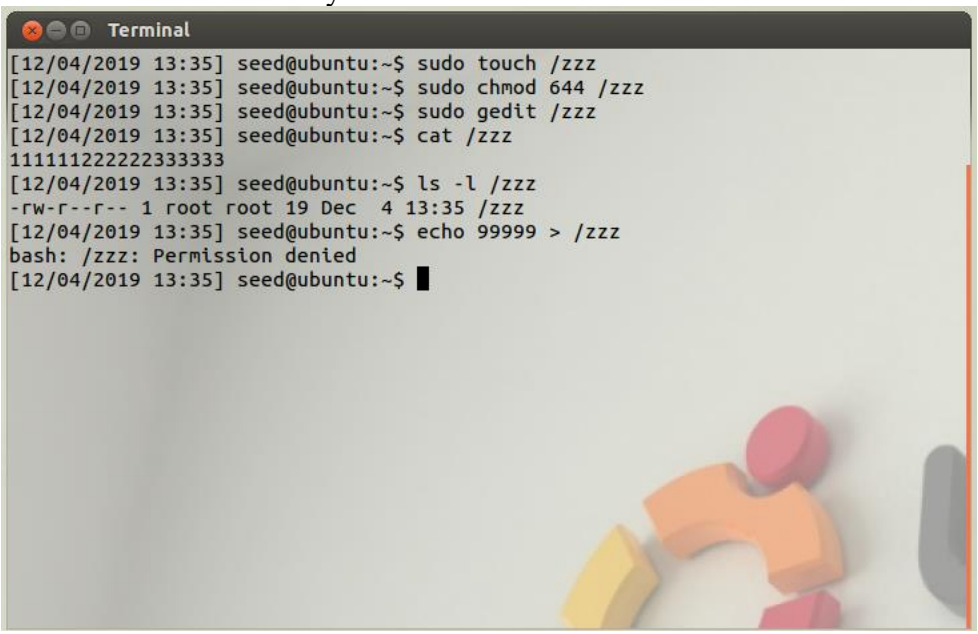
Lab 4: Dirty COW Attack Lab

Samuel Shen Prof. Kadri Brogi
CUNY John Jay College of Criminal Justice
November 6, 2019

1. Introduction
   Today, we will investigate and experience with the Dirty COW vulnerability. Dirty COW vulnerability is similar to the race condition vulnerability and existed in the Linux kernel since the September 2007. This vulnerability was discovered and exploited in October 2016.

   In order, for us to experiment with this vulnerability, we will be using the following:
   - SeedLab Ubuntu 12.04 VM
   - The Provided vulnerable file: cow_attack.c

2. Task 1: Modify a Dummy Read-Only File
   In this task, we run a test dirty COW attack on a dummy read-only file. We will create "/zzz", add "111111222222333333" and attempt to change "222222" to "******". The first thing we will do is create the file it, add the text, change to read-only, and attempt to edit it to ensure the file is read-only:



   Once we have our file as read-only, we will now launch "cow_attack.c" to change the text "222222" to "******":

```
Terminal
[12/04/2019 13:36] seed@ubuntu:~$ gcc cow_attack.c -lpthread
[12/04/2019 13:36] seed@ubuntu:~$ ./a.out
^C
[12/04/2019 13:36] seed@ubuntu:~$ cat /zzz
111111******333333
[12/04/2019 13:36] seed@ubuntu:~$
```

3. Task 2: Modify the password File to Gain the Root Privilege
   Since we were successful in changing “222222” to “******” we will now launch it on something more real. We will create a new user called “Charlie” and attempt to get root access.

```
Terminal
[12/04/2019 13:37] seed@ubuntu:~$ sudo adduser charlie
Adding user `charlie' ...
Adding new group `charlie' (1002) ...
Adding new user `charlie' (1001) with group `charlie' ...
Creating home directory `/home/charlie' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for charlie
Enter the new value, or press ENTER for the default
        Full Name []: charlie
        Room Number []: 100
        Work Phone []: 101
        Home Phone []: 102
        Other []: 103
Is the information correct? [Y/n] Y
[12/04/2019 13:37] seed@ubuntu:~$ cat /etc/passwd | grep charlie
charlie:x:1001:1002:charlie,100,101,102,103:/home/charlie:/bin/bash
[12/04/2019 13:38] seed@ubuntu:~$
```

   Once we have created the user Charlie, we can see that Charlie is just a standard user from “charlie:x:1001:”. We will now launch the attack on “/etc/passwd” to change charlie from standard user to root.

As you can see from the screenshot above, we have modified cow_attack.c to launch to /etc/passwd. Once it ran, we changed user to charlie and can notice that charlie now has root access.