Lab Report - SEED Labs – Dirty COW Attack Lab

Name: Kostia Kazakov

ID: 321827834

Task 1: Modify a Dummy Read-Only File

In this task, we create a dummy file which will be read only to us , the file will contain "111111222222333333", our final objective is to replace the pattern "222222" with "******".

```
Terminal
[11/16/2018 14:32] seed@ubuntu:~$ sudo touch /zzz
[sudo] password for seed:
[11/16/2018 14:32] seed@ubuntu:~$ sudo chmod 644 /zzz
[11/16/2018 14:33] seed@ubuntu:~$ sudo gedit /zzz
[11/16/2018 14:33] seed@ubuntu:~$ cat /zzz
111111222222333333
[11/16/2018 14:33] seed@ubuntu:~$  ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 16 14:33 /zzz
[11/16/2018 14:34] seed@ubuntu:~$ echo 99999 > /zzz
bash: /zzz: Permission denied
[11/16/2018 14:34] seed@ubuntu:~$  gcc cow_attack.c -lpthread
gcc: error: cow_attack.c: No such file or directory
[11/16/2018 14:37] seed@ubuntu:~$ cd Desktop/
[11/16/2018 14:37] seed@ubuntu:~/Desktop$  gcc cow_attack.c -lpthread
[11/16/2018 14:37] seed@ubuntu:~/Desktop$ ./a.out
```

After few seconds, we can observe that our string has been appended:

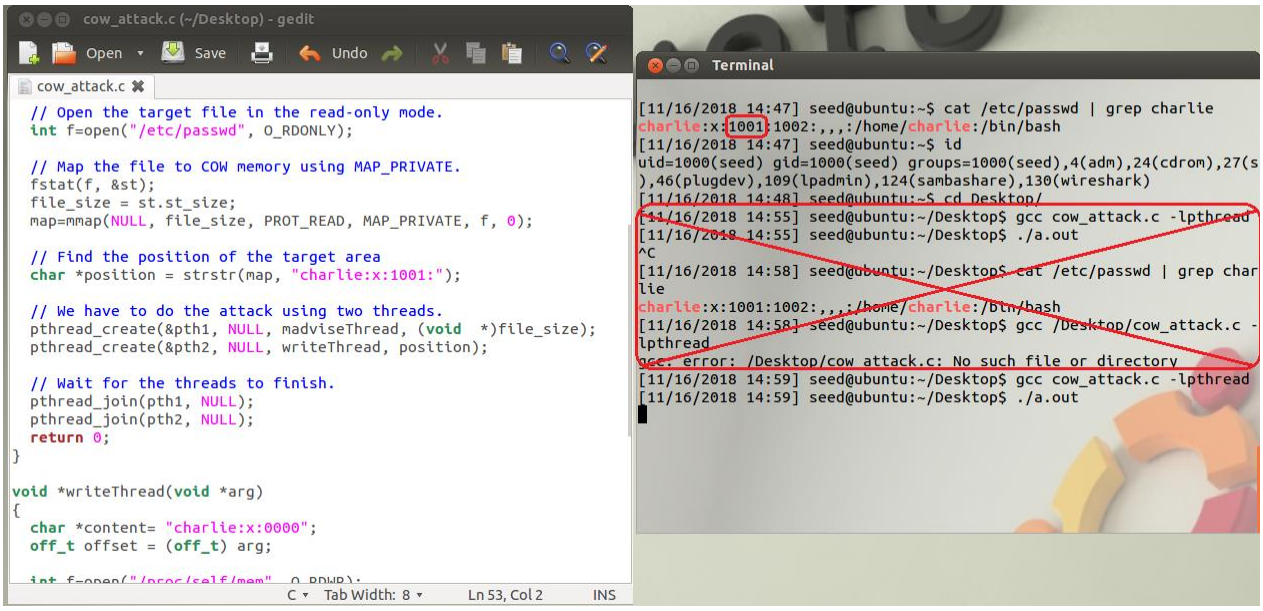
```
[11/16/2018 14:37] seed@ubuntu:~/Desktop$  gcc cow_attack.c -lpthread
[11/16/2018 14:37] seed@ubuntu:~/Desktop$ ./a.out
^C
[11/16/2018 14:39] seed@ubuntu:~/Desktop$ cd ..
[11/16/2018 14:39] seed@ubuntu:~$ cat /zzz
111111******333333
[11/16/2018 14:39] seed@ubuntu:~$
```

Ditry COW exploits a race condition in Linux Kernel. There is a race condition on the logic of copy-on write which enables attackers to write to the memory that actually maps to read-only file.

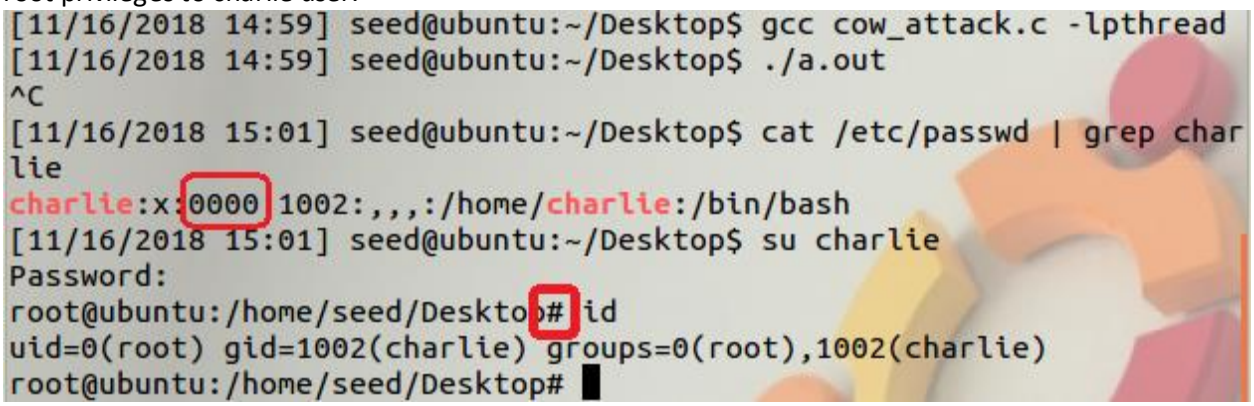
Task 2: Modify the Password File to Gain the Root Privilege

In this task, we'll use dirty cow vulnerability to attack /etc/passwd file.

We first create a new user named "charlie" which is not root user, then modify the attack file from task 1 to match our demands, and start to attack:



We used our cow_attack.c program to perform the attack on passwd file and we are successful in giving root privileges to charlie user.



We have successfully exploited the Dirty COW vulnerability to make changes to our /etc/passwd file. Race condition of copy-on-write gets exploited and we get the root access.