노출될 수 있는 위험이 존재함.	**취약**	웹 서버의 HTTP 헤더를 통해 서버 정보가 불필요하게 노출되어, 시스템에 대한 정보를 공격자가 수집할 수 있는 보안 위험이 존재함	웹 서버의 정보 노출을 최소화하기 위해 HTTP 헤더에 포함되는 정보를 제한해야 함. ServerTokens 지시자에 Prod 옵션을 설정하고, ServerSignature 지시자에 Off 옵션을 설정하여 서버의 상세 정보가 외부에 노출되지 않도록 조치해야 함.
	패치관리	U-42	최신 보안패치 및 벤더 권고사항 적용	상	- 패치 정책 설정: 미설정 - 패치 적용 상태: 정기적 적용 가능한 보안 패치 수: 0 적용 가능한 보안 패치 목록: - 없음 적용된 보안 패치 수 (최근 30일): 0 최근 적용된 보안 패치 목록: - 마지막 보안 패치 설치 날짜: 정보 없음	**취약**	패치 정책 미설정 최근 30일 내 보안 패치 없음 마지막 패치 설치 날짜 정보 부재로 인해 최신 보안패치가 적용되지 않아 알려진 취약점을 통해 공격자가 시스템을 침해할 위험이 있음	패치 정책 수립 및 적용 패치 적용 프로세스 점검 및 실행 패치 내역 및 적용 기록 관리를 실시할 것
	로그관리	U-43	로그의 정기적 검토 및 보고	상	FTP 서비스는 비활성화 상태임 (관련 로그 파일 xferlog 없음) 시스템 내에는 wtmp, btmp 로그 파일은 존재하나, utmp 파일 또는 디렉터리는 존재하지 않음 wtmp: 로그인 및 로그아웃 기록 btmp: 실패한 로그인 시도 기록 utmp: 현재 로그인 사용자 기록 (부재 시 현재 로그인 정보 확인 어려움) 정상적인 사용자 외에 허용되지 않는 사용자가 su - 명령어를 이용해 root 권한으로 전환에 성공한 기록 확인	**취약**	로그 검토 및 보고 절차 미비 시 문제점 외부 침입 시도를 신속하게 식별하지 못함 → 침입 탐지 및 대응이 지연될 위험 증가 침입 의심 사례 발생 시 관련 자료 분석이 어려움 → 정확한 사고 원인 규명 및 피해 범위 파악 불가 추가 조치 및 대응 방안 마련이 늦어짐 → 시스템 피해 확산 및 보안 위협 지속 가능성 상승 조직 내 보안 책임 소재 불분명 → 보안 관리 체계 취약으로 신뢰성 저하	로그 기록 주기적 검토 및 보고 절차 수립 필요성 로그 기록을 주기적으로 검토 및 분석하여 이상 징후, 침입 시도, 시스템 오류 등을 신속하게 탐지 분석 결과를 바탕으로 리포트를 작성하여 보안 현황 및 문제점을 체계적으로 파악 리포트를 정기적으로 관련 부서 및 담당자에게 보고하여 신속한 대응과 개선 조치가 이루어지도록 함 이를 통해 효과적인 보안 관리 체계 구축 및 운영 가능

	U-72	정책에 따른 시스템 로깅 설정	하	주요 시스템 로그 파일(/var/log/messages, /var/log/secure, /var/log/maillog)에 대한 로그 수집 및 관리 정책이 수립되어 있으나, *.emerg * 대신 *.emerg :omusrmsg:*로 설정되어 있음	**취약**	로깅 설정이 미비할 경우, 보안 사고 발생 시 원인 규명이 어렵고, 법적 대응에 필요한 증거 확보가 불가능할 수 있음	조직의 보안 정책에 따라 로그 기록 정책을 수립하고, 해당 정책에 따라 /etc/rsyslog.conf 또는 /etc/syslog.conf 파일을 적절히 설정해야 함 ex) *.emerg * 이렇게 수정 해야함