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

"J.W.P. MagicShop" 취약점 진단

WEB OS 진단 상세결과

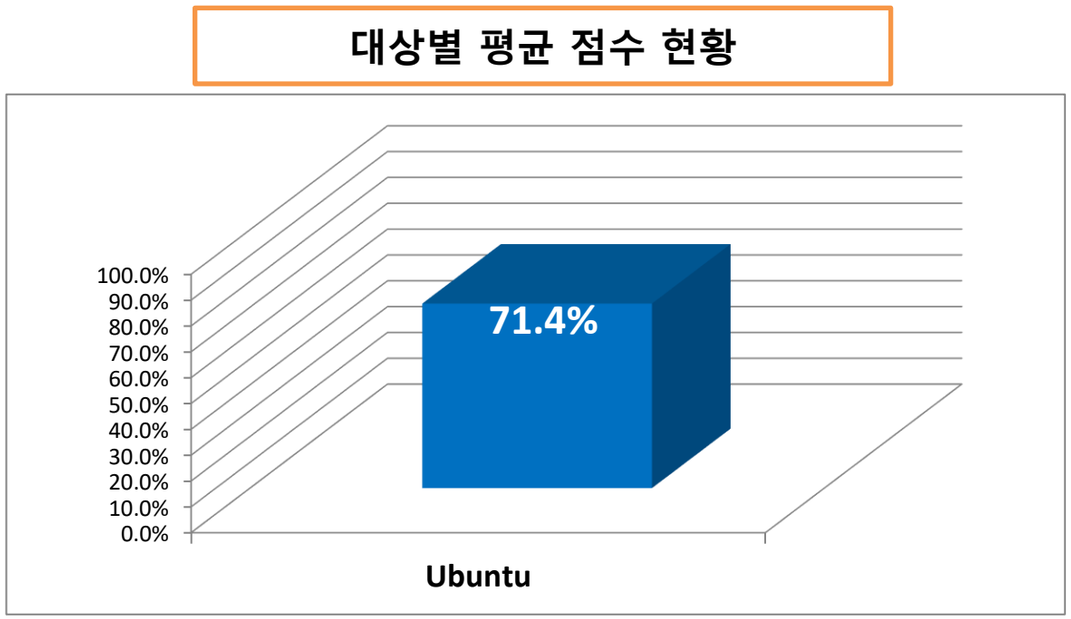
2025년 08월 25일

※ 진단 대상 리스트 - 서버 1대 (Ubuntu 1대)

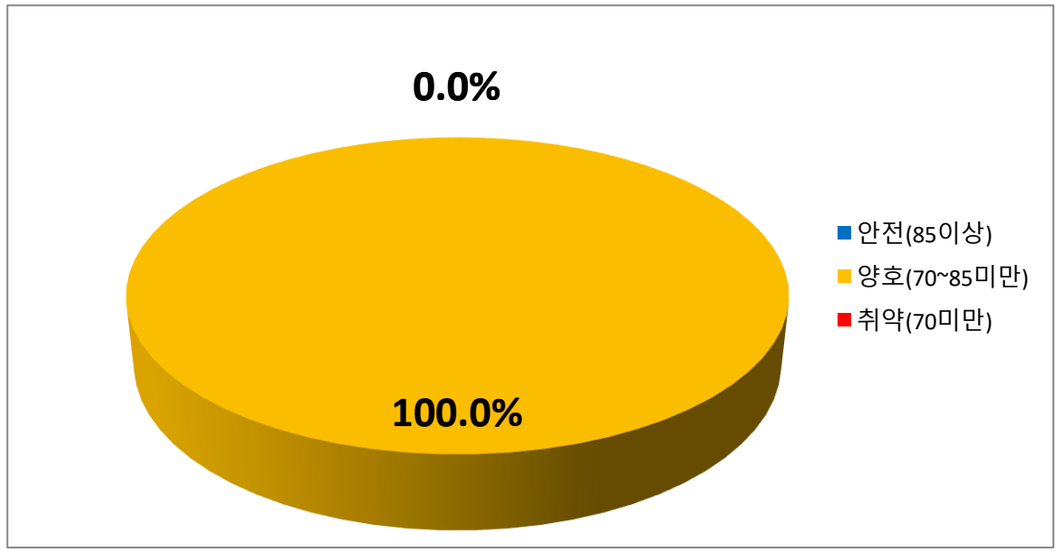
순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Linux					
1	jwp-web-01	10.0.0.14	Ubuntu 22.04 LTS	WEB OS	

※ 대상별 평균 점수 그래프

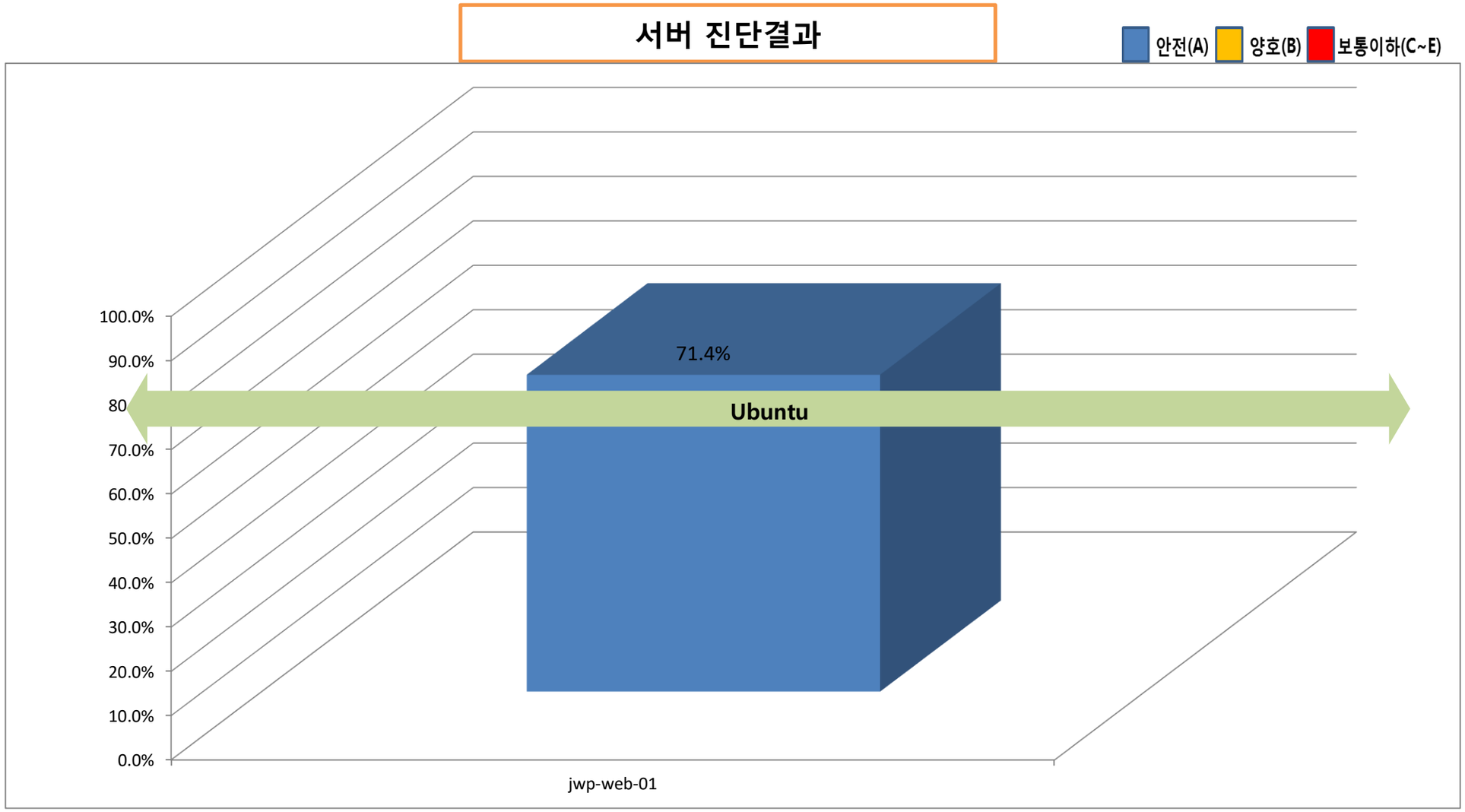
진단 대상	평균	수량
Ubuntu	71.4%	1



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



서버 진단결과

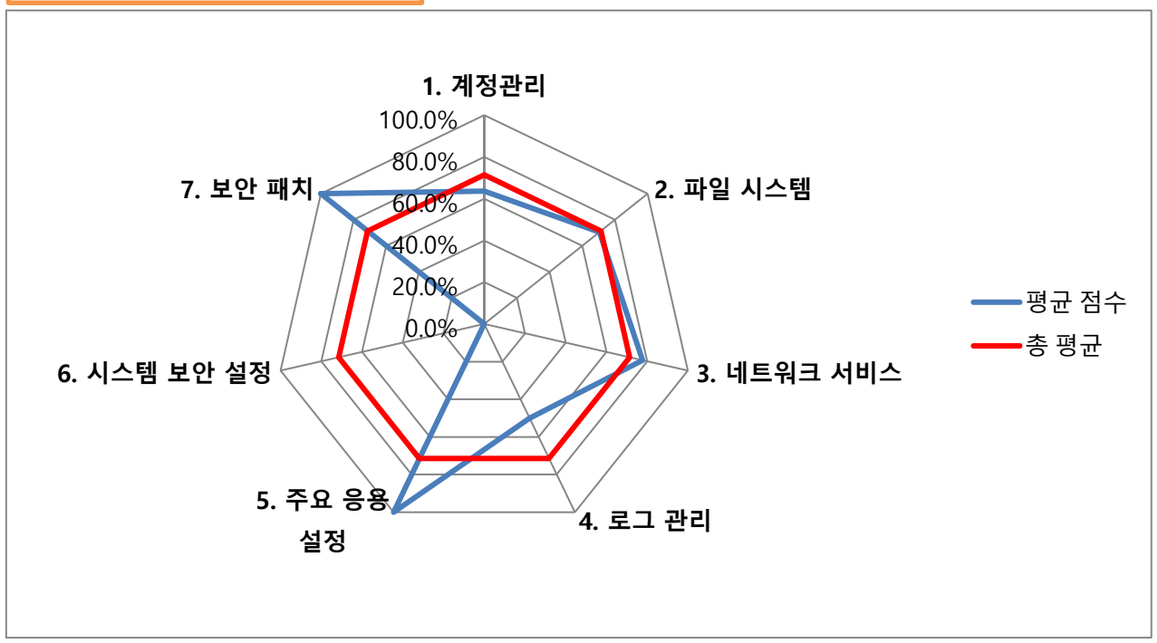


Ubuntu		
NO.	Hostname	점수
1	jwp-web-01	71.4%

Infosec | SK C&C

진단 도메인	평균 점수	총 평균
1. 계정관리	63.6%	71.4%
2. 파일 시스템	70.6%	71.4%
3. 네트워크 서비스	77.8%	71.4%
4. 로그 관리	50.0%	71.4%
5. 주요 응용	100.0%	71.4%
6. 시스템 보안 설정	N/A	71.4%
7. 보안 패치	100.0%	71.4%

Ubuntu 항목별 진단 결과



Ubuntu 취약점 진단 요약결과(58항목)

진단항목	No.	세부 진단항목	중요도	1 jwp-web-01 10.0.0.14
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	취약
	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 서비스	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 설정	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 파라메터 설정	N/A	N/A
	3	ISN(Initial Sequence Number) 파라메터 설정	N/A	N/A
7. 보안 패치	1	보안 패치 적용	상	양호
점검결과				12
		보안 적용율 (양호항목 / 진단항목) %		71.4%

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
70.6%	0.0%	0	1	0
	0.0%	0	1	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
	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
	0.0%	0	1	0
	N/A	0	0	1
	N/A	0	0	1
	N/A	0	0	1
	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
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

Ubuntu 취약점 진단 상세결과(58항목)

진단항목	No.	세부 진단항목	진단기준	1	jwp-web-01 10.0.0.14 WEB OS
1. 계정관리	1	로그인 설정	※ 해당 OS는 체크리스트에 포함하지 않음.	N/A	
	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-web@jwp-web-01:~$ cat /etc/passwd | grep "^lp:|^uucp:|^nuucp:"\ > | grep -v "false|nologin" lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin secu-web@jwp-web-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-web@jwp-web-01:~$ cat /etc/passwd | awk -F":" '{ if ($3 == 0) print $0 }' root:x:0:0:root:/root:/bin/bash secu-web@jwp-web-01:~$
	4	/etc/passwd 파일 권한 설정	양호 - /etc/passwd 파일의 소유주가 root, 권한이 644 일 경우 취약 - /etc/passwd 파일의 소유주가 root가 아니며, 권한이 644 가 아닌 경우	양호	secu-web@jwp-web-01:~$ ls -al /etc/passwd -rw-r--r-- 1 root root 2006 Aug 27 01:07 /etc/passwd secu-web@jwp-web-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-web@jwp-web-01:~$ ls -al /etc/group -rw-r--r-- 1 root root 938 Aug 27 01:07 /etc/group secu-web@jwp-web-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-web@jwp-web-01:~$ ls -al /etc/shadow -rw-r----- 1 root shadow 1125 Aug 27 01:07 /etc/shadow secu-web@jwp-web-01:~$ /etc/shadow 파일 권한이 640으로 설정되어 있어 그룹에 불필요한 읽기 권한이 부여됨
	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-web@jwp-web-01:~$ grep 'PASS_MIN_LEN|PASS_MAX_DAYS|PASS_MIN_DAYS' /etc/login.defs # PASS_MAX_DAYS Maximum number of days a password may be used. # PASS_MIN_DAYS Minimum number of days allowed between password changes. PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0 #PASS_MIN_LEN secu-web@jwp-web-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	담당자 인터뷰 결과 계정과 유사한 패스워드로 확인
	9	로그인이 불필요한 계정 shell 제한	양호 - 로그인이 필요하지 않은 아래 계정의 /bin/false(nologin) 쉘이 부여되어 있을 경우 취약 - 로그인이 필요하지 않은 아래 계정의 /bin/false(nologin) 쉘이 부여되어 있지 않을 경우	양호	secu-web@jwp-web-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 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/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 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:102:105::/nonexistent:/usr/sbin/nologin systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin syslog:x:104:111::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:/usr/sbin/nologin tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin sshd:x:109:65534::/run/sshd:/usr/sbin/nologin pollinate:x:110:1::/var/cache/pollinate:/bin/false landscape:x:111:116::/var/lib/landscape:/usr/sbin/nologin fwupd-refresh:x:112:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin ec2-instance-connect:x:113:65534::/nonexistent:/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-web@jwp-web-01:~$ sudo grep -Rin 'ALL=(ALL:ALL) ALL' /etc/sudoers /etc/sudoers.d /etc/sudoers:44:root ALL=(ALL:ALL) ALL /etc/sudoers:50:%sudo ALL=(ALL:ALL) ALL secu-web@jwp-web-01:~$ getent group sudo sudo:x:27:ubuntu,secu-web secu-web@jwp-web-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-web@jwp-web-01:~$ cat /etc/group | tail -n 10 fwupd-refresh:x:117: admin:x:118: netdev:x:119:ubuntu lxd:x:120:ubuntu _chrony:x:121: ubuntu:x:1000: ssl-cert:x:122: postfix:x:123: postdrop:x:124: secu-web:x:1001: secu-web@jwp-web-01:~$
	12	동일한 UID 금지	양호 - 동일한 UID로 설정된 사용자 계정이 존재하지 않을 경우 취약 - 동일한 UID로 설정된 사용자 계정이 존재하는 경우	양호	secu-web@jwp-web-01:~$ cut -d: -f3 /etc/passwd | sort | uniq -d secu-web@jwp-web-01:~$
	1	사용자 UMASK(User MASK) 설정	양호 - umask가 022(027)일 경우 취약 - umask가 022(027)보다 작을 경우	취약	secu-web@jwp-web-01:~$ cat /etc/profile | grep -i "umask" | grep -v "#" | awk '$2 >= 22' secu-web@jwp-web-01:~$ umask 0002 secu-web@jwp-web-01:~$ 사용자 umask가 0002로 확인됨
	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	-rwsr-xr-x 1 root root 35200 Mar 23 2022 /usr/bin/fusermount3 -rwsr-xr-x 1 root root 40496 Feb 6 2024 /usr/bin/newgrp -rwsr-xr-x 1 root root 44808 Feb 6 2024 /usr/bin/chsh -rwsr-xr-x 1 root root 47488 Apr 9 2024 /usr/bin/mount -rwsr-xr-x 1 root root 55680 Apr 9 2024 /usr/bin/su -rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd -rwsr-xr-x 1 root root 72072 Feb 6 2024 /usr/bin/gpasswd -rwsr-xr-x 1 root root 72712 Feb 6 2024 /usr/bin/chfn -rwsr-xr-x 1 root root 150824 Jan 15 2025 /usr/lib/snapd/snap-confine -rwsr-xr-x 1 root root 232416 Jun 25 12:48 /usr/bin/sudo -rwsr-xr-x 1 root root 338536 Apr 11 12:05 /usr/lib/openssh/ssh-keysign -rwxr-sr-x 1 root _ssh 293304 Apr 11 12:05 /usr/bin/ssh-agent -rwxr-sr-x 1 root crontab 39568 Mar 23 2022 /usr/bin/crontab -rwxr-sr-x 1 root shadow 22680 Jun 12 14:45 /usr/sbin/pam_extrausers_chkpwd -rwxr-sr-x 1 root shadow 23136 Feb 6 2024 /usr/bin/expiry /usr/bin/newgrp 파일에 SUID가 설정되어 있어 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	secu-web@jwp-web-01:~$ ls -al /etc/inetd.conf /etc/xinetd.conf ls: cannot access '/etc/inetd.conf': No such file or directory ls: cannot access '/etc/xinetd.conf': No such file or directory secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ sudo ls -l /root/{.bash_history,.sh_history,.history} \ > /home/ubuntu/{.bash_history,.sh_history,.history} \ > /home/secu-web/{.bash_history,.sh_history,.history} 2>/dev/null -rw------- 1 secu-web secu-web 15190 Aug 30 10:53 /home/secu-web/.bash_history -rw------- 1 ubuntu ubuntu 40130 Aug 30 10:53 /home/ubuntu/.bash_history -rw------- 1 root root 8622 Aug 28 00:37 /root/.bash_history secu-web@jwp-web-01:~$

	5	Crontab 파일 권한 설정 및 관리	양호 - Crontab 관련 파일의 소유자가 root이며, 타사용자의 권한이 제거되어 있을 경우 취약 - 기준대로 설정되어 있지 않을 경우	취약	secu-web@jwp-web-01:~$ ls -al /etc/crontab \ /etc/cron.daily/* \ /etc/cron.hourly/* \ /etc/cron.weekly/* \ /etc/cron.monthly/* \ /etc/var/spool/cron/* ls: cannot access '/etc/cron.hourly/*': No such file or directory ls: cannot access '/etc/cron.monthly/*': No such file or directory -rwxr-xr-x 1 root root 539 Mar 18 2024 /etc/cron.daily/apache2 -rwxr-xr-x 1 root root 376 Jul 24 2023 /etc/cron.daily/apport -rwxr-xr-x 1 root root 1478 Apr 8 2022 /etc/cron.daily/apt-compat -rwxr-xr-x 1 root root 123 Dec 5 2021 /etc/cron.daily/dpkg -rwxr-xr-x 1 root root 377 Jan 24 2022 /etc/cron.daily/logrotate -rwxr-xr-x 1 root root 1330 Mar 17 2022 /etc/cron.daily/man-db -rwxr-xr-x 1 root root 1020 Mar 17 2022 /etc/cron.weekly/man-db -rw-r--r-- 1 root root 1136 Mar 23 2022 /etc/crontab ls: cannot open directory '/var/spool/cron/crontabs': Permission denied secu-web@jwp-web-01:~$
					Crontab 관련 파일 권한이 755로 설정되어 있어 일반 사용자에 불필요한 실행 권한이 부여됨
	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	secu-web@jwp-web-01:~$ ls -al /etc/profile -rw-r--r-- 1 root root 582 Oct 15 2021 /etc/profile secu-web@jwp-web-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	secu-web@jwp-web-01:~$ ls -al /etc/hosts -rw-r--r-- 1 root root 221 May 15 22:41 /etc/hosts secu-web@jwp-web-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	secu-web@jwp-web-01:~$ ls -al /etc/issue /etc/issue.net -rw-r--r-- 1 root root 26 Sep 10 2024 /etc/issue -rw-r--r-- 1 root root 19 Sep 10 2024 /etc/issue.net secu-web@jwp-web-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 기준대로 설정되어 있지 않을 경우	양호	secu-web@jwp-web-01:~$ ls -ald /home/* drwxr-x--- 2 infra-web infra-web 4096 Aug 27 04:50 /home/infra-web drwxr-x--- 2 secu-web secu-web 4096 Aug 28 01:07 /home/secu-web drwxr-x--- 5 ubuntu ubuntu 4096 Sep 1 04:29 /home/ubuntu secu-web@jwp-web-01:~$ sudo ls -al /home/ubuntu/ total 105116 drwxr-x--- 5 ubuntu ubuntu 4096 Sep 1 04:29 . drwxr-xr-x 5 root root 4096 Aug 27 04:50 .. -rw------- 1 ubuntu ubuntu 1015 Sep 1 04:29 .Xauthority -rw------- 1 ubuntu ubuntu 40926 Sep 1 03:56 .bash_history -rw-r--r-- 1 ubuntu ubuntu 220 Jan 6 2022 .bash_logout -rw-r--r-- 1 ubuntu ubuntu 3771 Jan 6 2022 .bashrc drwx------ 3 ubuntu ubuntu 4096 Aug 12 23:54 .cache -rw-r--r-- 1 ubuntu ubuntu 807 Jan 6 2022 .profile drwx------ 2 ubuntu ubuntu 4096 Aug 7 00:19 .ssh -rw-r--r-- 1 ubuntu ubuntu 0 Aug 5 06:14 .sudo_as_admin_successful -rw------- 1 ubuntu ubuntu 13475 Aug 27 06:30 .viminfo -rw-r--r-- 1 root root 19 Aug 27 07:47 auth.log -rw-r--r-- 1 ubuntu ubuntu 97218 Aug 10 12:06 db_fin.sql -rw-r--r-- 1 ubuntu ubuntu 38916 Aug 10 14:34 db_fin2.sql -rw-r--r-- 1 ubuntu ubuntu 40318 Aug 5 06:43 db_insert.sql -rw-rw-r-- 1 ubuntu ubuntu 0 Aug 24 06:12 grep -rw-r--r-- 1 ubuntu ubuntu 98229 Aug 11 01:26 newdb.sql -rw-rw-r-- 1 ubuntu ubuntu 53459024 Jul 20 2022 oracle-instantclient19.16-basic-19.16.0.0. -rw-r--r-- 1 root root 52359550 Aug 5 06:31 oracle-instantclient19.16-basic_19.16.0.0. -rw-rw-r-- 1 ubuntu ubuntu 703356 Jul 20 2022 oracle-instantclient19.16-sqlplus-19.16.0. -rw-r--r-- 1 root root 721316 Aug 5 06:38 oracle-instantclient19.16-sqlplus_19.16.0.
	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	secu-web@jwp-web-01:~$ ls -ald /sbin /etc /bin /usr/bin /usr/sbin /usr/lib lrwxrwxrwx 1 root root 7 May 16 06:01 /bin -> usr/bin drwxr-xr-x 100 root root 4096 Aug 27 01:07 /etc lrwxrwxrwx 1 root root 8 May 16 06:01 /sbin -> usr/sbin drwxr-xr-x 2 root root 36864 Aug 24 08:46 /usr/bin drwxr-xr-x 92 root root 4096 Aug 20 06:08 /usr/lib drwxr-xr-x 2 root root 20480 Aug 24 08:46 /usr/sbin secu-web@jwp-web-01:~$
2. 파일 시스템	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	secu-web@jwp-web-01:~$ env | grep PATH PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin secu-web@jwp-web-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	secu-web@jwp-web-01:~$ ls -al /etc/ftpusers /etc/ftpd/ftpusers /etc/vsftpd/ftpusers ls: cannot access '/etc/ftpusers': No such file or directory ls: cannot access '/etc/ftpd/ftpusers': No such file or directory ls: cannot access '/etc/vsftpd/ftpusers': No such file or directory secu-web@jwp-web-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	secu-web@jwp-web-01:~$ ls -al /etc/pam.d/login -rw-r--r-- 1 root root 4126 Mar 14 2022 /etc/pam.d/login secu-web@jwp-web-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	secu-web@jwp-web-01:~$ ls -al /etc/exports ls: cannot access '/etc/exports': No such file or directory secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ ls -al /etc/services -rw-r--r-- 1 root root 12813 Mar 27 2021 /etc/services secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ ls -al /etc/rc*.d/ /etc/rc0.d/: total 8 drwxr-xr-x 2 root root 4096 Aug 12 23:56 . drwxr-xr-x 100 root root 4096 Aug 27 01:07 .. lrwxrwxrwx 1 root root 29 Aug 5 06:22 K01apache-htcacheclean -> ../init.d/apache-htcacheclean lrwxrwxrwx 1 root root 17 Aug 5 06:22 K01apache2 -> ../init.d/apache2 lrwxrwxrwx 1 root root 16 May 16 06:08 K01chrony -> ../init.d/chrony lrwxrwxrwx 1 root root 20 May 16 06:03 K01cryptdisks -> ../init.d/cryptdisks lrwxrwxrwx 1 root root 26 May 16 06:03 K01cryptdisks-early -> ../init.d/cryptdisks-early lrwxrwxrwx 1 root root 20 May 16 06:03 K01irqbalance -> ../init.d/irqbalance lrwxrwxrwx 1 root root 16 May 16 06:03 K01iscsid -> ../init.d/iscsid lrwxrwxrwx 1 root root 23 May 16 06:03 K01lvm2-lvmpolld -> ../init.d/lvm2-lvmpolld secu-web@jwp-web-01:~$ ls -al /etc/init.d total 152 drwxr-xr-x 2 root root 4096 Aug 14 06:40 . drwxr-xr-x 100 root root 4096 Aug 27 01:07 .. -rwxr-xr-x 1 root root 2269 Jan 25 2022 acpid -rwxr-xr-x 1 root root 2489 Mar 18 2024 apache-htcacheclean -rwxr-xr-x 1 root root 8181 Mar 18 2024 apache2 -rwxr-xr-x 1 root root 3740 Feb 23 2022 apparmor -rwxr-xr-x 1 root root 2920 May 22 20:40 apport -rwxr-xr-x 1 root root 1897 Feb 8 2022 chrony -rwxr-xr-x 1 root root 1232 Nov 22 2021 console-setup.sh -rwxr-xr-x 1 root root 3062 Mar 17 2021 cron -rwxr-xr-x 1 root root 937 Jan 13 2022 cryptdisks -rwxr-xr-x 1 root root 896 Jan 13 2022 cryptdisks-early -rwxr-xr-x 1 root root 3152 Jun 28 2021 dbus -rwxr-xr-x 1 root root 985 Dec 2 2022 grub-common -rwxr-xr-x 1 root root 1677 Nov 16 2023 hibagent

	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 기준대로 설정되어 있지 않을 경우	취약	secu-web@jwp-web-01:~$ cat /etc/hosts.allow /etc/hosts.deny # /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. # # /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 /etc/hosts.allow 및 /etc/hosts.deny 파일이 기본값 상태로 접근 제어 설정이 적용되어 있지 않음
	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	secu-web@jwp-web-01:~$ ls -al /etc/at.allow /etc/at.deny ls: cannot access '/etc/at.allow': No such file or directory ls: cannot access '/etc/at.deny': No such file or directory secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ ls -al /etc/hosts.lpd ls: cannot access '/etc/hosts.lpd': No such file or directory secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ ls -al /etc/rsyslog.conf -rw-r--r-- 1 root root 1382 Dec 23 2021 /etc/rsyslog.conf secu-web@jwp-web-01:~$ /etc/rsyslog.conf 파일 권한이 644로 설정되어 있어 일반 사용자에 불필요한 읽기 권한이 부여됨
	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 않는 경우	양호	secu-web@jwp-web-01:~$ sudo find /home/ubuntu/ -type f -perm -2 -exec ls -l {} \; sudo find /root/ -type f -perm -2 -exec ls -l {} \; find /home/secu-web/ -type f -perm -2 -exec ls -l {} \; secu-web@jwp-web-01:~$
	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	secu-web@jwp-web-01:~$ sudo find /dev -type f -exec ls -l {} \; secu-web@jwp-web-01:~$
	1	RPC(Remote Procedure Call) 서비스 제한	양호 - RPC 서비스가 구동 중에 있지 않을 경우 취약 - RPC 서비스가 구동 중에 있을 경우	양호	secu-web@jwp-web-01:~$ ps -ef | grep -E "rpcbind|rpc.statd|nfslock|portmap\ |rpc.idmapd|rpc.gssd|rpc.svcgssd" | grep -v "grep" secu-web@jwp-web-01:~$
	2	NFS(Network File System) 제한	양호 - NFS 서비스 사용시 설정 파일에 Everyone으로 mount 되어 있지 않은 경우 NFS 서비스 사용시 인가된 시스템을 mount 하고 있는 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	secu-web@jwp-web-01:~$ ps -ef | grep nfsd | grep -v "grep" secu-web@jwp-web-01:~$
	3	Automountd 서비스 제거	양호 - Automountd 서비스가 구동 중이지 않을 경우 취약 - Automountd 서비스가 구동 중일 경우	양호	secu-web@jwp-web-01:~$ ps -ef | grep "automount|autofs" secu-web 43771 43294 0 02:03 pts/3 00:00:00 grep --color=auto automount|autofs secu-web@jwp-web-01:~$
	4	NIS(Network Information Service) 제한	양호 - NIS, NIS+ 서비스가 구동 중이지 않을 경우 취약 - NIS, NIS+ 서비스가 구동 중일 경우	양호	secu-web@jwp-web-01:~$ ps -ef | grep "Ypserv|Ypbind|rpc.yppasswd|ypxfrd|rpc.ypupdated" secu-web 43784 43294 0 02:06 pts/3 00:00:00 grep --color=auto Ypserv|Ypbind|rpc.yppasswd|ypxfrd|rpc.ypupdated secu-web@jwp-web-01:~$
	5	'r' commands 서비스 제거	양호 - login, shell, exec 등 'r' commands 서비스가 구동 중이지 않거나 사용 시 /etc/hosts.equiv, ./$HOME/rhosts 파일 권한 400 및 접근 가능 고정 IP 설정된 경우 취약 - 'r' commands 서비스 사용 시 위의 기준대로 설정되어 있지 않을 경우	양호	secu-web@jwp-web-01:~$ cat /etc/inetd.conf | grep "shell|rlogin|rexec" cat /etc/xinetd.conf | grep "shell|rlogin|rexec" cat: /etc/inetd.conf: No such file or directory cat: /etc/xinetd.conf: No such file or directory secu-web@jwp-web-01:~$
3. 네트워크 서비스	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	secu-web@jwp-web-01:~$ netstat -tulnp (No info could be read for "-p": geteuid()=1001 but you should be root.) Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN - tcp 0 0 127.0.0.1:6010 0.0.0.0:* LISTEN - tcp 0 0 127.0.0.1:6012 0.0.0.0:* LISTEN - tcp 0 0 127.0.0.53:53 0.0.0.0:* LISTEN - tcp6 0 0 :::25 :::* LISTEN -
	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	secu-web@jwp-web-01:~$ cat /etc/motd /etc/issue.net /etc/welcome.msg \ /etc/vsftpd/vsftpd.conf cat: /etc/motd: No such file or directory Ubuntu 22.04.5 LTS cat: /etc/welcome.msg: No such file or directory cat: /etc/vsftpd/vsftpd.conf: No such file or directory Telnet 서비스 배너(/etc/issue.net)에 운영체제 및 버전 정보가 포함되어 있음
	8	session timeout 설정	양호 - session timeout이 "300초"로 설정되어 있을 경우 취약 - session timeout이 "300초"로 설정되어 있지 않을 경우	취약	secu-web@jwp-web-01:~$ cat /etc/profile | grep "TMOUT" cat /etc/.login | grep "autologout" cat: /etc/.login: No such file or directory secu-web@jwp-web-01:~$ /etc/profile 및 /etc/.login 파일에 session timeout에 대한 설정이 없어 해당 기능이 적용되지 않음
	9	root의 계정 telnet, ssh 접근 제한	양호 - 원격 접속(telnet, ssh) 시 root의 직접 접속이 불가능하도록 설정되어 있을 경우 취약 - 원격 접속(telnet, ssh) 시 root로 직접 접속이 가능할 경우	양호	secu-web@jwp-web-01:~$ ls -al /etc/security/user ls: cannot access '/etc/security/user': No such file or directory secu-web@jwp-web-01:~$ egrep "RootLogin" /etc/ssh/sshd_config #PermitRootLogin prohibit-password # the setting of "PermitRootLogin without-password". secu-web@jwp-web-01:~$ grep -i disable_root /etc/cloud/cloud.cfg disable_root: true secu-web@jwp-web-01:~$
	10	DNS 보안 버전 패치	양호 - DNS 서비스를 사용하지 않거나, 사용 시 주기적으로 패치를 관리하고 있는 경우 취약 - DNS 서비스를 사용하며, 주기적으로 패치를 관리하고 있지 않는 경우	양호	secu-web@jwp-web-01:~$ ps -ef | grep named secu-web 43840 43294 0 02:28 pts/3 00:00:00 grep --color=auto named secu-web@jwp-web-01:~$
	1	(x)inetd Services 로그 설정	※ 해당 OS는 체크리스트에 포함하지 않음.	N/A	

4. 로그관리	2	시스템 로그 설정	양호 - su 로깅 기록을 별도 파일에 저장되도록 설정되어 있을 경우 syslog에 중요 로그정보(*.notice, *alert, *.emerg)에 대한 설정이 존재할 경우 로그 파일 및 디렉터리 root 소유, 타사용자에 권한이 부여되어 있지 않을 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	양호	secu-web@jwp-web-01:~$ ls -al /var/log/syslog /var/log/auth.log /var/log/kern.log -rw-r----- 1 syslog adm 551280 Aug 27 02:18 /var/log/auth.log -rw-r----- 1 syslog adm 0 Aug 24 00:00 /var/log/kern.log -rw-r----- 1 syslog adm 213174 Aug 27 02:17 /var/log/syslog secu-web@jwp-web-01:~$ egrep '^[^#].*(info|notice|alert|debug|emerg|err|crit).' \ /etc/rsyslog.conf secu-web@jwp-web-01:~$ secu-web@jwp-web-01:~$ cat /etc/rsyslog.d/50-default.conf | egrep \ "auth|authpriv|*\.notice|*\.alert|*\.emerg" auth,authpriv.* /var/log/auth.log *.*;auth,authpriv.none -/var/log/syslog #auth,authpriv.none;\ #auth,authpriv.none;\ *.emerg :omusrmsg:* secu-web@jwp-web-01:~$ secu-web@jwp-web-01:~$ sudo grep -i "session opened for user root" \ /var/log/auth.log | head Aug 24 00:17:01 jwp-web-01 CRON[31651]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0) Aug 24 01:17:01 jwp-web-01 CRON[32081]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0) Aug 24 02:17:01 jwp-web-01 CRON[32121]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0) Aug 24 03:10:01 jwp-web-01 CRON[32310]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0) Aug 24 03:17:01 jwp-web-01 CRON[32316]: pam_unix(cron:session): session opened for user ro
	3	로그 저장 주기	양호 - 로그 파일의 최소 저장 기간 적용 및 정기적 감독, 백업하며 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 불가능할 경우 FTP UMASK 값이 077로 설정되어 있을 경우 /etc/passwd 파일에 FTP 계정이 존재하지 않거나 로그인이 불가능할 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	secu-web@jwp-web-01:~$ cat /etc/ftpusers | grep root | grep -v "#" cat: /etc/ftpusers: No such file or directory secu-web@jwp-web-01:~$
	2	SNMP(Simple Network Management Protocol) 서비스 설정	양호 - SNMP 서비스를 사용하지 않거나 Community String이 public, private 이 아닐 경우 취약 - SNMP 서비스 사용시 위의 기준대로 설정되어 있지 않을 경우	양호	secu-web@jwp-web-01:~$ ps -ef | grep snmp secu-web 43902 43294 0 03:40 pts/3 00:00:00 grep --color=auto snmp secu-web@jwp-web-01:~$
	3	SMTP(Simple Mail Transfer Protocol) 서비스 설정	양호 - SMTP 서비스 사용시 noexpn, novrfy, restrictqrun 옵션이 설정되어 있는 경우 릴레이 방지 및 릴레이 대상 접근제어가 설정되어 있는 경우 취약 - 위의 기준을 하나라도 만족하지 않을 경우	N/A	secu-web@jwp-web-01:~$ cat /etc/mail/sendmail.cf | grep -i "PrivacyOptions" | grep -v "^#" cat /etc/mail/sendmail.cf | grep -i "Relaying denied" | grep -v "^#" grep: /etc/mail/sendmail.cf: No such file or directory cat: /etc/mail/sendmail.cf: No such file or directory secu-web@jwp-web-01:~$
	4	DNS(Domain Name Service) 보안 설정	양호 - DNS 서비스 사용시 특정 서버로만 전송하도록 IP 제한이 설정되어 있는 경우 취약 - DNS 서비스 사용시 특정 서버로만 전송하도록 IP 제한이 설정되어 있지 않을 경우	N/A	secu-web@jwp-web-01:~$ ps -ef | grep named secu-web 43925 43294 0 03:43 pts/3 00:00:00 grep --color=auto named secu-web@jwp-web-01:~$ ls -l /etc/bind/ ls: cannot access '/etc/bind/': No such file or directory secu-web@jwp-web-01:~$
	5	SWAT(Samba Web Administration Tool) 보안 설정	양호 - (x)inetd 설정 파일에 SWAT 서비스가 활성화 되어 있지 않을 경우 취약 - (x)inetd 설정 파일에 SWAT 서비스가 활성화 되어 있을 경우	N/A	secu-web@jwp-web-01:~$ cat /etc/inetd.conf /etc/xinetd.conf | grep "swat" cat: /etc/inetd.conf: No such file or directory cat: /etc/xinetd.conf: No such file or directory secu-web@jwp-web-01:~$
	6	x-server 접속 제한 설정	양호 - 자동 실행화일 파일에 "xhost +" 설정이 존재하지 않을 경우 취약 - 자동 실행화일 파일에 "xhost +" 설정이 존재할 경우	양호	secu-web@jwp-web-01:~$ cat .login | grep "xhost +" cat .profile | grep "xhost +" cat .cshrc | grep "xhost +" cat .xinitrc | grep "xhost +" cat .xsession | grep "xhost +" cat: .login: No such file or directory cat: .cshrc: No such file or directory cat: .xinitrc: No such file or directory cat: .xsession: No such file or directory secu-web@jwp-web-01:~$
6. 시스템 보안 설정	1	/etc/system 파일 보안 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	
	2	Kernel 파라메터 설정	※ 해당 OS는 체크리스트에 포함하지 않음	N/A	
	3	ISN(Initial Sequence Number) 파라메터 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 미만, 점수와 관계없이 영향도가 높은 CVE가 존재하는 버전을 사용하지 않을 경우 취약 - 서버 내 설치되어 있는 패키지 중 CVE 점수가 9.0 이상, 점수와 관계없이 영향도가 높은 CVE가 존재하는 버전을 사용하는 경우	양호	secu-web@jwp-web-01:~$ uname -a Linux jwp-web-01 6.8.0-1033-aws #35~22.04.1-Ubuntu SMP Wed Jul 23 17:51:00 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux secu-web@jwp-web-01:~$
점검결과				12.0	
			보안 적용율 (양호항목 / 진단항목) %	71.4%	