AUTOISMS 개별 조치 보고서

날짜·시간	2026-02-20 12:00 (한국기준)
OS 타입	ubuntu
OS 버전	25.10
IP	172.20.10.5
HostName	target5

기존 취약 12건 → **조치 후 취약** 11건

로그 관리

U-65 NTP 시각 동기화 설정 MEDIUM

기존 설정 | **조치 후 설정**

설정 비교

```
{'점검항목': 'NTP 설정', '상태': '취약', '세부내용': '취약: Chrony 서비스는 구동 중이나 동기화 서버 설정이 누락되었습니다.', '점검명령어': "grep -vE '^[[:space:]]*#' /etc/chrony/chrony.conf | grep -E '^server|^pool'", '전체내용': ''}
```

```
-
```

세부사항

- {'점검항목': 'NTP 설정', '상태': '취약', '세부내용': '취약: Chrony 서비스는 구동 중이나 동기화 서버 설정이 누락되었습니다.', '점검명령어': "grep -vE '^[[:space:]]*#' /etc/chrony/chrony.conf | grep -E '^server|^pool'", '전체내용': ''}

수동 조치 필요

U-67 로그 디렉터리 권한 설정 MEDIUM

기존 설정 | **조치 후 설정**

설정 비교

Hardened/Safe	/var/log 내 주요 로그 파일 소유자가 root이고, 권한이 644 이하임

세부사항

- {'점검항목': '/var/log/kern.log', '상태': '취약', '세부내용': '취약: /var/log/kern.log : 소유자(syslog) 부적절', '점검명령어': "stat -c '%U %a' /var/log/kern.log; ls -ld /var/log/kern.log", '전체내용': '-rw-r----- 1 syslog adm 790890 Feb 20 11:55 /var/log/kern.log'}
- {'점검항목': '/var/log/auth.log', '상태': '취약', '세부내용': '취약: /var/log/auth.log : 소유자(syslog) 부적절', '점검명령어': "stat -c '%U %a' /var/log/auth.log; ls -ld /var/log/auth.log", '전체내용': '-rw-r----- 1 syslog adm 205647 Feb 20 11:58 /var/log/auth.log'}
- {'점검항목': '/var/log/syslog', '상태': '취약', '세부내용': '취약: /var/log/syslog : 소유자(syslog) 부적절', '점검명령어': "stat -c '%U %a' /var/log/syslog; ls -ld /var/log/syslog", '전체내용': '-rw-r----- 1 syslog adm 4505556 Feb 20 11:58 /var/log/syslog'}
- --- 조치 내역 ---
- 조치 전: Hardened/Safe
- 조치 후: /var/log 내 주요 로그 파일 소유자가 root이고, 권한이 644 이하임
- 조치 전: root가 아닌 파일(조치 전): /var/log/kern.log /var/log/auth.log /var/log/syslog (없음) 과도한 권한 파일(조치 전): (없음)
- 조치 후: root가 아닌 파일(조치 후): /var/log/kern.log /var/log/auth.log /var/log/syslog (없음) 과도한 권한 파일(조치 후): (없음)
- 조치 명령: find로 /var/log 비root 소유 및 과도 권한 파일을 chown root:root, chmod 644로 보정

조치 완료

파일 및 디렉터리 관리

U-19 /etc/hosts 파일 소유자 및 권한 설정 HIGH

기존 설정 **조치 후 설정**

설정 비교

{'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: 권한이 644 입니다. (기준: 600 이하)', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r-- 1 root root 222 Feb 19 15:42 /etc/hosts'}	-

세부사항

- {'점검항목': '소유자 설정', '상태': '양호', '세부내용': '양호: 소유자가 root 입니다.', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r-- 1 root root 222 Feb 19 15:42 /etc/hosts'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: 권한이 644 입니다. (기준: 600 이하)', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r-- 1 root root 222 Feb 19 15:42 /etc/hosts'}

수동 조치 필요

U-23 SUID/SGID/Sticky bit 설정 점검 HIGH

기존 설정 **조치 후 설정**

설정 비교

```
{'점검항목': 'SUID/SGID 설정', '상태': '취약', '세부내용': '취약: /usr/bin/newgrp (현재 설정: -rwsr-xr-x 1 root root 18968 Sep  7 00:37 /usr/bin/newgrp)', '점검명령어': 'ls -l /usr/bin/newgrp', '전체내용': '-rwsr-xr-x 1 root root 18968 Sep  7 00:37 /usr/bin/newgrp'}
```

```
위험 의심 파일 1개 발견 (수동 검토 필요)
```

세부사항

- {'점검항목': 'SUID/SGID 설정', '상태': '취약', '세부내용': '취약: /usr/bin/newgrp (현재 설정: -rwsr-xr-x 1 root root 18968 Sep 7 00:37 /usr/bin/newgrp)', '점검명령어': 'ls -l /usr/bin/newgrp', '전체내용': '-rwsr-xr-x 1 root root 18968 Sep 7 00:37 /usr/bin/newgrp'}

수동 조치 필요

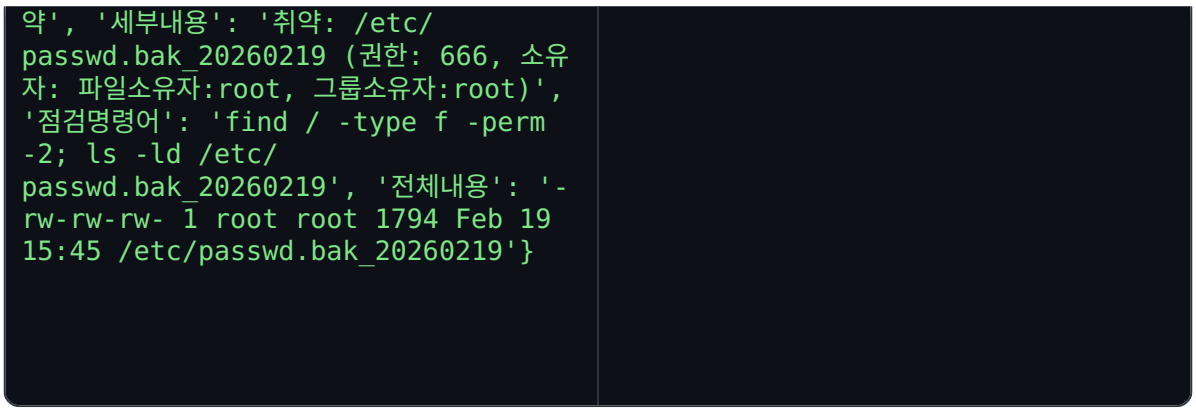
U-25 world writable 파일 점검 HIGH

기존 설정 **조치 후 설정**

설정 비교

```
{'점검항목': '/etc/passwd.bak_20260219', '상태': '취
```

```
-
```



세부사항

- {'점검항목': '/etc/passwd.bak_20260219', '상태': '취약', '세부내용': '취약: /etc/passwd.bak_20260219 (권한: 666, 소유자: 파일소유자:root, 그룹소유자:root)', '점검명령어': 'find / -type f -perm -2; ls -ld /etc/passwd.bak_20260219', '전체내용': '-rw-rw-rw- 1 root root 1794 Feb 19 15:45 /etc/passwd.bak_20260219'}
- {'점검항목': '/home/target5/.bashrc.bak_20260219', '상태': '취약', '세부내용': '취약: /home/target5/.bashrc.bak_20260219 (권한: 646, 소유자: 파일소유자:target5, 그룹소유자:target5)', '점검명령어': 'find / -type f -perm -2; ls -ld /home/target5/.bashrc.bak_20260219', '전체내용': '-rw-r--rw- 1 target5 target5 3771 Sep 8 22:20 /home/target5/.bashrc.bak_20260219'}

수동 조치 필요

U-28 접속 IP 및 포트 제한 HIGH

기존 설정 **조치 후 설정**

세부사항

- {'점검항목': 'etc/hosts.allow', '상태': '취약', '세부내용': '취약 /etc/hosts.allow 파일은 존재하나 설정된 접근 제어 규칙이 없음', '점검명령어': "grep -v '^#' /etc/hosts.allow | grep -v '^$'", '전체내용': 'rules=0'}
- {'점검항목': 'etc/hosts.deny', '상태': '취약', '세부내용': '취약 : /etc/hosts.deny 파일 존재하나 규칙 없음', '점검명령어': "grep -v '^#' /etc/hosts.deny | grep -v '^$'", '전체내용': 'rules=0'}
- {'점검항목': '방화벽 설정', '상태': '취약', '세부내용': '취약: ufw 비활성화', '점검명령어': 'ufw status', '전체내용': 'Status: inactive'}
- {'점검항목': '방화벽 설정', '상태': '취약', '세부내용': '취약 : iptables 규칙 없음', '점검명령어': 'iptables -L INPUT -n; iptables -L FORWARD -n; iptables -L OUTPUT -n', '전체내용': 'total=0'}

- {'점검항목': '방화벽 설정', '상태': '취약', '세부내용': '취약 : nftables 규칙 없음', '점검명령어': 'nft list ruleset', '전체내용': 'lines=0'}

수동 조치 필요

U-30 UMASK 설정 관리 MEDIUM

기존 설정	조치 후 설정
설정 비교	
{'점검항목': 'UMASK 설정', '상태': '취약', '세부내용': '취약: /etc/bash.bashrc (라인 114) - umask 000 (022 미만)', '점검명령어': "grep -n '^[^#]*umask' /etc/bash.bashrc", '전체내용': '/etc/bash.bashrc:114:umask 000'}	총 4개 파일 점검 (취약: 1개, 양호: 1개)

세부사항

- {'점검항목': 'UMASK 설정', '상태': '양호', '세부내용': '양호: 현재 UMASK 0022 (022 이상)', '점검명령어': 'umask', '전체내용': '0022'}
- {'점검항목': 'UMASK 설정', '상태': '양호', '세부내용': '양호: /etc/profile (라인 31) - umask 022 (022 이상)', '점검명령어': "grep -n '^[^#]*umask' /etc/profile", '전체내용': '/etc/profile:31:umask 022'}
- {'점검항목': 'UMASK 설정', '상태': '취약', '세부내용': '취약: /etc/bash.bashrc (라인 114) - umask 000 (022 미만)', '점검명령어': "grep -n '^[^#]*umask' /etc/bash.bashrc", '전체내용': '/etc/bash.bashrc:114:umask 000'}

조치 실패

계정 관리

U-03 계정 잠금 임계값 설정 HIGH

기존 설정	조치 후 설정
설정 비교	
{'점검항목': '계정 잠금 임계값', '상태': '취약', '세부내용': '취약: /etc/pam.d/common-auth(및 include) 내 계정 잠금 모듈 설정이 발견되지 않았습니다.', '점검명령어': "grep -v '^#' /etc/pam.d/	–

```
common-auth | grep 'pam_faillock\\
\\.so\\\\|pam_tally2\\\\.so\\\\|
pam_tally\\\\.so'", '전체내용': '/
etc/pam.d/common-auth'}
```

세부사항

- {'점검항목': '계정 잠금 임계값', '상태': '취약', '세부내용': '취약: /etc/pam.d/common-auth(및 include) 내 계정 잠금 모듈 설정이 발견되지 않았습니다.', '점검명령어': "grep -v '^#' /etc/pam.d/common-auth | grep 'pam_faillock\\\\.so\\\\|pam_tally2\\\\.so\\\\|pam_tally\\\\.so'", '전체내용': '/etc/pam.d/common-auth'}
- {'점검항목': 'U-03 조치 안내', '상태': '수동조치', '세부내용': '이 항목은 PAM 직접 수정 시 로그인 불가 위험이 있어 통합조치 스크립트에서 자동 적용하지 않습니다. deny=10, unlock_time=120 설정은 수동으로 적용하세요.'}

수동 조치 필요

U-06 사용자 계정 su 기능 제한 HIGH

기존 설정 **조치 후 설정**

설정 비교

```
{'점검항목': 'PAM su 설정', '상태': '취
약', '세부내용': '취약: pam_wheel.so
설정이 주석 처리되어 있음', '점검명령어':
"grep -E
'^[[:space:]]*#.*auth.*required.*
pam_wheel\\\\.so' /etc/pam.d/su",
'전체내용': '# auth       required
pam_wheel.so\n# auth
required   pam_wheel.so deny
group=nosu'}
```

```
-
```

세부사항

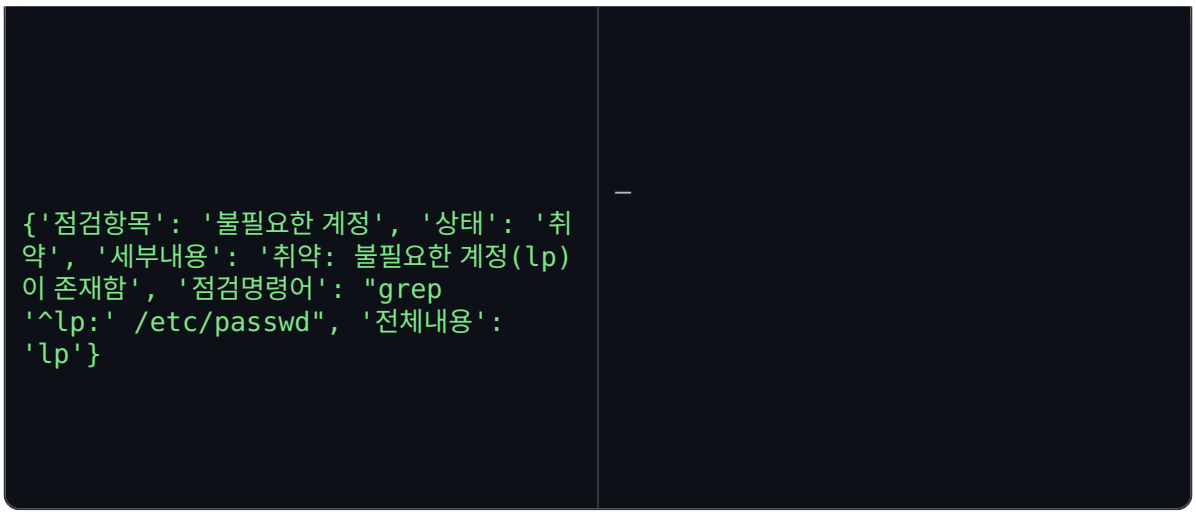
- {'점검항목': 'PAM su 설정', '상태': '취약', '세부내용': '취약: pam_wheel.so 설정이 주석 처리되어 있음', '점검명령어': "grep -E '^[[:space:]]*#.*auth.*required.*pam_wheel\\\\.so' /etc/pam.d/su", '전체내용': '# auth required pam_wheel.so\n# auth required pam_wheel.so deny group=nosu'}

수동 조치 필요

U-07 불필요한 계정 제거 LOW

기존 설정 **조치 후 설정**

설정 비교

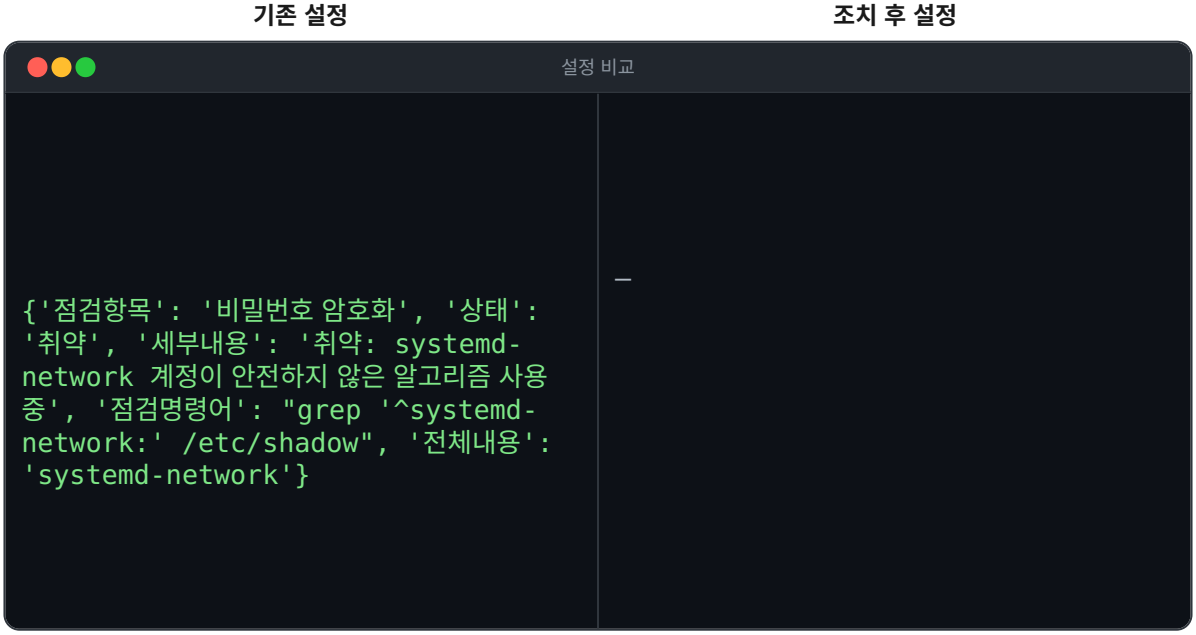


세부사항

- {'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(lp)이 존재함', '점검명령어': "grep '^lp:' /etc/passwd", '전체내용': 'lp'}
- {'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(uucp)이 존재함', '점검명령어': "grep '^uucp:' /etc/passwd", '전체내용': 'uucp'}
- {'점검항목': '불필요한 계정', '상태': '양호', '세부내용': '양호: 불필요한 계정(nuucp)이 없음', '점검명령어': "grep '^nuucp:' /etc/passwd", '전체내용': ''}
- {'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(games)이 존재함', '점검명령어': "grep '^games:' /etc/passwd", '전체내용': 'games'}

수동 조치 필요

U-13 안전한 비밀번호 암호화 알고리즘 사용 MEDIUM



세부사항

- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: systemd-network 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^systemd-network:' /etc/shadow", '전체내용': 'systemd-network'}
- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: messagebus 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^messagebus:' /etc/shadow", '전체내용': 'messagebus'}
- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: systemd-resolve 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^systemd-resolve:' /etc/shadow", '전체내용': 'systemd-resolve'}

- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: polkitd 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^polkitd:' /etc/shadow", '전체내용': 'polkitd'}
- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: fwupd-refresh 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^fwupd-refresh:' /etc/shadow", '전체내용': 'fwupd-refresh'}
- {'점검항목': '비밀번호 암호화', '상태': '취약', '세부내용': '취약: sshd 계정이 안전하지 않은 알고리즘 사용 중', '점검명령어': "grep '^sshd:' /etc/shadow", '전체내용': 'sshd'}

수동 조치 필요

서비스 관리

U-37 crontab 권한 설정 HIGH

기존 설정 | **조치 후 설정**

설정 비교

```
{'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /usr/bin/crontab (권한: 2755, 소유자: root:crontab) - 750 초과', '점검명령어': "stat -c '%U %a' /usr/bin/crontab; ls -ld /usr/bin/crontab", '전체내용': '/usr/bin/crontab:owner=root:crontab,perm=2755'}
```

```
총 9개 중 취약 9개, 안전 0개
```

세부사항

- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /usr/bin/crontab (권한: 2755, 소유자: root:crontab) - 750 초과', '점검명령어': "stat -c '%U %a' /usr/bin/crontab; ls -ld /usr/bin/crontab", '전체내용': '/usr/bin/crontab:owner=root:crontab,perm=2755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /bin/crontab (권한: 2755, 소유자: root:crontab) - 750 초과', '점검명령어': "stat -c '%U %a' /bin/crontab; ls -ld /bin/crontab", '전체내용': '/bin/crontab:owner=root:crontab,perm=2755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/crontab (권한: 644, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/crontab; ls -ld /etc/crontab", '전체내용': '/etc/crontab:owner=root:root,perm=644'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.d (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.d; ls -ld /etc/cron.d", '전체내용': '/etc/cron.d:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.daily (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.daily; ls -ld /etc/cron.daily", '전체내용': '/etc/cron.daily:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.hourly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.hourly; ls -ld /etc/cron.hourly", '전체내용': '/etc/cron.hourly:owner=root:root,perm=755'}

- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.monthly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.monthly; ls -ld /etc/cron.monthly", '전체내용': '/etc/cron.monthly:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.weekly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.weekly; ls -ld /etc/cron.weekly", '전체내용': '/etc/cron.weekly:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /var/spool/cron (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /var/spool/cron; ls -ld /var/spool/cron", '전체내용': '/var/spool/cron:owner=root:root,perm=755'}

수동 조치 필요