

문서번호	J.W.P. MagicShop-250825
작성자	취약점진단팀
보안등급	Confidential
Ver	ver 1.0

"J.W.P. MagicShop" 취약점 진단

# WAS OS 진단 상세결과

2025년 08월 25일



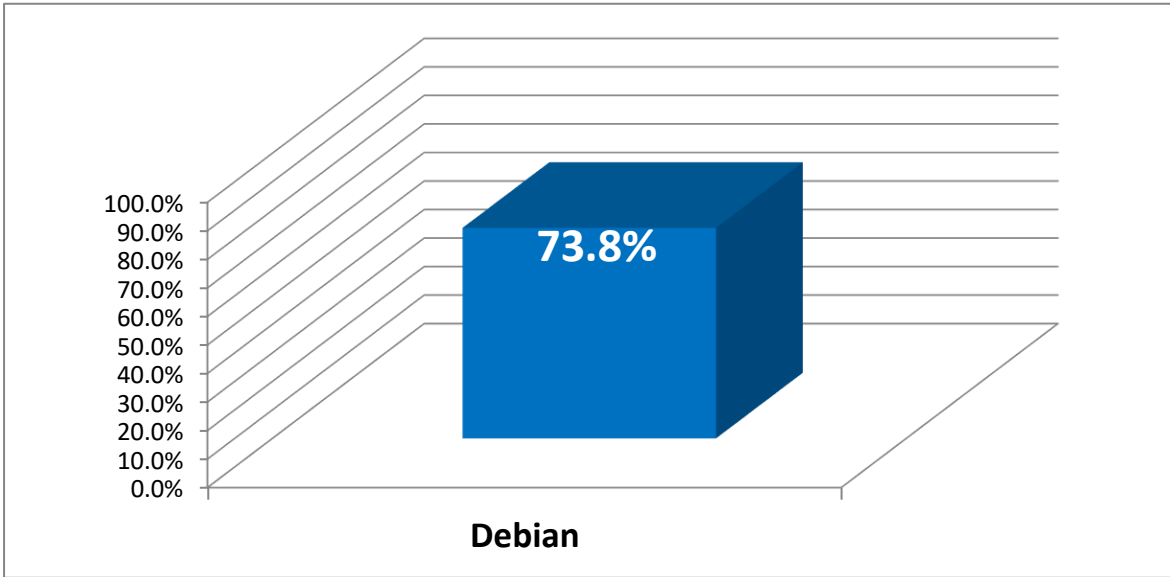
※ 진단 대상 리스트 - 서버 1대 (Debian 1대)

순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Linux					
1	jwp-was-01	10.0.4.135	Debian 12GNU/Linux12 (bookworm)	WAS OS	

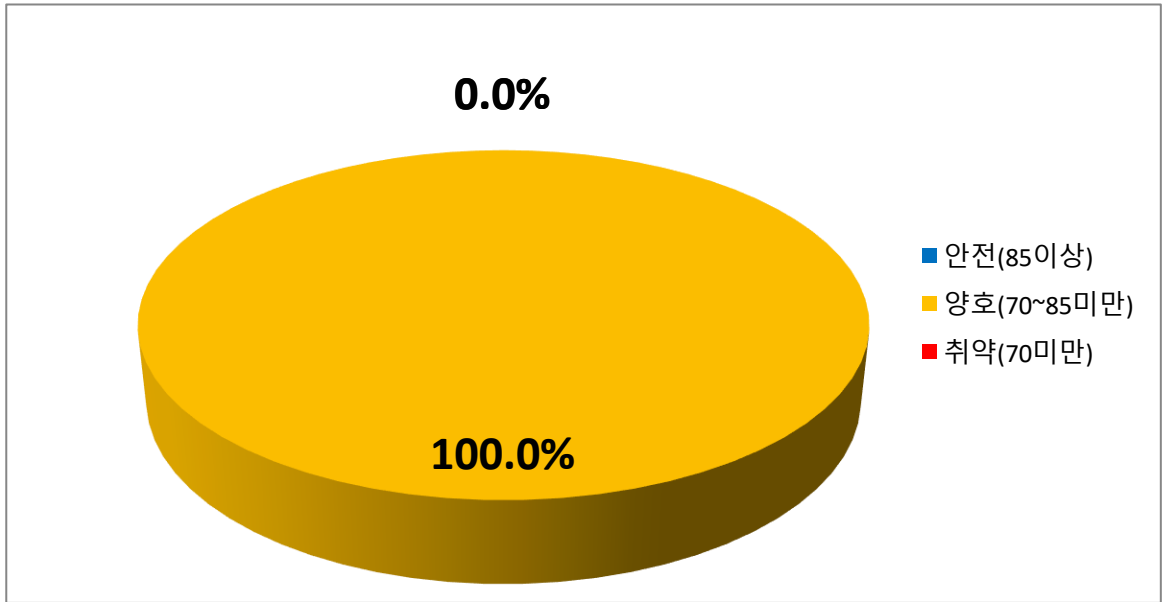
※ 대상별 평균 점수 그래프

진단 대상	평균	수량
Debian	73.8%	1

대상별 평균 점수 현황



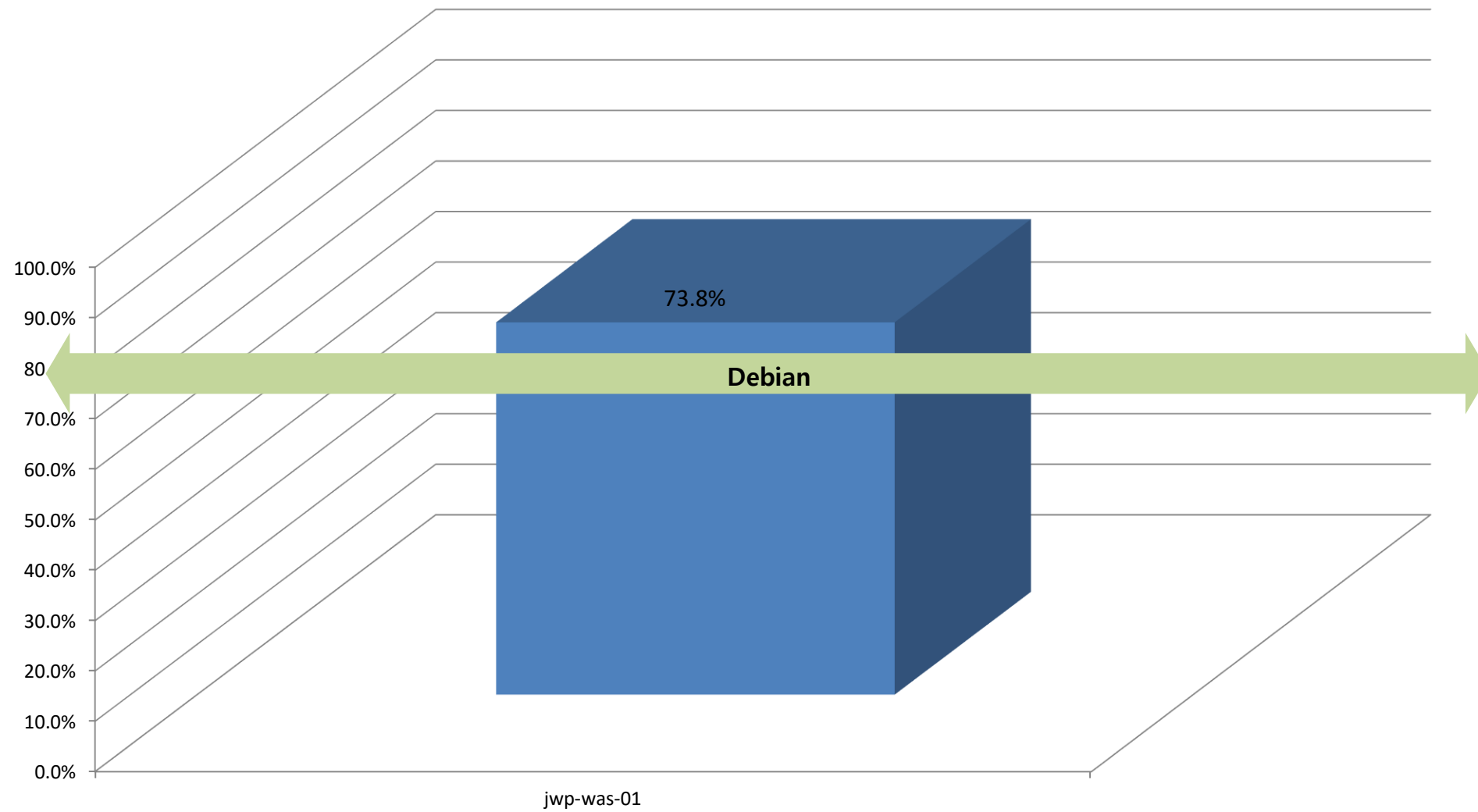
전체		수량
안전(85이상)	0.0%	0
양호(70~85미만)	100.0%	1
취약(70미만)	0.0%	0



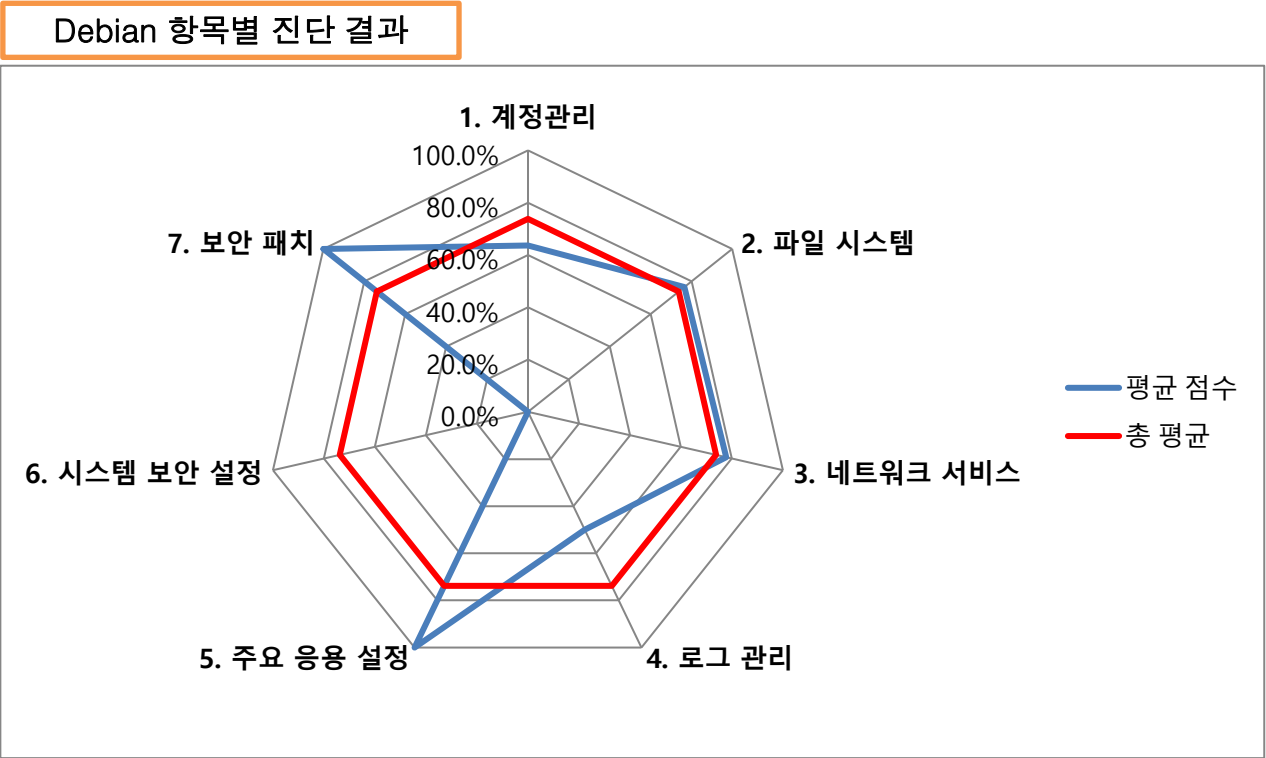
## 서버 진단결과

■ 안전(A) ■ 양호(B) ■ 보통이하(C~E)

Linux		
NO.	Hostname	점수
1	jwp-was-01	73.8%



진단 도메인	평균 점수	총 평균
1. 계정관리	63.6%	73.8%
2. 파일 시스템	76.5%	73.8%
3. 네트워크 서비스	77.8%	73.8%
4. 로그 관리	50.0%	73.8%
5. 주요 응용 설정	100.0%	73.8%
6. 시스템 보안 설정	N/A	73.8%
7. 보안 패치	100.0%	73.8%



Debian 취약점 진단 요약결과(58항목)

진단항목	No.	세부 진단항목	중 요 도	1
				jwp-was-01
				10.0.4.135
1. 계정관리	1	로그인 설정	N/A	N/A
	2	Default 계정 삭제	상	취약
	3	일반계정 root 권한 관리	상	양호
	4	/etc/passwd 파일 권한	상	양호
	5	/etc/group 파일 권한 설정	상	양호
	6	/etc/shadow 파일 권한 설정	상	취약
	7	패스워드 사용 규칙 적용	상	취약
	8	취약한 패스워드 점검	상	취약
	9	로그인이 불필요한 계정 shell 제한	중	양호
	10	SU(Select User) 사용 제한	상	양호
	11	계정이 존재하지 않는 GID 금지	중	양호
	12	동일한 UID 금지	하	양호
2. 파일 시스템	1	사용자 UMASK(User MASK) 설정	하	양호
	2	SUID(Set User-ID), SGID(Set Group-ID) 설정	하	취약
	3	/etc/(x)inetd.conf 파일 권한 설정	N/A	N/A
	4	.history 파일 권한 설정	중	양호
	5	Crontab 파일 권한 설정 및 관리	상	취약
	6	/etc/profile 파일 권한 설정	중	양호
	7	/etc/hosts 파일 권한 설정	중	양호
	8	/etc/issue 파일 권한 설정	중	양호
	9	사용자 홈 디렉터리 및 파일 관리	중	양호
	10	중요 디렉터리 파일 권한 설정	중	양호
	11	PATH 환경변수 설정	중	양호
	12	FTP(File Transfer Protocol) 접근제어 파일 권한 설정	N/A	N/A
	13	root 원격 접근제어 파일 권한 설정	중	양호
	14	NFS(Network File System) 접근제어 파일 권한 설정	N/A	N/A
	15	/etc/services 파일 권한 설정	중	양호
	16	부팅 스크립트 파일 권한 설정	상	양호
	17	/etc/hosts.allow, /etc/hosts.deny 설정	하	취약
	18	기타 중요 파일 권한 설정	N/A	N/A
	19	at 파일 소유자 및 권한 설정	N/A	N/A
	20	hosts.lpd 파일 소유자 및 권한 설정	N/A	N/A
	21	/etc/(r)syslog.conf 파일 소유자 및 권한 설정	상	취약
	22	world writable 파일 점검	상	양호
	23	/dev에 존재하지 않는 device 파일 점검	상	양호
3. 네트워크 서비 스	1	RPC(Remote Procedure Call) 서비스 제한	중	양호
	2	NFS(Network File System) 제한	N/A	N/A
	3	Automountd 서비스 제거	하	양호
	4	NIS(Network Information Service) 제한	상	양호
	5	'r' commands 서비스 제거	상	양호
	6	불필요한 서비스 제거	상	양호
	7	서비스 Banner 관리	중	취약
	8	session timeout 설정	하	취약
	9	root의 계정 telnet, ssh 접근 제한	상	양호
	10	DNS 보안 버전 패치	상	양호
4. 로그 관리	1	(x)inetd Services 로그 설정	N/A	N/A
	2	시스템 로그 설정	상	양호
	3	로그 저장 주기	상	취약
5. 주요 응용 설 정	1	FTP(File Transfer Protocol) 서비스 사용자 제한	N/A	N/A
	2	SNMP(Simple Network Management Protocol) 서비스 설정	상	양호
	3	SMTP(Simple Mail Transfer Protocol) 서비스 설정	N/A	N/A
	4	DNS(Domain Name Service) 보안 설정	N/A	N/A
	5	SWAT(Samba Web Administration Tool) 보안 설정	N/A	N/A
	6	x-server 접속 제한 설정	상	양호
6. 시스템 보안 설정	1	/etc/system 파일 보안 설정	N/A	N/A
	2	Kernel 파라미터 설정	N/A	N/A
	3	ISN(Initial Sequence Number) 파라미터 설정	N/A	N/A
7. 보안 패치	1	보안 패치 적용	상	양호
점검결과				11
	보안 적용율 (양호항목 / 진단항목) %			73.8%

영역별점수	점수	양호	취약	N/A
63.6%	N/A	0	0	1
	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	0
	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
76.5%	100.0%	1	0	0
	0.0%	0	1	0
	N/A	0	0	1
	100.0%	1	0	0
	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	N/A	0	0	1
	100.0%	1	0	0
	N/A	0	0	1
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	N/A	0	0	1
	N/A	0	0	1
77.8%	100.0%	1	0	0
	N/A	0	0	1
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
50.0%	N/A	0	0	1
	100.0%	1	0	0
	0.0%	0	1	0
100.0%	N/A	0	0	1
	100.0%	1	0	0
	N/A	0	0	1
	N/A	0	0	1
	N/A	0	0	1
	100.0%	1	0	0
N/A	N/A	0	0	1
	N/A	0	0	1
	N/A	0	0	1
100.0%	100.0%	1	0	0



Debian 취약점 진단 상세결과(58항목)

진단항목	No.	세부 진단항목	진단기준	1	jwp-was-01
					10.0.4.135
					WAS OS
1. 계정관리	1	로그인 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	secu-was@jwp-was-01:~\$ cat /etc/passwd   grep "^lp"   grep -v "false nologin" lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
	2	Default 계정 삭제	양호 - lp, uucp, nuucp 및 의심스러운 특이 계정이 존재하지 않을 경우 취약 - lp, uucp, nuucp 및 의심스러운 특이 계정이 존재하는 경우	취약	secu-was@jwp-was-01:~\$ cat /etc/passwd   grep "uucp"   grep -v "false nologin" uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin secu-was@jwp-was-01:~\$ cat /etc/passwd   grep "^nuucp"   grep -v "false nologin" secu-was@jwp-was-01:~\$ 시스템에 불필요한 기본 계정(lp, uucp)이 존재함
	3	일반계정 root 권한 관리	양호 - UID 가 "0"인 계정이 하나만 존재할 경우 취약 - UID 가 "0"인 계정이 둘 이상 존재할 경우	양호	secu-was@iwp-was-01:~\$ cat /etc/passwd   awk -F":" '{ if (\$3 == 0) print \$0 }' root:x:0:0:root:/root:/bin/bash secu-was@jwp-was-01:~\$
	4	/etc/passwd 파일 권한	양호 - /etc/passwd 파일의 소유주가 root, 권한이 644 일 경우 취약 - /etc/passwd 파일의 소유주가 root가 아니며, 권한이 644 가 아닌 경우	양호	secu-was@jwp-was-01:~\$ ls -al /etc/passwd -rw-r--r-- 1 root root 2239 8월 27일 10:04 /etc/passwd secu-was@jwp-was-01:~\$
	5	/etc/group 파일 권한 설정	양호 - /etc/group 파일의 소유자가 root, 권한이 644 이하일 경우 취약 - /etc/group 파일의 소유자가 root가 아니며, 권한이 644 이하가 아닌 경우	양호	secu-was@jwp-was-01:~\$ ls -al /etc/group -rw-r--r-- 1 root root 1141 8월 29일 16:26 /etc/group secu-was@jwp-was-01:~\$
	6	/etc/shadow 파일 권한 설정	양호 - /etc/shadow 파일 권한이 400 이하일 경우 취약 - /etc/shadow 파일 권한이 400 초과일 경우	취약	secu-was@jwp-was-01:~\$ ls -al /etc/shadow -rw-r----- 1 root shadow 1990 8월 27일 10:04 /etc/shadow secu-was@jwp-was-01:~\$ /etc/shadow 파일 권한이 640으로 설정되어 있어 기준을 초과함
	7	패스워드 사용 규칙 적용	양호 - 패스워드 최소 길이가 2종류 조합으로 8자리 이상, 조합없이 최소 10자리 이상 패스워드 최대 사용기간이 60일 이하 패스워드 최소 사용기간이 7일 이상 계정잠금 임계값 5이하로 위의 기준을 모두 만족할 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	취약	secu-was@jwp-was-01:~\$ cat /etc/login.defs   grep PASS_MIN_LEN #PASS_MIN_LEN secu-was@jwp-was-01:~\$ cat /etc/login.defs   grep PASS_MIN_DAYS # PASS_MIN_DAYS Minimum number of days allowed between password changes. PASS_MIN_DAYS 0 secu-was@jwp-was-01:~\$ cat /etc/login.defs   grep PASS_MAX_DAYS # PASS_MAX_DAYS Maximum number of days a password may be used. PASS_MAX_DAYS 99999 secu-was@jwp-was-01:~\$ 패스워드 최대 사용기간이 99999일, 최소 사용기간이 0일로 설정되어 있어 암호 정책 기준을 충족하지 못함
	8	취약한 패스워드 점검	양호 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호가 설정된 경우 취약 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호 설정되지 않은 경우	취약	담당자와 인터뷰 결과 계정과 유사한 패스워드로 확인
	9	로그인이 불필요한 계정 shell 제한	양호 - 로그인에 필요하지 않은 아래 계정의 /bin/false(nologin) 쉘이 부여되어 있을 경우 취약 - 로그인에 필요하지 않은 아래 계정의 /bin/false(nologin) 쉘이 부여되어 있지 않을 경우	양호	secu-was@jwp-was-01:~\$ cat /etc/passwd   grep "false\ nologin" daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin uidd:x:100:105::/run/uidd:/usr/sbin/nologin messagebus:x:101:106::/nonexistent:/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin tcpdump:x:102:107::/nonexistent:/usr/sbin/nologin sshd:x:103:65534::/run/sshd:/usr/sbin/nologin polkitd:x:995:995:polkit:/nonexistent:/usr/sbin/nologin rtkit:x:104:109:RealtimeKit,,:/proc:/usr/sbin/nologin
	10	SU(Select User) 사용 제한	양호 - su 명령어를 특정 그룹에 속한 사용자만 사용하도록 제한이 되어 있을 경우 취약 - su 명령어를 모든 사용자가 사용하도록 되어 있을 경우	양호	secu-was@jwp-was-01:~\$ sudo grep -E "%.*ALL.*ALL" /etc/sudoers %sudo ALL=(ALL:ALL) ALL secu-was@iwp-was-01:~\$ getent group sudo sudo:x:27:admin,khn,pjw,msy,ysm,jym,lsy,jsh,kyr,kth,pmj,secu-was secu-was@jwp-was-01:~\$
	11	계정이 존재하지 않는 GID 금지	양호 - 시스템 관리나 운용에 불필요한 그룹이 존재하지 않을 경우 취약 - 시스템 관리나 운용에 불필요한 그룹이 존재하는 경우	양호	secu-was@jwp-was-01:~\$ cat /etc/group root:x:0: daemon:x:1: bin:x:2: sys:x:3: adm:x:4:admin tty:x:5: disk:x:6: lp:x:7: mail:x:8: news:x:9: uucp:x:10: man:x:12: proxy:x:13: kmem:x:15: dialout:x:20:admin fax:x:21: voice:x:22: cdrom:x:24:admin floppy:x:25:admin tape:x:26: sudo:x:27:admin,khn,pjw,msy,ysm,jym,lsy,jsh,kyr,kth,pmj,secu-was audio:x:29:admin,pulse dip:x:30:admin www-data:x:33: backup:x:34: operator:x:37: list:x:38:
	12	동일한 UID 금지	양호 - 동일한 UID로 설정된 사용자 계정이 존재하지 않을 경우 취약 - 동일한 UID로 설정된 사용자 계정이 존재하는 경우	양호	secu-was@jwp-was-01:~\$ cut -d: -f3 /etc/passwd   sort   uniq -d secu-was@jwp-was-01:~\$
	1	사용자 UMASK(User MASK) 설정	양호 - umask가 022(027)일 경우 취약 - umask가 022(027)보다 작을 경우	양호	secu-was@jwp-was-01:~\$ grep -r -i "umask" /etc/profile* /etc/bash* /etc/login.defs 2>/dev/null   grep -v "#"   awk '\$2 >= 22' /etc/login.defs:UMASK 022 secu-was@jwp-was-01:~\$



2. 파일 시스템	2	SUID(Set User-ID), SGID(Set Group-ID) 설정	양호 - 불필요한 SUID, SGID가 설정되어 있지 않을 경우 취약 - 불필요한 SUID, SGID가 설정되어 있을 경우	취약	<pre>secu-was@jwp-was-01:~\$ sudo find / -user root -type f \( -perm -4000 -o -perm -2000 \) -exec ls -al {} \;</pre> <pre>-rwxr-sr-x 1 root shadow 39160 2023년  9월 22일 /usr/sbin/unix_chkpwd</pre> <pre>-rwsr-xr-- 1 root messagebus 51272 2023년  9월 16일 /usr/lib/dbus-1.0/dbus-daemon-launch-helper</pre> <pre>-rwxr-sr-x 1 root utmp 14416 2023년  2월 27일 /usr/lib/x86_64-linux-gnu/utempter/utempter</pre> <pre>-rwsr-xr-x 1 root root 18664 2023년  2월  1일 /usr/lib/polkit-1/polkit-agent-helper-1</pre> <pre>-1</pre> <pre>-rwsr-xr-x 1 root root 653888  5월  8일 19:54 /usr/lib/openssh/ssh-keysign</pre> <pre>-rwsr-sr-x 1 root root 14672  6월 20일 21:46 /usr/lib/xorg/Xorg.wrap</pre> <pre>-rwxr-sr-x 1 root _ssh 485760  5월  8일 19:54 /usr/bin/ssh-agent</pre> <pre>-rwsr-xr-x 1 root root 72000 2024년 11월 22일 /usr/bin/su</pre> <pre>-rwsr-xr-x 1 root root 35128 2023년  4월 19일 /usr/bin/fusermount3</pre> <pre>-rwsr-xr-x 1 root root 281624  6월 24일 16:29 /usr/bin/sudo</pre> <pre>-rwsr-xr-x 1 root root 59704 2024년 11월 22일 /usr/bin/mount</pre> <pre>-rwsr-xr-x 1 root root 88496  4월  7일 19:38 /usr/bin/gpasswd</pre> <pre>-rwsr-xr-x 1 root root 48896  4월  7일 19:38 /usr/bin/newgrp</pre> <pre>-rwsr-xr-x 1 root root 162752 2024년 10월 27일 /usr/bin/ntfs-3g</pre> <pre>-rwsr-xr-x 1 root root 68248  4월  7일 19:38 /usr/bin/passwd</pre> <pre>-rwsr-xr-x 1 root root 35128 2024년 11월 22일 /usr/bin/umount</pre> <pre>-rwxr-sr-x 1 root shadow 31184  4월  7일 19:38 /usr/bin/expiry</pre> <pre>-rwsr-xr-x 1 root root 26776 2023년  2월  1일 /usr/bin/pkexec</pre> <pre>-rwxr-sr-x 1 root shadow 80376  4월  7일 19:38 /usr/bin/chage</pre> /usr/bin/newgrp 파일에 불필요한 SUID 파일이 존재함
	3	/etc/(x)inetd.conf 파일 권한 설정	양호 - 해당 파일 및 디렉터리 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 및 디렉터리 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ find / -type f -name "*inetd.conf" 2&gt;/dev/null</pre> <pre>secu-was@jwp-was-01:~\$ █</pre>
	4	.history 파일 권한 설정	양호 - 사용자의 히스토리 파일의 권한이 600으로 소유자는 자신으로 설정되어 있을 경우 취약 - 해당 파일의 권한이 600으로 소유자는 자신으로 설정되어 있지 않을 경우	양호	<pre>secu-was@jwp-was-01:~\$ for dir in \$(awk -F: '(\$? ~ /(\/bin\/bash\/bin\/sh\/bin\/zsh)\$/) {print \$6}' /etc/passwd); do sudo ls -l \$dir/{.bash_history,.sh_history,.history} \&gt; 2&gt;/dev/null; done</pre> <pre>-rw----- 1 root root 15343  8월 29일 09:56 /root/.bash_history</pre> <pre>-rw----- 1 admin admin 18769  8월 30일 16:34 /home/admin/.bash_history</pre> <pre>-rw----- 1 pjw pjw 15  8월  6일 08:53 /home/pjw/.bash_history</pre> <pre>-rw----- 1 ysm ysm 41  8월  6일 19:13 /home/ysm/.bash_history</pre> <pre>-rw----- 1 secu-was secu-was 38270  8월 29일 15:58 /home/secu-was/.bash_history</pre> <pre>-rw----- 1 infra-was infra-was 44  8월 27일 20:52 /home/infra-was/.bash_history</pre> secu-was@jwp-was-01:~\$ █
	5	Crontab 파일 권한 설정 및 관리	양호 - Crontab 관련 파일의 소유자가 root이며, 타사용자의 권한이 제거되어 있을 경우 취약 - 기준으로 설정되어 있지 않을 경우	취약	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/cron*</pre> <pre>/etc/cron.d:</pre> <pre>합 계 12</pre> <pre>drwxr-xr-x 2 root root 4096  3월 16일 13:23 .</pre> <pre>drwxr-xr-x 94 root root 4096  8월 27일 10:05 ..</pre> <pre>-rw-r--r-- 1 root root 201 2023년  3월  5일 e2scrub_all</pre> /etc/cron.daily: 합 계 20 <pre>drwxr-xr-x 2 root root 4096  3월 16일 13:26 .</pre> <pre>drwxr-xr-x 94 root root 4096  8월 27일 10:05 ..</pre> <pre>-rwxr-xr-x 1 root root 1478 2023년  5월 25일 apt-compat</pre> <pre>-rwxr-xr-x 1 root root 123 2023년  3월 27일 dpkg</pre> <pre>-rwxr-xr-x 1 root root 1395 2023년  3월 13일 man-db</pre> /etc/cron.weekly: 합 계 12 <pre>drwxr-xr-x 2 root root 4096  3월 16일 13:26 .</pre> <pre>drwxr-xr-x 94 root root 4096  8월 27일 10:05 ..</pre> <pre>-rwxr-xr-x 1 root root 1055 2023년  3월 13일 man-db</pre> secu-was@jwp-was-01:~\$ █
	6	/etc/profile 파일 권한 설정	양호 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -ald /etc/profile</pre> <pre>-rw-r--r-- 1 root root 769 2021년  4월 11일 /etc/profile</pre> secu-was@jwp-was-01:~\$ █
	7	/etc/hosts 파일 권한 설정	양호 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -ald /etc/hosts</pre> <pre>-rw-r--r-- 1 root root 109  3월 16일 13:25 /etc/hosts</pre> secu-was@jwp-was-01:~\$ █
	8	/etc/issue 파일 권한 설정	양호 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일의 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/issue</pre> <pre>-rw-r--r-- 1 root root 27  3월  8일 02:30 /etc/issue</pre> <pre>secu-was@jwp-was-01:~\$ ls -al /etc/issue.net</pre> <pre>-rw-r--r-- 1 root root 20  3월  8일 02:30 /etc/issue.net</pre> secu-was@jwp-was-01:~\$ █
	9	사용자 홈 디렉터리 및 파일 관리	양호 - 홈 디렉터리 권한 중 Other에 아무런 권한도 부여되어 있지 않을 경우 홈 디렉터리 환경변수 파일 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 홈 디렉터리가 존재하지 않는 계정이 발견되지 않는 경우 취약 - 위의 기준으로 설정되어 있지 않을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -ald /home/*</pre> <pre>drwx----- 24 admin admin 4096  9월  1일 13:18 /home/admin</pre> <pre>drwx----- 2 infra-was infra-was 4096  8월 27일 20:52 /home/infra-was</pre> <pre>drwx----- 2 jsh jsh 4096  8월  6일 08:47 /home/jsh</pre> <pre>drwx----- 2 jym jym 4096  8월  6일 08:47 /home/jym</pre> <pre>drwx----- 16 khn khn 4096  8월 11일 15:58 /home/khn</pre> <pre>drwx----- 2 kth kth 4096  8월  6일 08:48 /home/kth</pre> <pre>drwx----- 2 kyr kyr 4096  8월  6일 08:47 /home/kyr</pre> <pre>drwx----- 2 lsy lsy 4096  8월  6일 08:47 /home/lsy</pre> <pre>drwx----- 15 msy msy 4096  8월  6일 12:46 /home/msy</pre> <pre>drwx----- 16 pjw pjw 4096  8월  6일 09:37 /home/pjw</pre> <pre>drwx----- 2 pmj pmj 4096  8월  6일 08:48 /home/pmj</pre> <pre>drwx----- 17 secu-was secu-was 4096  8월 29일 16:08 /home/secu-was</pre> <pre>drwx----- 16 ysm ysm 4096  8월 21일 09:07 /home/ysm</pre> secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/ <pre>합 계 620</pre> <pre>drwx----- 24 admin admin 4096  9월  1일 13:18 .</pre> <pre>drwxr-xr-x 15 root root 4096  8월 27일 13:49 ..</pre> <pre>-rw----- 1 admin admin 0  8월  5일 16:48 .ICEauthority</pre> <pre>-rw----- 1 admin admin 628  9월  1일 13:18 .Xauthority</pre> <pre>-rw----- 1 admin admin 21003  9월  1일 13:17 .bash_history</pre> <pre>-rw-r--r-- 1 admin admin 220 2024년  3월 30일 .bash_logout</pre> <pre>-rw-r--r-- 1 admin admin 3526 2024년  3월 30일 .bashrc</pre> <pre>drwx----- 9 admin admin 4096  8월 30일 22:48 .cache</pre> <pre>drwx----- 10 admin admin 4096  8월 29일 16:26 .config</pre> <pre>drwx----- 3 admin admin 4096  8월  5일 16:48 .dbus</pre> <pre>drwxr-xr-x 7 admin admin 4096  8월  6일 10:16 .eclipse</pre> <pre>drwx----- 3 admin admin 4096  8월  5일 16:48 .gnupg</pre>
	10	중요 디렉터리 파일 권한 설정	양호 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -ald /sbin /etc/ /bin /usr/bin/ /usr/sbin/ /usr/lib</pre> <pre>ls: '/usr/lib'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> <pre>lrwxrwxrwx 1 root root 7  3월 16일 13:22 /bin -&gt; usr/bin</pre> <pre>drwxr-xr-x 94 root root 4096  8월 27일 10:05 /etc/</pre> <pre>lrwxrwxrwx 1 root root 8  3월 16일 13:22 /sbin -&gt; usr/sbin</pre> <pre>drwxr-xr-x 2 root root 36864  8월 24일 06:35 /usr/bin/</pre> <pre>drwxr-xr-x 2 root root 16384  8월  6일 17:41 /usr/sbin/</pre> secu-was@jwp-was-01:~\$ █
	11	PATH 환경변수 설정	양호 - PATH 환경변수에 "." 이 맨 앞이나 중간에 포함되어 있지 않을 경우 (디렉터리명 제외) 취약 - PATH 환경변수에 "." 이 맨 앞이나 중간에 포함되어 있을 경우 (디렉터리명 제외)	양호	<pre>secu-was@jwp-was-01:~\$ env   grep PATH</pre> <pre>PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games</pre> <pre>secu-was@jwp-was-01:~\$ sudo cat /home/admin/.profile   grep PATH</pre> <pre># set PATH so it includes user's private bin if it exists</pre> <pre>PATH="\$HOME/bin:\$PATH"</pre> <pre># set PATH so it includes user's private bin if it exists</pre> <pre>PATH="\$HOME/.local/bin:\$PATH"</pre> <pre>secu-was@jwp-was-01:~\$ sudo cat /home/jsh/.profile   grep PATH</pre> <pre># set PATH so it includes user's private bin if it exists</pre> <pre>PATH="\$HOME/bin:\$PATH"</pre> <pre># set PATH so it includes user's private bin if it exists</pre> <pre>PATH="\$HOME/.local/bin:\$PATH"</pre> <pre>secu-was@jwp-was-01:~\$ cat /etc/profile   grep PATH</pre> <pre>PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"</pre> <pre>PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"</pre> <pre>export PATH</pre> secu-was@jwp-was-01:~\$ █
	12	FTP(File Transfer Protocol) 접근제어 파일 권한 설정	양호 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/ftusers /etc/ftpd/ftusers /etc/vsftpd/ftusers</pre> <pre>ls: '/etc/ftusers'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> <pre>ls: '/etc/ftpd/ftusers'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> <pre>ls: '/etc/vsftpd/ftusers'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> secu-was@jwp-was-01:~\$ █
	13	root 원격 접근제어 파일 권한 설정	양호 - /etc/pam.d/login, /etc/securetty 파일 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/pam.d/login</pre> <pre>-rw-r--r-- 1 root root 4126 2023년  3월 23일 /etc/pam.d/login</pre> secu-was@jwp-was-01:~\$ ls -al /etc/security/user <pre>ls: '/etc/security/user'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> secu-was@jwp-was-01:~\$ █
	14	NFS(Network File System) 접근제어 파일 권한 설정	양호 - 해당 파일 권한 중 Group, Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Group, Other에 쓰기 권한이 부여되어 있을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/exports</pre> <pre>ls: '/etc/exports'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다</pre> secu-was@jwp-was-01:~\$ dpkg -l   grep nfs-kernel-server secu-was@jwp-was-01:~\$ █



3. 네트워크 서버	15	/etc/services 파일 권한 설정	양호 - 해당 파일 권한 중 Group, Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Group, Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/services -rw-r--r-- 1 root root 12813 2021년 3월 28일 /etc/services secu-was@jwp-was-01:~\$</pre>
	16	부팅 스크립트 파일 권한 설정	양호 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있지 않을 경우 취약 - 해당 파일 권한 중 Other에 쓰기 권한이 부여되어 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/rc*.d/* lrwxrwxrwx 1 root root 22 3월 16일 13:26 /etc/rc0.d/K01cloud-config -&gt; ../init.d/cloud-config lrwxrwxrwx 1 root root 21 3월 16일 13:26 /etc/rc0.d/K01cloud-final -&gt; ../init.d/cloud-final lrwxrwxrwx 1 root root 20 3월 16일 13:26 /etc/rc0.d/K01cloud-init -&gt; ../init.d/cloud-init lrwxrwxrwx 1 root root 26 3월 16일 13:26 /etc/rc0.d/K01cloud-init-local -&gt; ../init.d/cloud-init-local lrwxrwxrwx 1 root root 20 3월 16일 13:23 /etc/rc0.d/K01hwclock.sh -&gt; ../init.d/hwclock.sh lrwxrwxrwx 1 root root 17 8월 5일 16:46 /etc/rc0.d/K01lightdm -&gt; ../init.d/lightdm lrwxrwxrwx 1 root root 18 8월 5일 16:45 /etc/rc0.d/K01plymouth -&gt; ../init.d/plymouth lrwxrwxrwx 1 root root 37 8월 5일 16:46 /etc/rc0.d/K01pulseaudio-enable-autospawn -&gt; ../init.d/pulseaudio-enable-autospawn lrwxrwxrwx 1 root root 15 8월 5일 16:46 /etc/rc0.d/K01saned -&gt; ../init.d/saned lrwxrwxrwx 1 root root 14 3월 16일 13:25 /etc/rc0.d/K01udev -&gt; ../init.d/udev lrwxrwxrwx 1 root root 29 3월 16일 13:26 /etc/rc0.d/K01unattended-upgrades -&gt; ../init.d/unattended-upgrades lrwxrwxrwx 1 root root 15 3월 16일 13:25 /etc/rc0.d/K01uuid -&gt; ../init.d/uuid lrwxrwxrwx 1 root root 14 8월 5일 16:46 /etc/rc0.d/K01xrdp -&gt; ../init.d/xrdp lrwxrwxrwx 1 root root 22 3월 16일 13:26 /etc/rc1.d/K01cloud-config -&gt; ../init.d/cloud-config lrwxrwxrwx 1 root root 21 3월 16일 13:26 /etc/rc1.d/K01cloud-final -&gt; ../init.d/cloud-final secu-was@jwp-was-01:~\$ ls -al /etc/init.d 합계 112 drwxr-xr-x 2 root root 4096 8월 6일 17:41 . drwxr-xr-x 94 root root 4096 8월 27일 10:05 .. -rwxr-xr-x 1 root root 3740 2023년 2월 14일 apparmor -rwxr-xr-x 1 root root 1367 2024년 9월 18일 cloud-config -rwxr-xr-x 1 root root 1510 2024년 9월 18일 cloud-final -rwxr-xr-x 1 root root 1348 2022년 11월 24일 cloud-init -rwxr-xr-x 1 root root 1284 2024년 9월 18일 cloud-init-local -rwxr-xr-x 1 root root 3152 2023년 9월 16일 dbus -rwxr-xr-x 1 root root 1748 2024년 11월 22일 hwclock.sh -rwxr-xr-x 1 root root 2063 2022년 12월 10일 kmod -rwxr-xr-x 1 root root 2610 2022년 1월 11일 lightdm -rwxr-xr-x 1 root root 883 2016년 5월 17일 lm-sensors -rwxr-xr-x 1 root root 1386 2023년 2월 2일 plymouth -rwxr-xr-x 1 root root 760 2023년 2월 2일 plymouth-log</pre>
	17	/etc/hosts.allow, /etc/hosts.deny 설정	양호 - hosts.deny에 ALL:ALL 설정이 되어 있고, host.allow에 접근 허용 호스트 설정이 되어 있을 경우 취약 - 위의 기준으로 설정되어 있지 않을 경우	취약	<pre>secu-was@jwp-was-01:~\$ cat /etc/hosts.allow # /etc/hosts.allow: list of hosts that are allowed to access the system. # See the manual pages hosts_access(5) and hosts_options(5). # # Example:      ALL: LOCAL @some_netgroup #              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu # # If you're going to protect the portmapper use the name "rpcbind" for the # daemon name. See rpcbind(8) and rpc.mountd(8) for further information. # secu-was@jwp-was-01:~\$ cat /etc/hosts.deny # /etc/hosts.deny: list of hosts that are _not_ allowed to access the system. # See the manual pages hosts_access(5) and hosts_options(5). # # Example:      ALL: some.host.name, .some.domain #              ALL EXCEPT in.fingerd: other.host.name, .other.domain # # If you're going to protect the portmapper use the name "rpcbind" for the # daemon name. See rpcbind(8) and rpc.mountd(8) for further information. # # The PARANOID wildcard matches any host whose name does not match its # address. # # You may wish to enable this to ensure any programs that don't # validate looked up hostnames still leave understandable logs. In past # versions of Debian this has been the default. # ALL: PARANOID</pre> <p>/etc/hosts.allow, /etc/hosts.deny 파일의 접근 제어 설정이 적용되어 있지 않음</p>
	18	기타 중요 파일 권한 설정	※ 해당 OS는 체크리스트에 포함하지 않음.	N/A	
	19	at 파일 소유자 및 권한 설정	양호 - 해당 파일의 소유자가 root이고 권한이 640 이하인 경우 취약 - 해당 파일의 소유자가 root가 아니거나 권한이 640 이상인 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/at.allow ls: '/etc/at.allow'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ ls -al /etc/at.deny ls: '/etc/at.deny'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ which at secu-was@jwp-was-01:~\$ find / -type f -name "at.*" 2&gt;/dev/null /usr/include/netatalk/at.h /usr/share/xfce4/xfce4-flags/at.svg secu-was@jwp-was-01:~\$</pre>
	20	hosts.lpd 파일 소유자 및 권한 설정	양호 - 해당 파일의 소유자가 root이고 권한이 600 이하인 경우 취약 - 해당 파일의 소유자가 root가 아니거나 권한이 600 이상인 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/hosts.lpd ls: '/etc/hosts.lpd'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$</pre>
	21	/etc/(r)syslog.conf 파일 소유자 및 권한 설정	양호 - 해당 파일의 소유자가 root이고 권한이 640 이하인 경우 취약 - 해당 파일의 소유자가 root가 아니거나 권한이 640보다 이상인 경우	취약	<pre>secu-was@iwp-was-01:~\$ ls -al /etc/rsyslog.conf -rw-r--r-- 1 root root 1430 2025년 1월 9일 /etc/rsyslog.conf secu-was@jwp-was-01:~\$</pre> <p>/etc/rsyslog.conf 파일 권한이 644로 설정되어 있어 일반 사용자에게 불필요한 읽기 권한이 부여됨</p>
	22	world writable 파일 점검	양호 - world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우 취약 - world writable 파일이 존재하지만 해당 설정 이유를 확인하고 있지 않은 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo find /root -type f -perm -2 -exec ls -l {} \; [sudo] secu-was 암호: secu-was@jwp-was-01:~\$ sudo find /home/admin -type f -perm -2 -exec ls -l {} \; secu-was@jwp-was-01:~\$</pre>
	23	/dev에 존재하지 않는 device 파일 점검	양호 - dev에 대한 파일 점검 후 존재하지 않은 device 파일을 제거한 경우 취약 - dev에 대한 파일 미점검 또는, 존재하지 않은 device 파일을 방치한 경우	양호	<pre>secu-was@jwp-was-01:~\$ find /dev -type f -exec ls -l {} \; secu-was@jwp-was-01:~\$</pre>
	1	RPC(Remote Procedure Call) 서비스 제한	양호 - RPC 서비스가 구동 중에 있지 않을 경우 취약 - RPC 서비스가 구동 중에 있을 경우	양호	<pre>secu-was@jwp-was-01:~\$ systemctl list-units --type=service   grep -E 'rpc nfs portmap' secu-was@jwp-was-01:~\$</pre>
	2	NFS(Network File System) 제한	양호 - NFS 서비스 사용자 설정 파일에 Everyone으로 mount 되어 있지 않은 경우 NFS 서비스 사용자 인가된 시스템을 mount 하고 있는 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ps -ef   egrep "nfs statd lockd"   grep -v "grep" root      32      0 13:48 ?        00:00:00 [kblockd] root      36      0 13:48 ?        00:00:00 [kworker/0:1H-kblockd] secu-was@jwp-was-01:~\$ ps -ef   egrep "nfs statd lockd"   grep "everyone" secu-was@jwp-was-01:~\$</pre>
	3	Automountd 서비스 제거	양호 - Automountd 서비스가 구동 중이지 않을 경우 취약 - Automountd 서비스가 구동 중일 경우	양호	<pre>secu-was@iwp-was-01:~\$ ps -ef   grep "automount\ autofs" secu-was      1139      922  0 14:16 pts/3    00:00:00 grep automount\ autofs secu-was@jwp-was-01:~\$</pre>
	4	NIS(Network Information Service) 제한	양호 - NIS, NIS+ 서비스가 구동 중이지 않을 경우 취약 - NIS, NIS+ 서비스가 구동 중일 경우	양호	<pre>secu-was@jwp-was-01:~\$ ps -ef   egrep "Ypserv Ypbind rpoxfrd rpc.yppupdated" secu-was      1146      922  0 14:18 pts/3    00:00:00 grep -E Ypserv Ypbind rpoxfrd rpc.yppupdated secu-was@jwp-was-01:~\$</pre>
	5	'r' commands 서비스 제거	양호 - login, shell, exec 등 'r' commands 서비스가 구동 중이지 않거나 사용 시 /etc/hosts.equiv, /\$HOME/.rhosts 파일 권한 400 및 접근 가능 고정 IP 설정된 경우 취약 - 'r' commands 서비스 사용 시 위의 기준으로 설정되어 있지 않을 경우	양호	<pre>secu-was@jwp-was-01:~\$ cat /etc/inetd.conf 2&gt;/dev/null   grep -v '^#'   egrep "shell rlogin rexec"   grep -v "grep klogin kshell kexec" secu-was@jwp-was-01:~\$ ls -al \$HOME/.rhosts ls: '/home/secu-was/.rhosts'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ ls -al /etc/hosts.equiv ls: '/etc/hosts.equiv'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ sudo find / -name ".rhosts" -exec ls -al {} \; [sudo] secu-was 암호: secu-was@jwp-was-01:~\$</pre>
	6	불필요한 서비스 제거	양호 - White List에 포함되지 않거나 시스템 운영부서와 협의되지 않은 불필요한 서비스가 구동 중이지 않을 경우 취약 - 시스템 운영 부서와 협의되지 않은 불필요한 서비스가 구동 중일 경우, 서버 진단 시 서비스 담당자 측 추가 확인을 거쳐 불필요한 서비스로 식별되는 경우	양호	<pre>secu-was@jwp-was-01:~\$ systemctl list-units --type=service --state=running   \ &gt; grep "echo chargen finger nntp netbios_dgm ldap ntalk ldaps nfsd discard \ &gt; time sftp netbios_ssn printer uucp ingreslock dtspcd daytime tftp \ &gt; uucp-path bftpl talk pcserver www-ldap-gw" secu-was@jwp-was-01:~\$</pre>



스	7	서비스 Banner 관리	양호 - SSH, Telnet, FTP, SMTP, DNS가 구동 중이지 않거나 배너에 O/S 및 버전 정보가 없을 경우 취약 - SSH, Telnet, FTP, SMTP, DNS가 구동 중이며 서비스 배너에 O/S 및 버전 정보가 있을 경우	취약	<pre>secu-was@jwp-was-01:~\$ cat /etc/motd  The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.  Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. secu-was@jwp-was-01:~\$ cat /etc/issue.net Debian GNU/Linux 12 secu-was@jwp-was-01:~\$ cat /etc/welcome.msg cat: /etc/welcome.msg: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ cat /etc/vsftpd/vsftpd.conf /etc/mail/sendmail.cf /etc/named.conf cat: /etc/vsftpd/vsftpd.conf: 그런 파일이나 디렉터리가 없습니다 cat: /etc/mail/sendmail.cf: 그런 파일이나 디렉터리가 없습니다 cat: /etc/named.conf: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ █ Telnet 서비스 배너(/etc/issue.net)에 운영체제 및 버전 정보가 포함되어 있음</pre>
	8	session timeout 설정	양호 - session timeout이 "300초"로 설정되어 있을 경우 취약 - session timeout이 "300초"로 설정되어 있지 않을 경 우	취약	<pre>secu-was@jwp-was-01:~\$ cat /etc/profile   grep "TMOUT" secu-was@jwp-was-01:~\$ cat /etc/.login   grep "autologout" cat: /etc/.login: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ █</pre> <p>세션 타임아웃이 설정되어 있지 않아, /etc/profile 파일에서 session timeout이 적용되지 않음</p>
	9	root의 계정 telnet, ssh 접근 제한	양호 - 원격 접속(telnet, ssh) 시 root의 직접 접속이 불가능 하도록 설정되어 있을 경우 취약 - 원격 접속(telnet, ssh) 시 root로 직접 접속이 가능할 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /etc/security/user ls: '/etc/security/user'에 접근할 수 없음: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ egrep "RootLogin" /etc/ssh/sshd_config #PermitRootLogin prohibit-password # the setting of "PermitRootLogin prohibit-password". secu-was@jwp-was-01:~\$ grep -i disable_root /etc/cloud/cloud.cfg disable_root: true secu-was@jwp-was-01:~\$ █</pre>
	10	DNS 보안 버전 패치	양호 - DNS 서비스를 사용하지 않거나, 사용 시 주기적으로 패치를 관리하고 있는 경우 취약 - DNS 서비스를 사용하며, 주기적으로 패치를 관리하 고 있지 않는 경우	양호	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep named secu-was 2737 2244 0 15:08 pts/4 00:00:00 grep named secu-was@jwp-was-01:~\$ named -v bash: named: 명령어를 찾을 수 없음 secu-was@jwp-was-01:~\$ █</pre>
4. 로그관리	1	(x)inetd Services 로그 설정	※ 해당 OS는 체크리스트에 포함하지 않음.	N/A	
	2	시스템 로그 설정	양호 - su 로그인 기록을 별도 파일에 저장되도록 설정되어 있 을 경우 syslog에 중요 로그정보(*.notice, *.alert, *.emerg)에 대한 설 정이 존재할 경우 로그 파일 및 디렉터리 root 소유, 타사용자에 권한이 부여 되어 있지 않을 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ls -al /var/log/syslog /var/log/auth.log /var/log/kern.log -rw-r----- 1 root adm 14017 8월 31일 13:44 /var/log/auth.log -rw-r----- 1 root adm 687573 8월 31일 13:44 /var/log/kern.log -rw-r----- 1 root adm 2015868 8월 31일 13:44 /var/log/syslog secu-was@jwp-was-01:~\$ cat /etc/rsyslog.d/50-default.conf \ &gt;   egrep "auth authpriv \*\.notice \*\.alert \*\.emerg" auth.notice /var/log/auth.log *.notice /var/log/syslog *.alert /dev/console *.emerg * secu-was@jwp-was-01:~\$ sudo grep -i "session opened for user root" /var/log/auth.log   head 2025-08-31T00:57:20.935844+09:00 jwp-was-01 sudo: pam_unix(sudo:session): session opened fo r user root(uid=0) by admin(uid=1011) 2025-08-31T00:57:38.990636+09:00 jwp-was-01 sudo: pam_unix(sudo:session): session opened fo r user root(uid=0) by admin(uid=1011) 2025-08-31T10:49:27.092087+09:00 jwp-was-01 sshd[4744]: pam_unix(sshd:session): session ope ned for user root(uid=0) by (uid=0) 2025-08-31T10:49:27.137069+09:00 jwp-was-01 (systemd): pam_unix(systemd-user:session): sess ion opened for user root(uid=0) by (uid=0) 2025-08-31T11:11:02.887257+09:00 jwp-was-01 sudo: secu-was : TTY=pts/1 ; PWD=/home/secu-was ; USER=root ; COMMAND=/usr/bin/grep -i 'session opened for user root' /var/log/auth.log 2025-08-31T11:11:02.890229+09:00 jwp-was-01 sudo: pam_unix(sudo:session): session opened fo r user root(uid=0) by admin(uid=1011) 2025-08-31T11:23:52.846498+09:00 jwp-was-01 sudo: pam_unix(sudo:session): session opened fo r user root(uid=0) by admin(uid=1011) 2025-08-31T11:24:06.612565+09:00 jwp-was-01 sudo: pam_unix(sudo:session): session opened fo r user root(uid=0) by admin(uid=1011)</pre>
	3	로그 저장 주기	양호 - 로그 파일의 최소 저장 기간 적용 및 정기적 감독, 백 업하며 쓰기 권한 제한을 둘 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	취약	담당자 인터뷰 결과 로그 관리 정책이 없는 것을 확인
5. 주요 응용 설정	1	FTP(File Transfer Protocol) 서비스 사용자 제한	양호 - FTP 서비스 사용시 root 및 불필요한 계정 접속이 불 가능할 경우 FTP UMASK 값이 077로 설정되어 있을 경우 /etc/passwd 파일에 FTP 계정이 존재하지 않거나 로그인 불가능할 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep -E "ftp vsftpd"   grep -v grep secu-was@jwp-was-01:~\$ systemctl status vsftpd Unit vsftpd.service could not be found. secu-was@jwp-was-01:~\$ systemctl status ftpd Unit ftpd.service could not be found. secu-was@jwp-was-01:~\$ systemctl status pure-ftpd Unit pure-ftpd.service could not be found. secu-was@jwp-was-01:~\$ █</pre>
	2	SNMP(Simple Network Management Protocol) 서비스 설 정	양호 - SNMP 서비스를 사용하지 않거나 Community String 이 public, private 이 아닐 경우 취약 - SNMP 서비스 사용시 위의 기준으로 설정되어 있지 않을 경우	양호	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep snmp secu-was 2921 2244 0 15:20 pts/4 00:00:00 grep snmp secu-was@jwp-was-01:~\$ cat /etc/snmp/snmp.conf   grep "public private" secu-was@jwp-was-01:~\$ systemctl status snmp Unit snmp.service could not be found. secu-was@jwp-was-01:~\$ █</pre>
	3	SMTP(Simple Mail Transfer Protocol) 서비스 설정	양호 - SMTP 서비스 사용시 noexpn, novrfy, restrictqrn 옵션이 설정되어 있는 경우 릴레이 방지 및 릴레이 대상 접근제어가 설정되어 있는 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ cat /etc/mail/c cat: /etc/mail/: 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ █</pre>
	4	DNS(Domain Name Service) 보안 설정	양호 - DNS 서비스 사용시 특정 서버로만 전송하도록 IP 제 한이 설정되어 있는 경우 취약 - DNS 서비스 사용시 특정 서버로만 전송하도록 IP 제 한이 설정되어 있지 않을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep named   grep -v "grep" secu-was@jwp-was-01:~\$ █</pre>
	5	SWAT(Samba Web Administration Tool) 보안 설정	양호 - (x)inetd 설정 파일에 SWAT 서비스가 활성화 되어 있 지 않을 경우 취약 - (x)inetd 설정 파일에 SWAT 서비스가 활성화 되어 있 을 경우	N/A	<pre>secu-was@jwp-was-01:~\$ cat /etc/*inetd.conf   grep "swat" cat: '/etc/*inetd.conf': 그런 파일이나 디렉터리가 없습니다 secu-was@jwp-was-01:~\$ █</pre>
	6	x-server 접속 제한 설정	양호 - 자동 실행화일 파일에 "xhost +" 설정이 존재하지 않 을 경우 취약 - 자동 실행화일 파일에 "xhost +" 설정이 존재할 경우	양호	<pre>secu-was@jwp-was-01:~\$ for file in .login .profile .bashrc .cshrc .xinitrc .xsession .bash_ profile; do if [ -f "\$file" ]; then echo "=== \$file ===" grep -n "xhost" "\$file" 2&gt;/dev/null fi done === .profile === === .bashrc === secu-was@jwp-was-01:~\$ █</pre>
6. 시스템 보안 설 정	1	/etc/system 파일 보안 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	
	2	Kernel 파라미터 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	
	3	ISN(Initial Sequence Number) 파라미터 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	
7. 보안 패치	1	보안 패치 적용	양호 - 서버 내 설치되어 있는 패키지 중 CVE 점수가 9.0 미 만, 점수와 관계없이 영향도가 높은 CVE가 존재하는 버전을 사용하지 않을 경우 취약 - 서버 내 설치되어 있는 패키지 중 CVE 점수가 9.0 이 상, 점수와 관계없이 영향도가 높은 CVE가 존재하는 버전을 사용하는 경우	양호	<pre>secu-was@jwp-was-01:~\$ cat /etc/os-release PRETTY_NAME="Debian GNU/Linux 12 (bookworm)" NAME="Debian GNU/Linux" VERSION_ID="12" VERSION="12 (bookworm)" VERSION_CODENAME=bookworm ID=debian HOME_URL="https://www.debian.org/" SUPPORT_URL="https://www.debian.org/support" BUG_REPORT_URL="https://bugs.debian.org/" secu-was@jwp-was-01:~\$ █</pre>
점검결과				11.0	
	보안 적용율 (양호항목 / 진단항목) %			73.8%	