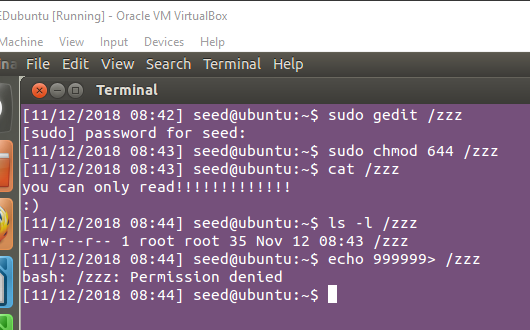
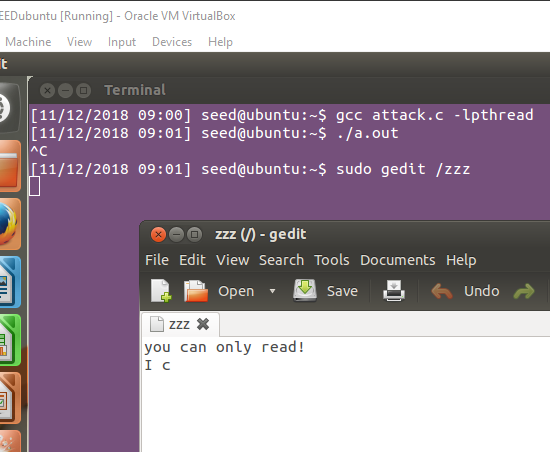
**Name:** Alexey Titov

**Dirty COW Attack Lab**

***Task 1: Modify a Dummy Read-Only File***



**Observation:** I create a file called zzz in the root directory, change its permission to read-only for normal users, and put content into the file: “you can only read!!!!!!!!!!!! 😊” .

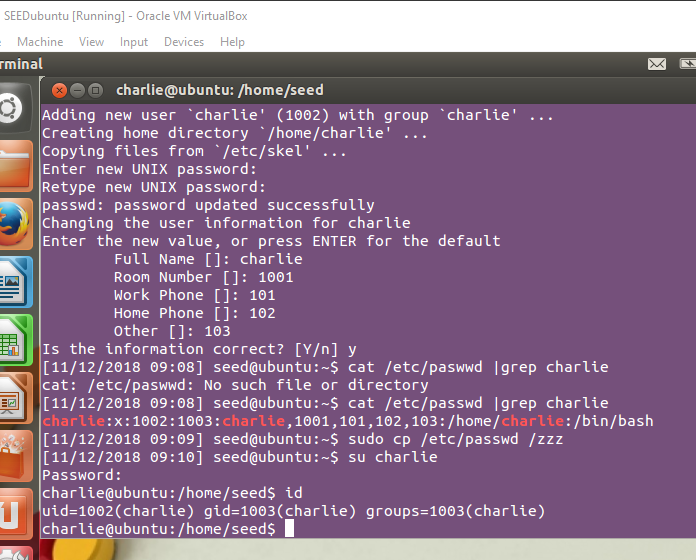




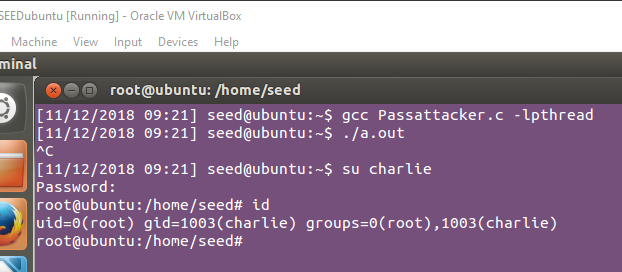
**Observation:** I compile the *attack.c* and run it for a few seconds. Now, we can observe that our string has been appended.

**Explanation:** Dirty 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***



**Observation:** I create a new account called *Charlie.* After, i copy contents of */etc/passwd* file into */zzz* and attack.





**Observation:** I use my *Passattacker.c* program to perform the attack on /etc/*passwd* file and I am successful in giving root privileges to *charlie* user.

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