LAB 6

Secure coding lab

Ananthanarayanan S

CB.EN.P2CYS23007

Turn a program into set-Uid

Change the owner of a file to root

```
[08/16/23]seed@VM:~$ sudo cp /bin/cat ./mycat
[08/16/23]seed@VM:~$ sudo chown root mycat
[08/16/23]seed@VM:~$ ls -l mycat
-rwxr-xr-x+ 1 root seed 43416 Aug 16 05:22 mycat
```

Before and After Enabling Set -UID bit

```
[08/16/23]seed@VM:~$ sudo chown root mycat
[08/16/23]seed@VM:~$ ls -l mycat
-rwxr-xr-x+ 1 root seed 43416 Aug 16 05:22 mycat
[08/16/23]seed@VM:~$ mycat /etc/shadow
mycat: /etc/shadow: Permission denied
[08/16/23]seed@VM:~$ sudo chmod 4755 mycat
[08/16/23]seed@VM:~$ mycat /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:::
```

```
[08/16/23]seed@VM:~$ sudo chown seed mycat
[08/16/23]seed@VM:~$ sudo chmod 4755 mycat
[08/16/23]seed@VM:~$ mycat /etc/shadow
mycat: /etc/shadow: Permission denied
```

It is still a privileged program, but not the root privilege

2. id

```
[08/16/23]seed@VM:~$ sudo cp /bin/id ./myid
[08/16/23]seed@VM:~$ ls -l
total 124
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Desktop
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Documents
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Downloads
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Music
-rw-rw-r--  1 seed seed     0 Aug 15 13:53 myca
-rwsr-xr-x+ 1 root seed 43416 Aug 16 05:22 mycat
-rwxr-xr-x  1 root root 47480 Aug 16 06:05 myid
-rw-------  1 seed seed     0 Aug 15 13:59 nee
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Pictures
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Public
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Templates
drwxr-xr-x  2 seed seed  4096 Nov 24  2020 Videos
[08/16/23]seed@VM:~$ ls -l ./myid
-rwxr-xr-x 1 root root 47480 Aug 16 06:05 ./myid
[08/16/23]seed@VM:~$ sudo chown root myid
[08/16/23]seed@VM:~$ ls -l ./myid
-rwxr-xr-x 1 root root 47480 Aug 16 06:05 ./myid
[08/16/23]seed@VM:~$ sudo chown seed myid
[08/16/23]seed@VM:~$ ls -l ./myid
-rwxr-xr-x 1 seed root 47480 Aug 16 06:05 ./myid
[08/16/23]seed@VM:~$ sudo chown root myid
[08/16/23]seed@VM:~$ id
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(docke
r)
[08/16/23]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(docke
r)
[08/16/23]seed@VM:~$ sudo chmod +s myid
[08/16/23]seed@VM:~$ ls -l ./myid
-rwsr-sr-x 1 root root 47480 Aug 16 06:05 ./myid
```

```
[08/16/23]seed@VM:~$ myid
uid=1000(seed) gid=1000(seed) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),13
2(sambashare),136(docker),1000(seed)
[08/16/23]seed@VM:~$
```

We have chosen the function id here. We are copying the functions of cat command into the myid file. Then changed the ownership from seed to root. And accessing this file gives the same result as normal id. Setting Uid in this file changes the EUid if seed to root's id, i.e zero. The change of alphabet 'x' which stands for executable changes to 's'. This indicates that Uid has been to the respective file