U-49 (하)

1. 점검 내용

- 시스템 계정 중 불필요한 계정이 존재하는지 점검

---

2. 점검 목적

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

---

3. 점검 전 지식

3.1. lp 계정

- Line Printer 의 약자
- 인쇄 작업을 처리하는 시스템 계정
- 프린트 데몬과 관련된 작업을 처리하고 프린터와의 통신을 관리한다
- 대부분 현재는 사용되지 않지만 프린터 관련 서비스에서 여전히 사용 될 수 있다

*데몬 : 리눅스 시스템에서 백그라운드에서 실행되는 프로그램이나 프로세스

3.2. uucp 계정

- Unix-to-Unix Copy Program 의 약자
- 원격 시스템 간 파일 전송을 위해 사용되는 계정
- 과거에는 뉴스 그룹, 이메일, 파일 전송 등을 위해 사용되었다
- 주로 UUCP 네트워크에서 파일과 메시지를 전송하는데 사용되었다
- 대부분 현재는 사용되지 않고 보안상의 이유로 시스템에서는 불필요하다

3.3. nuucp 계정

- uucp 계정과 유사한 역할을 한다

- Nu-Union 간의 파일 전송을 위해 사용된다
- uucp 계정과 마찬가지로 UUCP 네트워크에서 파일과 메시지를 전송하는데 사용되었다
- 대부분 현재는 사용되지 않으며 보안상의 이유로 시스템에서는 불필요하다

3.4. UUCP 네트워크

- UUCP(Unix-to-Unix Copy Program) 네트워크
- 1970년대 후반에 개발된 시스템
- 유닉스 시스템 간의 파일을 전송하고 명령을 실행하며 전자 메일과 뉴스 그룹 메시지를 교환하는데 사용하였다
- 주로 전화 모뎀, 초기 인터넷 연결을 위해 작동했다
- 현재는 인터넷의 발전으로 인해 TCP/IP 기반의 프로토콜이 주류가 되면서 SSH, SCP, FTP 등 현대적인 파일 전송 및 원격 명령 실행 도구들이 UUCP를 대체하게 되었다

---

4. 점검 방법 및 결과 값

4.1. 계정 확인

```
cat /etc/passwd
```

- /etc/passwd 파일은 시스템의 모든 사용자 계정 정보가 저장되어 있다
  - 해당 파일을 출력하여 미사용 계정, 의심스러운 계정을 확인한다

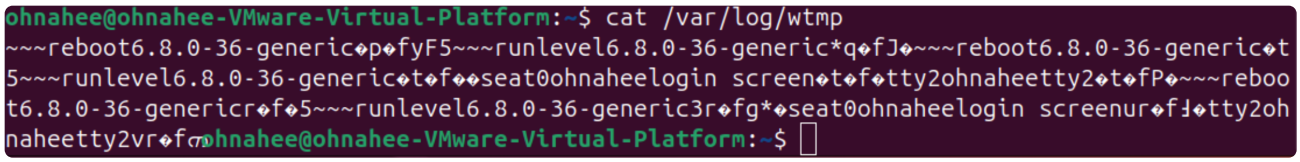
4.2. 기본적으로 생성되는 Dafault 계정 점검

```
cat /etc/passwd | egrep "lp|uucp|nuucp"
```

```
ohnahee@ohnahee-VMware-Virtual-Platform:~$ cat /etc/passwd | egrep "ip|uucp|nuucp"
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
```

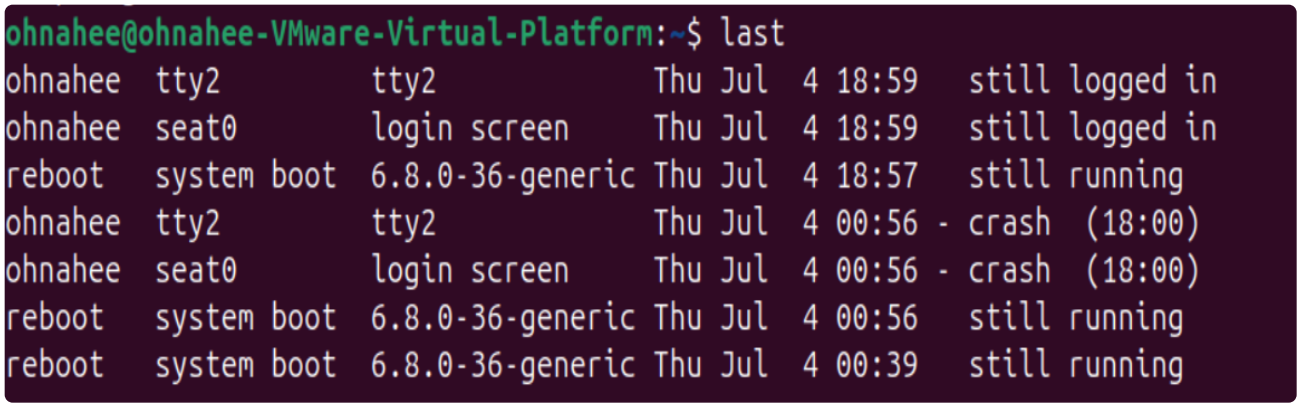
4.3. 최근 로그인 하지 않은 계정 및 의심스러운 계정 확인

```
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**

```
last
```



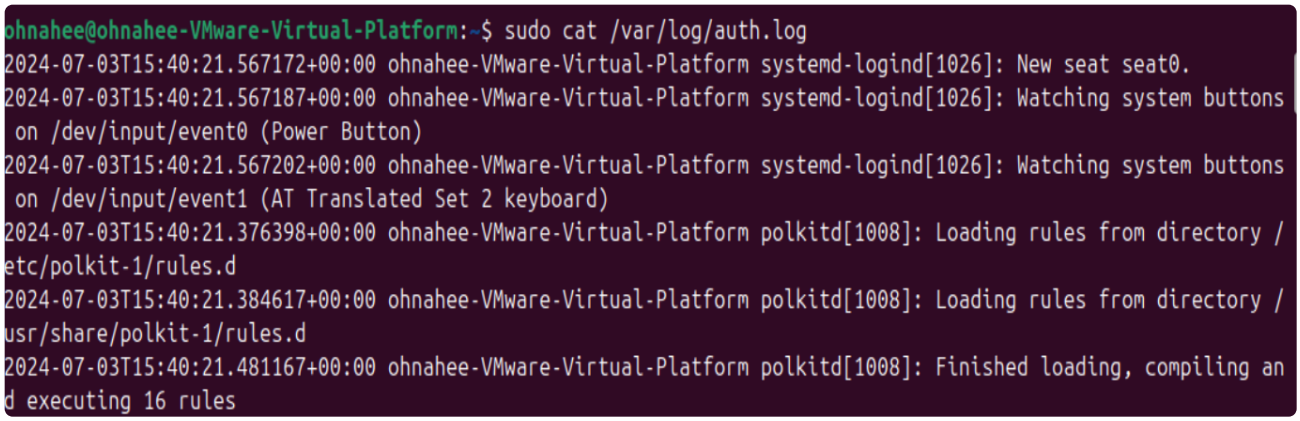
- last 명령어는 /var/log/wtmp 파일을 사람이 읽을 수 있는 형식으로 출력해준다
- 왼쪽부터 사용자 이름, 사용자가 접속한 터미널, 호스트(사용자가 접속한 원격 호스트 또는 로그인 타입), 사용자가 로그인 한 시간, 사용자가 로그아웃한 시간과 상태를 나타낸다

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

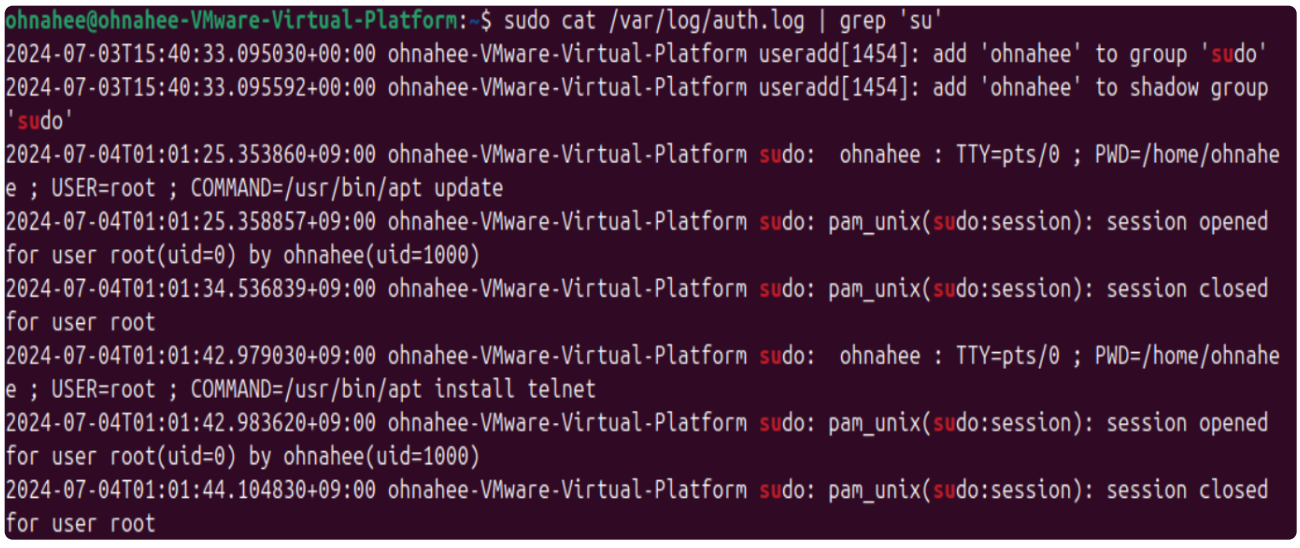
auth.log 파일 확인

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



- /var/log/auth/log 파일
  - 시스템의 인증 관련 로그를 기록한다
  - su 명령어 사용 내역도 포함된다

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

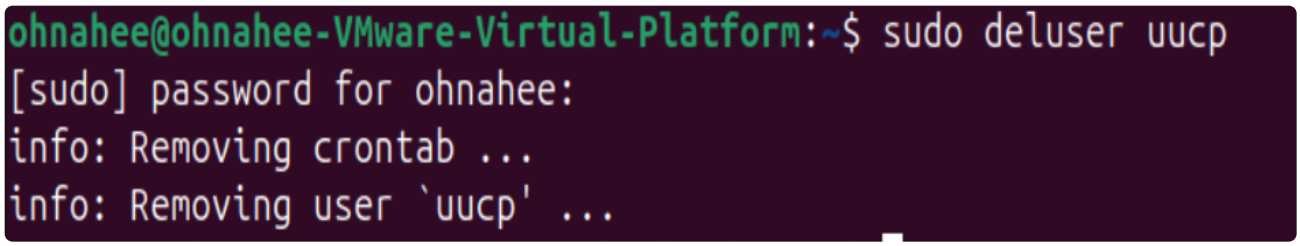


- 파일에서 su 명령어의 사용 내역만 볼 수 있다

5. 조치 방법

5.1. uucp 계정 삭제

```
sudo deluser uucp
```



5.2. uucp 관련 홈 디렉토리 및 파일 제거

```
sudo deluser --remove-home uucp
sudo deluser --remove-all-files uucp
```

6. 보안 조치 확인

- 필요 없는 사용자가 제거되었음을 확인할 수 있다