AI 보안 컨설팅 보고서

대상: 10.8.2.210 | 호스트: localhost-302405 | 생성: 2026-03-05 14:56

스캔 요약

시작 시간	완료 시간	소요 시간	대상 IP	운영체제	계정
2026-03-05 14:56:01	2026-03-05 14:56:02	0 초	10.8.2.2	Ubuntu 24.04.3 LTS	root

점검 결과 요약

1	6	2
✔ 안전	⚠️ 취약	🔍 수동점검

시스템 정보

호스트명	OS	커널	CPU 모델	CPU 코어	업타임	부팅 시각	Load Avg
localhost-302405	Ubuntu 24.04.3 LTS	6.8.0-101-generic	Intel(R) Xeon(R) Silver 4314 C	8 코어	up 5 hours, 18 minutes	2026-03-05 09:37:53	0.78 / 0.31 / 0.20

리소스 사용률

항목	사용률	상태	상세
CPU	**0.0%**	**정상**	
메모리	**5.2%**	**정상**	3.0 GB / 58.9 GB
스왑	**0.0%**	**정상**	0.0 B / 0.0 B

디스크 사용량

장치	마운트	FS	전체	사용	여유	사용률	상태
/dev/vda1	/	ext4	96G	38G	59G	**40%**	**정상**
/dev/vda16	/boot	ext4	881M	168M	652M	**21%**	**정상**
/dev/vda15	/boot/efi	vfat	105M	6.2M	99M	**6%**	**정상**

GPU 상태

#	모델	온도	사용률	VRAM
0	Tesla V100-SXM2-32GB	56°C	0%	24534/32768MB

서비스 상태

서비스	상태
nginx	**inactive**
apache2	**inactive**
postgresql	**inactive**

mysql	inactive
redis	inactive
docker	inactive
fail2ban	inactive
ssh	active
openclaw-gateway	inactive

보안 점검 결과 (취약/수동점검 항목)

[1-1] root 계정 원격 접속 제한	□□
현재 설정	root 원격 SSH 허용
점검 명령어	grep -i PermitRootLogin /etc/ssh/sshd_config 2>/dev/null
점검 결과	PermitRootLogin yes # the setting of "PermitRootLogin prohibit-password".
AI 컨설팅	root 원격 SSH 로그인은 가장 위험한 설정입니다. 무차별 대입 공격으로 root 패스워드가 노출되면 시스템이 완전히 탈취됩니다.
조치 방법	sed -i 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config && systemctl restart sshd

[1-2] 패스워드 복잡도 설정	□□
현재 설정	복잡도 정책 미설정
점검 명령어	grep -vE '^#|^$' /etc/security/pwquality.conf 2>/dev/null | head -8
점검 결과	(출력 없음)
AI 컨설팅	패스워드 복잡도 미설정 시 단순 패스워드 사용이 허용되어 무차별 대입 공격에 취약합니다.
조치 방법	apt install -y libpam-pwquality sed -i 's/# minlen = 8/minlen = 12/' /etc/security/pwquality.conf

[1-3] 계정 잠금 임계값	□□
현재 설정	계정 잠금 정책 없음
점검 명령어	grep pam_faillock /etc/pam.d/common-auth 2>/dev/null | head -2
점검 결과	(출력 없음)
AI 컨설팅	faillock 미설정 시 무제한 패스워드 시도가 가능합니다.
조치 방법	apt install -y libpam-modules && pam-auth-update --enable faillock

[1-4] 패스워드 최대 사용 기간	□□
현재 설정	PASS_MAX_DAYS 99999 일 (90 일 초과)
점검 명령어	grep '^PASS_MAX_DAYS' /etc/login.defs 2>/dev/null
점검 결과	PASS_MAX_DAYS 99999
AI 컨설팅	패스워드 최대 사용 기간이 너무 길면 탈취된 계정이 장기간 악용될 수 있습니다.
조치 방법	sed -i 's/^PASS_MAX_DAYS.*/PASS_MAX_DAYS 90/' /etc/login.defs

[2-1] SUID/SGID □ □ □ □	□□□□
현재 설정	SUID 파일 11 개 발견
점검 명령어	find /usr/bin /usr/sbin /bin /sbin -perm /4000 -type f 2>/dev/null
점검 결과	/usr/bin/su

	/usr/bin/newgrp /usr/bin/passwd /usr/bin/pkexec /usr/bin/gpasswd /usr/bin/sudo /usr/bin/chfn /usr/bin/umount /usr/bin/mount /usr/bin/fusermount3 /usr/bin/chsh
AI 컨설팅	SUID 파일은 권한 상승에 악용될 수 있습니다. 각 파일의 필요성을 검토하세요.

[2-2] 방화벽 상태	□□
현재 설정	방화벽 비활성화
점검 명령어	ufw status 2>/dev/null | head -2
점검 결과	Status: inactive
AI 컨설팅	방화벽 미설정 시 모든 포트가 외부에 노출됩니다.
조치 방법	ufw --force enable && ufw allow ssh && ufw default deny incoming

[2-3] SSH 보안 설정	□□□□
현재 설정	기본값 사용 중 (Port 22, MaxAuthTries 6)
점검 명령어	grep -E '^MaxAuthTries|^Port ' /etc/ssh/sshd_config 2>/dev/null
점검 결과	(출력 없음)
AI 컨설팅	SSH 기본 포트(22)와 인증 시도 제한이 없으면 자동화 공격의 주요 타겟이 됩니다.
조치 방법	# /etc/ssh/sshd_config # MaxAuthTries 3 # Port 22222

[3-2] SSH 브루트포스 탐지	□□
현재 설정	SSH 로그인 실패 6794 회
점검 명령어	grep 'Failed password' /var/log/auth.log 2>/dev/null | wc -l
점검 결과	6794
AI 컨설팅	반복적인 SSH 로그인 실패는 브루트포스 공격 진행 중일 수 있습니다.
조치 방법	apt install -y fail2ban && systemctl enable --now fail2ban

SSH 브루트포스 공격 TOP IP

2521 178.128.197.202

1662 157.230.99.215

943 46.101.173.204

704 143.198.173.15

704 134.209.177.228

39 188.166.111.63

32 80.94.92.186

21 91.224.92.108

로그 에러 / 보안 이슈

```
[SYS]  2026-03-05T13:25:05.910714+09:00 localhost-302405 ollama[795]: time=2026-03-05T13:25:05.910+09:00
level=WARN so

[SYS]  2026-03-05T14:44:04.008528+09:00 localhost-302405 openclaw[26472]: 2026-03-05T05:44:04.008Z [telegram]
tool rep

[SYS]  2026-03-05T14:46:00.252434+09:00 localhost-302405 openclaw[26472]: 2026-03-05T05:46:00.249Z [telegram]
tool rep

[AUTH] 2026-03-05T14:55:50.687431+09:00 localhost-302405 sshd[28730]: Connection closed by invalid user bit
157.230.99

[AUTH] 2026-03-05T14:55:50.886677+09:00 localhost-302405 sshd[28734]: Invalid user perforce from 178.128.197.202
port

[AUTH] 2026-03-05T14:55:53.483159+09:00 localhost-302405 sshd[28734]: Failed password for invalid user perforce
from 1

[AUTH] 2026-03-05T14:55:54.326713+09:00 localhost-302405 sshd[28736]: Invalid user pink from 157.230.99.215 port
36422

[AUTH] 2026-03-05T14:55:54.632875+09:00 localhost-302405 sshd[28734]: Connection closed by invalid user perforce
178.1

[AUTH] 2026-03-05T14:55:56.691608+09:00 localhost-302405 sshd[28736]: Failed password for invalid user pink from
157.2

[AUTH] 2026-03-05T14:55:58.399909+09:00 localhost-302405 sshd[28747]: Invalid user pink from 157.230.99.215 port
33578

[AUTH] 2026-03-05T14:55:58.653074+09:00 localhost-302405 sshd[28738]: Failed password for root from
178.128.197.202 po

[AUTH] 2026-03-05T14:55:59.252847+09:00 localhost-302405 sshd[28736]: Connection closed by invalid user pink
157.230.9

[AUTH] 2026-03-05T14:56:01.899949+09:00 localhost-302405 sshd[28747]: Failed password for invalid user pink from
157.2
```

최근 로그인 이력

```
root     pts/1        0.0.0.0    Thu Mar  5 09:43   still logged in

root     pts/0       0.0.0.0    Thu Mar  5 09:42   still logged in

reboot   system boot  0.0.0.0-generi Thu Mar  5 09:37   still running

root     pts/1        0.0.0.0    Wed Mar  4 16:46 - crash  (16:51)

root     pts/0        0.0.0.0    Wed Mar  4 16:46 - crash  (16:51)

reboot   system boot 0.0.0.0-generi Wed Mar  4 16:43   still running

root     pts/1        0.0.0.0    Wed Mar  4 16:22 - down   (00:20)

root     pts/0        0.0.0.0   Wed Mar  4 16:22 - down   (00:20)

reboot   system boot  0.0.0.0-generi Wed Mar  4 16:22 - 16:43  (00:21)

root     pts/0        0.0.0.0    Wed Mar  4 16:09 - down   (00:12)


wtmp begins Wed Mar  4 16:07:12 2026
```