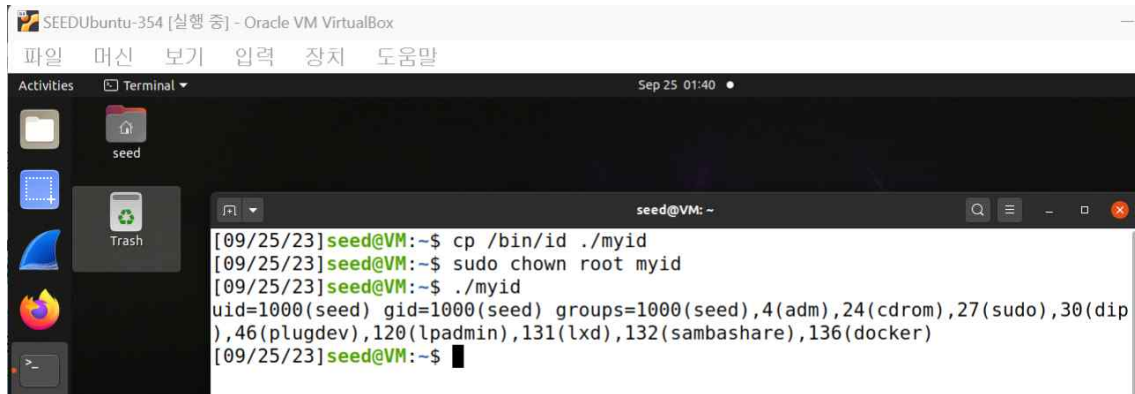


소프트웨어 보안 실습 일지

| | | | |
|-------|----------------|----|---|
| 학번/이름 | 2022111354/한아림 | 주차 | 4 |
|-------|----------------|----|---|

1. 화면 캡처 3장 및 이의 설명 적기



```
SEEDUbuntu-354 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities Terminal Sep 25 01:40
seed
Trash
[09/25/23] seed@VM: ~$ cp /bin/id ./myid
[09/25/23] seed@VM: ~$ sudo chown root myid
[09/25/23] seed@VM: ~$ ./myid
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
[09/25/23] seed@VM: ~$
```

cp /bin/id ./myid

: /bin/id 파일을 현재 작업 디렉토리로 복사하고, 복사한 파일의 이름을 myid로 지정

sudo chown root myid

: myid 파일의 소유자가 root 사용자가 되도록 변경

./myid

: 현재 디렉토리에서 myid 파일을 실행



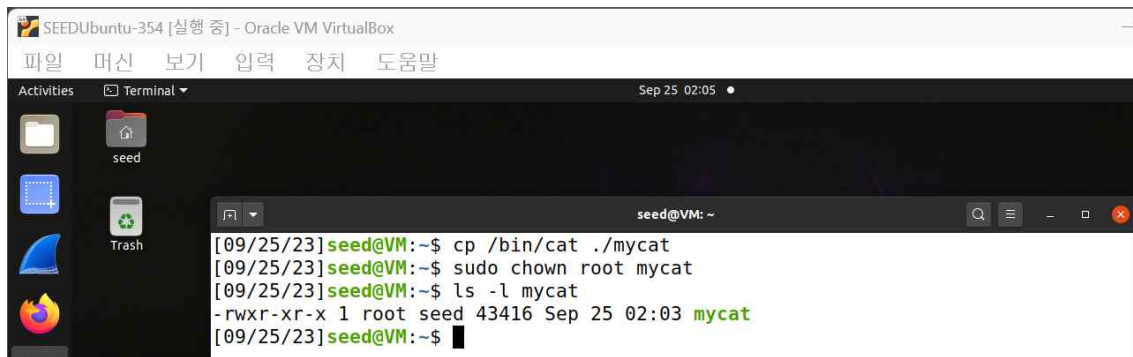
```
SEEDUbuntu-354 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities Terminal Sep 25 01:43
seed
Trash
[09/25/23] seed@VM: ~$ sudo chmod 4775 myid
[09/25/23] seed@VM: ~$ ./myid
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
[09/25/23] seed@VM: ~$
```

sudo chmod 4775 myid

: myid 파일에 SUID 비트를 설정하고, 소유자와 그룹에 대해서는 읽기, 쓰기, 실행 권한을 부여하는 명령어 (다른 사용자에게는 읽기와 실행 권한만 부여)

./myid

: 이전에 권한을 변경한 myid 파일을 실행 (SUID 비트가 설정되었기 때문에 해당 파일은 소유자의 권한으로 실행됨)



cp /bin/cat ./mycat

: /bin/cat 파일을 현재 작업 디렉토리로 복사하고, 복사한 파일의 이름을 mycat으로 지정

sudo chown root mycat

: mycat 파일의 소유자를 변경하는데, 파일을 root 사용자로 소유하도록 변경

ls -l mycat

: 현재 디렉토리에 있는 파일 중 mycat 파일의 상세 정보를 나열

2. 느낀점 적기

sudo chown과 sudo chmod 등의 명령어를 사용하여 파일의 권한과 소유자를 변경해보며 이를 통해 파일에 대한 접근 및 실행 권한을 제어하고, 파일을 다른 사용자의 소유로 만들 수 있었다. 또 SUID 비트를 사용하여 실행 파일이 특정 사용자의 권한으로 실행되도록 설정해보기도 하였으며, 관련된 파일의 권한과 정보를 확인해보기도 하였다. 위와 같은 내용들을 악용하면 다양한 공격에 사용될 수 있겠다는 생각이 들었고, 보안적인 요소 추가의 필요성을 깨달을 수 있었다.