U-49 (하)

1. 점검 내용

- 시스템 계정 중 불필요한 계정(퇴직, 전직, 휴직 등의 이유로 사용하지 않는 계정)이 존재하는지 점검

---

2. 점검 목적

- 불필요한 계정이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 대비하는지 확인하기 위함

---

3. 취약 판단 기준

- 불필요한 계정이 존재하는 경우 취약하다고 판단

3.1. 불필요할 수 있는 계정

계정 이름	설명	불필요할 수 있는 경우
games	게임 관련 데이터를 저장하는 계정	시스템에서 게임을 실행하지 않는 경우
lp	프린터 시스템(LPD) 계정	시스템에 프린터가 없거나 사용하지 않는 경우
mail	메일 전송 에이전트 계정	메일 서비스를 운영하지 않는 경우
news	뉴스 그룹 소프트웨어 계정	뉴스 그룹 서비스를 운영하지 않는 경우
uucp	유니버설 유니언 커뮤니케이션 프로토콜 계정	UUCP를 사용하지 않는 경우
proxy	프록시 서버 계정	프록시 서버를 운영하지 않는 경우
irc	IRC 서버 계정	IRC 서비스를 운영하지 않는 경우
gnats	GNATS 버그 추적 시스템 계정	GNATS를 사용하지 않는 경우
list	메일링 리스트 관리 계정	메일링 리스트 서비스를 운영하지 않는 경우

---

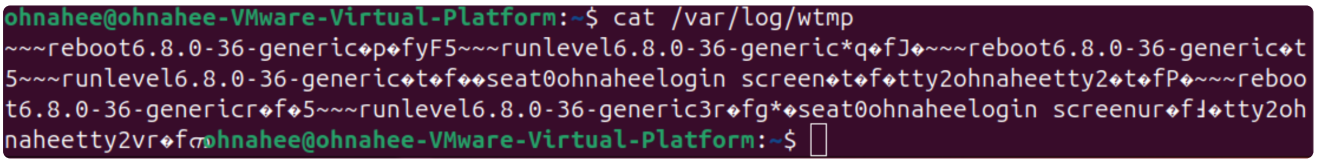
4. 점검 방법

4.1. /etc/passwd 파일 확인

```
cat /etc/passwd
```

4.2. Log 확인 (/var/log/wtmp 파일 확인)

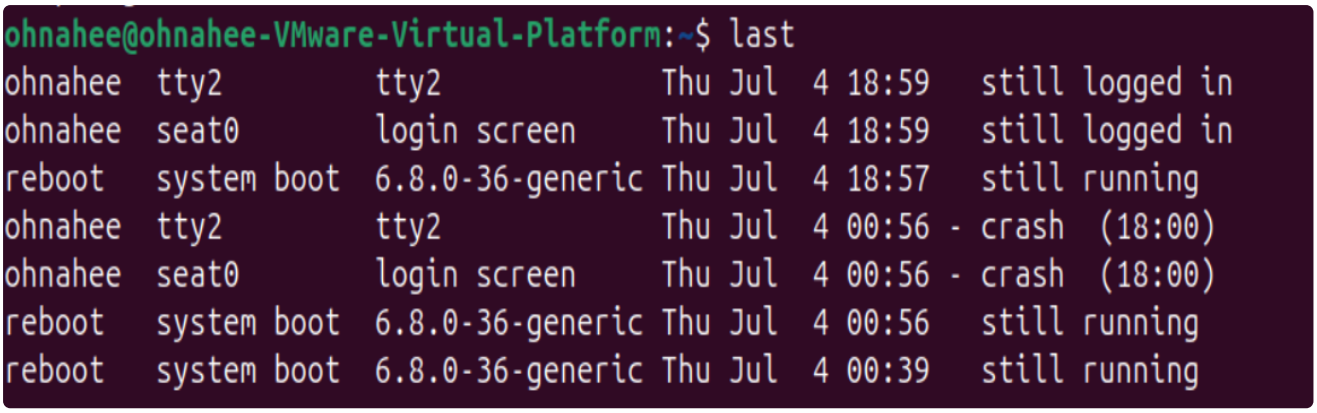
```
cat /var/log/wtmp
```



- /var/log/wtmp 파일은 시스템의 모든 로그인, 로그아웃, 시스템 부팅 및 종료 이벤트를 기록하는 이진 로그 파일이다
  - **텍스트 편집기로 직접 읽을 수 없다**

4.3. last 로 /var/log/wtmp 파일 확인

```
last
```



- 사람이 읽을 수 있는 형식으로 출력해준다
- 왼쪽부터 사용자 이름, 사용자가 접속한 터미널, 호스트(사용자가 접속한 원격 호스트 또는 로그인 타입), 사용자가 로그인 한 시간, 사용자가 로그아웃한 시간과 상태를 나타낸다

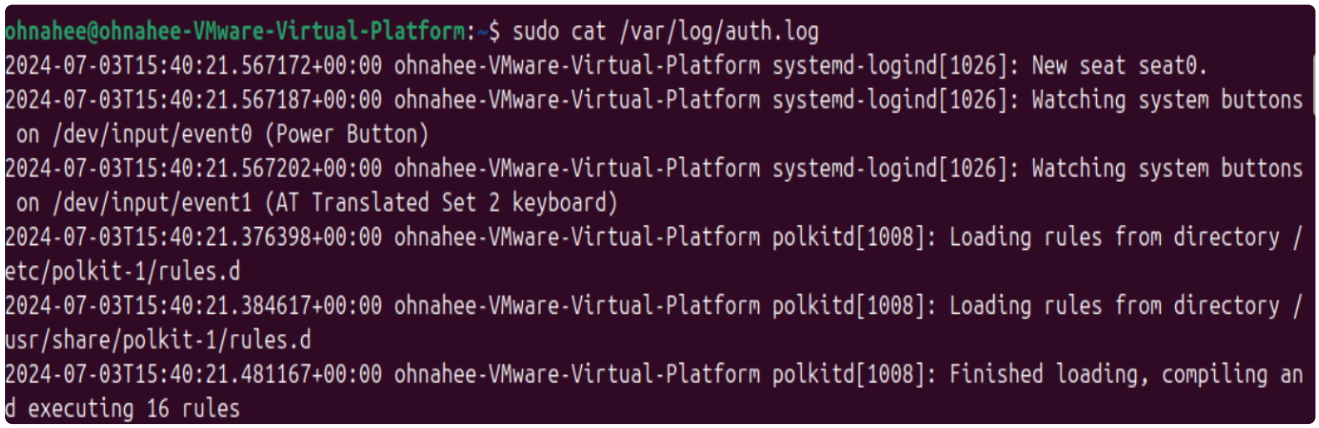
---

1. ohnahee tty2 tty2 Thu Jul 4 18:59 still logged in
    - 사용자 ohnahee 가 tty2 터미널을 통해 Thu Jul 4 18:59 에 로그인 했고 현재 로그인 된 상태
2. reboot system boot 6.8.0-36-generic Thu Jul 4 18:57 still running
    - 시스템이 Thu Jul 4 18:57 에 커널버전 6.8.0-36-generic 로 부팅되었으며 현재 시스템이 계속 실행중
3. ohnahee seat0 login screen Thu Jul 4 00:56 - crash (18:00)
    - 사용자 ohnahee가 seat0를 통해 Thu Jul 4 00:56 에 로그인 했으나 시스템이 18시간 후에 크래시 (crash) 로 인해 세션이 종료되었다

*크래시 : 컴퓨터 시스템, 소프트웨어 어플리케이션, 또는 운영 체제가 예기치 않게 작동을 멈추거나 종료하는 현상

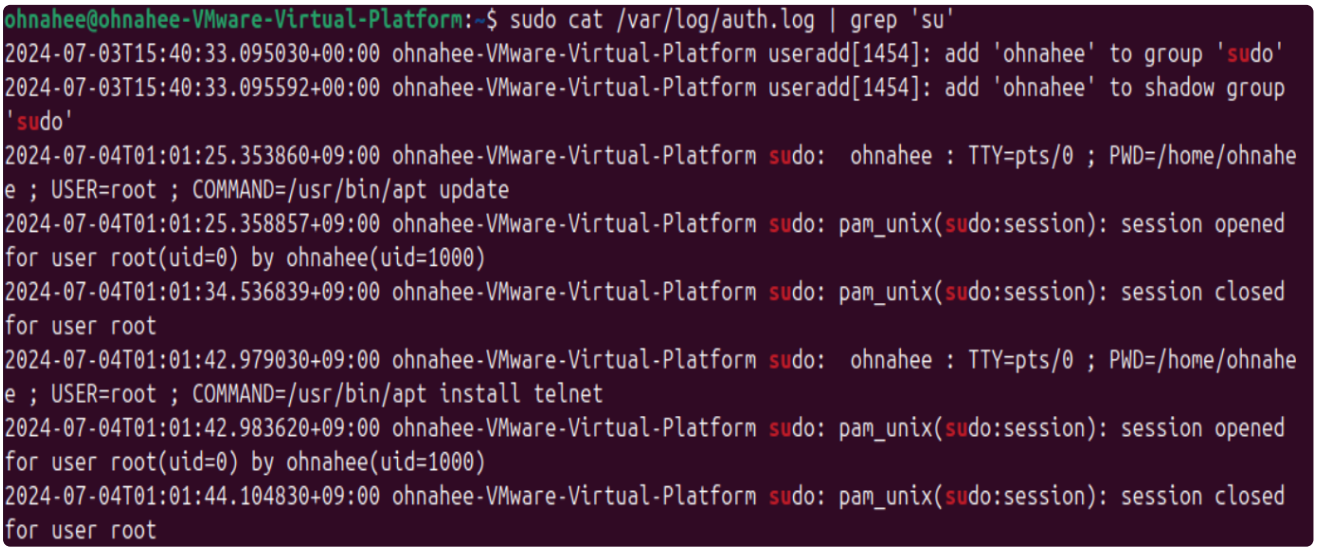
4.4. auth.log 파일 확인

```
sudo cat /var/log/auth.log
```



- 시스템의 인증 관련 로그를 기록한다
    - su 명령어 사용 내역 포함

```
sudo cat /var/log/auth.log | grep 'su'
```



5.보안 조치 방법

```
sudo deluser uucp
```

- 불필요한 계정 삭제