SETUID and Attacks

Rahul M Menon
CB.EN.P2CYS23015

Mycat

Change the owner of the 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 05:23 mycat
[08/16/23]seed@VM:~$
```

Before enabling setuid

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

After enabling setuid

```
[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:::
```

CP

We have chosen the function **cp-copy** here.

We are copying the functions of the cp command into the **mycp** file.

```
[09/01/23]seed@VM:~$ cp /bin/cp ./mycp
[09/01/23]seed@VM:~$ ls -l
total 1164
drwxr-xr-x  2 seed seed   4096 Aug 24 06:01 Desktop
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Documents
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Downloads
-rwxr-xr-x  1 seed seed 878288 Aug 24 06:07 ls
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Music
-rwsr-xr-x  1 root seed  43416 Aug 16 05:23 mycat
-rwxr-xr-x  1 seed seed 153976 Sep  1 12:41 mycp
-rwsr-sr-x  1 root seed  47480 Aug 16 05:55 myid
-rw-rw-r--+ 1 bob  seed      0 Aug 15 13:57 newfile
-rw-r-----+ 1 seed seed      0 Aug 15 13:57 newfile1
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Public
```

Now we are changing the ownership of mycp file to root

```
[09/01/23]seed@VM:~$ sudo chown root mycp
[09/01/23]seed@VM:~$ ls -l mycp
-rwxr-xr-x 1 root seed 153976 Sep  1 12:41 mycp
[09/01/23]seed@VM:~$
```

When seed tries to acces it it shows permission denied now

```
[09/01/23]seed@VM:~$ mycp /etc/shadow .
mycp: cannot open '/etc/shadow' for reading: Permission denied
```

We change mycp to setuid file now

```
[09/01/23]seed@VM:~$ sudo chmod +s mycp
[09/01/23]seed@VM:~$ ls -l mycp
-rwsr-sr-x 1 root seed 153976 Sep  1 12:41 mycp
```

Now seed can function mycp function

```
[09/01/23]seed@VM:~$ mycp /etc/shadow .
[09/01/23]seed@VM:~$ ls -l
total 1168
drwxr-xr-x  2 seed seed   4096 Aug 24 06:01 Desktop
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Documents
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Downloads
-rwxr-xr-x  1 seed seed 878288 Aug 24 06:07 ls
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Music
-rwsr-xr-x  1 root seed  43416 Aug 16 05:23 mycat
-rwsr-sr-x  1 root seed 153976 Sep  1 12:41 mycp
-rwsr-sr-x  1 root seed  47480 Aug 16 05:55 myid
-rw-rw-r--+ 1 bob  seed      0 Aug 15 13:57 newfile
-rw-r-----+ 1 seed seed      0 Aug 15 13:57 newfile1
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Public
-rw-rw-r--  1 seed seed    503 Aug 24 14:01 SEC.c
-rw-r-----  1 root seed   1644 Sep  1 12:51 shadow
-rwsr-xr-x  1 root root  16696 Aug 24 06:06 system
-rw-rw-r--  1 seed seed     39 Aug 24 06:06 system.c
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x  2 seed seed   4096 Nov 24  2020 Videos
```

Now seed was able to copy shadow

```
[09/01/23]seed@VM:~$ cat 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:::
```

Id

```
[08/16/23]seed@VM:~$ sudo cp /bin/id ./myid
[08/16/23]seed@VM:~$ sudo chown root myid
[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),13
6(docker)
```

```
[08/16/23]seed@VM:~$ sudo chmod 4755 myid
[08/16/23]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(s
ambashare),136(docker)
```

```
[08/16/23]seed@VM:~$ ls -l myid
-rwsr-xr-x 1 root seed 47480 Aug 16 05:55 myid
[08/16/23]seed@VM:~$ sudo chmod +s myid
[08/16/23]seed@VM:~$ ls -l myid
-rwsr-sr-x 1 root seed 47480 Aug 16 05:55 myid
[08/16/23]seed@VM:~$
```

We have chosen the function id here. We are copying the functions of id 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.

Shell

we have chosed sh shell here and copied it to mysh

```
[09/01/23]seed@VM:~$ cp /bin/sh ./mysh
[09/01/23]seed@VM:~$ ls -l
total 2324
drwxr-xr-x  2 seed seed    4096 Aug 24 06:01 Desktop
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Documents
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Downloads
-rwxr-xr-x  1 seed seed  878288 Aug 24 06:07 ls
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Music
-rwsr-xr-x  1 root seed   43416 Aug 16 05:23 mycat
-rwsr-sr-x  1 root seed  153976 Sep  1 12:41 mycp
-rwsr-sr-x  1 root seed   47480 Aug 16 05:55 myid
-rwxr-xr-x  1 seed seed 1183448 Sep  1 13:25 mysh
-rw-rw-r--+ 1 bob  seed       0 Aug 15 13:57 newfile
-rw-r-----+ 1 seed seed       0 Aug 15 13:57 newfile1
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Pictures
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Public
-rw-rw-r--  1 seed seed     503 Aug 24 14:01 SEC.c
-rw-r-----  1 root seed    1644 Sep  1 12:51 shadow
-rwsr-xr-x  1 root root   16696 Aug 24 06:06 system
-rw-rw-r--  1 seed seed      39 Aug 24 06:06 system.c
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Templates
drwxr-xr-x  2 seed seed    4096 Nov 24  2020 Videos
```

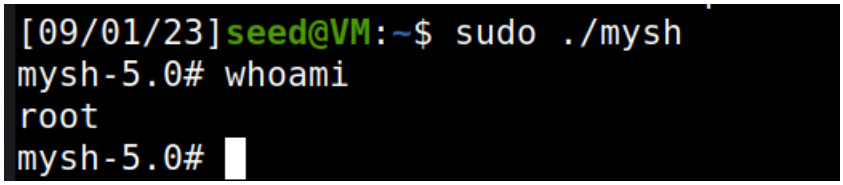
Now we change ownership to root

```
[09/01/23]seed@VM:~$ sudo chown root mysh
[09/01/23]seed@VM:~$ ls -l mysh
-rwxr-xr-x 1 root seed 1183448 Sep  1 13:25 mysh
```

Now we changed it to setuid

```
[09/01/23]seed@VM:~$ sudo chmod +s mysh
[09/01/23]seed@VM:~$ ls -l mysh
-rwsr-sr-x 1 root seed 1183448 Sep  1 13:25 mysh
```

Seed can now use the mysh terminal


[09/01/23]seed@VM:~$ sudo ./mysh
mysh-5.0# whoami
root
mysh-5.0#