SET UID PRIVILEGED PROGRAMS

Muhammed Nifal V

Assignment 6 CB.EN.P2CYS23017

1. **CAT – Used for concatenate**

Here we are copying the functions of CAT command to the nifal file.

```
[09/03/23]seed@VM:~$ cp /bin/cat ./nifal
[09/03/23]seed@VM:~$ ls -l
total 120
drwxr-xr-x 2 seed seed  4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed 43416 Sep  3 01:59 mycat
-rwxr-xr-x 1 seed seed 43416 Sep  3 02:06 nifal
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
[09/03/23]seed@VM:~$
```

To change the ownership pf the file from seed to root

```
[09/03/23]seed@VM:~$ sudo chown root nifal
[09/03/23]seed@VM:~$ ls -l
total 120
drwxr-xr-x 2 seed seed  4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed 43416 Sep  3 01:59 mycat
-rwxr-xr-x 1 root seed 43416 Sep  3 02:06 nifal
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
[09/03/23]seed@VM:~$
```

As the ownership was changed from seed to root, seed cannot access the file without root's privilege.

```
[09/03/23]seed@VM:~$ nifal /etc/shadow
nifal: /etc/shadow: Permission denied
[09/03/23]seed@VM:~$
```

This file can be accessed only when the EUid = 0(root's 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.

```
[09/03/23]seed@VM:~$ nifal /etc/shadow
nifal: /etc/shadow: Permission denied
[09/03/23]seed@VM:~$ sudo chmod +s nifal
[09/03/23]seed@VM:~$ ls -l
total 120
drwxr-xr-x 2 seed seed  4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed 43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 43416 Sep  3 02:06 nifal
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
[09/03/23]seed@VM:~$ nifal /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:::
```

This should enable the seed to perform mycat function as root

2. CP

We have chosen the function cp-copy here. We are copying the functions of the cp command into the mycp file.

```
[09/03/23]seed@VM:~$ cp /bin/cp ./mycp
[09/03/23]seed@VM:~$ ls -l
total 272
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwxr-xr-x 1 seed seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
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
```

To change the ownership from seed to root

```
[09/03/23]seed@VM:~$ sudo chown root mycp
[09/03/23]seed@VM:~$ ls -l
total 272
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwxr-xr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
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
[09/03/23]seed@VM:~$
```

As the ownership was changed from seed to root, seed cannot access the file without root's privilege.

```
[09/03/23]seed@VM:~$ mycp /etc/shadow .
mycp: cannot open '/etc/shadow' for reading: Permission denied
```

This file can be accessed only when the EUid = 0(root's 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.

```
[09/03/23]seed@VM:~$ sudo chmod +s mycp
[09/03/23]seed@VM:~$ ls -l
total 272
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
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
[09/03/23]seed@VM:~$
```

This should enable the seed to perform mycp function as root.

```
[09/03/23]seed@VM:~$ mycp /etc/shadow .
[09/03/23]seed@VM:~$ ls -l
total 276
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
[Show Applications eed@VM:~$
```

Here mycp enabled us to copy the shadow file and place it in the present directory

```
[09/03/23]seed@VM:~$ cat shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
```

3.ID

We have chosen the function id here. We are copying the functions of id command into the myid file.

```
[09/03/23]seed@VM:~$ cp /bin/id ./myid
[09/03/23]seed@VM:~$ ls -l
total 324
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwxr-xr-x 1 seed seed  47480 Sep  3 02:34 myid
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
```

Ownership from seed to root

```
[09/03/23]seed@VM:~$ sudo chown root myid
[09/03/23]seed@VM:~$ ls -l
total 324
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwxr-xr-x 1 root seed  47480 Sep  3 02:34 myid
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
```

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

```
[09/03/23]seed@VM:~$ sudo chmod +s myid
[09/03/23]seed@VM:~$ ls -l
total 324
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  47480 Sep  3 02:34 myid
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
[09/03/23]seed@VM:~$
```

4. Shell

We have chosen the function sh-shell here.

We are copying the functions of sh command into the mysh file.

```
[09/04/23]seed@VM:~$ cp /bin/sh ./mysh
cp: cannot create regular file './mysh': Permission denied
[09/04/23]seed@VM:~$ sudo cp /bin/sh ./mysh
[09/04/23]seed@VM:~$ sudo chown root mysh
[09/04/23]seed@VM:~$ ls -l
total 2152
-rw-rw-r-- 1 seed seed     18 Sep  3 14:12 amrita.txt
-rw-rw-r-- 1 seed seed     15 Sep  3 14:12 cyber.txt
drwxr-xr-x 6 seed seed   4096 Sep  3 14:33 Desktop
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Documents
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Downloads
-rwxrwxr-x 1 seed seed  17192 Sep  3 14:20 group
-rw-rw-r-- 1 seed seed    757 Sep  3 14:20 group.c
-rwxr-xr-x 1 seed seed 878288 Sep  3 12:41 ls
-rwxrwxr-x 1 seed seed  17136 Sep  3 14:11 merge
-rw-rw-r-- 1 seed seed    653 Sep  3 14:10 merge.c
-rw-rw-r-- 1 seed seed    117 Sep  3 14:14 merged.txt
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Music
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  47480 Sep  3 02:34 myid
-rwxrwxr-x 1 seed seed  16920 Sep  3 13:53 myprint
-rw-rw-r-- 1 seed seed   1199 Sep  3 13:53 myprint.c
-rwxr-xr-x 1 root seed 878288 Sep  4 01:41 mysh
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rwsr-xr-x 1 root root  16696 Sep  3 12:40 sample
-rw-rw-r-- 1 seed seed     39 Sep  3 12:39 sample.c
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
```

Now we are the ownership from seed to root.

```
[09/03/23]seed@VM:~$ sudo chown root mysh
[09/03/23]seed@VM:~$ ls -l
total 452
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  47480 Sep  3 02:34 myid
-rwxr-xr-x 1 root seed 129816 Sep  3 02:41 mysh
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
```

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.

```
[09/03/23]seed@VM:~$ sudo chmod +s mysh
[09/03/23]seed@VM:~$ ls -l
total 452
drwxr-xr-x 2 seed seed   4096 Sep  3 00:50 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
-rwxr-xr-x 1 seed seed  43416 Sep  3 01:59 mycat
-rwsr-sr-x 1 root seed 153976 Sep  3 02:18 mycp
-rwsr-sr-x 1 root seed  47480 Sep  3 02:34 myid
-rwsr-sr-x 1 root seed 129816 Sep  3 02:41 mysh
-rwsr-sr-x 1 root seed  43416 Sep  3 02:06 nifal
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Public
-rw-r----- 1 root seed   1646 Sep  3 02:28 shadow
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed   4096 Nov 24  2020 Videos
[09/03/23]seed@VM:~$ ./mysh
$ whoami
seed
$
```

This lets seed to enable a separate shell within the terminal and perform all functions as root.

```
$ 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)
$
```