



Sri Lanka Institute of Information Technology

IE2012 - Systems and Network Programming

Final Assignment

Name: Peiris W.S.S.N

Registration Number: IT23227286

Table of Contents

1	Basics of Linux Environments.....	3
1.1	Virtual Machine Setup.....	3
1.2	Command Line Introduction.....	23
1.3	System Information and User Management.....	29
2	DHCP, DNS and NTP Services.....	33
2.1	DHCP (Dynamic Host Configuration Protocol)	33
2.2	DNS (Domain Name System).....	40
2.3	NTP (Network Time Protocol).....	45
3	Shell Scripting and Security.....	48
3.1	Shell Scripting	48
3.2	SSH (Secure Shell).....	55
3.3	IPtables and ACLs.....	58
3.3.1	Web Server Security.....	58
3.3.2	Remote Administration Access	58
3.3.3	Allow Specific Applications	59
3.3.4	Allow Pings.....	59
3.3.5	Printer Server Access	59
4	Best practices	60
4.1	Disable Unused Network Interfaces.....	60
4.2	Enable a Firewall.....	60
4.3	Disable IPv6 if Not Needed	61
4.4	Limit Network Service Exposure.....	62
4.5	Configure Network Interface Security Settings	63

1 Basics of Linux Environments

1.1 Virtual Machine Setup

Go to this link <https://www.virtualbox.org/wiki/Downloads> and download virtual machine setup and go through the setup.



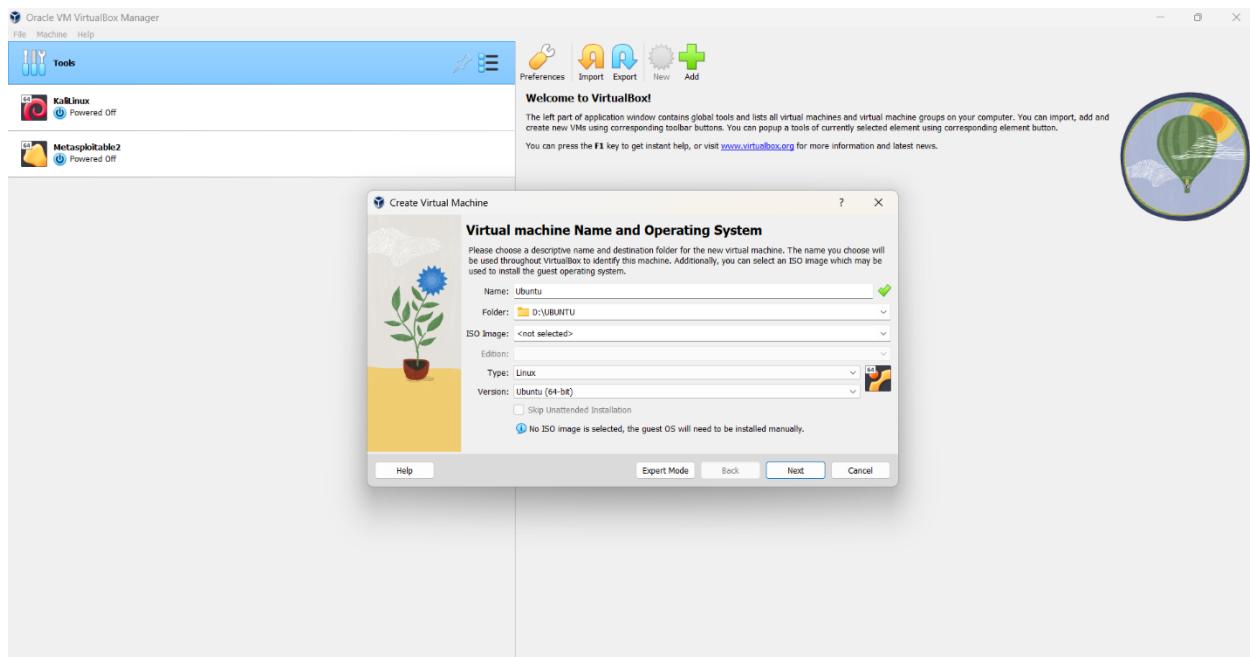
Below screenshot shows VirtualBox software after installation. I have already installed VirtualBox and added Kali Linux and Metasploitable2.



To download Ubuntu go through this link <https://ubuntu.com/download/desktop> and press “Download 24.04.1 LTS” button. Then an iso file will start downloading.

The screenshot shows the Ubuntu download page. At the top, there's a navigation bar with links like 'Products', 'Use cases', 'Support', 'Community', 'Get Ubuntu', 'All Canonical', 'Sign in', and a search bar. Below the navigation bar, there are tabs for 'Downloads' (selected), 'Desktop', 'Server', 'Core', and 'Cloud'. The main content area has a heading 'Download Ubuntu Desktop' and a sub-section for 'Ubuntu 24.04.1 LTS'. It includes a large orange crown icon, a 'Download 24.04.1 LTS' button (5.8GB), and a note about LTS support. There are also links for 'What's new', 'System requirements', 'How to install', and a note about the new desktop installer.

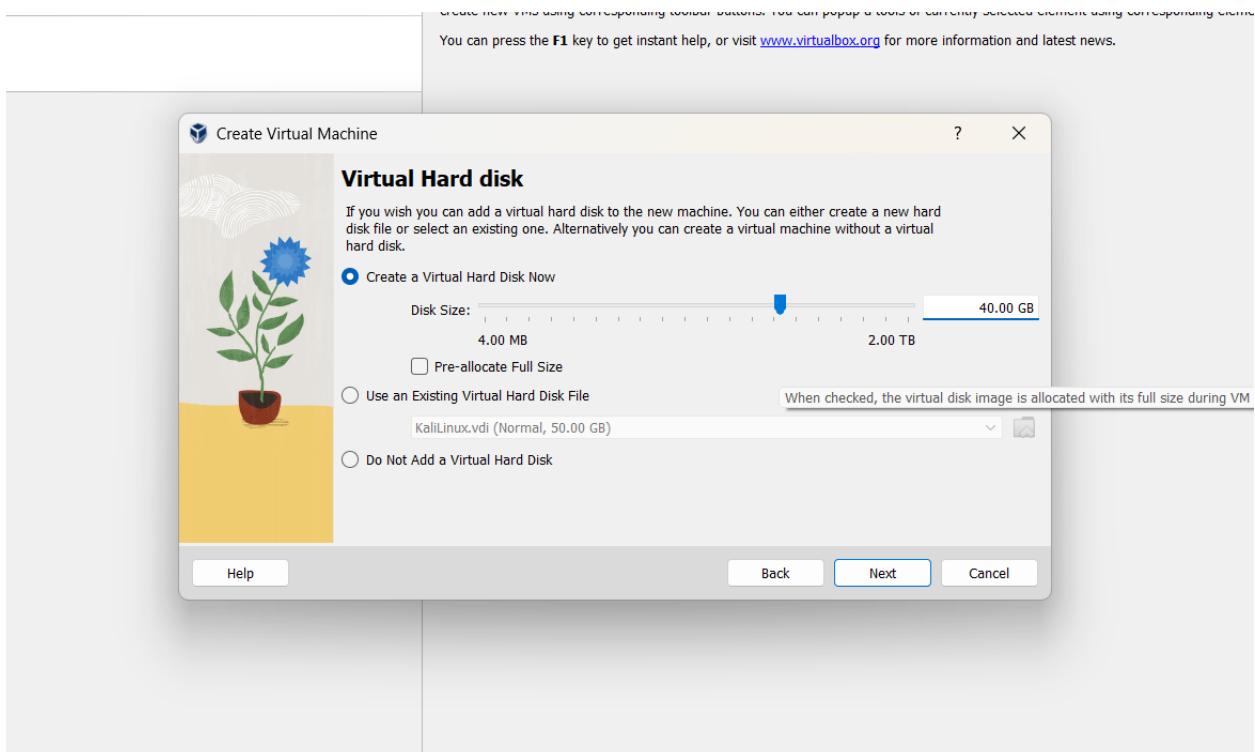
After downloading the iso file open virtualbox and press new button. In the create virtual machine window put a name and a folder to install Ubuntu. Automatically type will be selected to Linux and the version to Ubuntu (64-bit). Then select next to configure hardware.



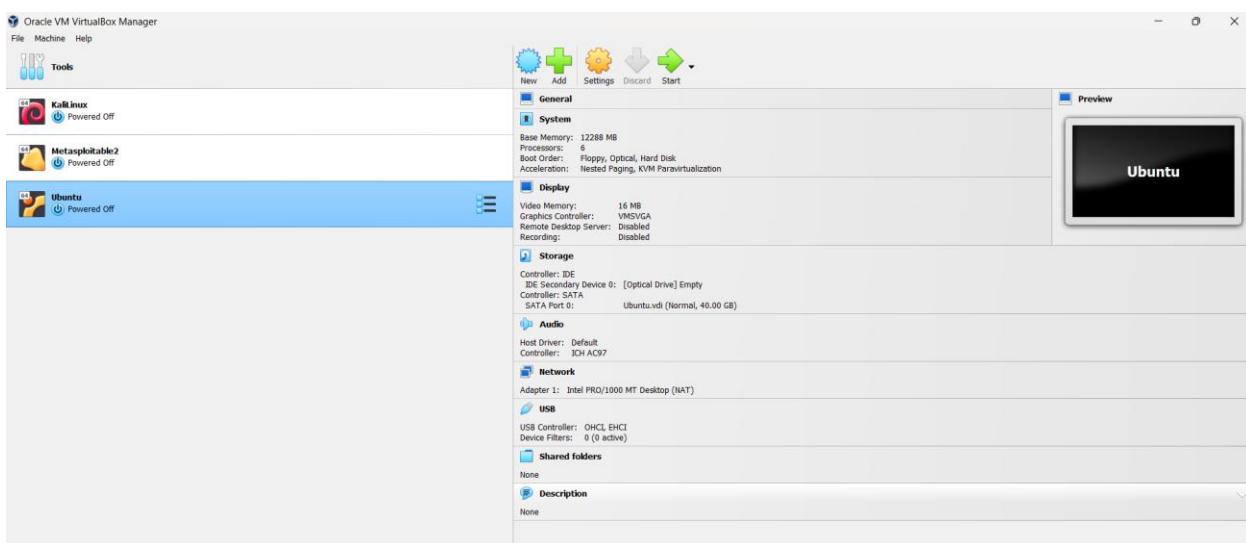
In the hardware section select a suitable base memory for Ubuntu considering the amount of RAM installed in your device. I have selected 12GB ram for faster installation. Then select the amount of CPUs you want to allocate for Ubuntu I have selected 6 CPUs. In both base memory

and processors sections make sure you select a number inside the green part of the line. Then select next to configure virtual hard disk.

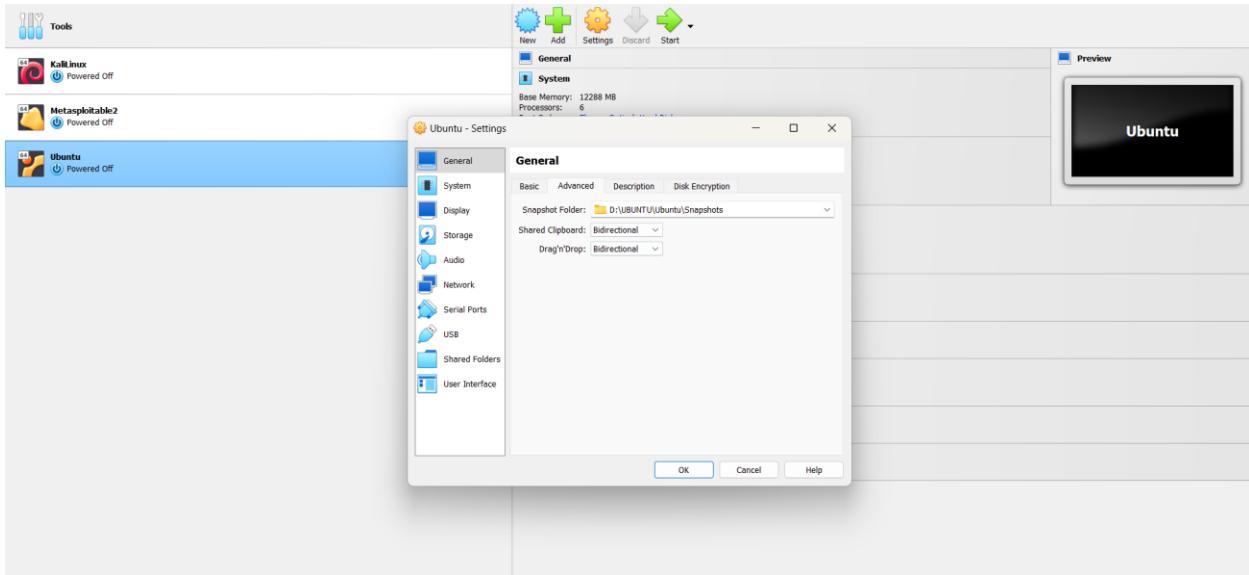
Select create a virtual hard disk now. Then select enough disk size to accommodate the Ubuntu OS. I chose to give 40GB.



Select next to see the summary and press finish.

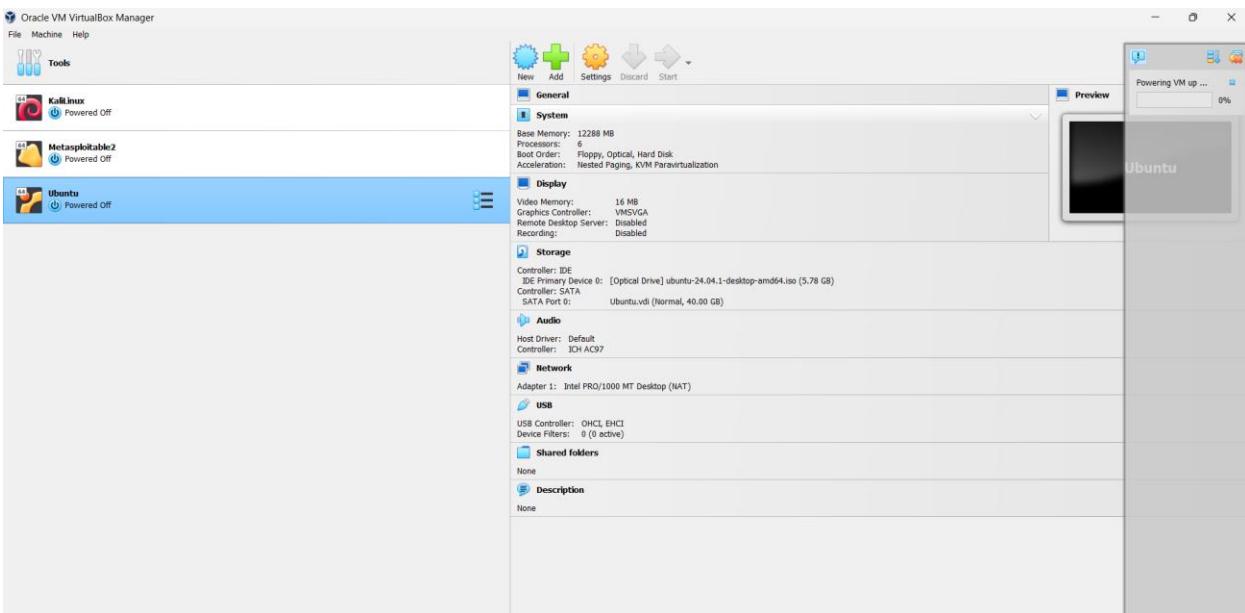
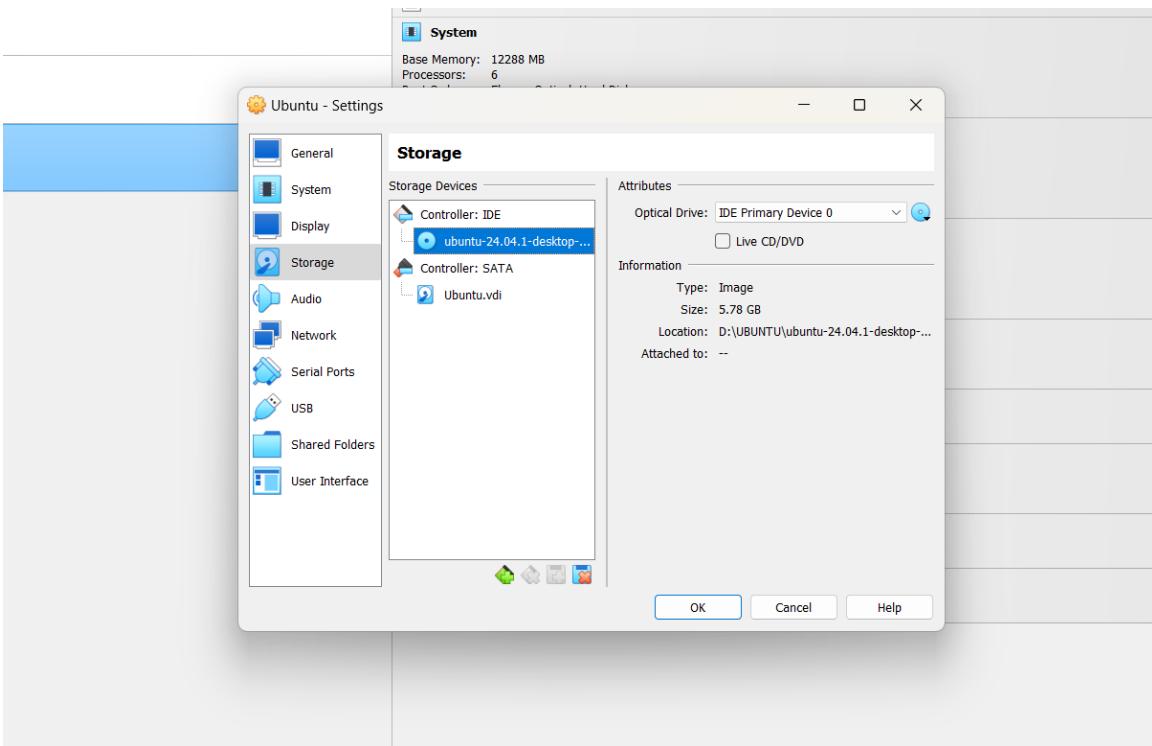


Go to settings of Ubuntu by selecting Ubuntu and pressing settings icon. In “General” section select Advanced tab change shared clipboard and Drag’n’Drop to Bidirectional from Disabled.



This will enable copy/paste and drag and drop functions across Ubuntu and the Windows. Then select storage. Under controller: IDE click on the empty disc. Then under attributes select optical drive by selecting the disc icon. Then select the relevant iso file containing Ubuntu.

Then you can see the selected iso file under controller: IDE . Once that done click ok. Now we are ready to installUbuntu using virtualbox.

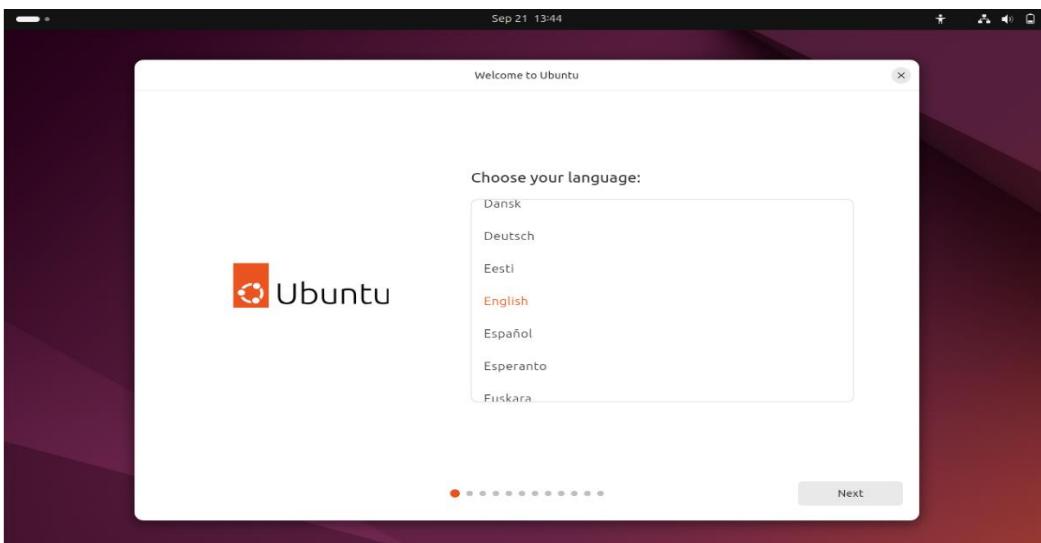


After selecting Ubuntu press start. Below steps will lead to a successful install.

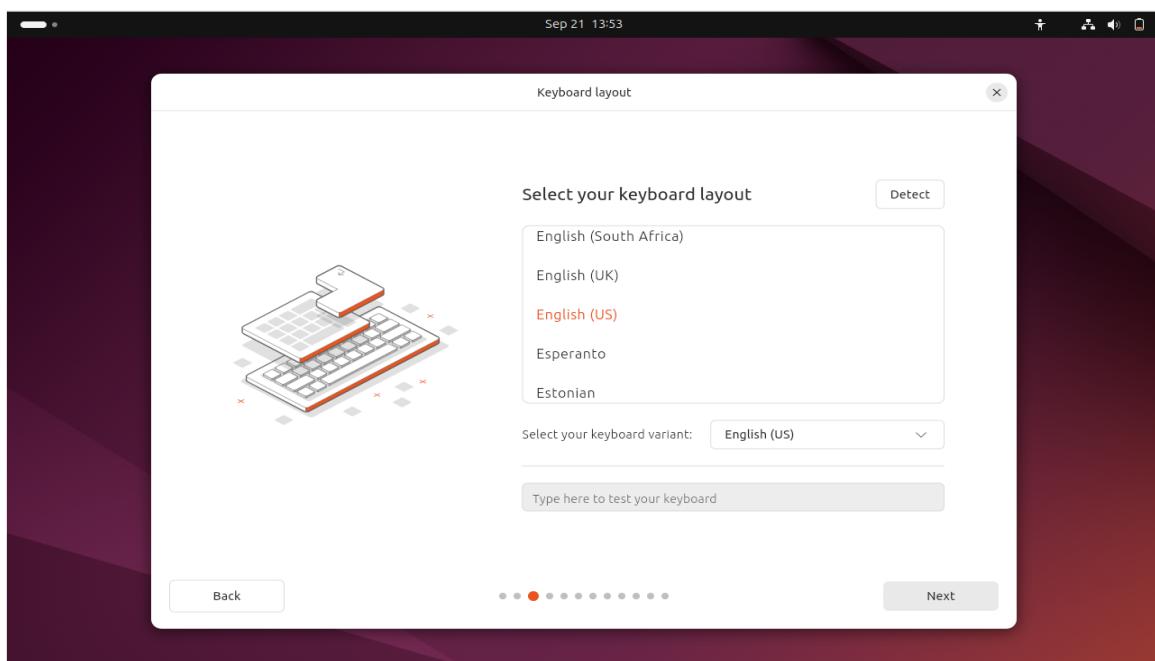
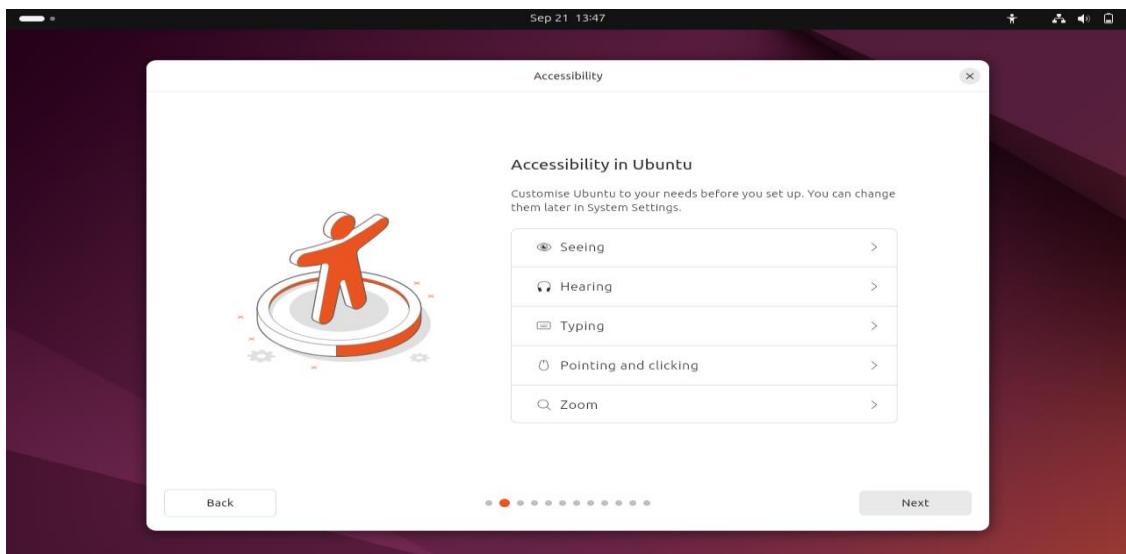


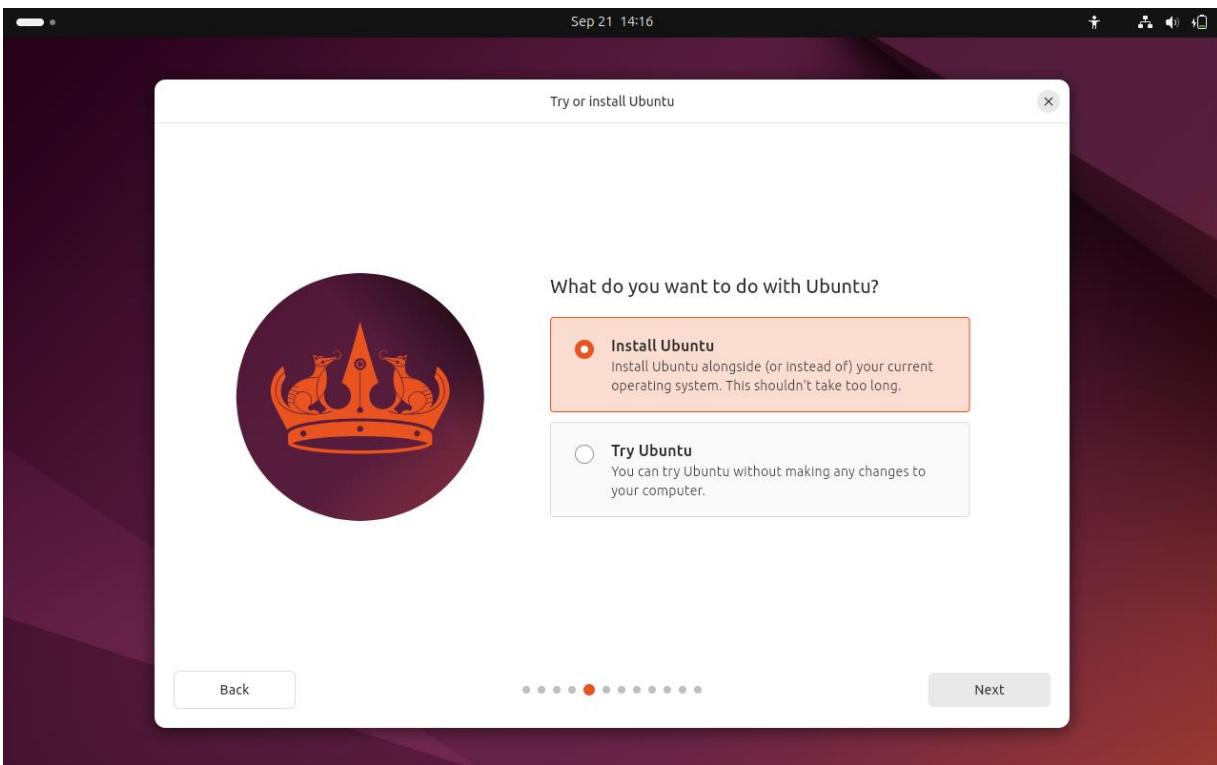
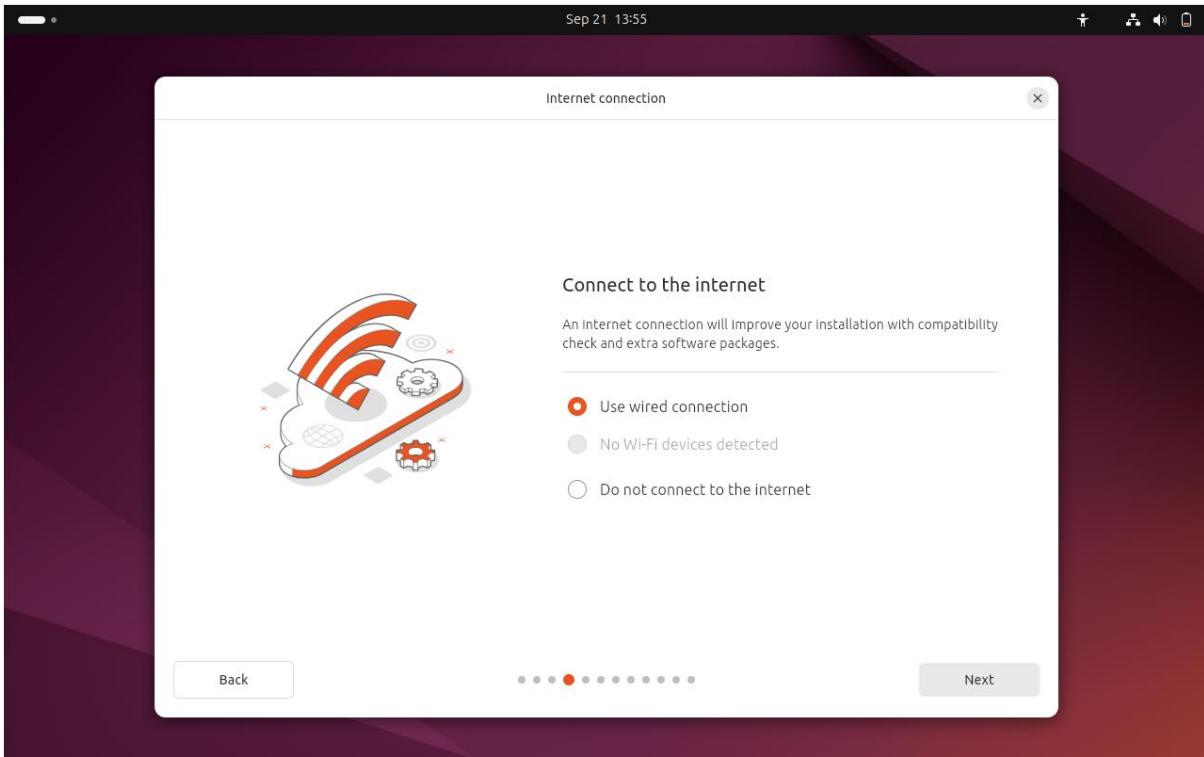
Select Try or Install Ubuntu here by pressing enter.

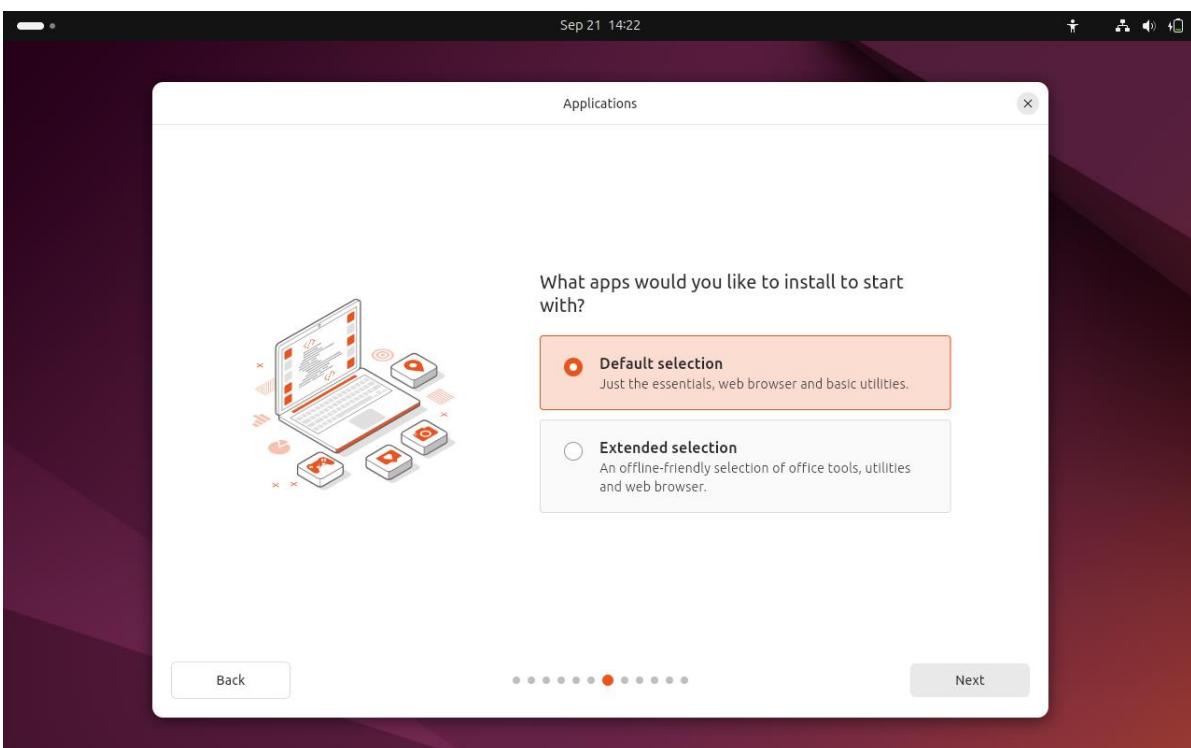
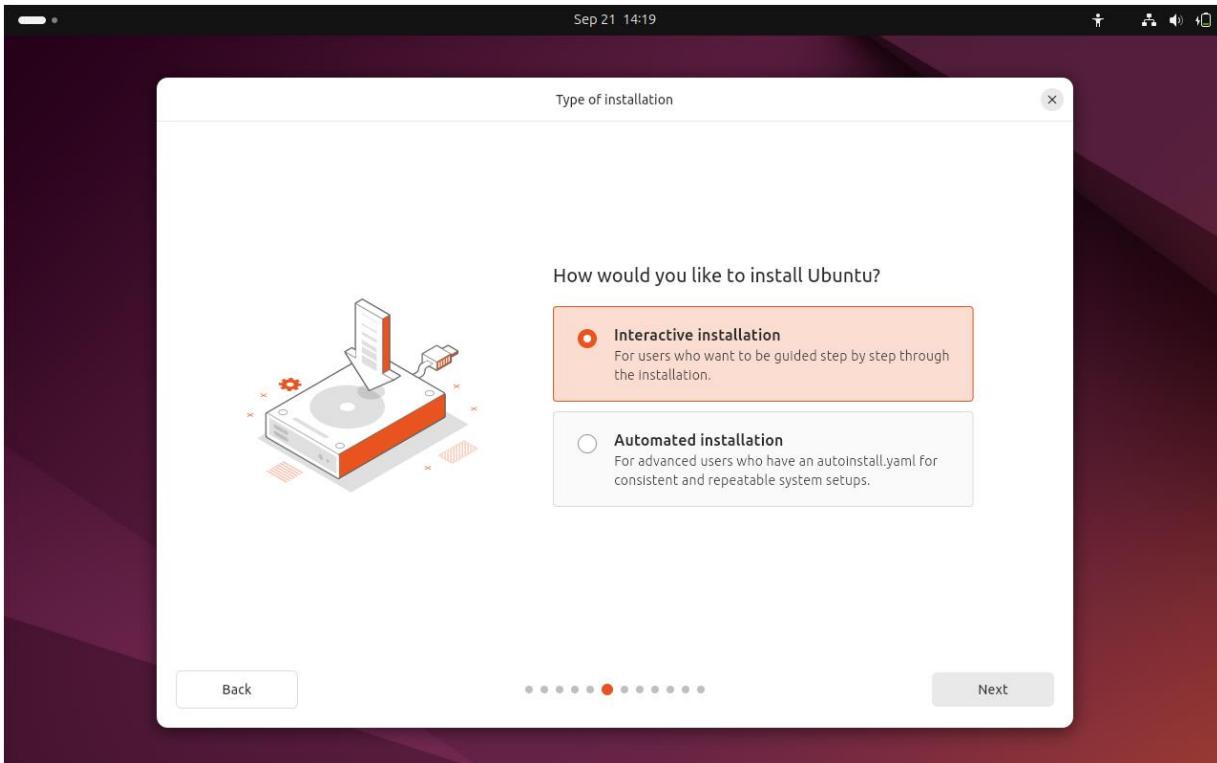
Select English and press next.



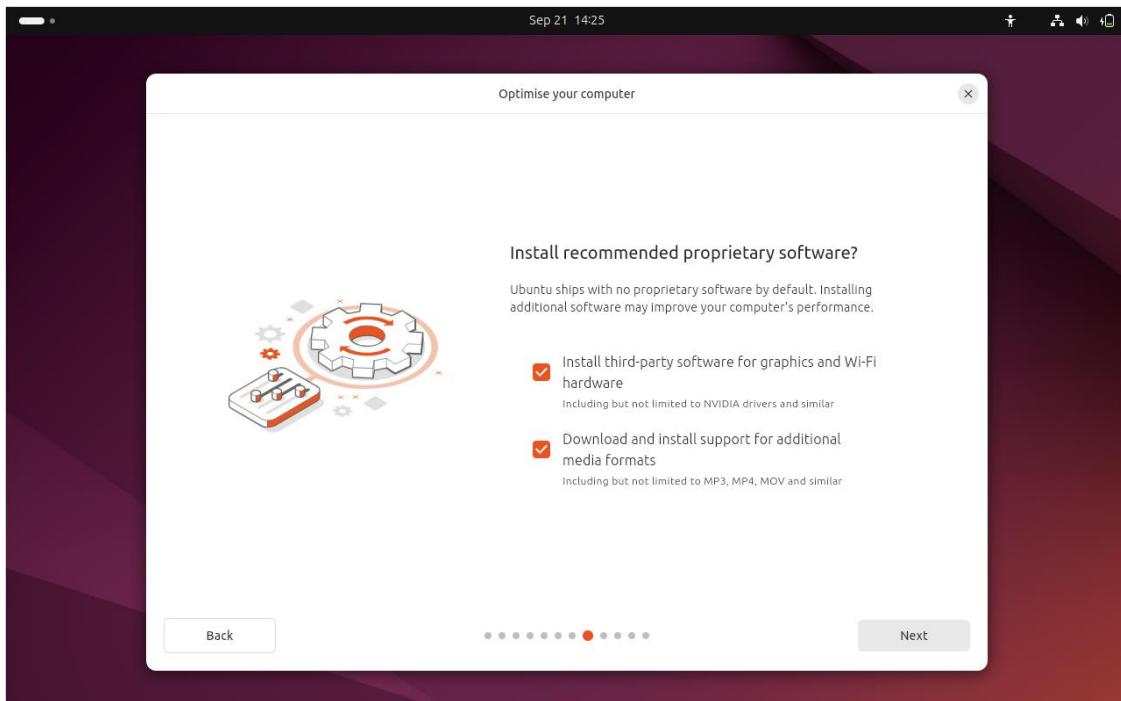
Select the accessibility settings to your liking. I didn't change anything here because everything is according to my preference here.



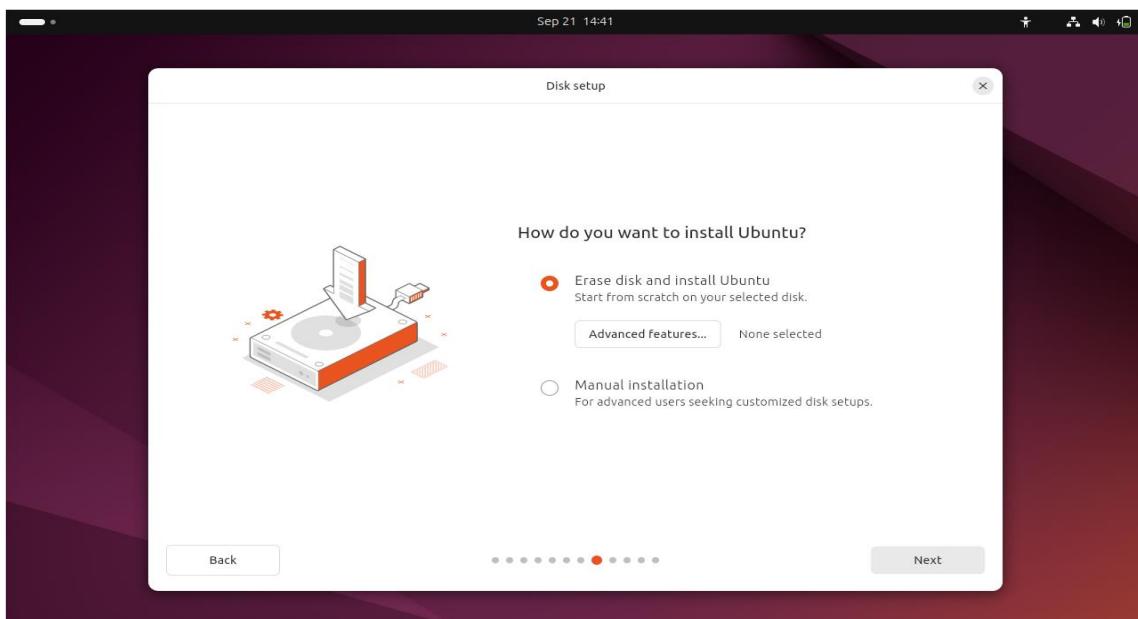




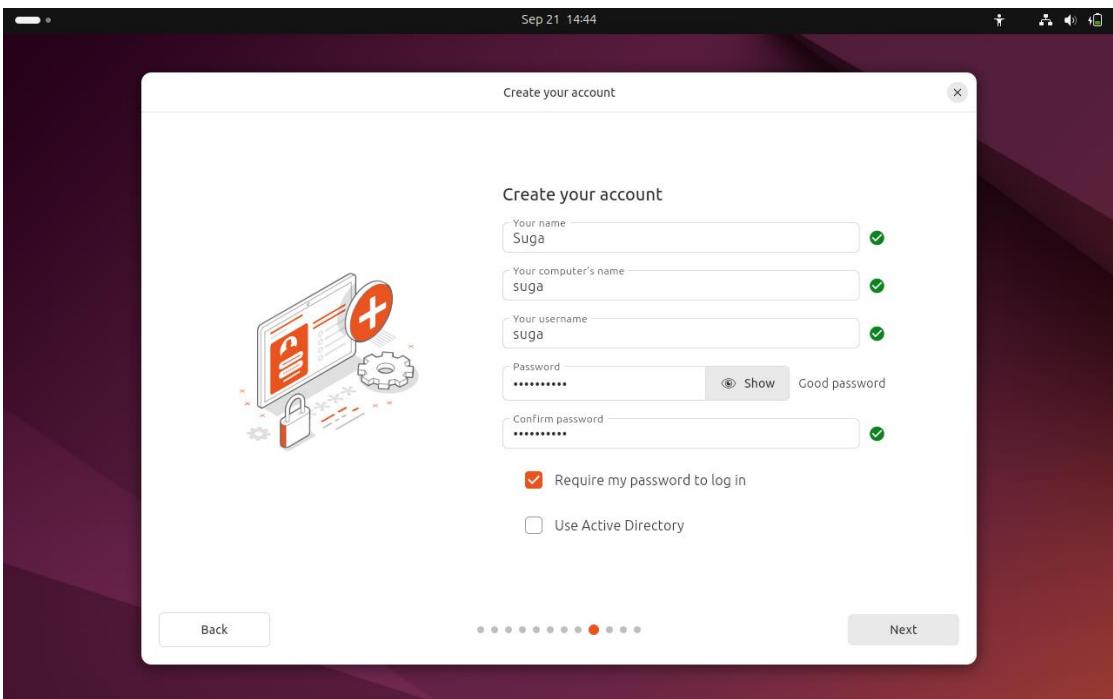
Check both of these checkboxes to install third-party software for graphics and WIFI hardware and to download and install support for additional media formats.



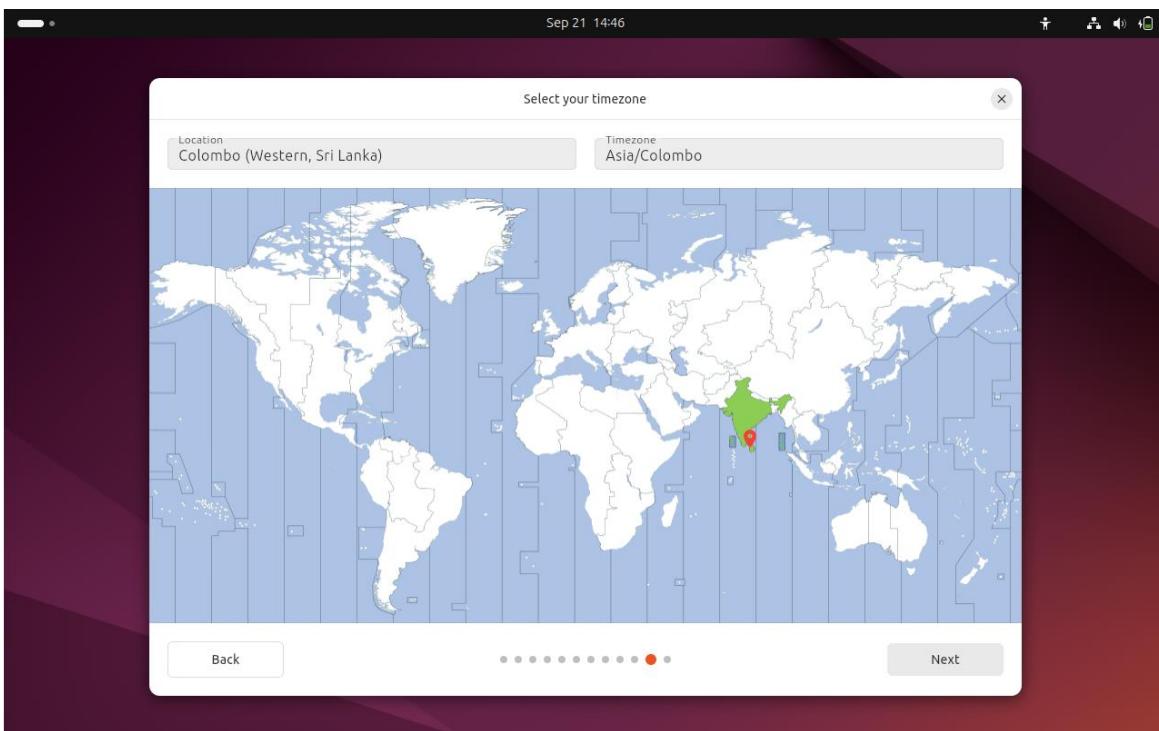
Below configuration will only clear the virtual disk space I allocated previously.



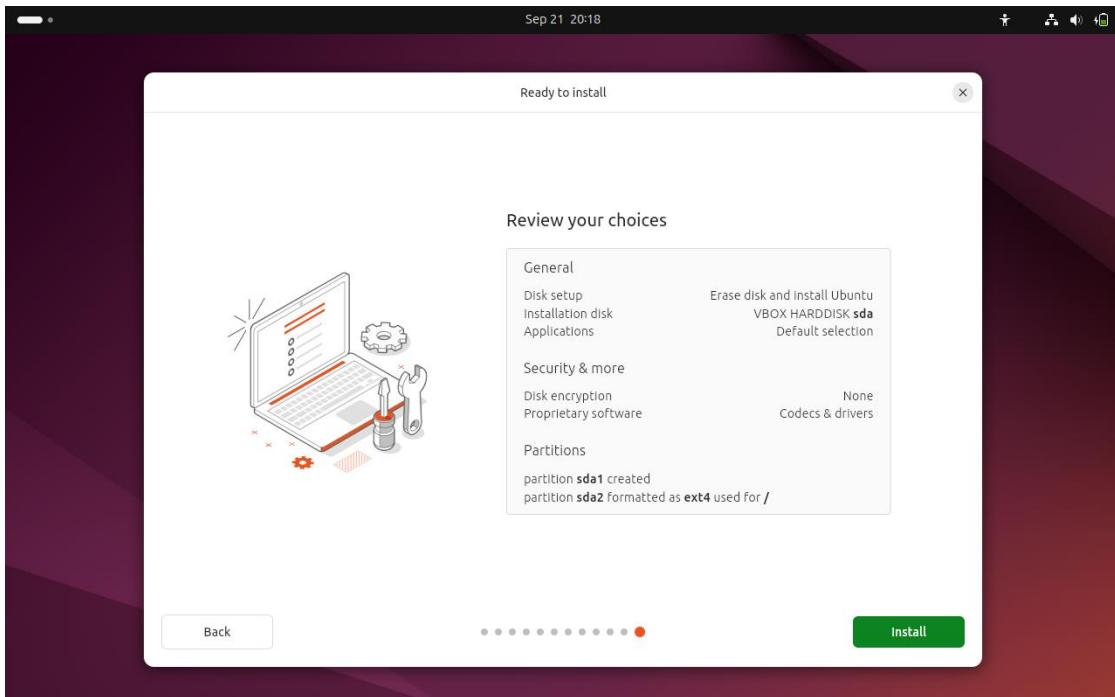
Set credentials for the user account.



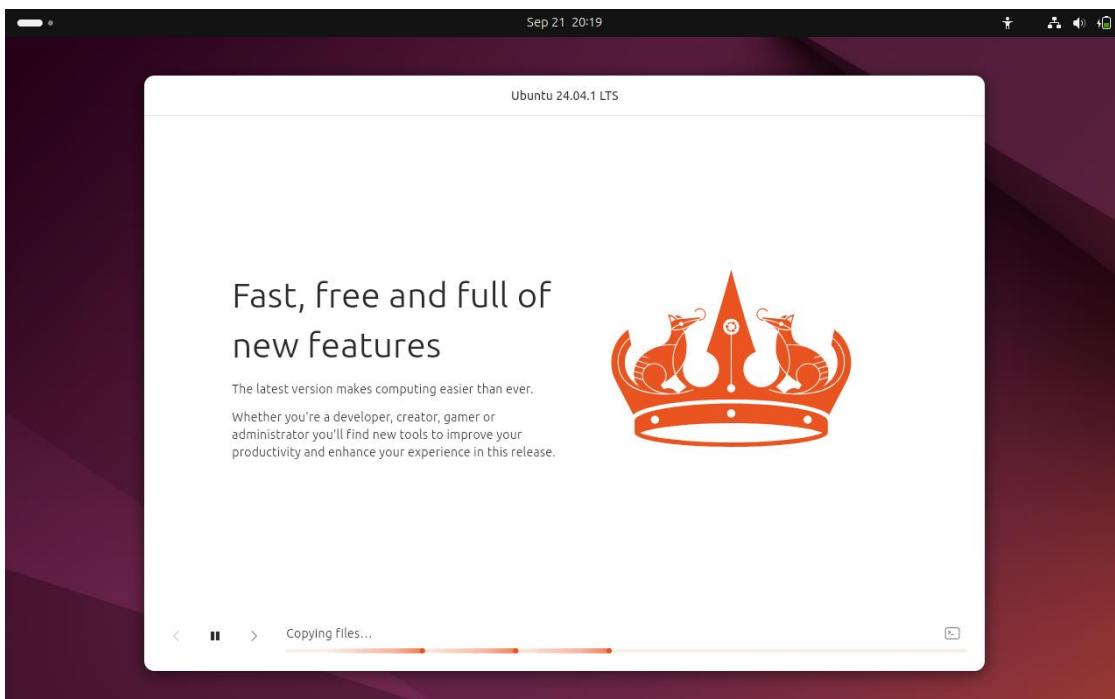
Region will be automatically detected. If not select it manually.



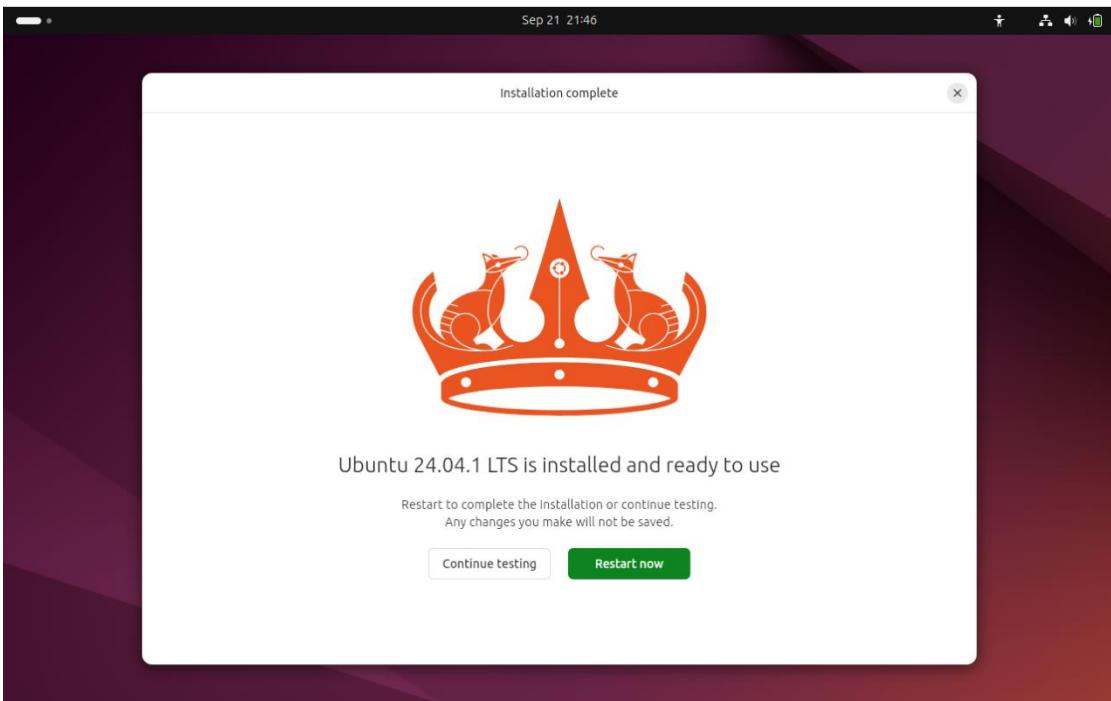
Check the summary to make sure everything is alright.



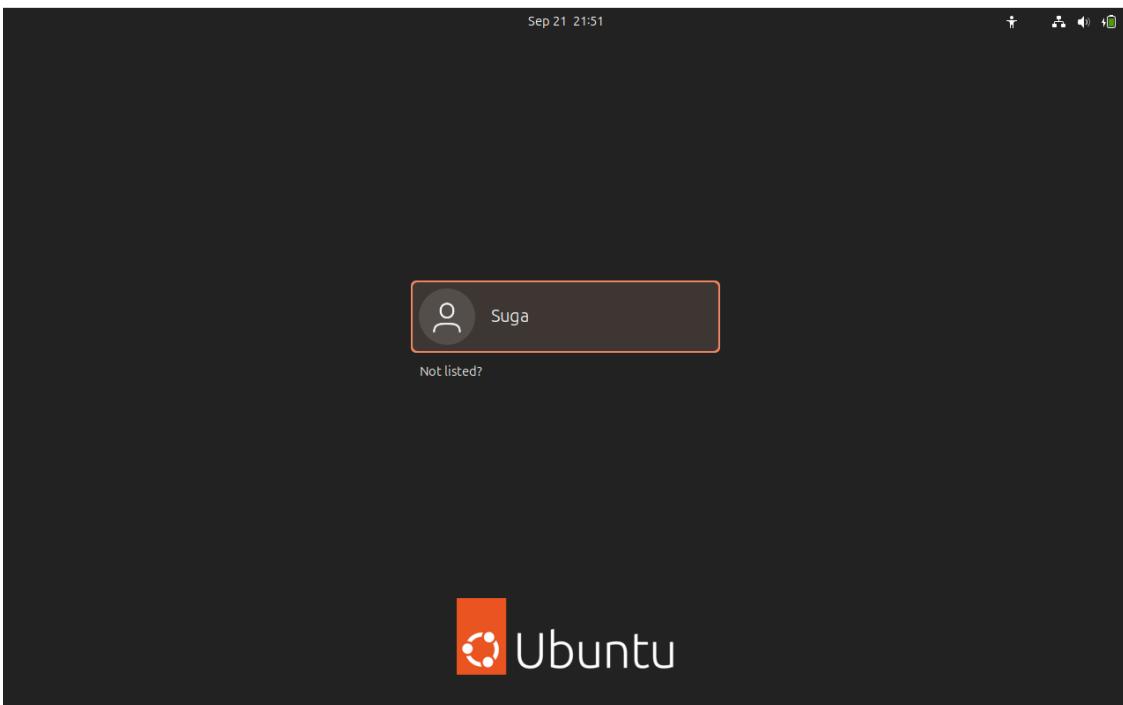
Below process will take few minutes.



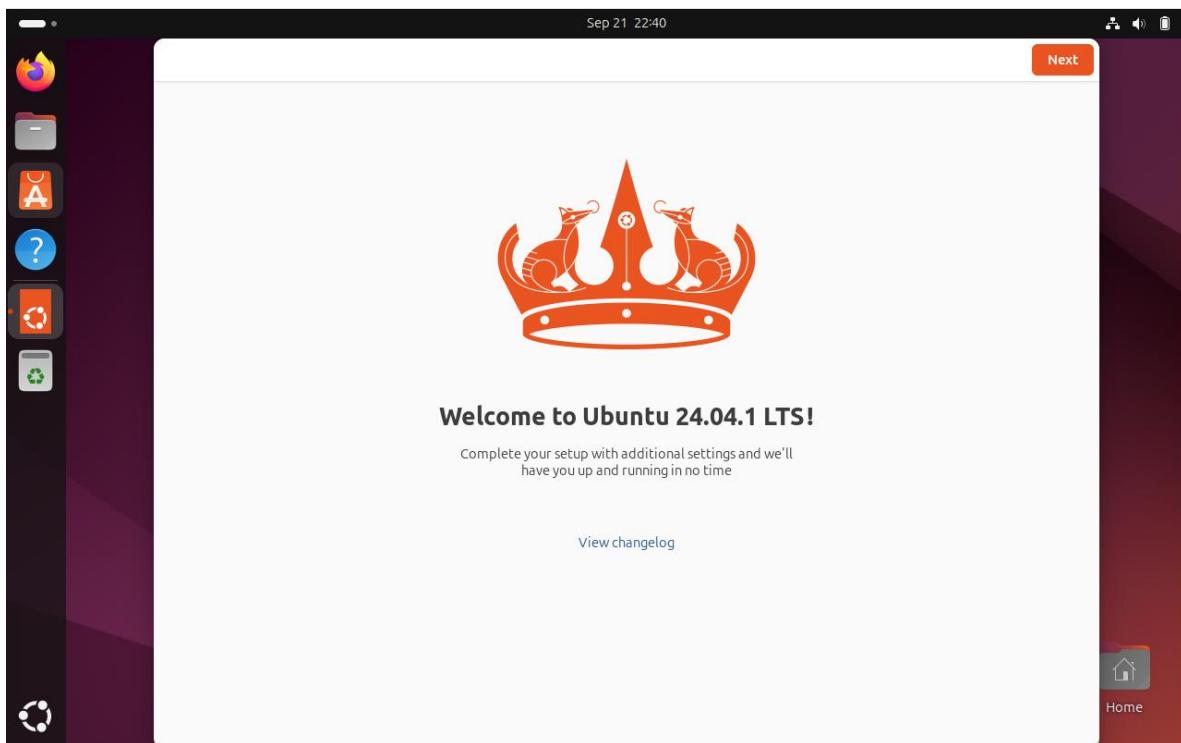
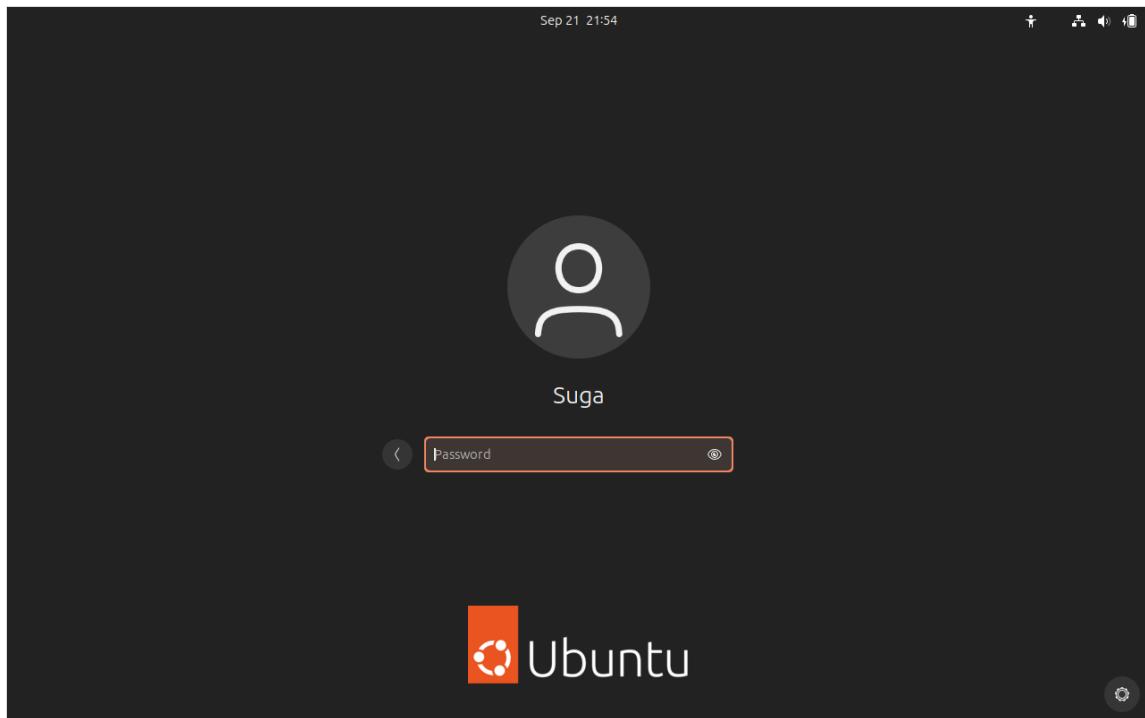
After the installation system will ask to restart.



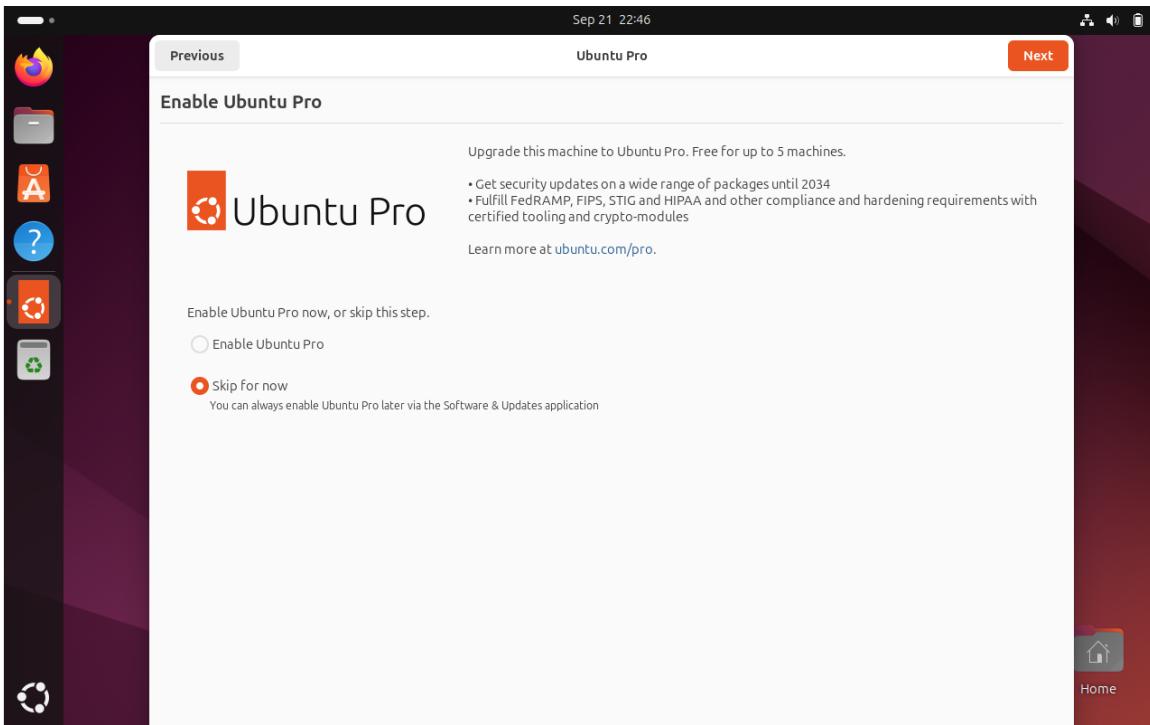
Select your account and press enter.



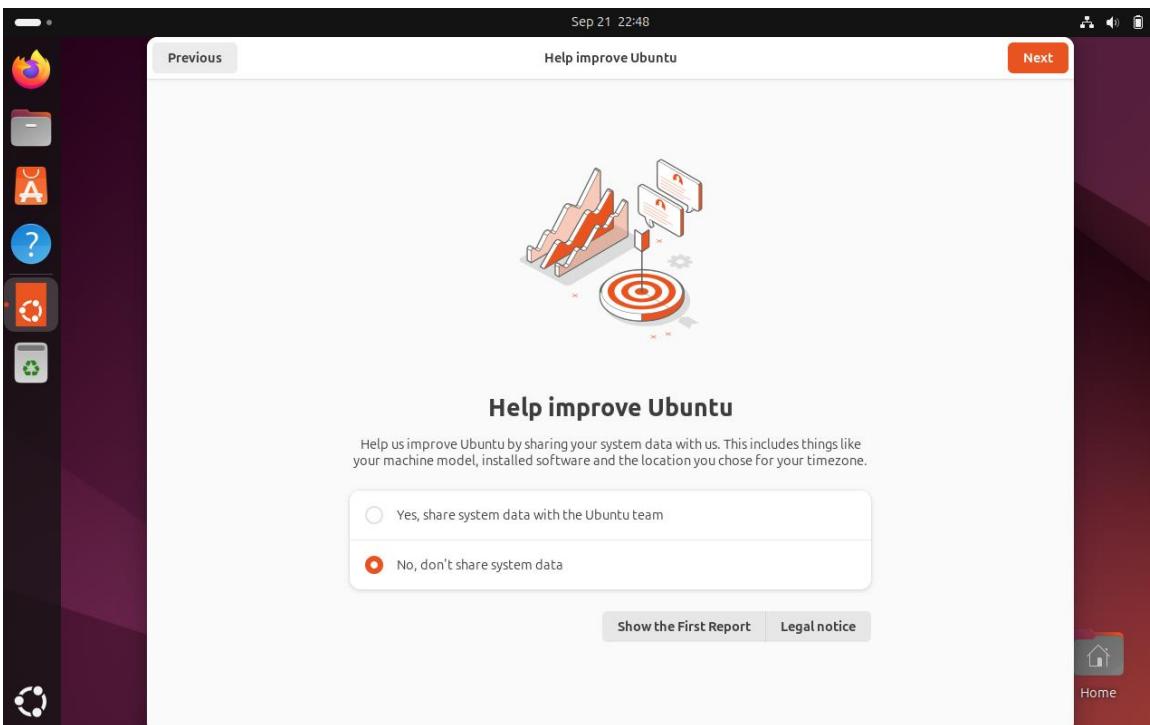
Entered the password I provided earlier.



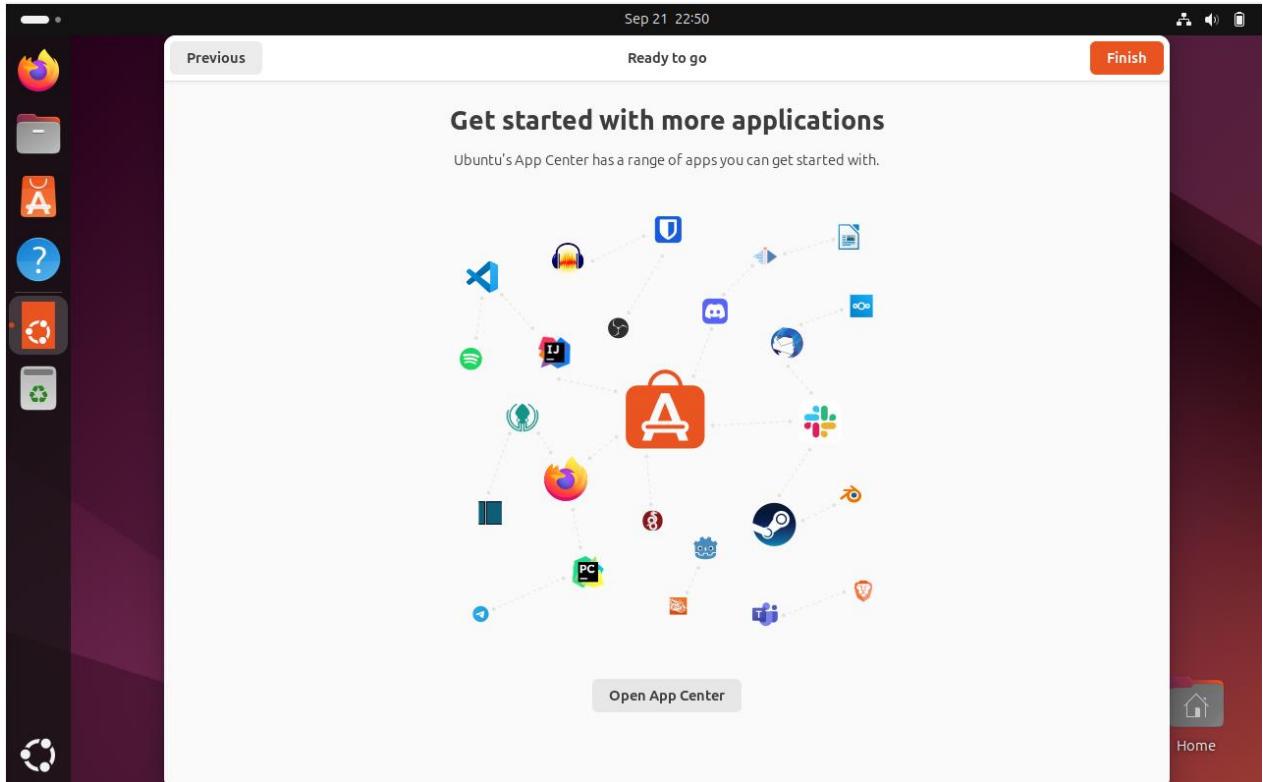
Chose skip for now below for this demonstration.



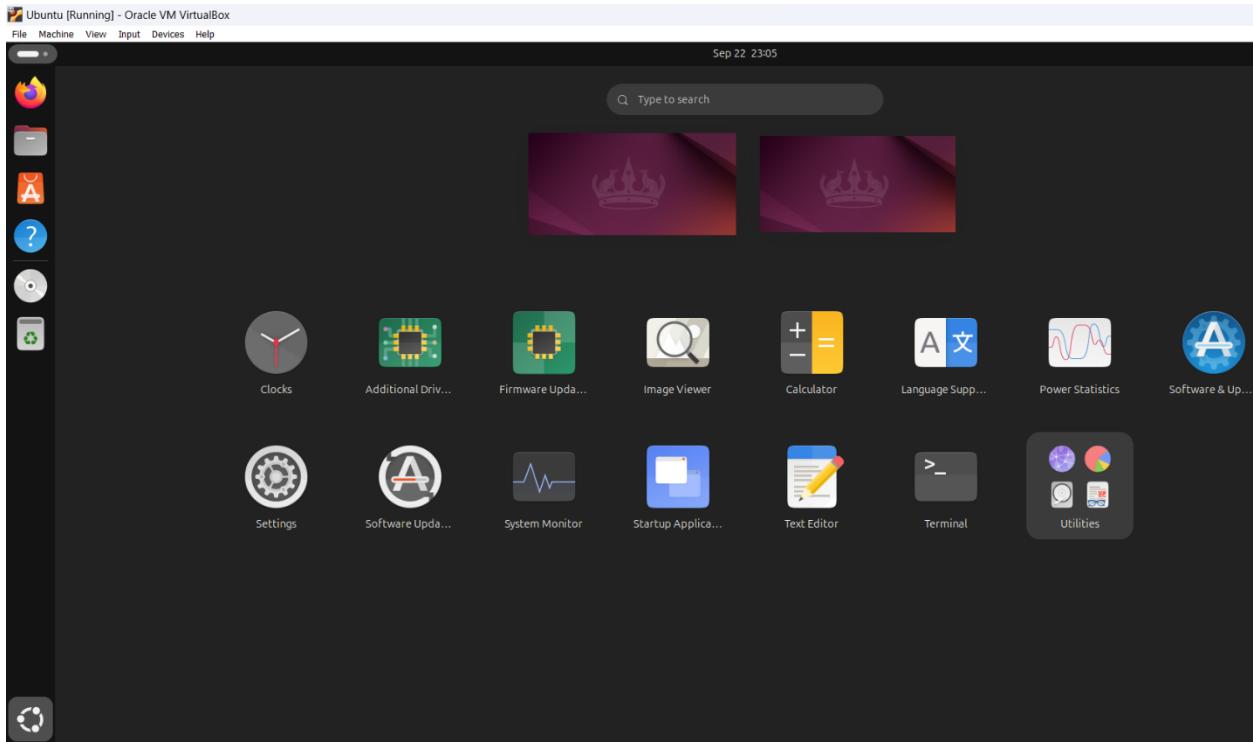
Chose no below because of privacy concerns.



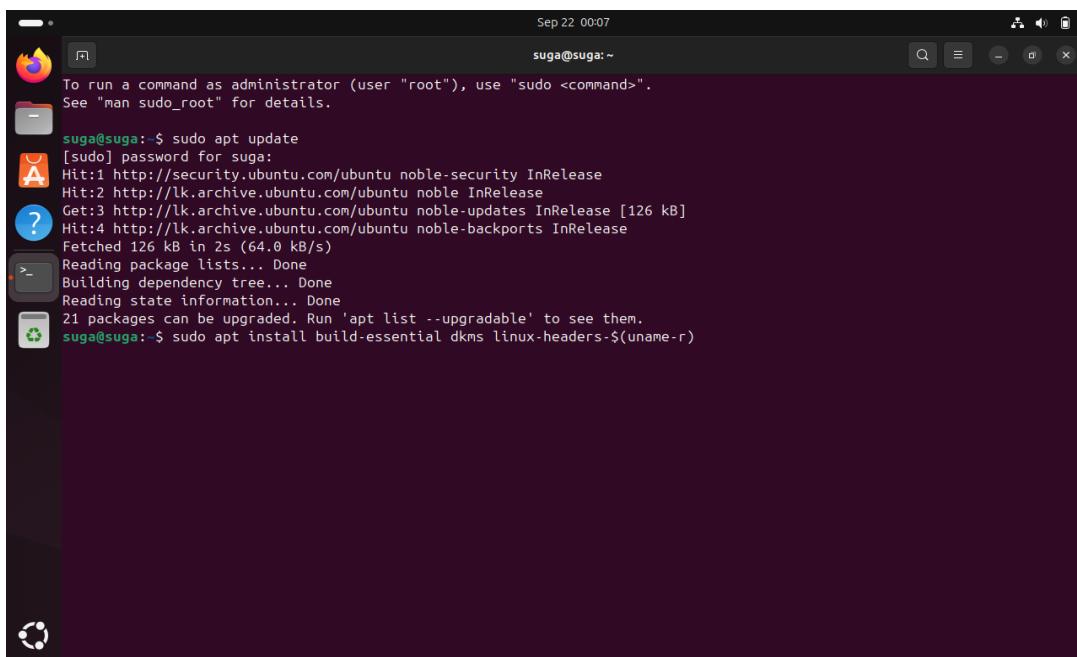
Press finish to end initial setting up process.



After installation VirtualBox doesn't give Ubuntu on full screen. That issue can be solved by installing VirtualBox guest editions through Ubuntu terminal. To access the terminal press the show apps button in the bottom left corner and then select terminal.



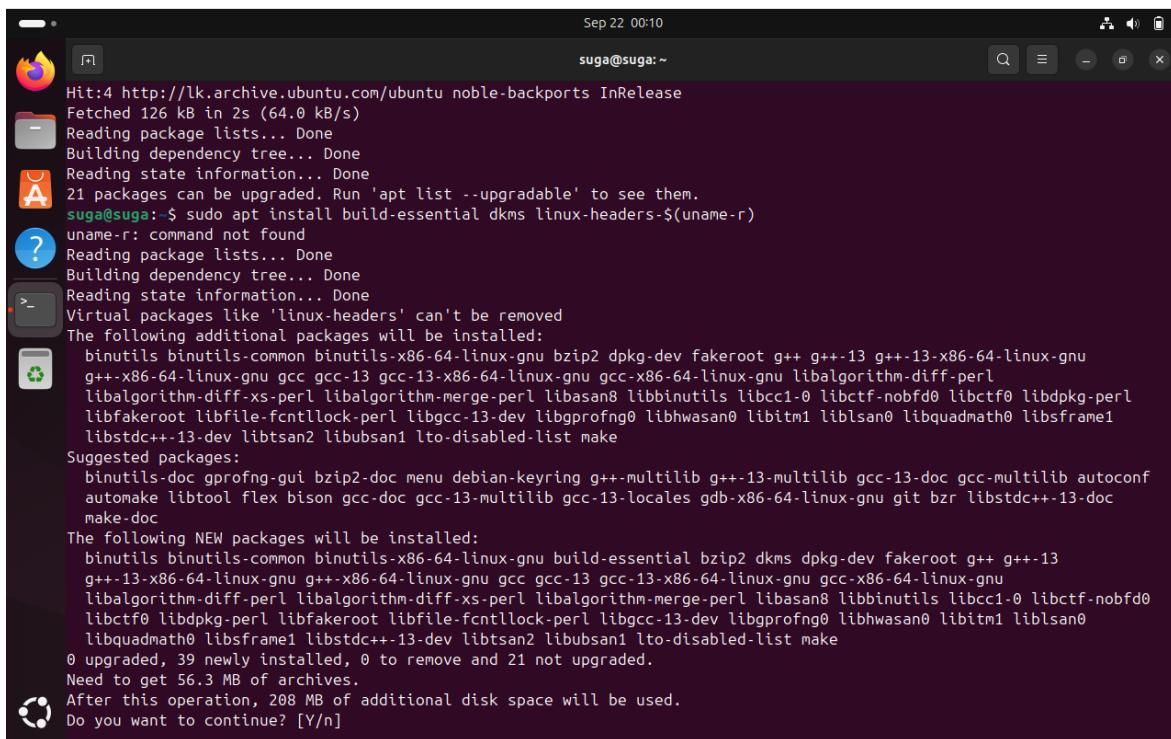
First run **sudo apt update** command on Ubuntu terminal. Enter the password to commence. This will update packages and repository information. Then run **sudo apt install build-essential dkms linux-headers-\$(uname -r)** command. This command will install build essentials, dkms and Linux headers.



```
Sep 22 00:07
suga@suga: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

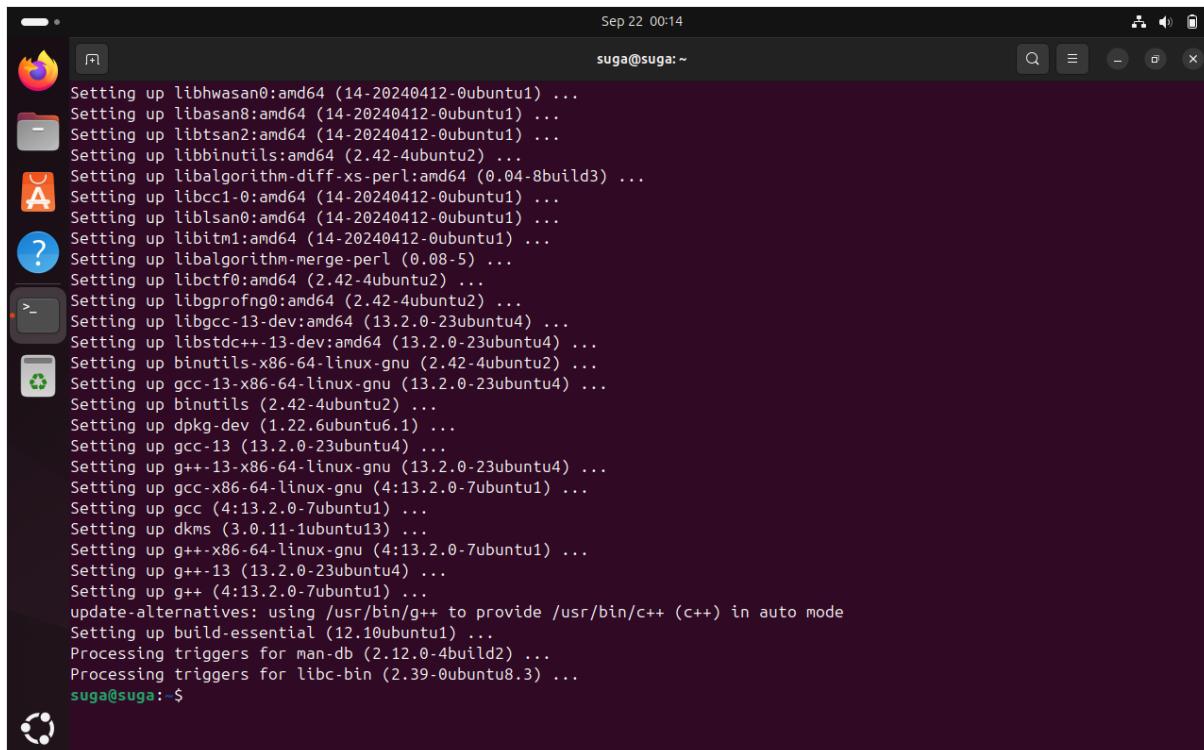
[sudo] password for sua:
suga@suga:~$ sudo apt update
[sudo] password for sua:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 2s (64.0 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
suga@suga:~$ sudo apt install build-essential dkms linux-headers-$(uname -r)
```

Press Y to continue.



Sep 22 00:10
suga@suga:~

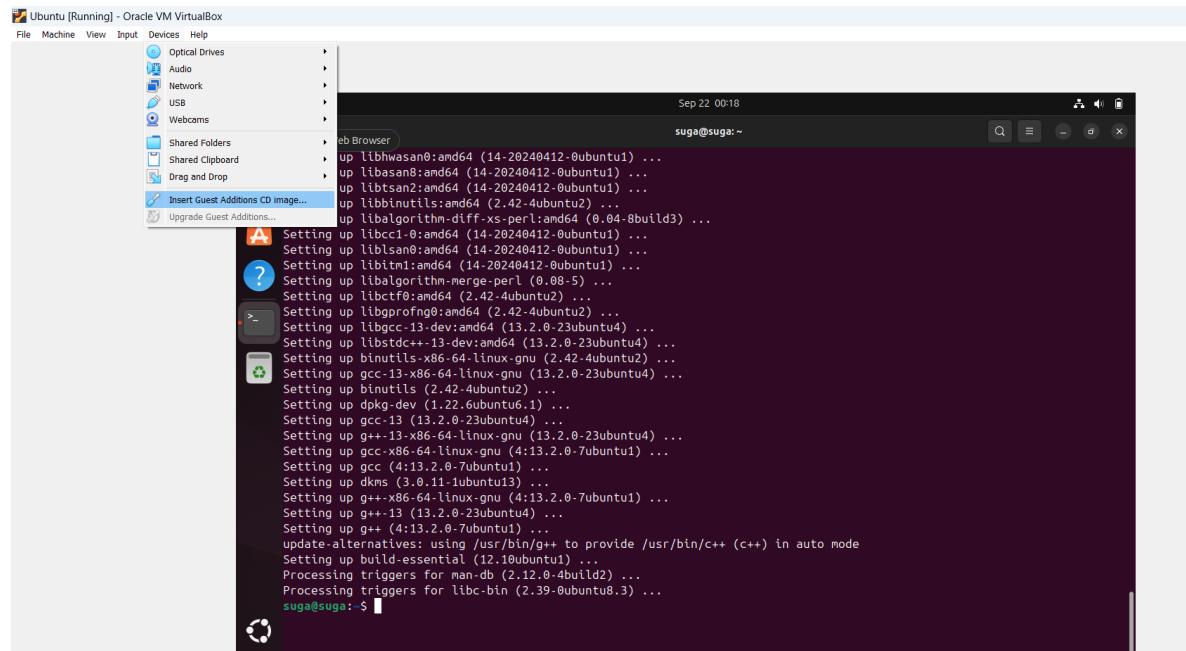
```
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 2s (64.0 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
suga@suga:~$ sudo apt install build-essential dkms linux-headers-$(uname -r)
uname-r: command not found
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Virtual packages like 'linux-headers' can't be removed
The following additional packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu bzip2 dpkg-dev fakeroot g++ g++-13 g++-13-x86_64-linux-gnu
g++-x86_64-linux-gnu gcc gcc-13 gcc-13-x86_64-linux-gnu gcc-x86_64-linux-gnu libalgorithm-diff-perl
libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libbinutils libcc1-0 libctf-nobfd0 libctf0 libdpkg-perl
libfakeroot libfile-fcntllock-perl libgcc-13-dev libgprofng0 libhwasan0 libitm1 liblsan0 libquadmath0 libsframe1
libstdc++-13-dev libtsan2 libubsan1 lto-disabled-list make
Suggested packages:
binutils-doc gprofng-gui bzip2-doc menu debian-keyring g++-multilib g++-13-multilib gcc-13-doc gcc-multilib autoconf
automake libtool flex bison gcc-doc gcc-13-multilib gcc-13-locales gdb-x86_64-linux-gnu git bzr libstdc++-13-doc
make-doc
The following NEW packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu build-essential bzip2 dkms dpkg-dev fakeroot g++ g++-13
g++-13-x86_64-linux-gnu g++-x86_64-linux-gnu gcc gcc-13 gcc-13-x86_64-linux-gnu gcc-x86_64-linux-gnu
libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libbinutils libcc1-0 libctf-nobfd0
libctf0 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-13-dev libgprofng0 libhwasan0 libitm1 liblsan0
libquadmath0 libsframe1 libstdc++-13-dev libtsan2 libubsan1 lto-disabled-list make
0 upgraded, 39 newly installed, 0 to remove and 21 not upgraded.
Need to get 56.3 MB of archives.
After this operation, 208 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



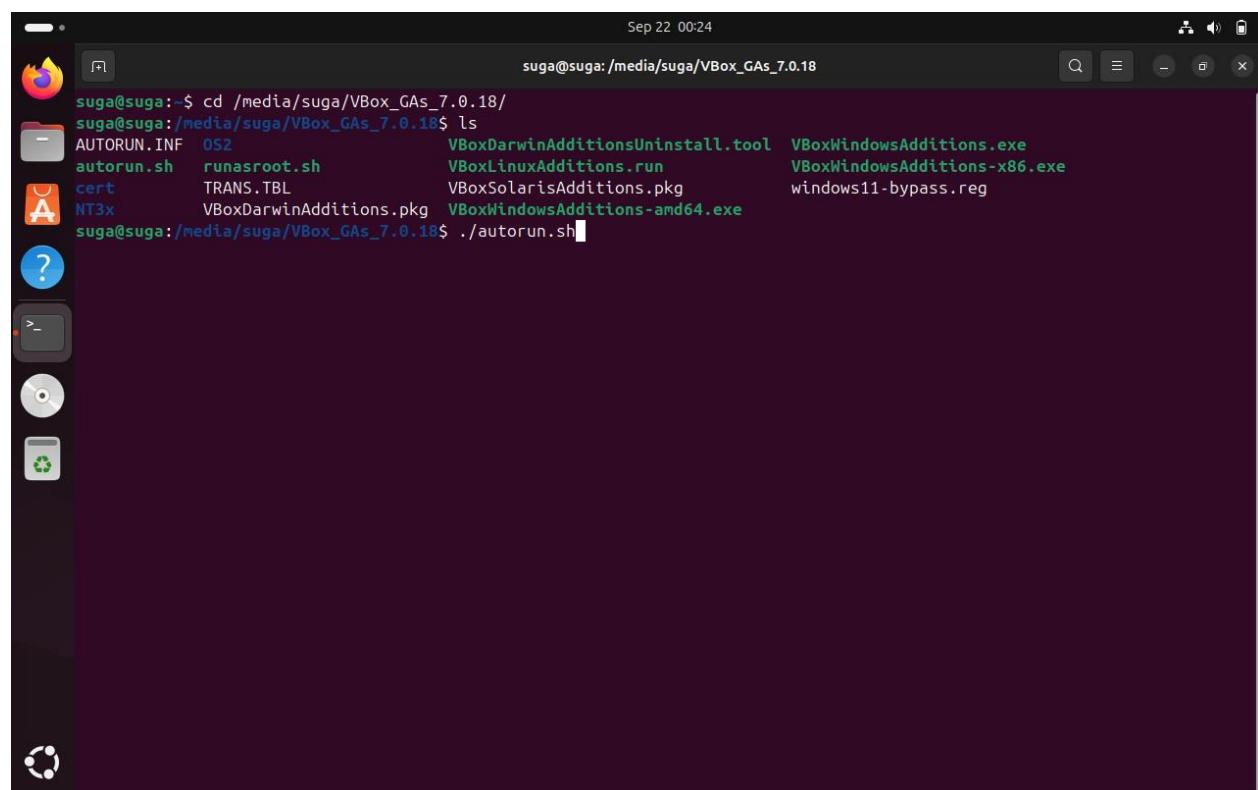
Sep 22 00:14
suga@suga:~

```
Setting up libhwasan0:amd64 (14-20240412-0ubuntu1) ...
Setting up libasan8:amd64 (14-20240412-0ubuntu1) ...
Setting up libtsan2:amd64 (14-20240412-0ubuntu1) ...
Setting up libbinutils:amd64 (2.42-4ubuntu2) ...
Setting up libalgorithm-diff-xs-perl:amd64 (0.04-8build3) ...
Setting up libcc1-0:amd64 (14-20240412-0ubuntu1) ...
Setting up liblsan0:amd64 (14-20240412-0ubuntu1) ...
Setting up libitm1:amd64 (14-20240412-0ubuntu1) ...
Setting up libalgorithm-merge-perl (0.08-5) ...
Setting up libctf0:amd64 (2.42-4ubuntu2) ...
Setting up libgprofng0:amd64 (2.42-4ubuntu2) ...
Setting up libgcc-13-dev:amd64 (13.2.0-23ubuntu4) ...
Setting up libstdc++-13-dev:amd64 (13.2.0-23ubuntu4) ...
Setting up binutils-x86_64-linux-gnu (2.42-4ubuntu2) ...
Setting up gcc-13 (13.2.0-23ubuntu4) ...
Setting up g++-13-x86_64-linux-gnu (13.2.0-23ubuntu4) ...
Setting up gcc-x86_64-linux-gnu (4:13.2.0-7ubuntu1) ...
Setting up gcc (4:13.2.0-7ubuntu1) ...
Setting up dkms (3.0.11-1ubuntu13) ...
Setting up g++-x86_64-linux-gnu (4:13.2.0-7ubuntu1) ...
Setting up g++-13 (13.2.0-23ubuntu4) ...
Setting up g++ (4:13.2.0-7ubuntu1) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.10ubuntu1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
suga@suga:~$
```

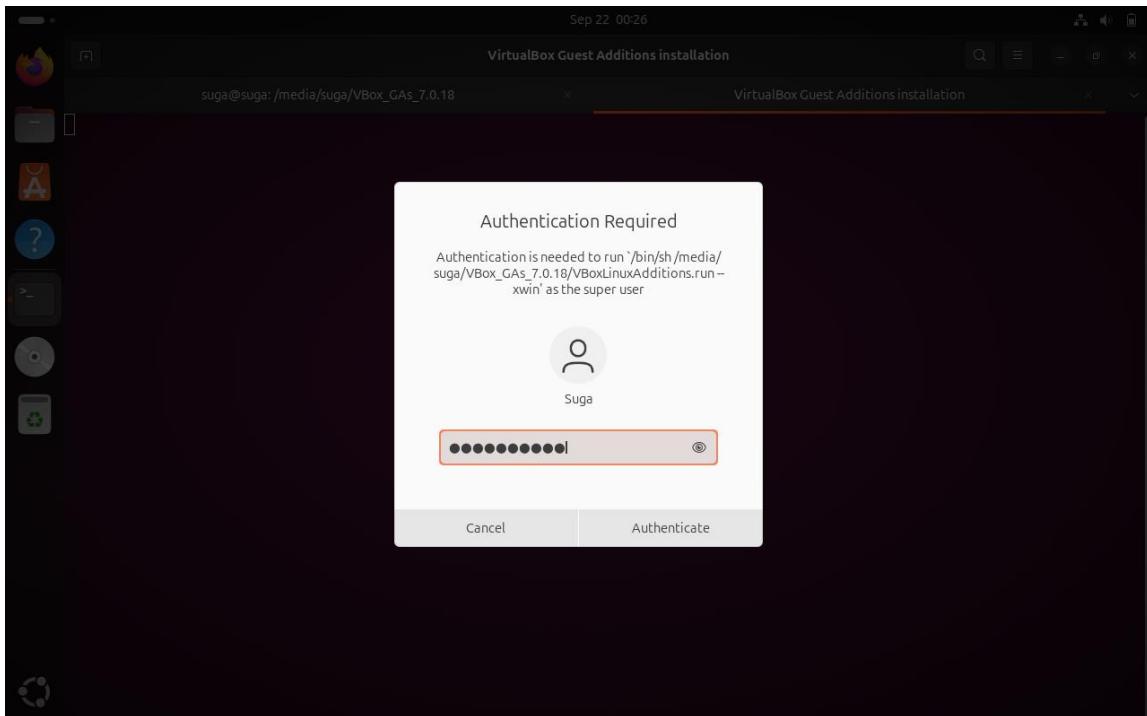
After installation click on devices option on the top left VirtualBox menu and select insert guest additions CD image. It will mount guest additions to Ubuntu OS.



Then navigate in to /media/suga/VBox_Gas_7.0.18/ folder and look for autorun.sh file.



Run the autorun.sh file using `./autorun.sh` command. Then enter the password.



It will start installing guest additions in VirtualBox.

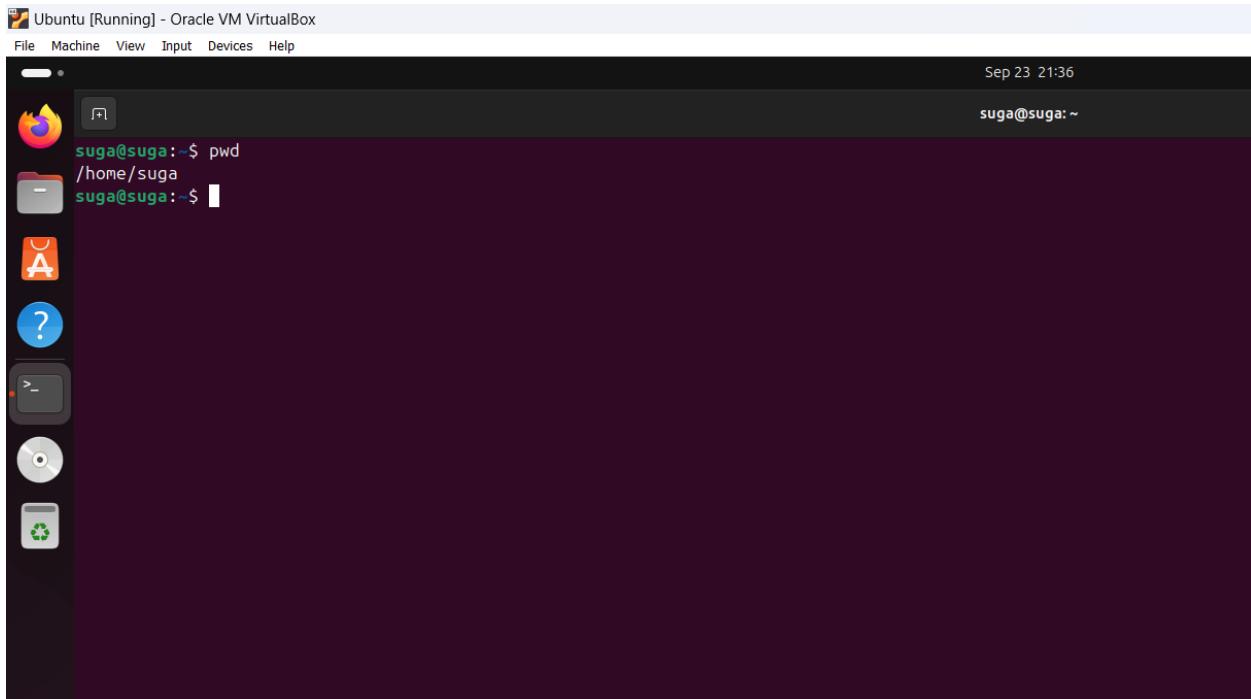
```
Sep 22 00:30
VirtualBox Guest Additions installation
suga@suga: /media/suga/VBox_GAs_7.0.... × VirtualBox Guest Additions installation ×
VirtualBox Guest Additions: To build modules for other installed kernels
, run
VirtualBox Guest Additions: /sbin/rcvboxadd quicksetup <version>
VirtualBox Guest Additions: or
VirtualBox Guest Additions: /sbin/rcvboxadd quicksetup all
VirtualBox Guest Additions: Building the modules for kernel 6.8.0-45-gen
eric.
update-initramfs: Generating /boot/initrd.img-6.8.0-45-generic
VirtualBox Guest Additions: Running kernel modules will not be replaced
until
the system is restarted or 'rcvboxadd reload' triggered
VirtualBox Guest Additions: reloading kernel modules and services
VirtualBox Guest Additions: kernel modules and services 7.0.18 r162988 r
eloaded
VirtualBox Guest Additions: NOTE: you may still consider to re-login if
some
user session specific services (Shared Clipboard, Drag and Drop, Seamles
s or
Guest Screen Resize) were not restarted automatically
Press Return to close this window...
```

A screenshot of a terminal window titled "VirtualBox Guest Additions installation". The window shows the output of the command "suga@suga: /media/suga/VBox_GAs_7.0....". The output details the process of building modules for the kernel, running "rcvboxadd quicksetup", and reloading kernel modules and services. It also includes a note about user session specific services and a prompt to press Return to close the window.

After the installation restart the virtual machine. Then you will be able to resize the window as you want.

1.2 Command Line Introduction

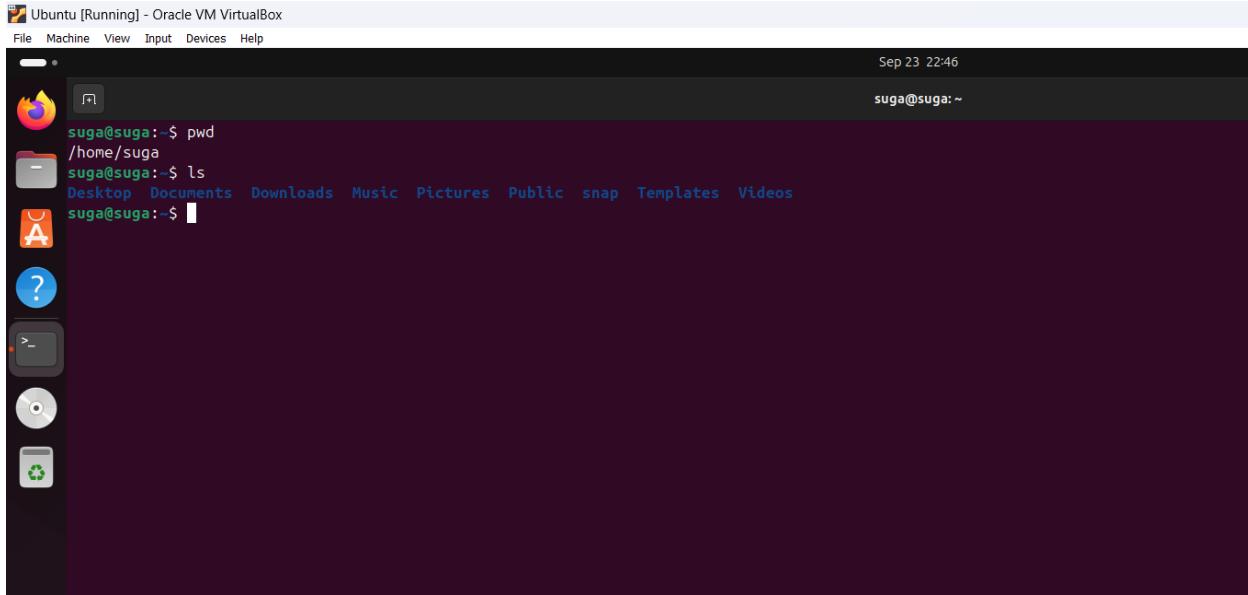
1.pwd



The command **pwd** stands for print working directory. It will provide the full path to the directory that you are currently working on. This command is useful when you need to confirm current directory location when navigating through the directories.

2.ls

The **ls** command is used when you need to list contents of a certain directory. It displays files and subdirectories of the current directory or a certain directory. This is the basic form of command.



ls -l will show us the content in long listing format displaying file permissions, ownership, size and modification dates. **ls -a** will list all files including hidden files. **ls -lh** will display content in long listing format with more human readable file size interpretation using KB, MB etc.

```
suga@suga:~$ ls -l
total 36
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Desktop
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Documents
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Downloads
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Music
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Pictures
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Public
drwx----- 3 suga suga 4096 Sep 21 21:56 snap
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Templates
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Videos
suga@suga:~$ ls -lh
total 36K
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Desktop
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Documents
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Downloads
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Music
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Pictures
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Public
drwx----- 3 suga suga 4.0K Sep 21 21:56 snap
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Templates
drwxr-xr-x 2 suga suga 4.0K Sep 21 21:56 Videos
```

ls -R will display contents recursively. Meaning it will lists files and directories including those in subdirectories.

```
suga@suga:~$ ls -R
.:
Desktop Documents Downloads Music Pictures Public snap Templates Videos

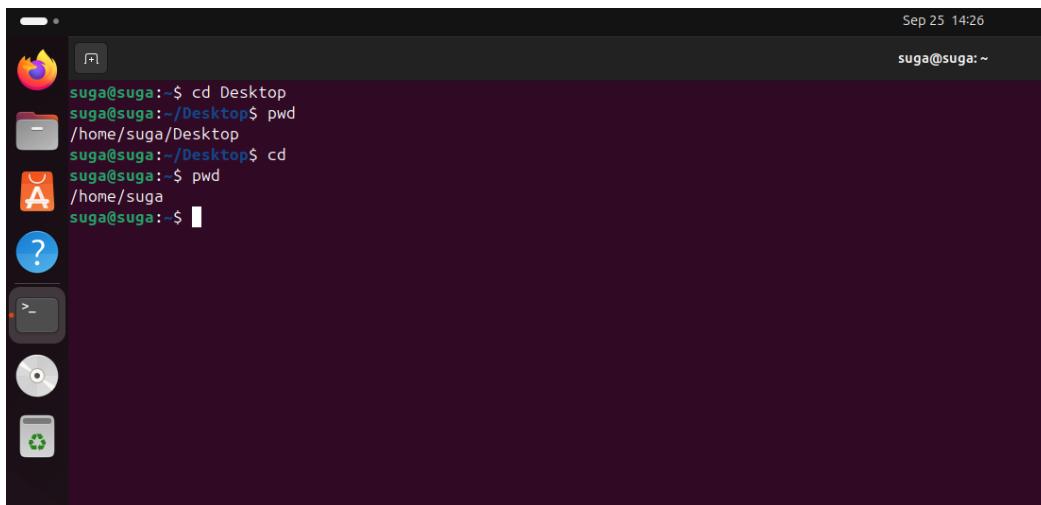
./Desktop:
./Documents:
./Downloads:
./Music:
./Pictures:
./Public:
./snap:
snapd-desktop-integration
./snap/snapd-desktop-integration:178 common current

./snap/snapd-desktop-integration/178:
Desktop Documents Downloads Music Pictures Public Templates Videos

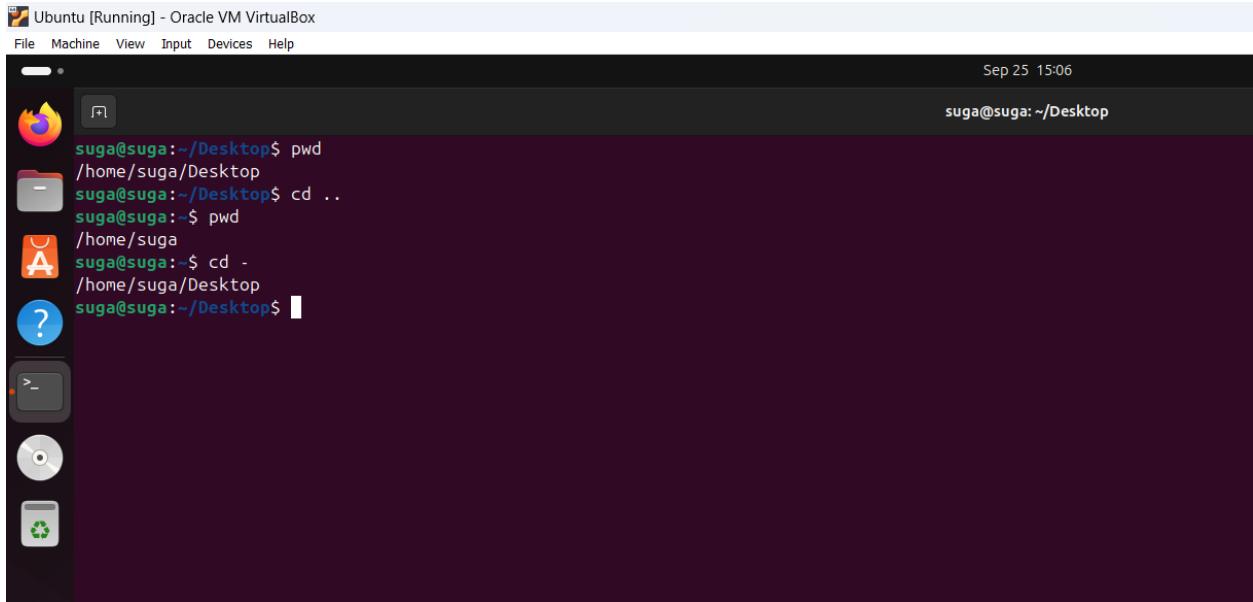
./snap/snapd-desktop-integration/178/Desktop:
./snap/snapd-desktop-integration/178/Documents:
./snap/snapd-desktop-integration/178/Downloads:
./snap/snapd-desktop-integration/178/Music:
./snap/snapd-desktop-integration/178/Pictures:
./snap/snapd-desktop-integration/178/Public:
```

3.cd

Command **cd** stands for change directory. It allows us to navigate between different directories. Running **cd** alone will take you to home directory from the current directory. If you use **cd** and a specific path it will take you to that specified directory.



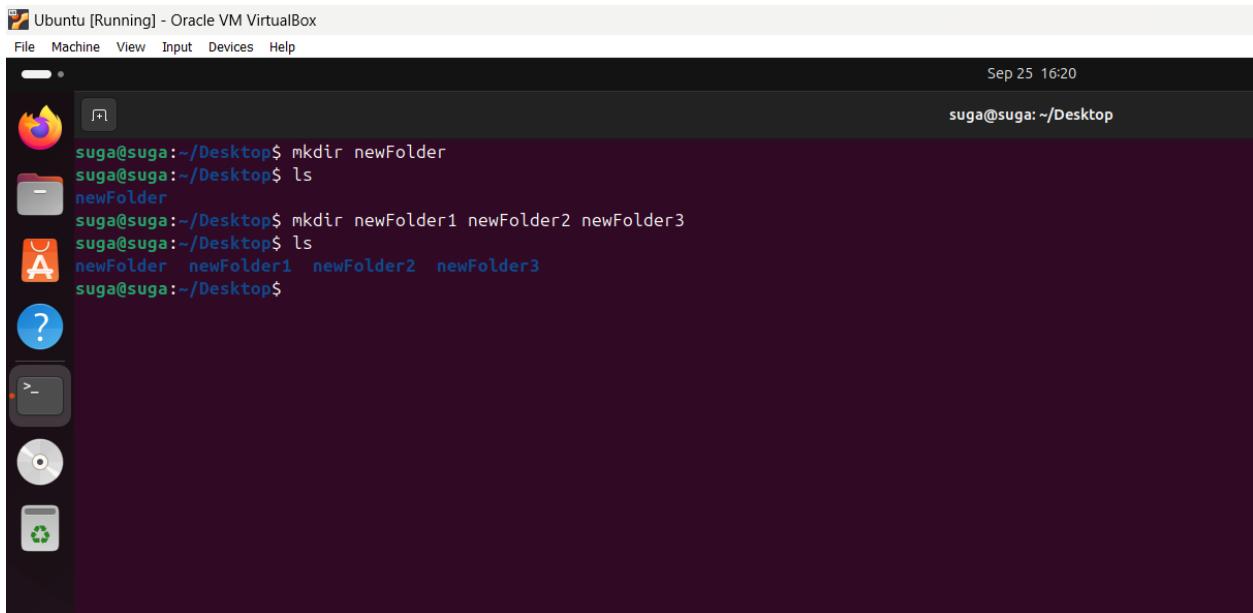
If you use `cd ..` command terminal will take you to parent directory. The command `cd -` will take you to previous directory.

A screenshot of an Ubuntu desktop environment running in Oracle VM VirtualBox. The terminal window is open at the bottom of the screen, showing a dark purple background. The terminal prompt is `suga@suga:~/Desktop$`. The user has run the command `pwd`, which outputs `/home/suga/Desktop`. Then, they ran `cd ..`, followed by `pwd`, which outputs `/home/suga`. Finally, they ran `cd -`, followed by `pwd`, which outputs `/home/suga/Desktop` again. The desktop interface includes a dock on the left with icons for Dash, Home, Applications, and others, and a top panel with the system menu, file manager, and help icons.

```
suga@suga:~/Desktop$ pwd  
/home/suga/Desktop  
suga@suga:~/Desktop$ cd ..  
suga@suga:~$ pwd  
/home/suga  
suga@suga:~$ cd -  
/home/suga/Desktop  
suga@suga:~/Desktop$
```

4.mkdir

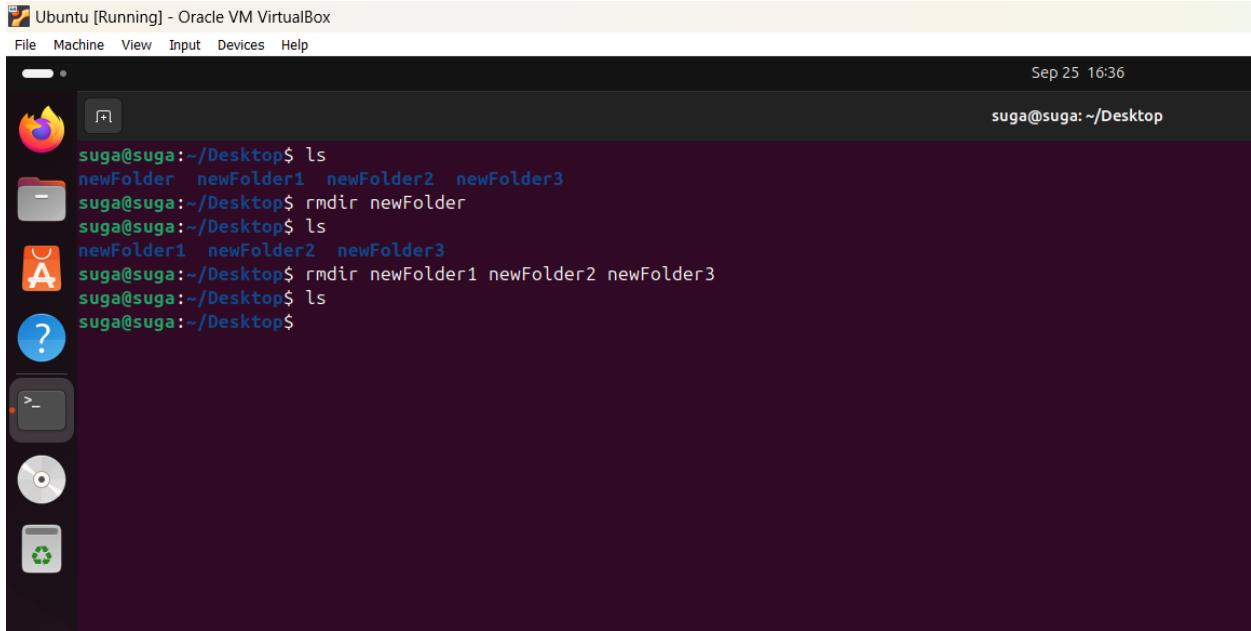
The command `mkdir` is used to create new directories. It can be used to create a single or multiple new directories at once.

A screenshot of an Ubuntu desktop environment running in Oracle VM VirtualBox. The terminal window is open at the bottom of the screen, showing a dark purple background. The terminal prompt is `suga@suga:~/Desktop$`. The user has run the command `mkdir newFolder`, then `ls`, which shows a folder named `newFolder`. They then ran `mkdir newFolder1 newFolder2 newFolder3`, followed by another `ls`, which shows three new folders: `newFolder`, `newFolder1`, `newFolder2`, and `newFolder3`. The desktop interface includes a dock on the left with icons for Dash, Home, Applications, and others, and a top panel with the system menu, file manager, and help icons.

```
suga@suga:~/Desktop$ mkdir newFolder  
suga@suga:~/Desktop$ ls  
newFolder  
suga@suga:~/Desktop$ mkdir newFolder1 newFolder2 newFolder3  
suga@suga:~/Desktop$ ls  
newFolder newFolder1 newFolder2 newFolder3  
suga@suga:~/Desktop$
```

5.rmdir

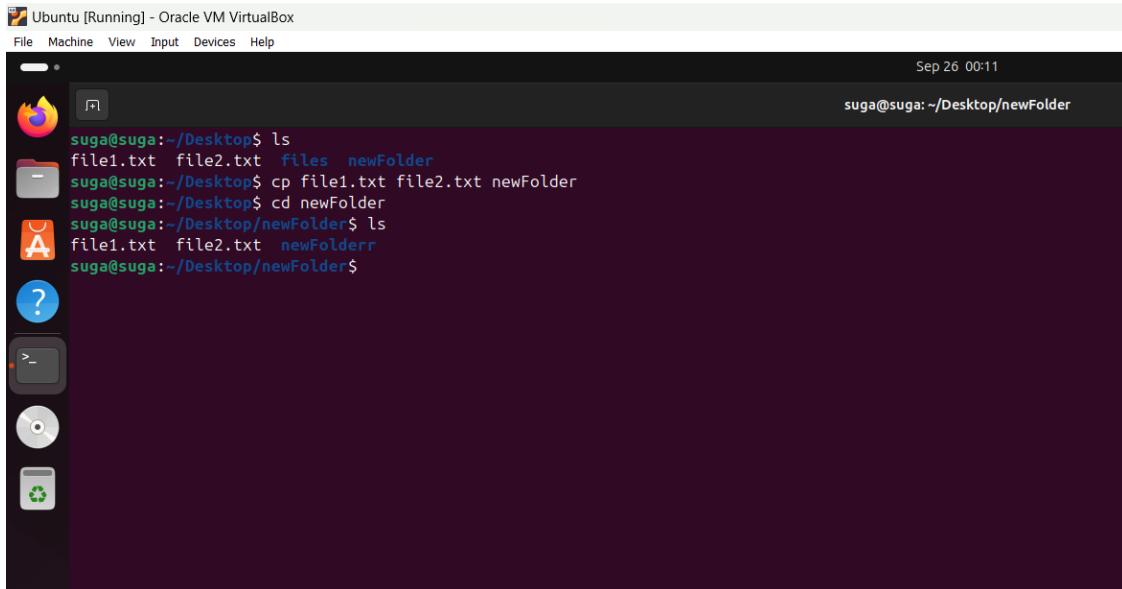
The **rmdir** command is used to remove(delete) empty directories. It can remove single or multiple empty directories at once.



```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sep 25 16:36
suga@suga: ~/Desktop
suga@suga:~/Desktop$ ls
newFolder newFolder1 newFolder2 newFolder3
suga@suga:~/Desktop$ rmdir newFolder
suga@suga:~/Desktop$ ls
newFolder1 newFolder2 newFolder3
suga@suga:~/Desktop$ rmdir newFolder1 newFolder2 newFolder3
suga@suga:~/Desktop$ ls
suga@suga:~/Desktop$
```

6.cp

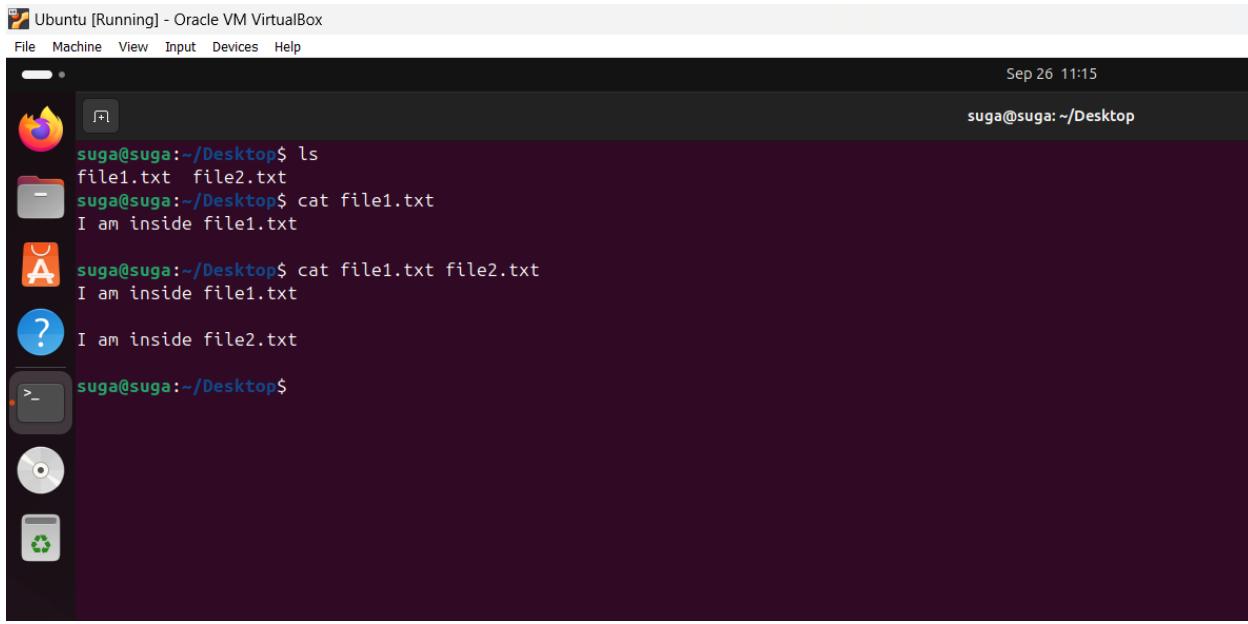
The **cp** command is used to copy files and directories.



```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sep 26 00:11
suga@suga:~/Desktop
suga@suga:~/Desktop$ ls
file1.txt file2.txt files newFolder
suga@suga:~/Desktop$ cp file1.txt file2.txt newFolder
suga@suga:~/Desktop$ cd newFolder
suga@suga:~/Desktop/newFolder$ ls
file1.txt file2.txt newFolder
suga@suga:~/Desktop/newFolder$
```

7.cat

The **cat** command is used to display the content of a file or concatenate multiple files and print their output.

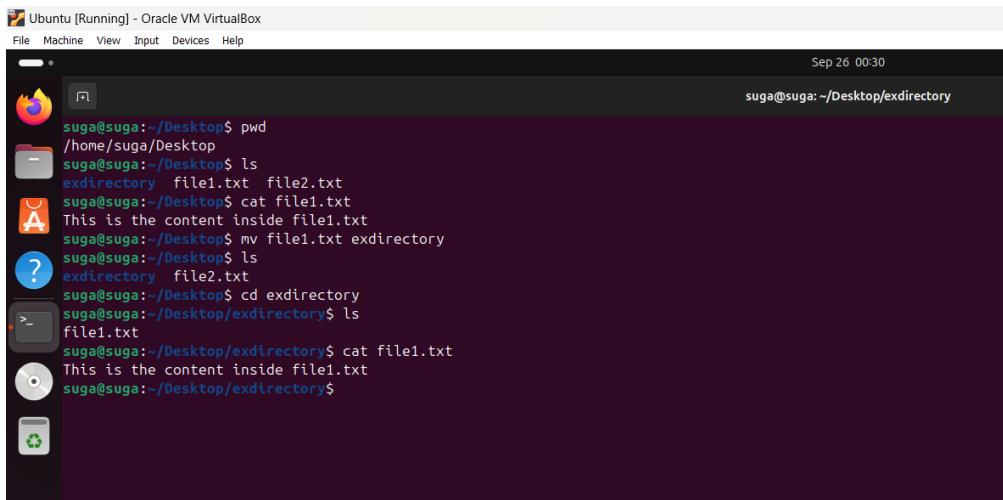


A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal shows the following session:

```
suga@suga:~/Desktop$ ls
file1.txt  file2.txt
suga@suga:~/Desktop$ cat file1.txt
I am inside file1.txt
suga@suga:~/Desktop$ cat file1.txt file2.txt
I am inside file1.txt
suga@suga:~/Desktop$ I am inside file2.txt
suga@suga:~/Desktop$
```

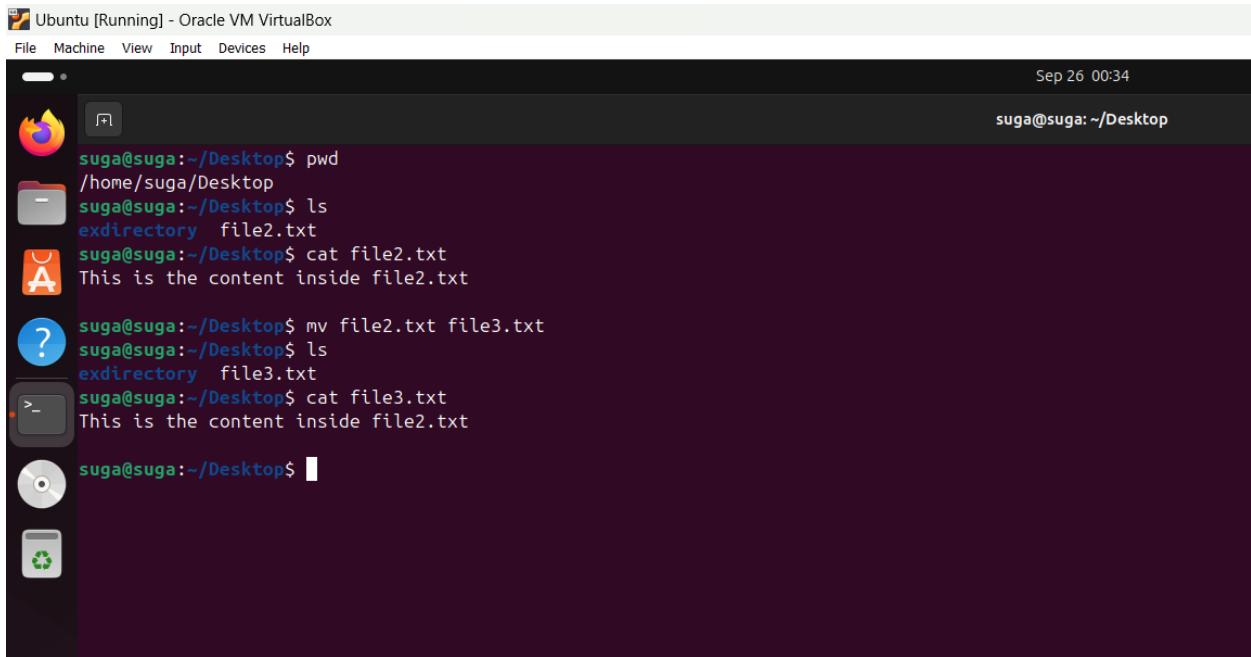
8.mv

The **mv** command is used to move or rename files and directories. If the destination is a directory the source file will be moved to that directory. If the destination is file name the source will be renamed to that destination file name.



A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal shows the following session:

```
suga@suga:~/Desktop$ pwd
/home/suga/Desktop
suga@suga:~/Desktop$ ls
exdirectory  file1.txt  file2.txt
suga@suga:~/Desktop$ cat file1.txt
This is the content inside file1.txt
suga@suga:~/Desktop$ mv file1.txt exdirectory
suga@suga:~/Desktop$ ls
exdirectory  file2.txt
suga@suga:~/Desktop$ cd exdirectory
suga@suga:~/Desktop/exdirectory$ ls
file1.txt
suga@suga:~/Desktop/exdirectory$ cat file1.txt
This is the content inside file1.txt
suga@suga:~/Desktop/exdirectory$
```



A screenshot of an Ubuntu desktop environment running in Oracle VM VirtualBox. The terminal window shows the following session:

```
suga@suga:~/Desktop$ pwd
/home/suga/Desktop
suga@suga:~/Desktop$ ls
exdirectory file2.txt
suga@suga:~/Desktop$ cat file2.txt
This is the content inside file2.txt

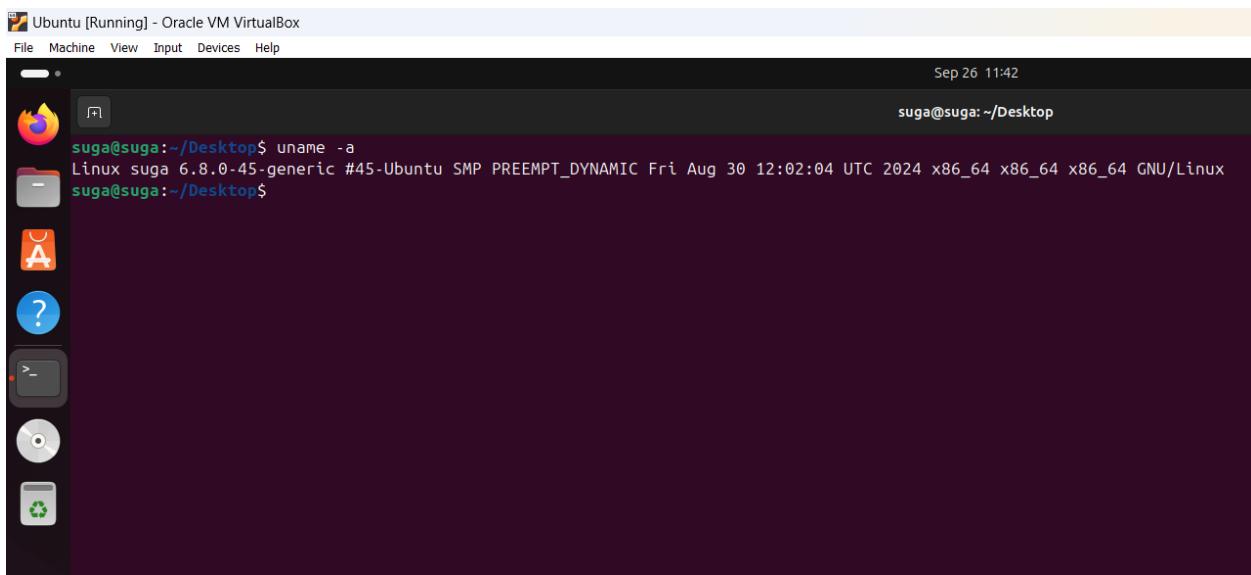
suga@suga:~/Desktop$ mv file2.txt file3.txt
suga@suga:~/Desktop$ ls
exdirectory file3.txt
suga@suga:~/Desktop$ cat file3.txt
This is the content inside file2.txt

suga@suga:~/Desktop$
```

1.3 System Information and User Management

9.uname -a

The **uname -a** command provides detailed information about the system and the kernel. It outputs a combination of system information, including the kernel name, version, hardware details, and more. It's often used for troubleshooting or when sharing system details for technical support.

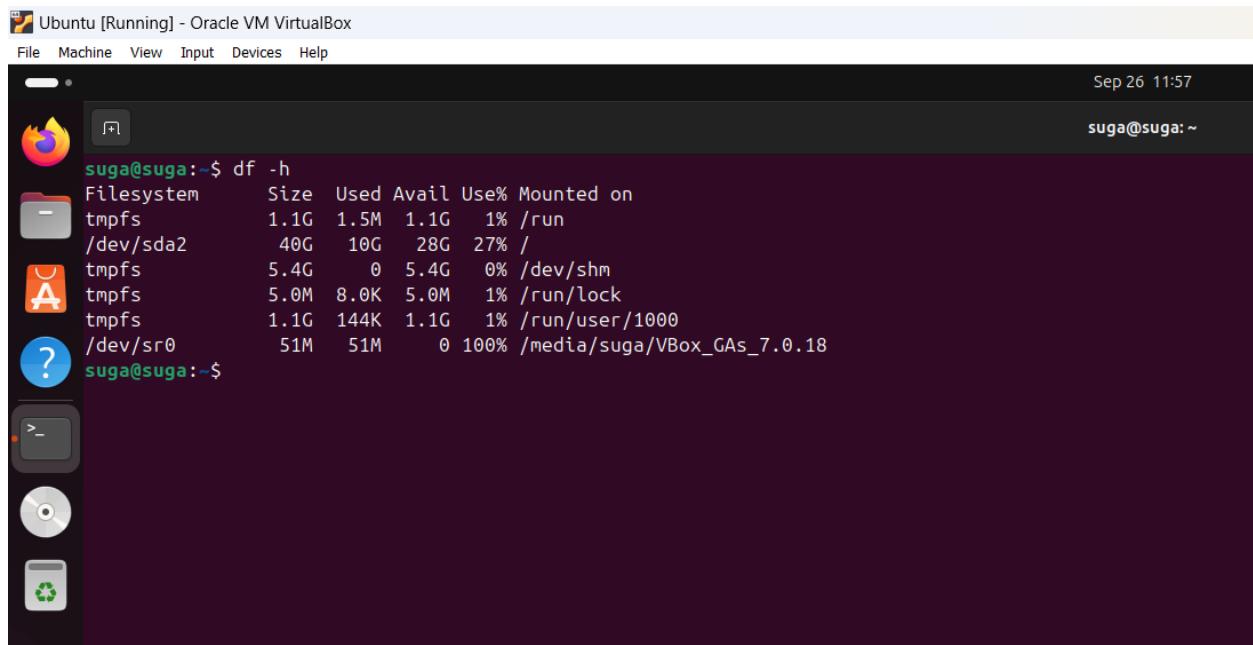


A screenshot of an Ubuntu desktop environment running in Oracle VM VirtualBox. The terminal window shows the following session:

```
suga@suga:~/Desktop$ uname -a
Linux suga 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
suga@suga:~/Desktop$
```

10.df -h

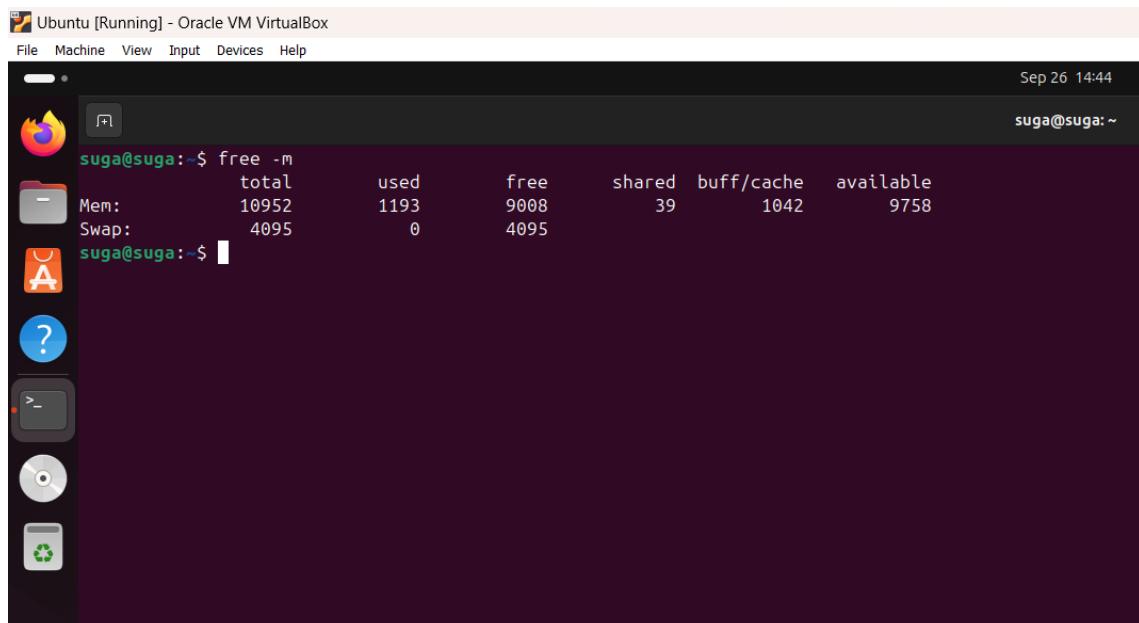
This command shows the disk space usage on our system in a human readable format.



```
suga@suga:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs          1.1G   1.5M  1.1G  1% /run
/dev/sda2        40G   10G  28G  27% /
tmpfs          5.4G     0  5.4G  0% /dev/shm
tmpfs          5.0M  8.0K  5.0M  1% /run/lock
tmpfs          1.1G  144K  1.1G  1% /run/user/1000
/dev/sr0         51M   51M     0 100% /media/suga/VBox_GAs_7.0.18
suga@suga:~$
```

11.free -m

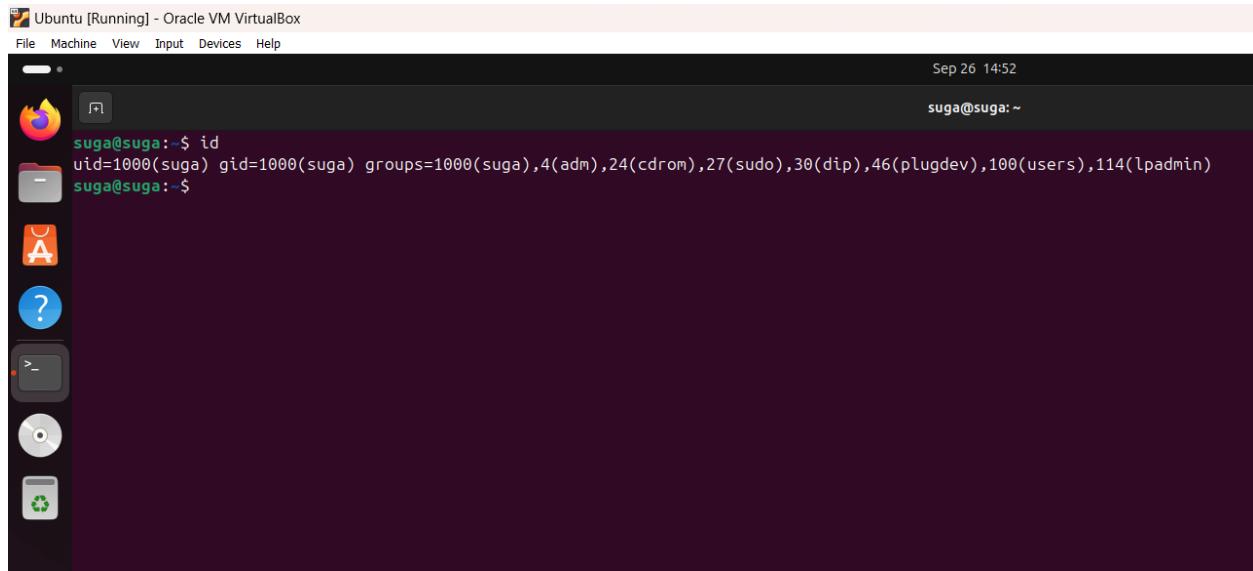
The command free -m displays the system memory usage in megabytes.



```
suga@suga:~$ free -m
              total        used        free      shared  buff/cache   available
Mem:       10952       1193       9008         39       1042       9758
Swap:      4095         0       4095
suga@suga:~$
```

12.id

The id command in the Ubuntu terminal is used to display user and group information for the current user or a specified user.

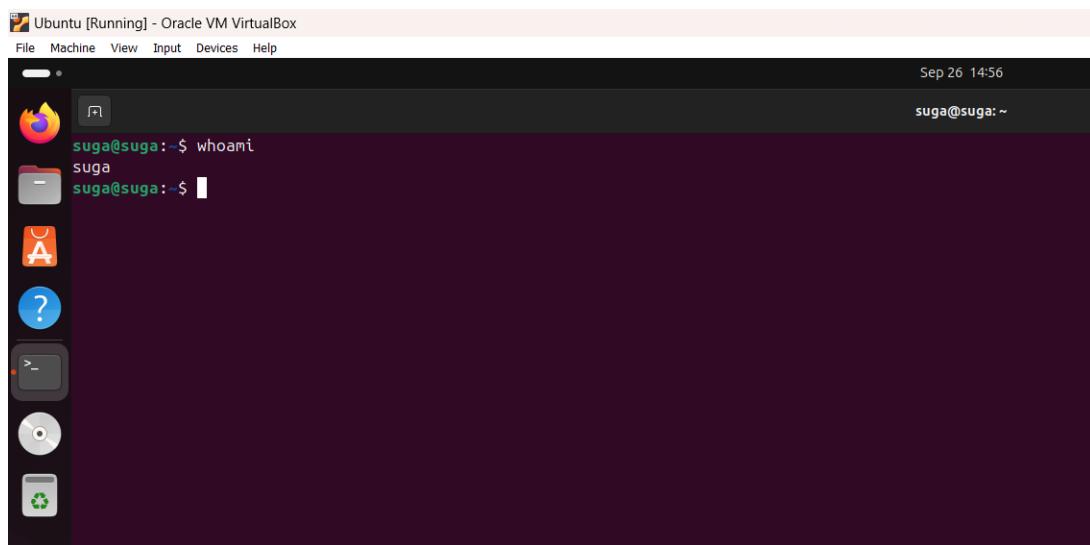


```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sep 26 14:52
suga@suga:~$ id
uid=1000(suga) gid=1000(suga) groups=1000(suga),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114(lpadmin)
suga@suga:~$
```

A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The window has a dark theme with white text. The title bar includes the window name, application menu, and system status. The terminal prompt is "suga@suga:~\$". The user runs the "id" command, which outputs their user ID (uid=1000), group ID (gid=1000), and supplementary groups (groups=1000, adm, cdrom, sudo, dip, plugdev, users, lpadmin). The window also shows a vertical dock on the left with icons for file operations like Open, Save, Copy, Paste, and Delete, along with other system icons.

13. whoami

The **whoami** command in the Ubuntu terminal is used to display the current logged-in username. It tells you who you are in terms of the user account you're using at that moment.

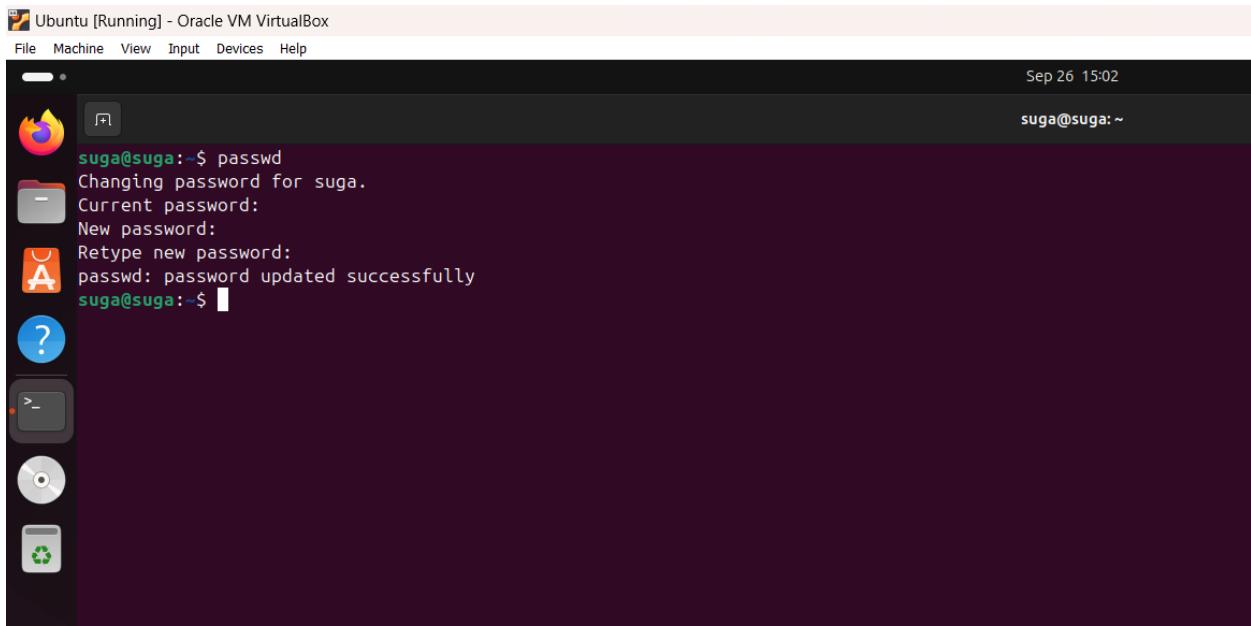


```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sep 26 14:56
suga@suga:~$ whoami
suga
suga@suga:~$
```

A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The window has a dark theme with white text. The title bar includes the window name, application menu, and system status. The terminal prompt is "suga@suga:~\$". The user runs the "whoami" command, which outputs their username "suga". The window also shows a vertical dock on the left with icons for file operations like Open, Save, Copy, Paste, and Delete, along with other system icons.

14. passwd

The **passwd** command is used to change a user's password. By default, it changes the password for the current user, but it can also be used to modify passwords for other users (with superuser privileges).

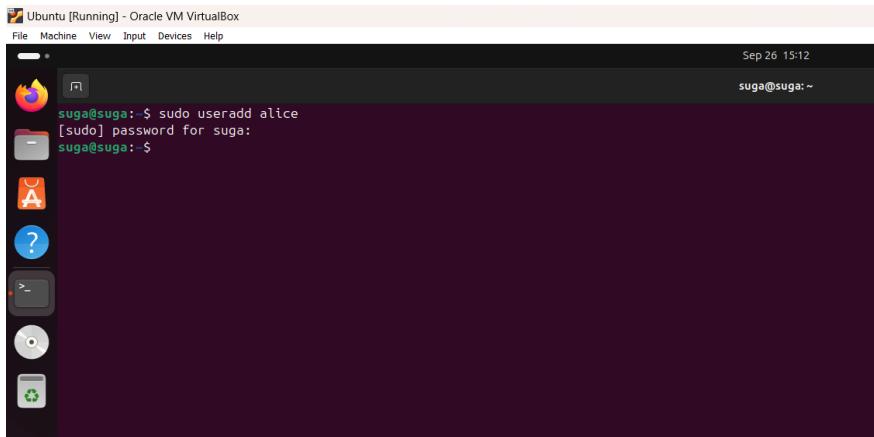


A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The window has a dark theme. The terminal prompt is "suga@suga:~\$". The user runs the command "passwd". The terminal asks for the current password, which is left blank. Then it asks for a new password, which is also left blank. Finally, it asks to retype the new password, which is also left blank. The terminal then displays the message "passwd: password updated successfully". The date and time at the top right of the terminal window are "Sep 26 15:02".

```
suga@suga:~$ passwd
Changing password for suga.
Current password:
New password:
Retype new password:
passwd: password updated successfully
suga@suga:~$
```

15. useradd

The **useradd** command is used to create a new user account on the system. This command allows system administrators to add users with specific configurations, such as setting the home directory.



A screenshot of a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The window has a dark theme. The terminal prompt is "suga@suga:~\$". The user runs the command "sudo useradd alice". The terminal prompts for a password, which is left blank. The user then types "suga" as the password. The terminal then displays the message "suga@suga:~\$". The date and time at the top right of the terminal window are "Sep 26 15:12".

```
suga@suga:~$ sudo useradd alice
[sudo] password for suga:
suga@suga:~$
```

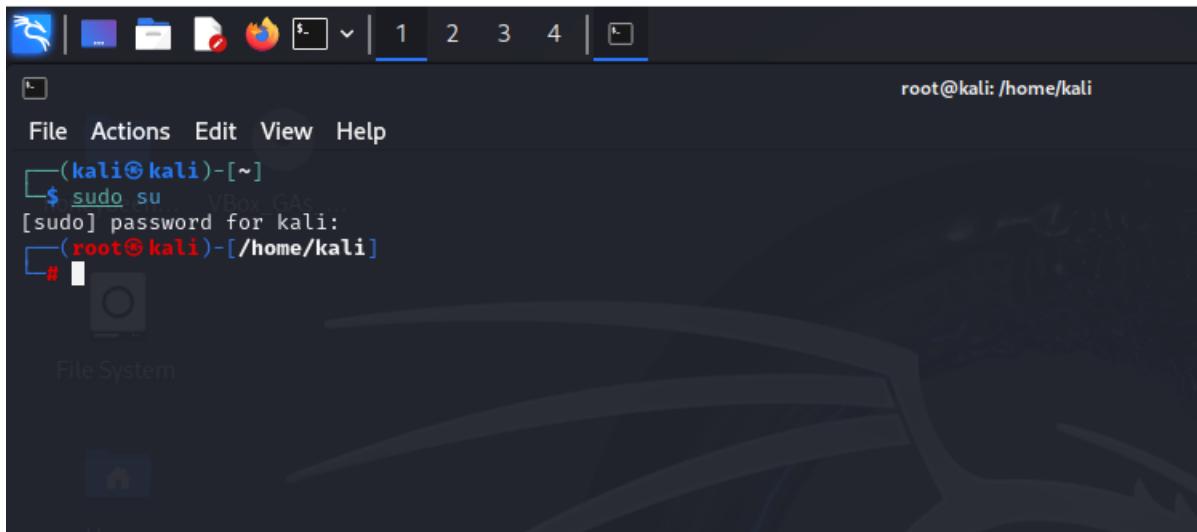
2 DHCP, DNS and NTP Services

2.1 DHCP (Dynamic Host Configuration Protocol)

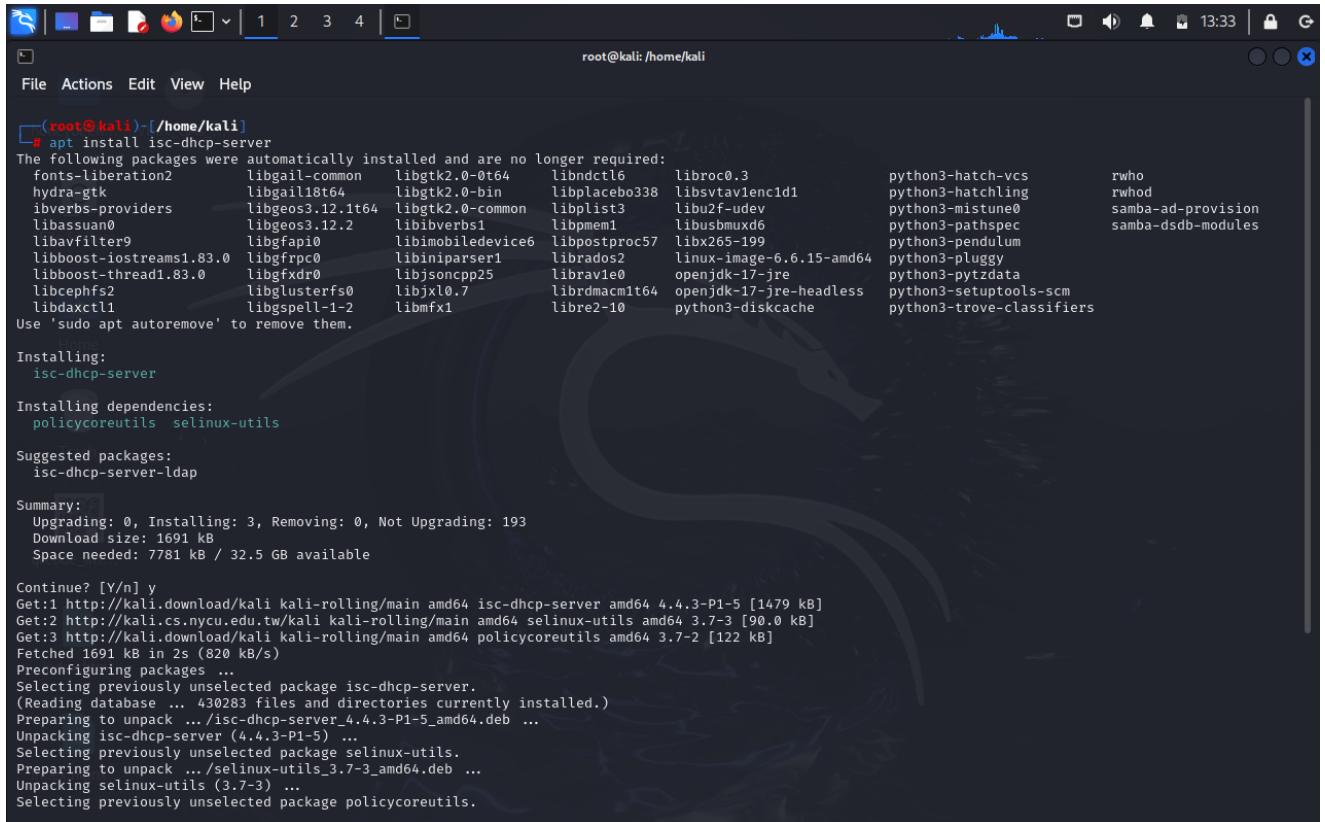
My Ubuntu VM started to be so buggy to the point I couldn't use it anymore. So I switched to Kali.

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used on IP networks. It automatically assigns IP addresses and other communication settings to devices on the network.

First login as root by giving the command `sudo su` and enter the password.

A screenshot of a Kali Linux terminal window. The title bar shows "root@kali: /home/kali". The terminal window has a dark background with a faint image of a person's face. The terminal prompt is "# ". The user has run the command "sudo su" and is prompted for a password. The terminal window also shows icons for various applications at the top.

To install DHCP server open Kali terminal and give the command `apt install isc-dhcp-server`.



```

root@kali:~/home/kali
# apt install isc-dhcp-server
The following packages were automatically installed and are no longer required:
fonts-liberation2 libgail-common libgtk2.0-0-t64 libndctl6 libroc0.3 python3-hatch-vcs
hydra-gtk libgail18t64 libgtk2.0-bin libplacebo338 libsvtavenc1d1 python3-hatchling
libverbs-providers libgeos3.12.1t64 libgtk2.0-common libplist3 libu2f-udev python3-mistune0
libbassuan0 libgeos3.12.2 libibverbs1 libpmem1 libusbxmxd6 python3-pathspect
libavfilter9 libgfapi0 libimobiledevice6 libpostproc57 libx265-199 python3-pendulum
libboost-iostreams1.83.0 libgfrpc0 libiniparser1 librados2 linux-image-6.6.15-amd64 python3-pluggy
libboost-thread1.83.0 libgwdx0 libjsoncpp25 librav1e0 openjdk-17-jre python3-ptzdata
libcephfs2 libglusterfs0 libjxl0.7 librdmacm1t64 openjdk-17-jre-headless python3-setuptools-scm
libdaxctl1 libgspell-1-2 libmfx1 libre2-10 python3-diskcache python3-trove-classifiers
Use 'sudo apt autoremove' to remove them.

Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed:
isc-dhcp-server
Policycoreutils  selinux-utils

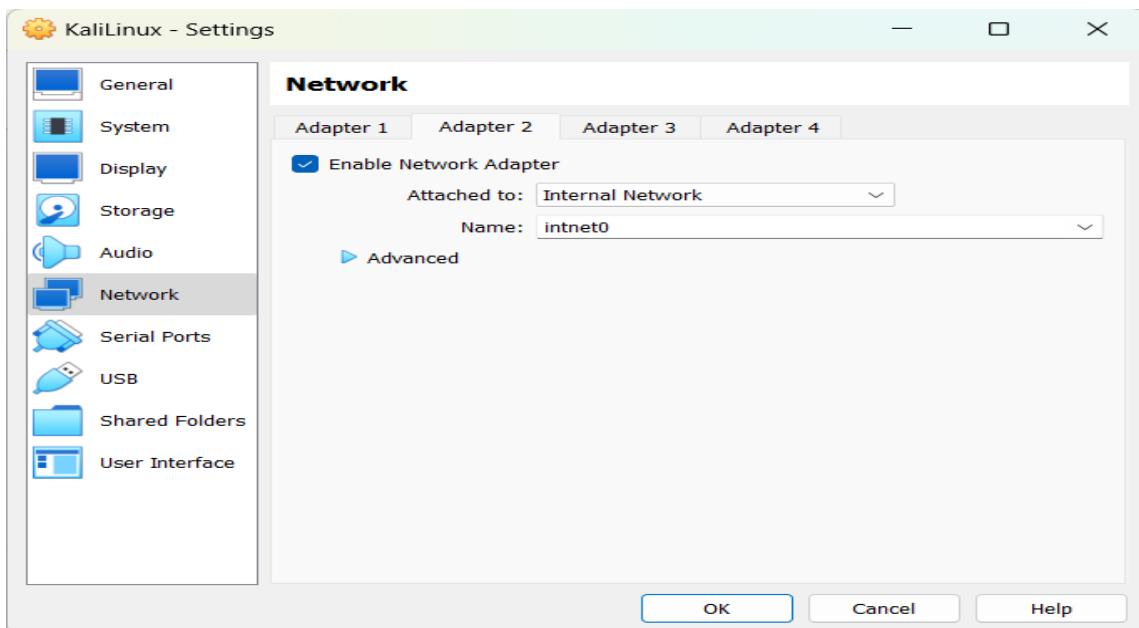
Suggested packages:
  isc-dhcp-server-ldap

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 193
  Download size: 1691 kB
  Space needed: 7781 kB / 32.5 GB available

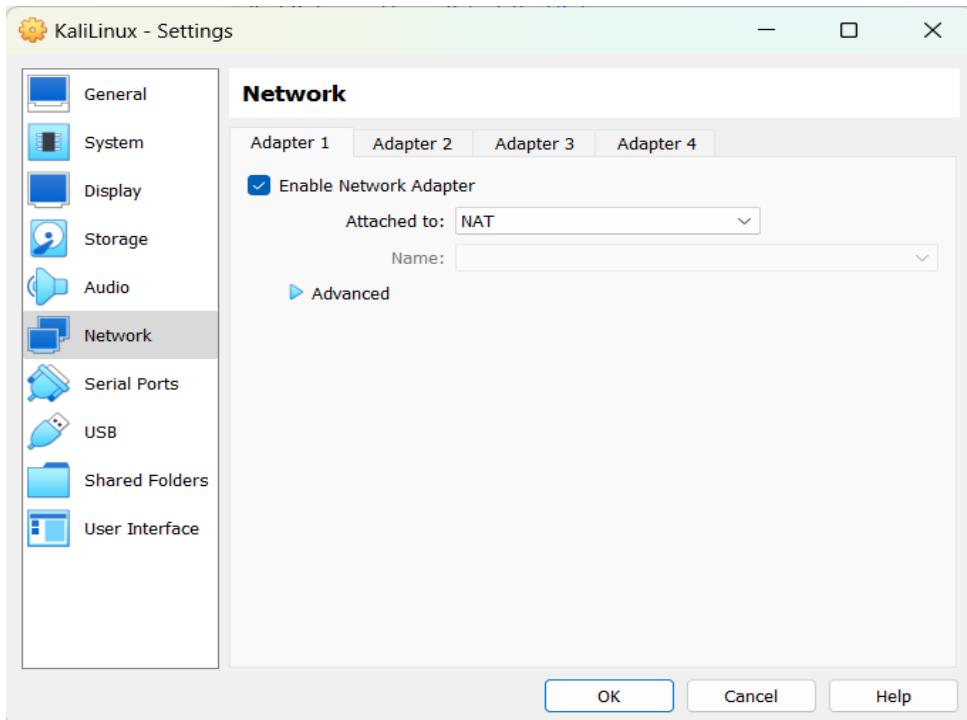
Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 isc-dhcp-server amd64 4.4.3-P1-5 [1479 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 selinux-utils amd64 3.7-3 [90.0 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 policycoreutils amd64 3.7-2 [122 kB]
Fetched 1691 kB in 2s (820 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 430283 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-5_amd64.deb ...
Unpacking isc-dhcp-server (4.4.3-P1-5) ...
Selecting previously unselected package selinux-utils.
Preparing to unpack .../selinux-utils_3.7-3_amd64.deb ...
Unpacking selinux-utils (3.7-3) ...
Selecting previously unselected package policycoreutils.

```

After installation go to setting of Kali VM and select network. Then press adopter 2 tab and tick enable network adopter and change “attached to:” option to **internal network**. And I have changed the name to intnet0 for easier identification.



Do not change the adopter one because it provides the connection to windows network.



To make the initial lease database use the command `touch /var/lib/dhcp/dhcpd.leases`

A screenshot of a terminal window titled "KaliLinux [Running] - Oracle VM VirtualBox". The window title bar includes "File Machine View Input Devices Help". The terminal window shows a root shell session. The user runs "sudo su", enters the password for kali, and then runs the command "# touch /var/lib/dhcp/dhcpd.leases". The prompt ends with a "#". The status bar at the bottom right shows "root@kali: /home/kali".

Then type `dhcpd` you can initiate the DHCP server and test the server configuration.

```
(root㉿kali)-[~/home/kali]
# dhcpcd
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.

No subnet declaration for eth2 (no IPv4 addresses).
** Ignoring requests on eth2. If this is not what
you want, please write a subnet declaration
in your dhcpd.conf file for the network segment
to which interface eth2 is attached. **

No subnet declaration for eth1 (no IPv4 addresses).
** Ignoring requests on eth1. If this is not what
you want, please write a subnet declaration
in your dhcpd.conf file for the network segment
to which interface eth1 is attached. **

No subnet declaration for eth0 (no IPv4 addresses).
** Ignoring requests on eth0. If this is not what
you want, please write a subnet declaration
in your dhcpd.conf file for the network segment
to which interface eth0 is attached. **

index.html

Not configured to listen on any interfaces!

If you think you have received this message due to a bug rather
than a configuration issue please read the section on submitting
bugs on either our web page at www.isc.org or in the README file
before submitting a bug. These pages explain the proper
process and the information we find helpful for debugging.

exiting.
```

To verify whether it's working properly or not, type **ifconfig**.

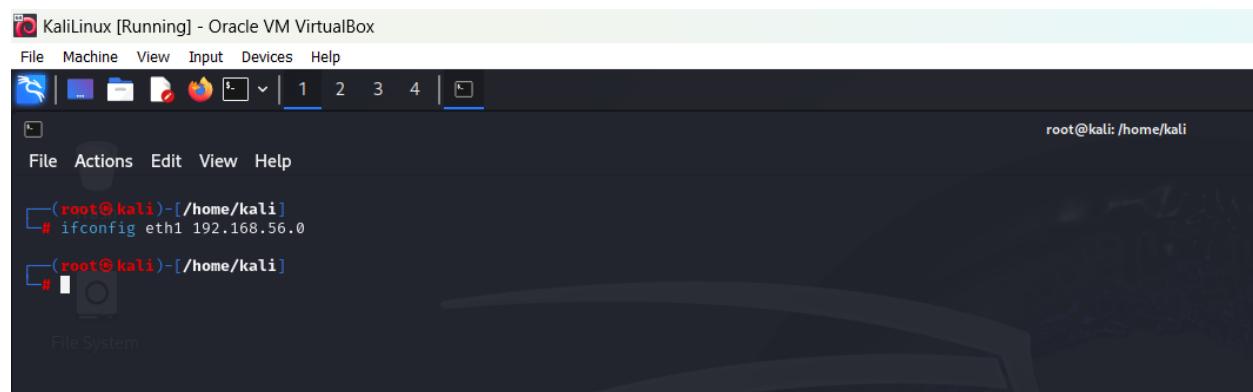
```

└─(root㉿kali)-[~/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      ether 08:00:27:42:3e:52  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

VBox_Guru
qrcode
index.html
honeybeeh
└─(root㉿kali)-[~/home/kali]
# ┌──

```

We will assign IPv4 address to eth1 by using the command **ifconfig eth1 192.168.56.0** as user's DHCP IP address.



To define the subnet and the IP range we will go to **dhcpd.conf** file in **/etc/dhcp**.

```
File Actions Edit View Help
GNU nano 8.1
# dhcpd.conf
#
# Sample configuration file for ISC dhcpcd
#
# option definitions common to all supported networks ...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.56.0 netmask 255.255.255.0{
    range 192.168.56.10 192.168.56.100;
    option routers 192.168.56.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.1, 192.168.1.2;
    option domain-name "snpdhcp";
    # interface eth1;
    # INTERFACESv4=eth1;
}
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;
```

Type below information inside **the dhcpd.conf** file.

subnet 192.168.56.0 netmask 255.255.255.0 – Defines the subnet that the DHCP will be managing.

range 192.168.56.10 192.168.56.100 – This is the range that the DHCP can assign clients to

option routers 192.168.56.1 – Defines the default gateway

option domain-name-servers 192.168.1.1 192.168.1.2 – DNS servers clients should use

option domain-name “snpdhcp” – Defines the domain name

Go to **/etc/default/isc-dhcp-server** and change INTERFACESv4 to **eth1**.

KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

GNU nano 8.1

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth1"
INTERFACESv6=""
```

Then use the command `systemctl restart isc-dhcp-server` to restart the server.

KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
[root@kali]~[/home/kali]
# systemctl restart isc-dhcp-server
[root@kali]~[/home/kali]
```

To check the status of the server type `systemctl status isc-dhcp-server` and `dhcpd`

KaliLinux [Running] - Oracle VM VirtualBox

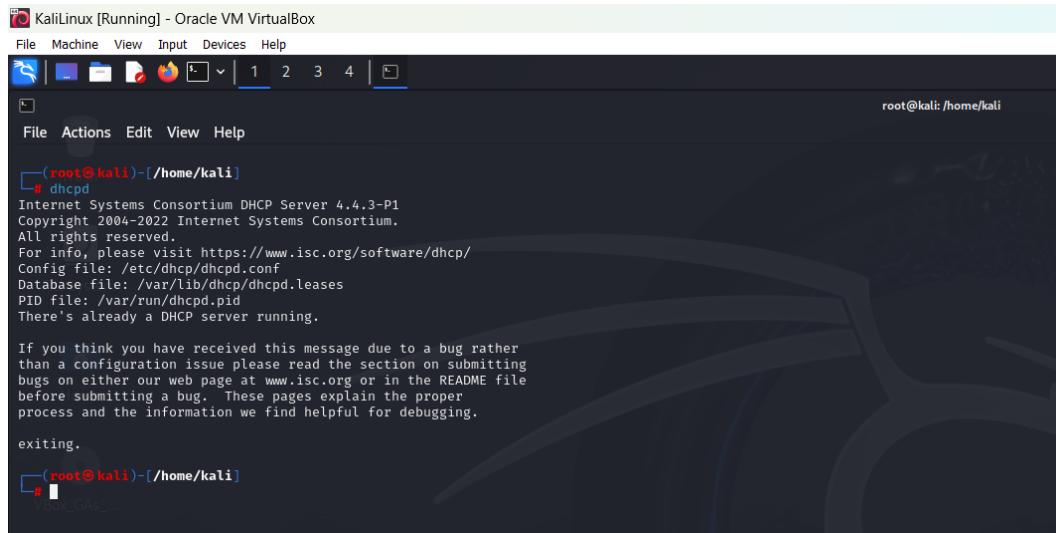
File Machine View Input Devices Help

File Actions Edit View Help

```
[root@kali]~[/home/kali]
# systemctl restart isc-dhcp-server
[root@kali]~[/home/kali]
# systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
  Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
  Active: active (running) since Sun Oct  3 17:15:02 2024-10-03 17:15:02 +0530; 2min 48s ago
    Docs: man:systemd-sysv-generator(8)
   Process: 68321 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Tasks: 1 (limit: 14213)
     Memory: 3.9M (peak: 6.2M)
      CPU: 70ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─68334 /usr/sbin/dhcpd -n -q -cf /etc/dhcp/dhcpd.conf eth1

Oct 03 17:15:00 kali systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server ...
Oct 03 17:15:00 kali isc-dhcp-server[68321]: Launching IPv4 server only.
Oct 03 17:15:00 kali dhcpcd[68334]: Wrote 0 leases to leases file.
Oct 03 17:15:00 kali dhcpcd[68334]: Server starting service.
Oct 03 17:15:02 kali isc-dhcp-server[68321]: Starting ISC DHCPv4 server: dhcpd.
Oct 03 17:15:02 kali systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.

[root@kali]~[/home/kali]
```



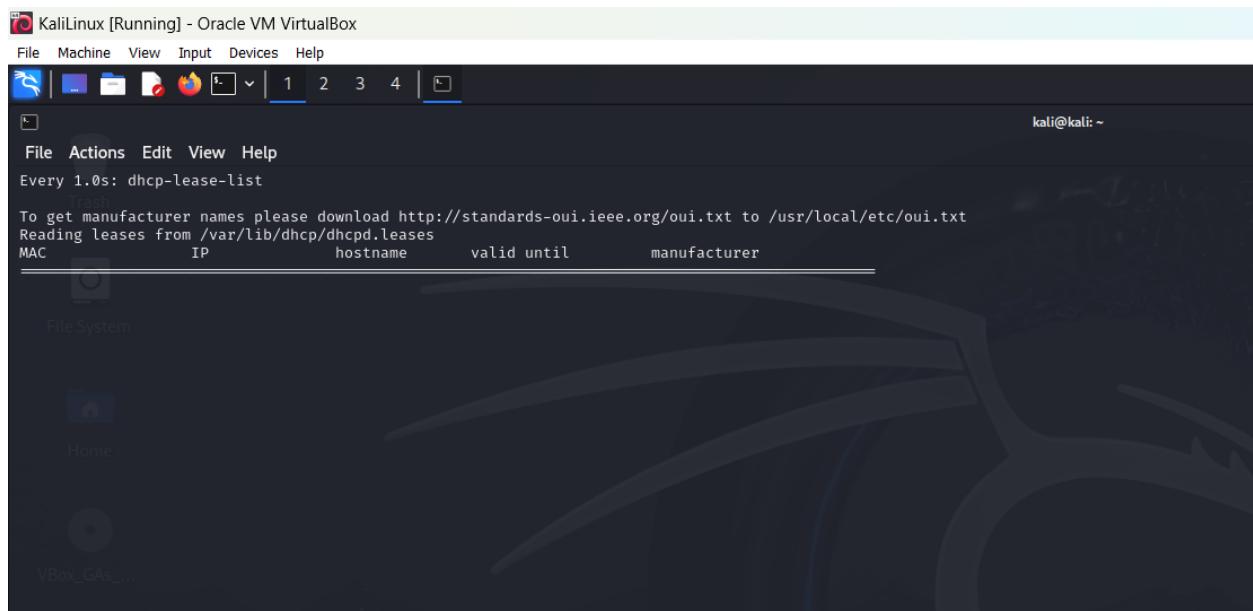
```
(root@kali)-[~/home/kali]
# dhcpcd
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpcd.conf
Database file: /var/lib/dhcp/dhcpcd.leases
PID file: /var/run/dhcpcd.pid
There's already a DHCP server running.

If you think you have received this message due to a bug rather
than a configuration issue please read the section on submitting
bugs on either our web page at www.isc.org or in the README file
before submitting a bug. These pages explain the proper
process and the information we find helpful for debugging.

exiting.

[root@kali]-[~/home/kali]
```

Use the command **watch -n 1 dhcp-lease-list** to view how devices get assigned IP addresses.



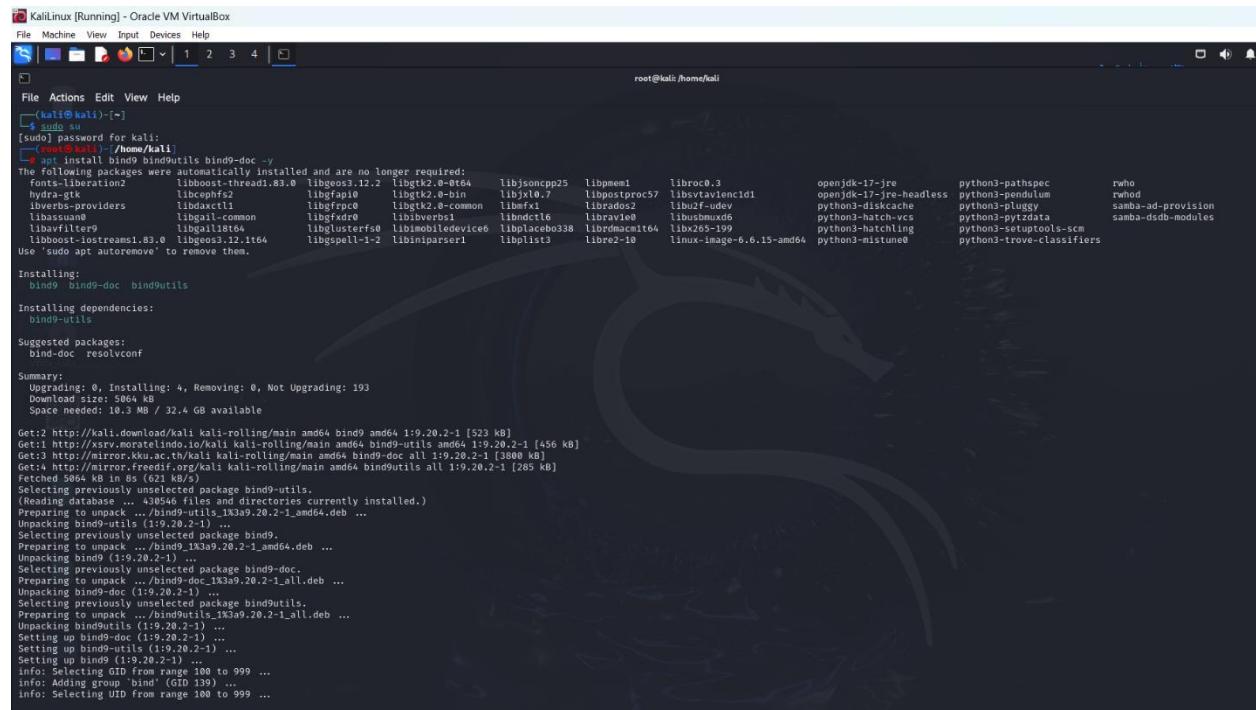
```
kali@kali: ~
File Actions Edit View Help
Every 1.0s: dhcp-lease-list
To get manufacturer names please download http://standardsoui.ieee.org/oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpcd.leases
MAC          IP           hostname      valid until    manufacturer
_____

```

2.2 DNS (Domain Name System)

DNS is a very important component of the internet. It translates human-readable domain names into IP addresses which computers use to communicate with each other.

First we will install BIND9 and all the utilities that comes with bind9 using the command `apt install bind9 bind9utils bind9-doc -y`.



```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
$ sudo su
[sudo] password for kali:
[root@kali:~]
# apt install bind9 bind9utils bind9-doc -y
The following packages were automatically installed and are no longer required:
  fonts-liberation2 libboost-thread1.83.0 libgeoip3.12.2 libgtk2.0-0t64 libjsoncpp25 libpmem1 libroc0.3
  openjdk-17-jre python3-pathspec rwho
  hydra-gtk libcephfs2 libgfaio libgtk2.0-bin libjxl0.7 libpostproc5 libsvavencld1 openjdk-17-jre-headless python3-pendulum rwmod
  libverbs-providers libdaxctl libgfrpc libgtk2.0-common libmfx1 libradis2 libu2f-udev python3-diskcache python3-pluggy samba-ad-provision
  libassuan libgal-common libgrx0 libibverbs1 libinotify0 libibusmuxd python3-hatch-vcs python3-ptzdata samba-dsdb-modules
  libhavfilter9 libgbal11t64 libgusterfs9 libimobiledevice6 libplacebo338 librdmacm1t64 libx265-199 python3-hatching python3-setuptools-scm
  libboost-iostreams1.83.0 libgeoip3.12.1t64 libgspell-1-2 libiniparser1 libplist3 libre2-10 linux-image-6.6.15-amd64 python3-mistune0
Use 'sudo apt autoremove' to remove them.

Installing:
bind9 bind9-doc bind9utils

Installing dependencies:
bind9-utils

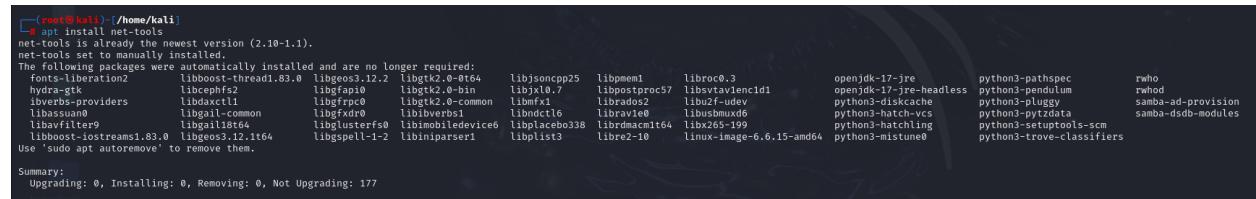
Suggested packages:
bind-doc resolvconf

Summary:
Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 193
Download size: 5064 kB
Space needed: 10.3 MB / 32.4 GB available

Get:2 http://http://kali/download/kali-kali-rolling/main amd64 bind9 amd64 1:9.20.2-1 [523 kB]
Get:3 http://http://xrv.moratellino.it/kali-kali-rolling/main amd64 bind9-utils all 1:9.20.2-1 [456 kB]
Get:4 http://http://mirror.freedomsoft.org/kali/kali-rolling/main amd64 bind9utils all 1:9.20.2-1 [285 kB]
Fetched 5064 kB in 8s (621 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 439546 files and directories currently installed.)
Prepating to unpack .../bind9_1x3a9.20.2-1_amd64.deb ...
Unpacking bind9-utils (19.20.2-1) ...
Selecting previously unselected package bind9,
Preparing to unpack .../bind9_1x3a9.20.2-1_amd64.deb ...
Unpacking bind9 (19.20.2-1) ...
Selecting previously unselected package bind9-doc.
Preparing to unpack .../bind9-doc_1x3a9.20.2-1_all.deb ...
Unpacking bind9-doc (19.20.2-1) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1x3a9.20.2-1_all.deb ...
Unpacking bind9utils (19.20.2-1) ...
Setting up bind9 (19.20.2-1) ...
Setting up bind9-utils (19.20.2-1) ...
Setting up bind9 (19.20.2-1) ...
info: Selecting GID from range 100 to 999 ...
info: Adding group bind (GID 139) ...
info: Selecting UID from range 100 to 999 ...


```

Then we need to install net tools. For that we'll use the command `apt install net-tools`

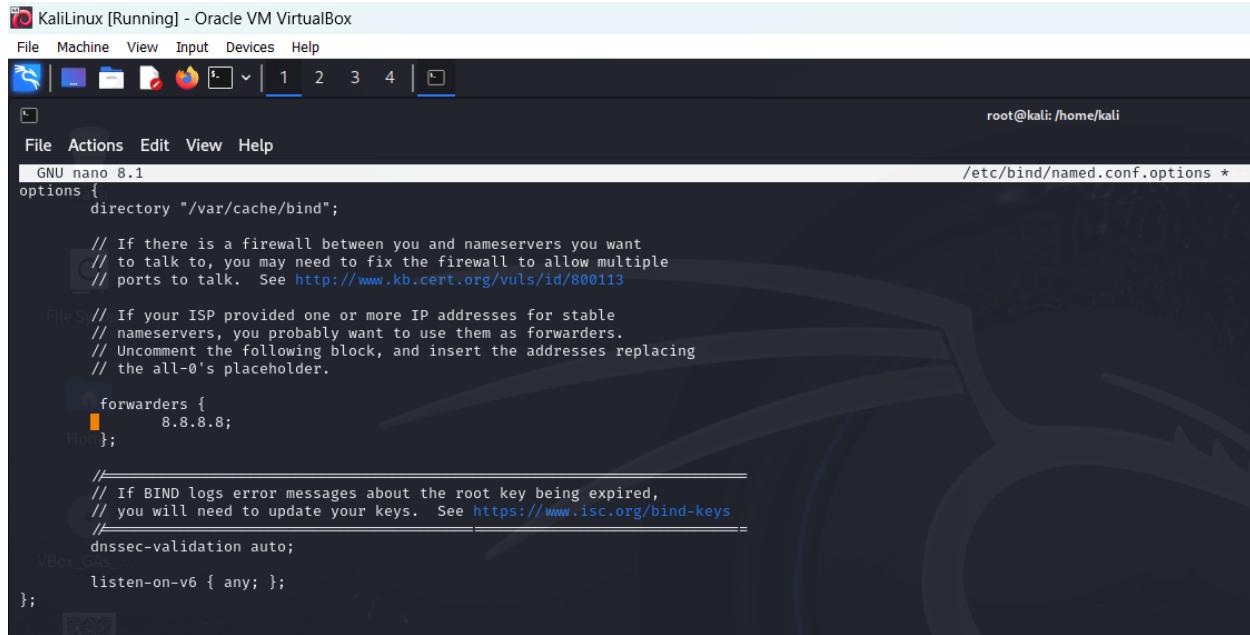


```
[root@kali:~]
# apt install net-tools
net-tools is already the newest version (2.10-1.1).
net-tools set to manually install.
The following packages were automatically installed and are no longer required:
  fonts-liberation2 libboost-thread1.83.0 libgeoip3.12.2 libgtk2.0-0t64 libjsoncpp25 libpmem1 libroc0.3
  openjdk-17-jre python3-pathspec rwho
  hydra-gtk libcephfs2 libgfaio libgtk2.0-bin libjxl0.7 libpostproc5 libsvavencld1 openjdk-17-jre-headless python3-pendulum rwmod
  libverbs-providers libdaxctl libgfrpc libgtk2.0-common libmfx1 libradis2 libu2f-udev python3-diskcache python3-pluggy samba-ad-provision
  libassuan libgal-common libgrx0 libibverbs1 libinotify0 libibusmuxd python3-hatch-vcs python3-ptzdata samba-dsdb-modules
  libhavfilter9 libgbal11t64 libgusterfs9 libimobiledevice6 libplacebo338 librdmacm1t64 libx265-199 python3-hatching python3-setuptools-scm
  libboost-iostreams1.83.0 libgeoip3.12.1t64 libgspell-1-2 libiniparser1 libplist3 libre2-10 linux-image-6.6.15-amd64 python3-mistune0
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 177
```

Next we'll use the command `nano /etc/bind/named.conf.options` to edit the file

`named.conf.options`. Uncomment the forwarders and change it to 8.8.8.8(google DNS). Then save the changes made.



```
root@kali: /home/kali
GNU nano 8.1
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

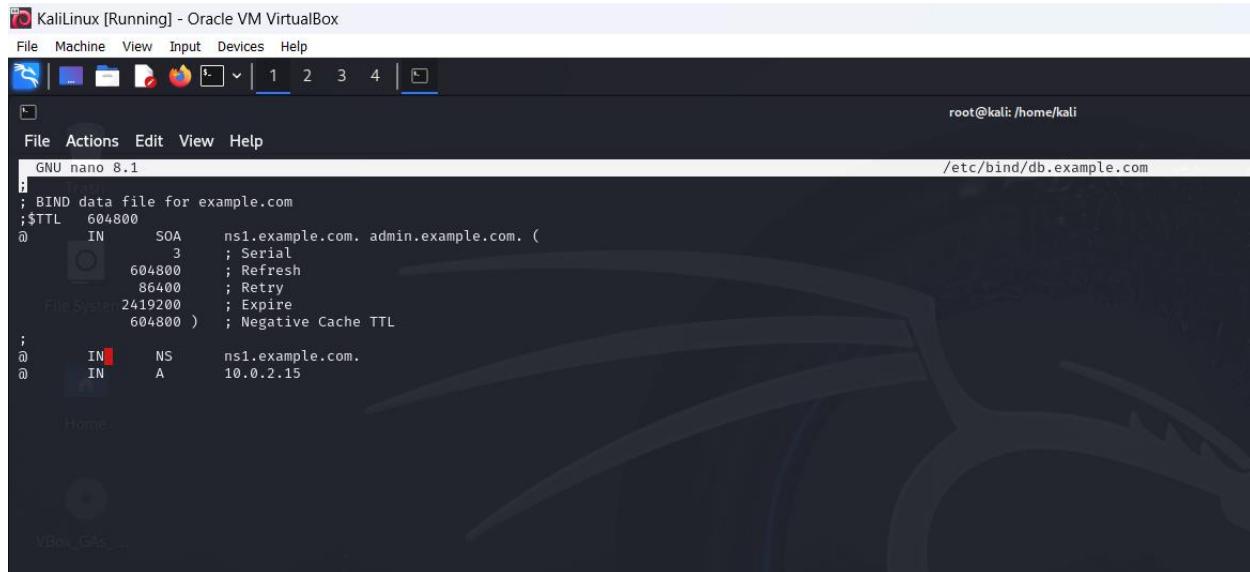
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
    };

    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    dnssec-validation auto;
}
listen-on-v6 { any; };
};
```

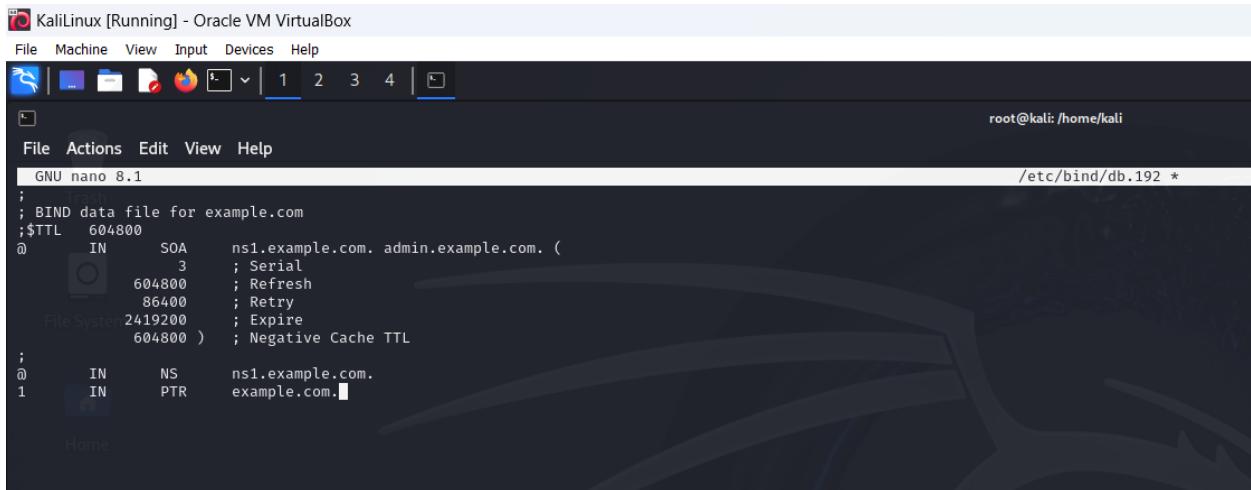
Next we'll use the command `nano /etc/bind/db.example.com` to edit the file `db.example.com`.

Add the below information(I have added my current IP address below) and then save the changes made.



```
root@kali: /home/kali
GNU nano 8.1
;
; BIND data file for example.com
;$TTL 604800
@ IN SOA ns1.example.com. admin.example.com. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns1.example.com.
@ IN A 10.0.2.15
```

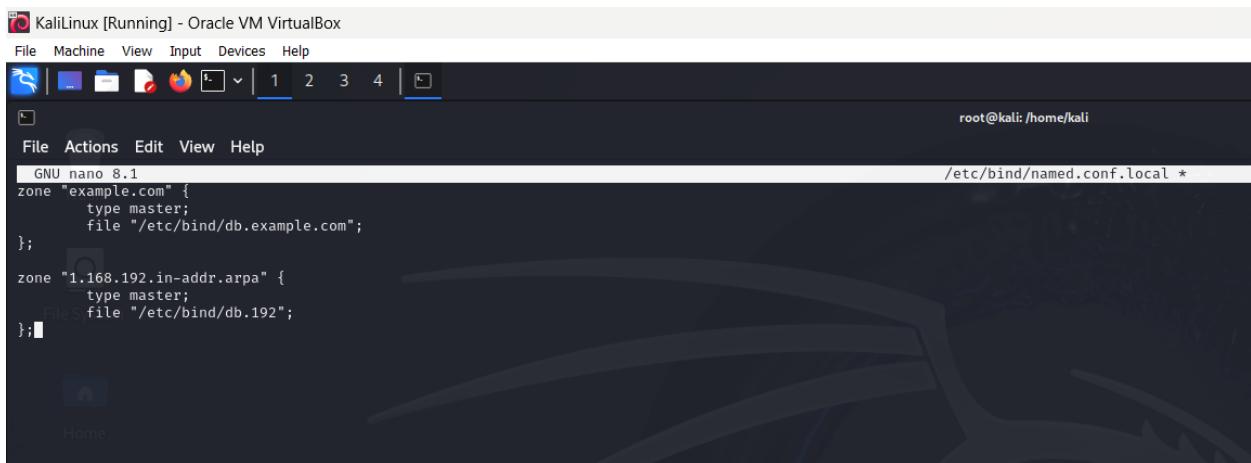
Next we'll use the command `nano /etc/bind/db.192` to edit the file `db.192`. Add the below information and then save the changes made.



```
root@kali: /home/kali
GNU nano 8.1
;
; BIND data file for example.com
;TTL    604800
@      IN      SOA     ns1.example.com. admin.example.com. (
                      3          ; Serial
                     604800    ; Refresh
                     86400     ; Retry
                    2419200   ; Expire
                     604800 )  ; Negative Cache TTL
;
@      IN      NS      ns1.example.com.
1      IN      PTR     example.com.
```

Next we'll use the command `nano /etc/bind/named.conf.local` to edit the file `named.conf.local`.

Add the below information and then save the changes made.



```
root@kali: /home/kali
GNU nano 8.1
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

To start bind9 use the command `systemctl restart bind9`. In my case the terminal gave me a error as shown below. To troubleshoot that I used the command `systemctl enable named` and `systemctl start named`. Then use the command `systemctl restart bind9` to start bind9 and to check the status type `systemctl status bind9` and hit enter.

```

[root@kali]~[/]
# systemctl restart bind9
Failed to restart bind9.service: Unit bind9.service not found.

[root@kali]~[/]
# systemctl enable named
Synchronizing state of named.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable named
Created symlink '/etc/systemd/system/bind9.service' → '/usr/lib/systemd/system/named.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.

[root@kali]~[/]
# systemctl start named

[root@kali]~[/]
# systemctl restart bind9

[root@kali]~[/]
# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
     Active: active (running) since Fri 2024-10-04 17:09:35 +0530; 15s ago
   Invocation: cdc1442583a547db8e1le9670dd1cd
   Docs: man:named(8)
 Main PID: 60001 (named)
    Status: "running"
      Tasks: 26 (limit: 14213)
     Memory: 46M (peak: 47.1M)
        CPU: 12ms
      CGroup: /system.slice/named.service
              └─60001 /usr/sbin/named -f -u bind

Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:500:2::cf#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Oct 04 17:09:35 kali named[60001]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Oct 04 17:09:35 kali named[60001]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)

[root@kali]~[/]
# 

```

We need to make sure that bind9 is allowed through my firewall. In order to do that we need to check the firewall is active or not by typing the command **ufw status**. Then we'll add the rules that allows bind9 to go through the firewall by using the command **ufw allow bind9**. After adding the rules, to reload the firewall use the command **ufw reload**. To check the status of the firewall type **ufw status**.

The screenshot shows a terminal window titled 'KaliLinux [Running] - Oracle VM VirtualBox'. The terminal displays the following commands and their outputs:

```

File Machine View Input Devices Help
File Actions Edit View Help
[root@kali]~[/]
# ufw status
Status: active

[root@kali]~[/]
# ufw allow bind9
Rule added
Rule added (v6)

[root@kali]~[/]
# ufw reload
Firewall reloaded

[root@kali]~[/]
# ufw status
Status: active

To          Action      From
--          ALLOW      Anywhere
Bind9       ALLOW      Anywhere (v6)

[root@kali]~[/]
# 

```

Then go to windows OS and open command prompt. In the command prompt type **ping www.example.com**. If we get a response that means the DNS is up and running.

```
C:\Users\hp-pc>ping www.example.com

Pinging www.example.com [2606:2800:21f:cb07:6820:80da:af6b:8b2c] with 32 bytes of data:
Reply from 2606:2800:21f:cb07:6820:80da:af6b:8b2c: time=276ms
Reply from 2606:2800:21f:cb07:6820:80da:af6b:8b2c: time=292ms
Reply from 2606:2800:21f:cb07:6820:80da:af6b:8b2c: time=324ms
Reply from 2606:2800:21f:cb07:6820:80da:af6b:8b2c: time=348ms

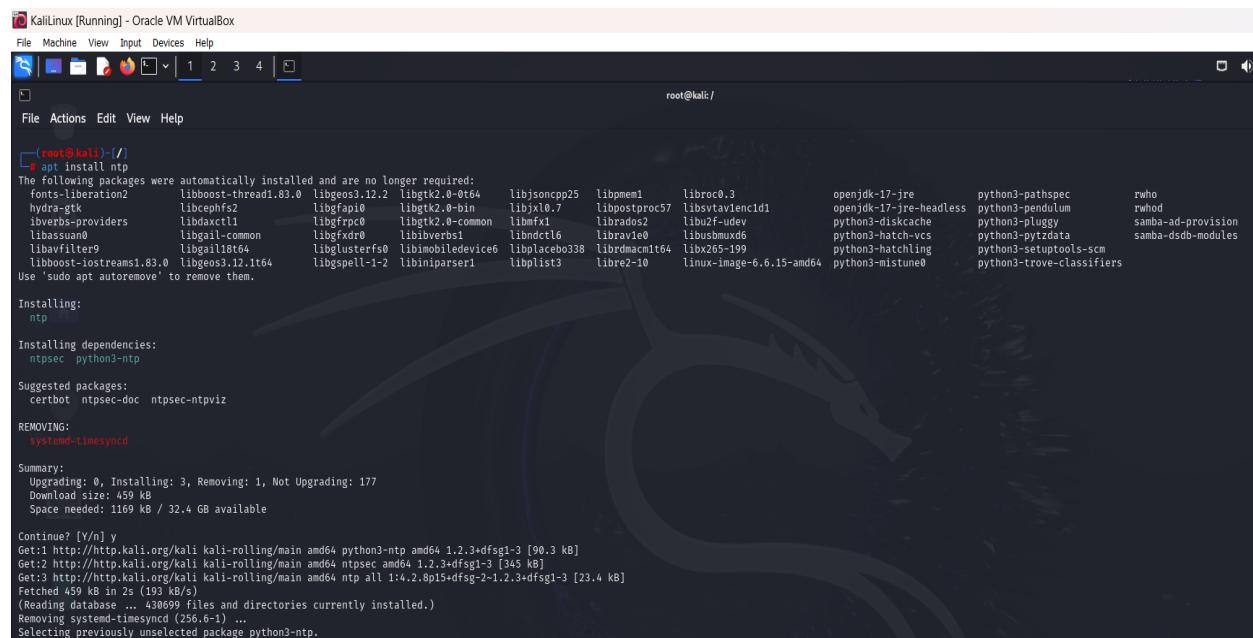
Ping statistics for 2606:2800:21f:cb07:6820:80da:af6b:8b2c:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 276ms, Maximum = 348ms, Average = 310ms

C:\Users\hp-pc>
```

2.3 NTP (Network Time Protocol)

NTP (Network Time Protocol) is a protocol used to synchronize the system time with remote servers over a network. It ensures that your system's clock is accurate by synchronizing it with trusted time sources, usually time servers that are synchronized to atomic clocks.

In order to install NTP use the command **apt install ntp**.



The screenshot shows a terminal window on Kali Linux with the root user logged in. The command `apt install ntp` is being run. The terminal output shows the package manager listing automatically installed packages that are no longer required, installing the `ntp` package, and removing the `systemd-timesyncd` package. It also shows the upgrade, download, and space usage details. The terminal ends with a prompt asking if the user wants to continue.

```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# apt install ntp
The following packages were automatically installed and are no longer required:
fonts-liberation2 libboost-thread1.83.0 libgeos3.12.2 libgtk2.0-0.164 libjsoncpp25 libpnm1 libroco.3
hydra-gtk libcephfs2 libgapi0 libgtk2.0-bin libjxl0.7 libpostproc57 libsvtavenc1d1
libverbs-providers libdaxctl libgrpc0 libgtk2.0-common libimx1 librados2 libuf-udev
libassuan0 libgail-common libgxr0 libibverbs1 libndctl6 libravel0 libusbmuxd6
libavfilter9 libgallib864 libglusterfs0 libimobiledevice6 libplacebo338 librdmacm1t64 libx265-199
libboost-iostreams1.83.0 libgeos3.12.1t64 libgspell-1-2 libiniparser1 libplist3 libre2-10 linux-image-6.6.15-amd64
Use 'sudo apt autoremove' to remove them.

Installing:
ntp

Installing dependencies:
ntpsec python3-ntp

Suggested packages:
certbot ntpsec-doc ntpsec-ntpviz

REMOVING:
systemd-timesyncd

Summary:
Upgrading: 0, Installing: 3, Removing: 1, Not Upgrading: 177
Download size: 459 kB
Space needed: 1169 kB / 32.4 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-ntp amd64 1.2.3+dfsg1-3 [90.3 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 ntpsec amd64 1.2.3+dfsg1-3 [345 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 ntp all 1:4.2.8p15+dfsg-2-1.2.3+dfsg1-3 [23.4 kB]
Fetched 459 kB in 25 (193 kB/s)
(Reading database ... 430699 files and directories currently installed.)
Removing systemd-timesyncd (256.6-1) ...
Selecting previously unselected package python3-ntp.
```

Startup the NTP service with **ntpd** command.

```
File Actions Edit View Help

└─(root㉿kali)-[~/]
# ntpd
2024-10-04T23:50:42 ntpd[204624]: INIT: ntpd ntpsec-1.2.3: Starting
2024-10-04T23:50:42 ntpd[204624]: INIT: Command line: ntpd
```

Type the command **ntpq** to test the server.

```
└─(root㉿kali)-[~/]
# ntpq
ntpq> ?
System

Documented commands (type help <topic>):
=====
:config      debug      logfile      opeers      rv
EOF          delay      lopeers      passociations  showvars
addvars      direct      lpassociations  passwd      sysinfo
apeers      doflake      lpeers      peers      sysstats
associations  exit      monstats      poll      timeout
authenticate  help      mreadlist      pstats      timerstats
authinfo      host      mreadvar      quit      units
cl           hostnames      mrl      raw      version
clearvars    ifstats      mrulist      readlist      writelist
clocklist    iostats      mrv      readvar      writevar
clockvar     kerninfo      mssntpinfo      reslist
config-from-file  keyid      noflake      rl
cooked       keytype      ntpversion      rmvars
cv           lassociations  ntsinfo      rpeers
ntpq> [REDACTED]
```

The command **ntpstat** will display the synchronization status.

```
└─(root㉿kali)-[~/]
# ntpstat
unsynchronised
polling server every 1 s
honeybee@kali:~$
```

Install **systemd-timesyncd** package by using **apt install systemd-timesyncd** command. This implies getting the NTP service as well as synchronizing time in this package.

```
(root@kali)-[/]
# apt install systemd-timesyncd
[...]
The following packages were automatically installed and are no longer required:
fonts-liberation libboost-thread1.83.0 libgeos3.12.2 libgtk2.0-0t64 libjsoncpp25 libpmem1 libroc0.3 openjdk-17-jre python3-pathspec rwho
hydra-gtk libcephfs2 libgapi0 libgtk2.0-bin libjxl0.7 libpostproc57 libstavlenc1d1 openjdk-17-jre-headless python3-pendulum rwtmp
libverbs-providers libdaxctl1 libgprc0 libgtk2.0-common libmfx1 librados2 libuf-udev python3-diskcache python3-pluggy samba-ad-provision
libassuan0 libgail-common libgxr0 libibusvrs1 libndctl6 libravie0 libusbmuxd python3-hatch-vcs python3-pytzdata samba-dsdb-modules
libafilter9 libgail0t64 libglusterfs0 libimobiledevice6 libplacebo338 librdmacm164 libx265-199 python3-hatchling python3-setupools-scm
libboost-iostreams1.83.0 libgeos3.12.1t64 libgspell-1-2 libiniparser1 libplist3 libre2-10 linux-image-6.6.15-amd64 python3-mistune0 python3-trove-classifiers
Use 'sudo apt autoremove' to remove them.

Installing:
systemd-timesyncd

REMOVING:
ntpsec

Summary:
Upgrading: 0, Installing: 1, Removing: 1, Not Upgrading: 17
Download size: 85.4 kB
Free disk space: 740 kB

Continue? [y/n] y
Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 systemd-timesyncd amd64 256.6-1 [85.4 kB]
Fetched 85.4 kB in 2s (36.7 kB/s)
(Reading database ... 430770 files and directories currently installed.)
Removing ntpsec (1.2.3+dfsg1-3) ...
Warning: The unit file /etc/systemd/system/ntpsec.rotate-statistics.timer changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file /etc/systemd/system/ntpsec-systemd-netif.path changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file /etc/systemd/system/ntpsec.service changed on disk. Run 'systemctl daemon-reload' to reload units.
Selecting previously unselected package systemd-timesyncd.
(Reading database ... 430729 files and directories currently installed.)
Preparing to unpack .../systemd-timesyncd_256.6-1_amd64.deb ...
Unpacking systemd-timesyncd (256.6-1) ...
Setting up systemd-timesyncd (256.6-1) ...
systemd-time-wait-sync.service is a disabled or a static unit not running, not starting it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for dbus (1.14.10-4+b1) ...
Processing triggers for kali-menu (2024.3.1) ...
```

After that run the command **timedatectl** status to check the status of the NTP.

```
(root@kali)-[/]
# timedatectl status
    Local time: Sat 2024-10-05 00:02:04 +0530
    Universal time: Fri 2024-10-04 18:32:04 UTC
          RTC time: Fri 2024-10-04 18:32:04
        Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
File System  NTP service: active
      RTC in local TZ: no

(root@kali)-[/]
#
```

3 Shell Scripting and Security

3.1 Shell Scripting

- i. First create a shell script file called **system_report.sh**. in order to do that write the command **sudo nano system_report.sh** in the terminal.

```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[root@kali ~]# nano system_report.sh
--(Kali㉿kali)-~/system_reports
-- cd..
cd..: Command not found
-- cd..
cd..: Command not found
--(Kali㉿kali)-~/system_reports
-- cd..
```

Then write the below script inside the **system_report.sh**.

```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
GNU nano 8.1
#!/bin/bash
# Define the destination directory for reports
DEST_DIR="/home/kali/system_reports"
# Create the destination directory if it doesn't exist
if [ ! -d "$DEST_DIR" ]; then
    mkdir -p "$DEST_DIR"
fi
# Define the report file name with the current date
DATE=$(date +%Y-%m-%d)
REPORT_FILE="$DEST_DIR/system_report_$DATE.txt"
# Collect system information and write to the report file
{
    echo "System Report - $DATE"
    echo "-----"
    echo "Date and Time: $(date)"
    echo "System Uptime: $(uptime -p)"
    echo "Free Memory: $(free -h | grep Mem | awk '{print $4}')"
    echo "Disk Usage:"
    df -h /home/
    echo "-----"
} > "$REPORT_FILE"
# Display success message
echo "System report created: $REPORT_FILE"
```

```

#!/bin/bash

# Define the destination directory for reports

DEST_DIR="/home/kali/system_reports"

# Create the destination directory if it doesn't exist

if [ ! -d "$DEST_DIR" ]; then

    mkdir -p "$DEST_DIR"

fi

# Define the report file name with the current date

DATE=$(date +%Y-%m-%d)

REPORT_FILE="$DEST_DIR/system_report_$DATE.txt"

# Collect system information and write to the report file

{

echo "System Report - $DATE"

echo "-----"

echo "Date and Time: $(date)"

echo "System Uptime: $(uptime -p)"

echo "Free Memory: $(free -h | grep Mem | awk '{print $4}')"

echo "Disk Usage:"

df -h

echo "-----"

} > "$REPORT_FILE"

echo "System report created: $REPORT_FILE"

```

DEST_DIR: The script will store the report in `/home/kali/system_reports`. If the directory doesn't exist if statement will create a directory.

Filename: The report file is named as `system_report_YYYY-MM-DD.txt` using the current date.

The script captures the following:

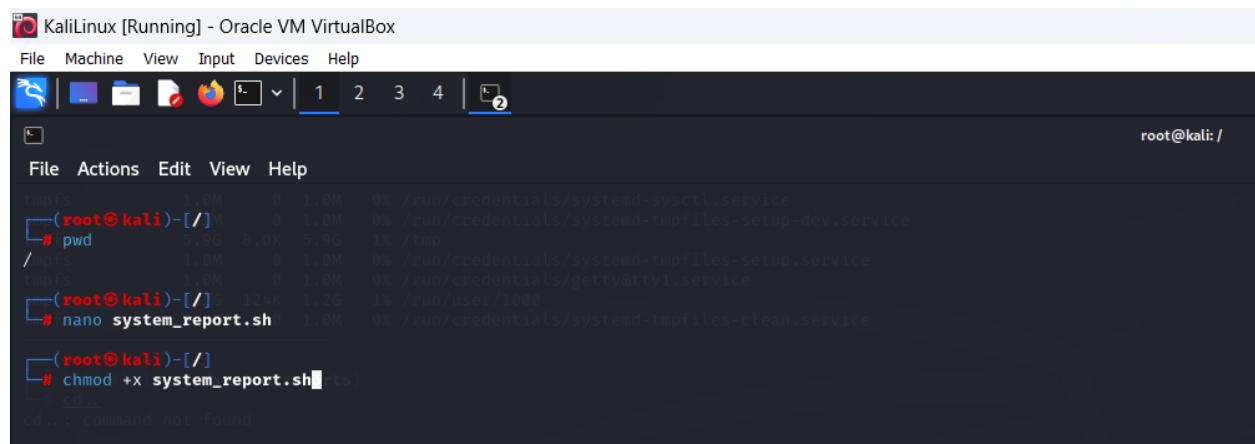
Date and Time: Using the `$DATE` command.

Uptime: `uptime -p`, will show how long the system has been running.

Free Memory: `free -h` will show the amount of free memory in human-readable format.

Disk Usage: `df -h` will display disk space usage for all mounted filesystems.

After writing the script we need to give executable permissions.



KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
root@kali: ~
[1]# (root㉿kali)-[~/] 0 1.0M 0% /run/credentials/systemd-sysctl.service
[2]# (root㉿kali)-[~/] 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
[3]# (root㉿kali)-[~/] 5.9G 8.0K 5.9G 1% /tmp
[4]# (root㉿kali)-[~/] 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
[5]# (root㉿kali)-[~/] 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
[6]# (root㉿kali)-[~/] 124K 1.2G 1% /run/user/1000
[7]# (root㉿kali)-[~/] nano system_report.sh
[8]# (root㉿kali)-[~/] chmod +x system_report.sh
[9]# cd ..
cd: ..: command not found
```

After that lets run the script file.

```

root@kali:~# ./system_report.sh
System report created: /home/kali/system_reports/system_report_2024-10-02.txt
root@kali:~#

```

Then we will see the content of the resulted file at /home/kali/system_reports/.

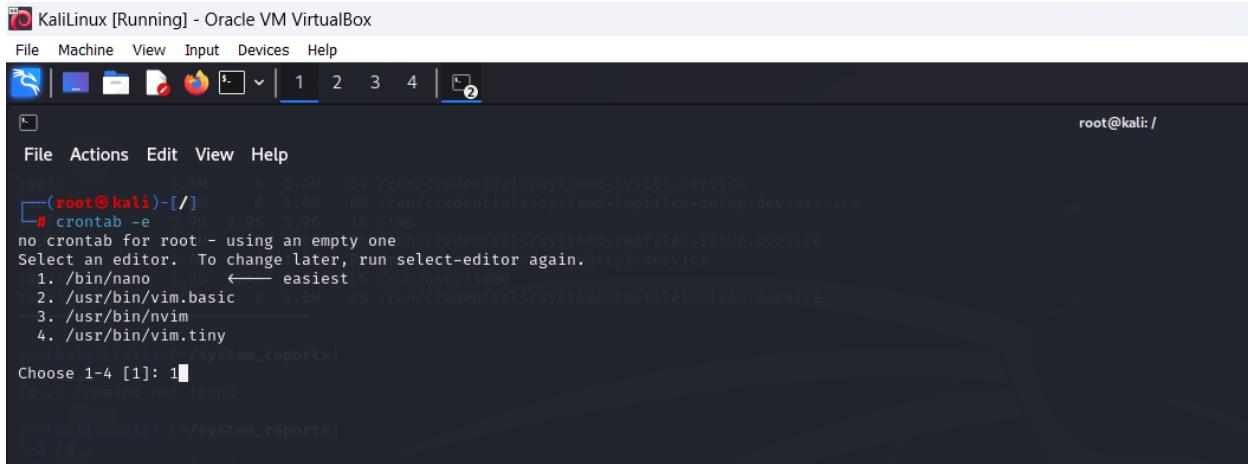
```

root@kali:/home/kali/system_reports# cat system_report_2024-10-02.txt
System Report - 2024-10-02

Date and Time: Wed Oct 2 23:44:17 +0530 2024
System Uptime: up 43 minutes
Free Memory: 1061
Disk Usage:
Filesystem      Size  Used Avail Use% Mounted on
udev            5.9G   0B  5.9G  0% /dev
tmpfs           1.2G  1.2G  0     100% /run
(/dev/sda1      486M  32G  447M  7% /)
tmpfs           5.9G   0B  5.9G  0% /dev/shm
tmpfs           5.0M   0B  5.0M  0% /run/lock
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-journald.service
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           5.9G  120K  5.9G  1% /tmp
tmpfs           1.0M   0B  1.0M  0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs           1.0M   0B  1.0M  0% /run/credentials/getty@tty1.service
tmpfs           1.2G  124K  1.2G  1% /run/user/1000
root@kali:/home/kali/system_reports#

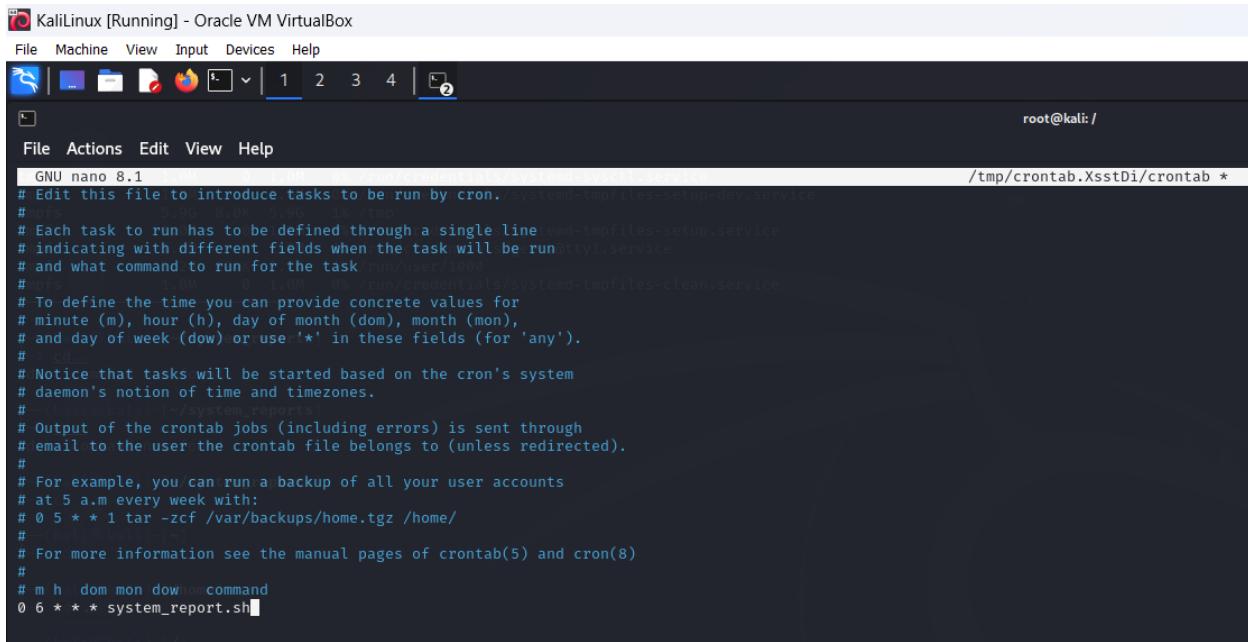
```

As the next step type **crontab -e** command in the terminal and select a preferred editor.



```
File Actions Edit View Help
tmps 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
└─(root@kali)-[/] 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
# crontab -e 3.0G 8.0K 3.0G 16 /tmp
no crontab for root - using an empty one /run/credentials/systemd-tmpfiles-setup.service
Select an editor. To change later, run select-editor again. /tmp/attyl.service
1. /bin/nano 1.6 ← easiest 1.6M /run/user/1000
2. /usr/bin/vim.basic 0 1.0M 0% /run/credentials/systemd-tmpfiles-clean.service
3. /usr/bin/nvim
4. /usr/bin/vim.tiny
Choose 1-4 [1]: 1
cd: command not found
[root@kali ~] (~system_reports)
→ cd ..
```

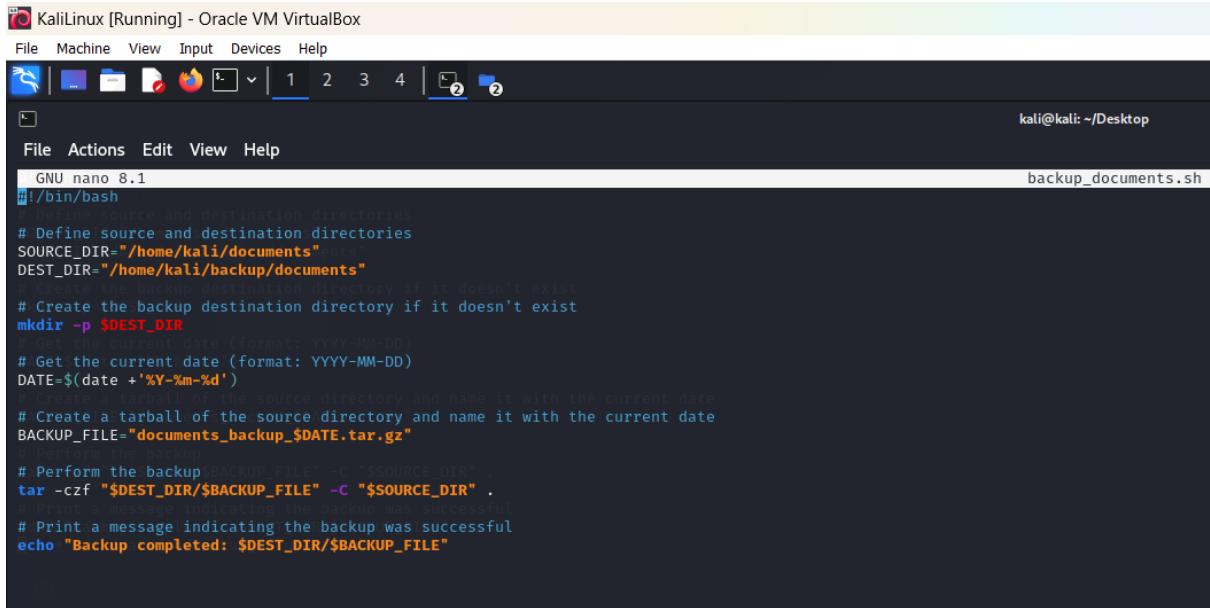
Inside the crontab write following code and save.



```
File Actions Edit View Help
GNU nano 8.1 /tmp/crontab.XsstDi/crontab *
# Edit this file to introduce tasks to be run by cron. /tmp/crontab.XsstDi/crontab *
# tasks will be run as user root in the directory /tmp
# Each task to run has to be defined through a single line /tmp/credentials/systemd-tmpfiles-setup.service
# indicating with different fields when the task will be run /tmp/attyl.service
# and what command to run for the task /tmp/attyl.service
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezone.
# Example: 0 2 <user> /usr/local/bin/twilight
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
0 6 * * * system_report.sh
```

This tells cron to run the command at 6:00 AM every day

- ii. create a shell script in the file **backup_documents.sh** in desktop. Using the command **nano backup_documents.sh**. Inside the file add the below shell script.



```
GNU nano 8.1
#!/bin/bash
# Define source and destination directories
# Define source and destination directories
SOURCE_DIR="/home/kali/documents"
DEST_DIR="/home/kali/backup/documents"
# Create the backup destination directory if it doesn't exist
mkdir -p $DEST_DIR
# Get the current date (format: YYYY-MM-DD)
DATE=$(date +'%Y-%m-%d')
# Create a tarball of the source directory and name it with the current date
BACKUP_FILE="documents_backup_$DATE.tar.gz"
# Perform the backup
# Perform the backup BACKUP_FILE" -C "$SOURCE_DIR"
tar -czf "$DEST_DIR/$BACKUP_FILE" -C "$SOURCE_DIR".
# Print a message indicating the backup was successful
# Print a message indicating the backup was successful
echo "Backup completed: $DEST_DIR/$BACKUP_FILE"
```

```
#!/bin/bash

# Define source and destination directories

SOURCE_DIR="/home/kali/documents"

DEST_DIR="/home/kali/backup/documents"

# Create the backup destination directory if it doesn't exist

mkdir -p $DEST_DIR

# Get the current date (format: YYYY-MM-DD)

DATE=$(date +'%Y-%m-%d')

# Create a tarball of the source directory and name it with the current date

BACKUP_FILE="documents_backup_$DATE.tar.gz"

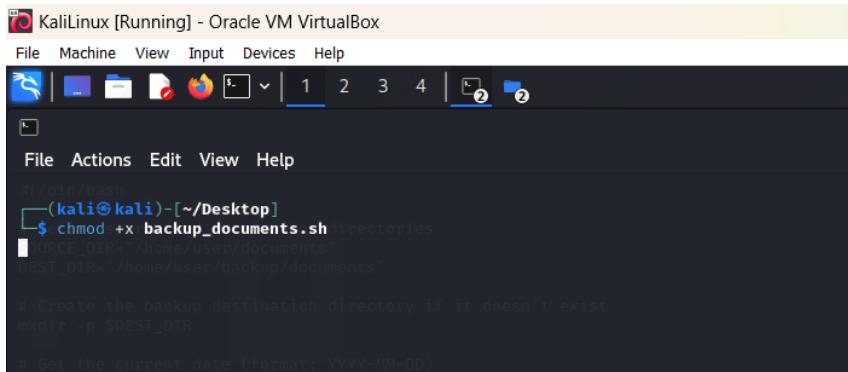
# Perform the backup

tar -czf "$DEST_DIR/$BACKUP_FILE" -C "$SOURCE_DIR".

# Print a message indicating the backup was successful

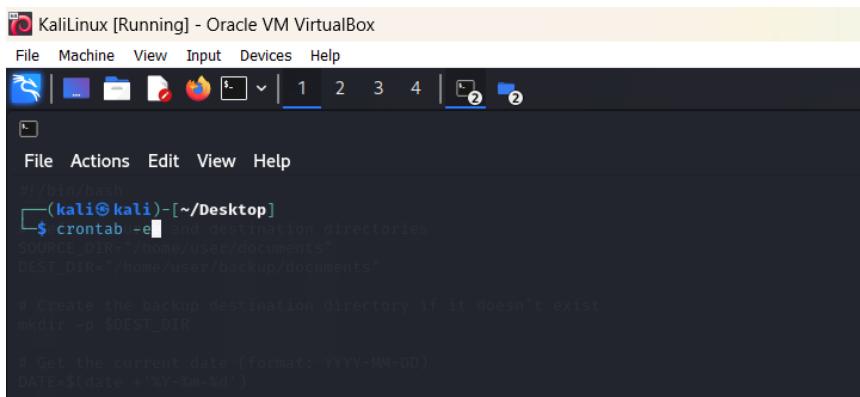
echo "Backup completed: $DEST_DIR/$BACKUP_FILE"
```

Then we'll make the script executable by using the command `chmod +x backup_documents.sh`.



```
#!/bin/bash
#(kali㉿kali)-[~/Desktop]
$ chmod +x backup_documents.sh
```

After that we will open crontab to schedule the script to run periodically. For that type the command `crontab -e`.



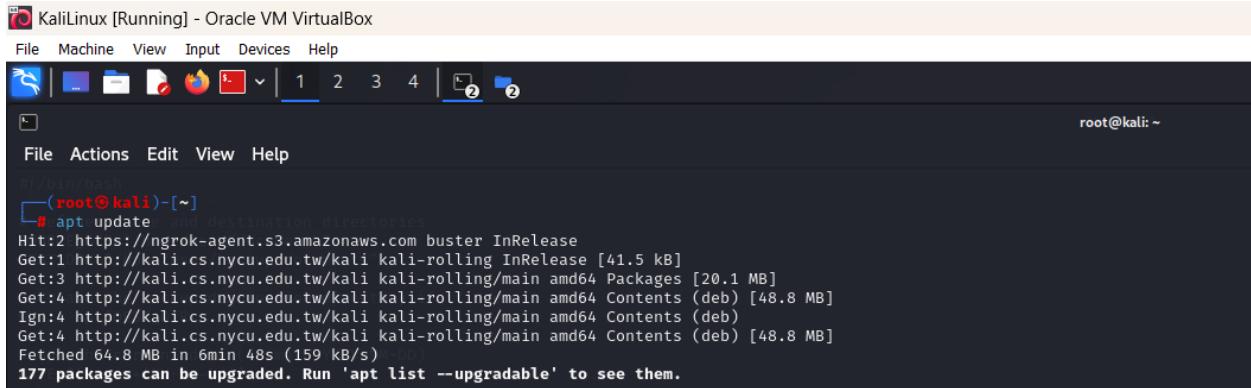
```
#!/bin/bash
#(kali㉿kali)-[~/Desktop]
$ crontab -e
```

Next add a cron job to run the script daily. For that type below code inside the crontab.

```
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
# 0 5 * * * tar -zcf "/var/backups/home.tgz" /home/
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 2 * * * backup_documents.sh
```

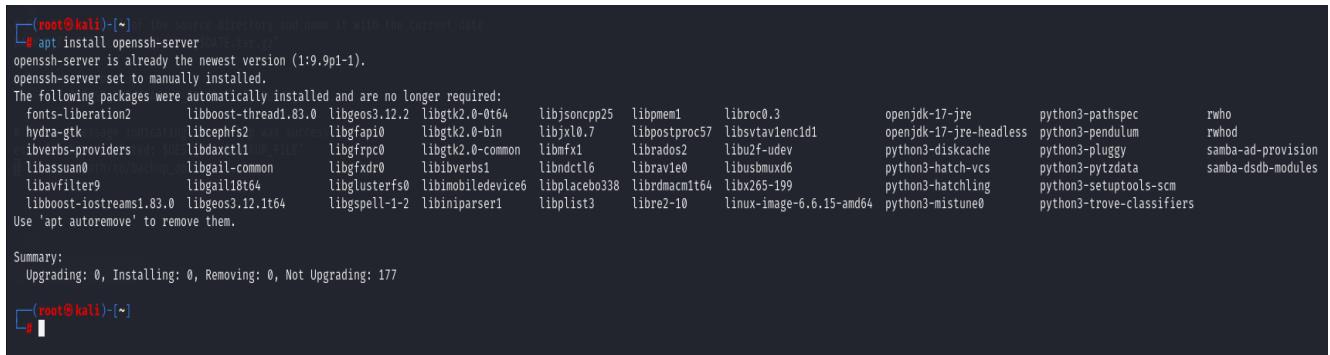
3.2 SSH (Secure Shell)

First run the **apt update** command and download packages.



KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: ~
apt update
Hit:2 https://ngrok-agent.s3.amazonaws.com buster InRelease
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling InRelease [41.5 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Ign:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Fetched 64.8 MB in 6min 48s (159 kB/s)
177 packages can be upgraded. Run 'apt list --upgradable' to see them.

Then we need to install open ssh server. To do that run the command **apt install openssh-server**.



```
(root@kali: ~) # apt install openssh-server  
The package openssh-server is already the newest version (1:9.9p1-1).  
openssh-server set to manually installed.  
The following packages were automatically installed and are no longer required:  
  fonts-iberation2   libboost-thread1.83.0  libgeos3.12.2  libgtk2.0-0t64  libjsoncpp25  libpmem1  libroc0.3      openjdk-17-jre          python3-pathspec    rwho  
  hydra-gtk        libcmhfs2           libgapi0       libgtk2.0-0-bin   libjxl0.7     libpostproc57  libsvtavlenc1d1  openjdk-17-jre-headless  python3-pendulum  rwtmp  
  ibverbs-providers libdaxctl1         libgfrpc0     libgtk2.0-common  libimfx1      librados2  libu2f-udev    python3-diskcache  python3-pluggy    samba-ad-provision  
  libassuan0       libgail-common     libgwdx0      libibverbs1     libndctl6    libravel0  libusbxmud6  python3-hatch-vcs  python3-ptzdata  samba-dsdb-modules  
  libavfilter9     libgail18t64      libglusterfs0  libimobiledevice6 libplacebo338  librdmacm1t64  libx265-199  python3-hatching  python3-setuptools-scm  
  libboost-iostreams1.83.0 libgeos3.12.1t64  libgspell-1-2  libiniparser1  libplist3    libre2-10   linux-image-6.6.15-amd64 python3-mistune0  python3-trove-classifiers  
Use 'apt autoremove' to remove them.  
Summary:  
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 177  
(root@kali: ~) #
```

Next start the ssh by **systemctl restart ssh** and to check the status of the ssh use **systemctl status ssh**.

```

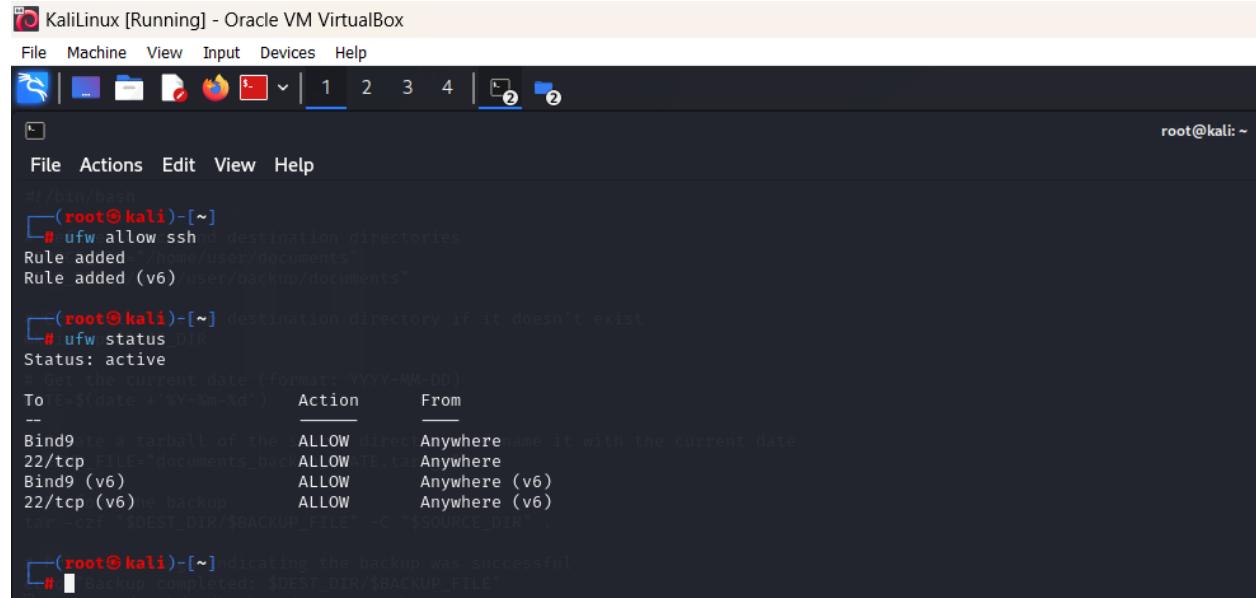
└─(root㉿kali)-[~]
  # systemctl restart ssh

└─(root㉿kali)-[~]
  # systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-10-05 01:02:33 +0530; 3s ago
    Invocation: 530f35a453484ac2ab62c2e42f167243
      Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 240216 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 240217 (sshd)
     Tasks: 1 (limit: 14213)
    Memory: 1.7M (peak: 2.1M)
       CPU: 43ms
      CGroup: /system.slice/ssh.service
              └─240217 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 05 01:02:33 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Oct 05 01:02:33 kali sshd[240217]: Server listening on 0.0.0.0 port 22.
Oct 05 01:02:33 kali sshd[240217]: Server listening on :: port 22.
Oct 05 01:02:33 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

```

To allow ssh through the firewall with which it can listen for incoming requests. Run below commands.



KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

#/bin/bash

```

└─(root㉿kali)-[~]
  # ufw allow ssh
  Rule added: 22/tcp (v6) to Anywhere
  Rule added (v6) to Anywhere

└─(root㉿kali)-[~] destination directory if it doesn't exist
  # ufw status
  Status: active
  Get the current date (format: YYYY-MM-DD)
  ToTETs$(date '+%Y-%m-%d') Action From
  -- 
  Bind9 to a tarball of the $SOURCE_DIR directory name it with the current date
  22/tcp FILE="$DEST_DIR/$BACKUP_FILE" -C "$SOURCE_DIR"
  Bind9 (v6) ALLOW Anywhere (v6)
  22/tcp (v6) BACKUP ALLOW Anywhere (v6)
  tar -czf "$DEST_DIR/$BACKUP_FILE" -C "$SOURCE_DIR" .

└─(root㉿kali)-[~] indicating the backup was successful
  # █ Backup completed: $DEST_DIR/$BACKUP_FILE

```

Port 22/tcp is the TCP port that is used for the SSH protocol by default. For the next step we need the IP address. Use **ifconfig** to view it.

```

└─(root㉿kali)-[~] indicating the backup was successful
└─# ifconfig completed: $DEST_DIR/$BACKUP_FILE"
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe42:3e52 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:42:3e:52 txqueuelen 1000 (Ethernet)
            RX packets 165536 bytes 240705118 (229.5 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 53233 bytes 3261530 (3.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 20 bytes 3094 (3.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 20 bytes 3094 (3.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

```
└─(root㉿kali)-[~]
```

```
└─#
```

We will use another terminal as the client computer to put this one into reality. Then enter the username and ip address of the server after the ssh command to connect to the server. Type the command [ssh kali@10.0.2.15](#).

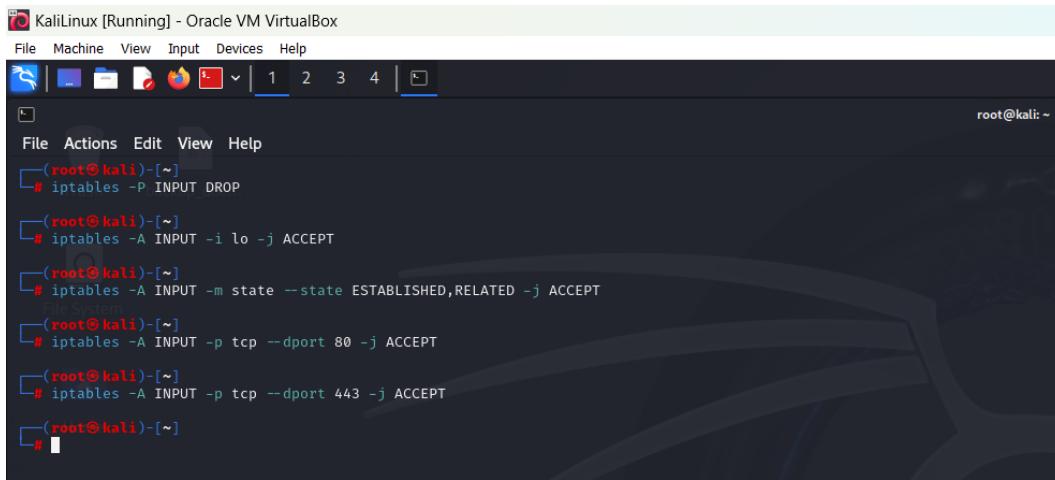
```

KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
└─(kali㉿kali)-[~] sshd[263928]: Server listening on 0.0.0.0 port 22.
└─$ ssh kali@10.0.2.15 sshd[263928]: Server listening on : port 22.
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established. Shell server.
ED25519 key fingerprint is SHA256:0h3s0+Q+FAgMElbBebY3cfZ44x5CIZ0i7lz2VL15LIM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
kali@10.0.2.15's password:
Linux kali 6.10.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.9-1kali1 (2024-09-09) x86_64
        named service: BIND Domain Name Server
The programs included with the Kali GNU/Linux system are free software; those disabled
the exact distribution terms for each program are described in the files
individual files in /usr/share/doc/*copyright.
        Docs/named/named.8
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.

```

3.3 IP tables and ACLs

3.3.1 Web Server Security

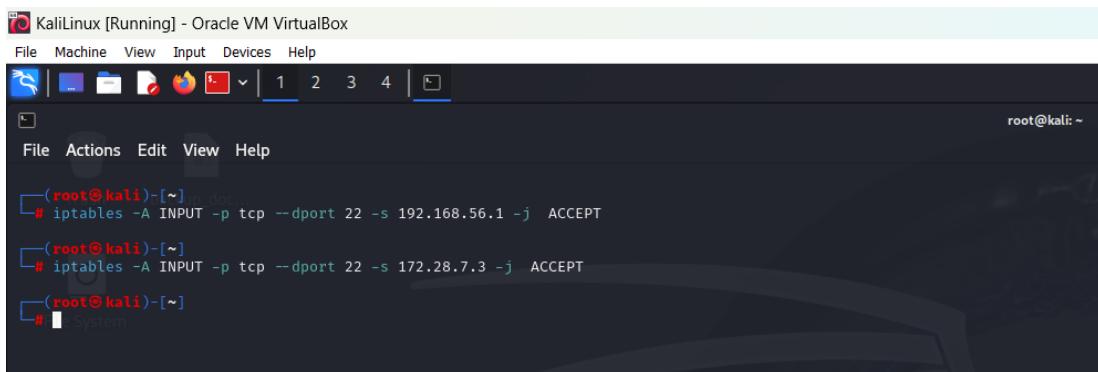


```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# iptables -P INPUT DROP
(root@kali)-[~]
# iptables -A INPUT -i lo -j ACCEPT
(root@kali)-[~]
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
File System
(root@kali)-[~]
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
(root@kali)-[~]
# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
(root@kali)-[~]
#
```

To allow incoming traffic only on ports 80 (HTTP) and 443 (HTTPS) for the web server and block everything else we need to make the drop policy to default by using **iptables -P INPUT DROP** command. Next allow traffic on localhost by **iptables -A INPUT -i lo -j ACCEPT**. Then allow established connections to continue by **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**. Then allow incoming port 80 and port 443 traffic by **iptables -A INPUT -p tcp --dport 80 -j ACCEPT** and **iptables -A INPUT -p tcp --dport 443 -j ACCEPT** commands.

3.3.2 Remote Administration Access

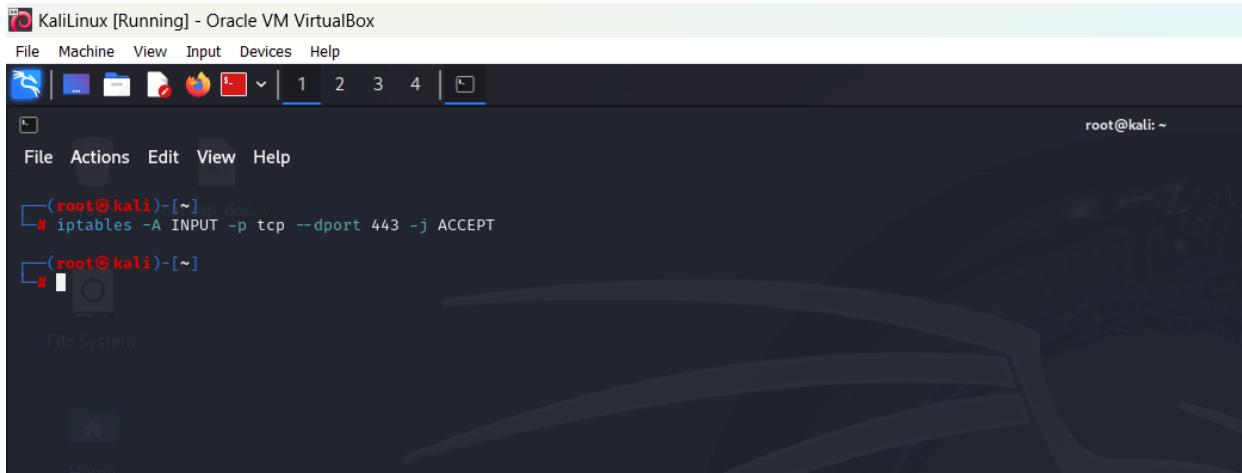
Allow SSH access port 22 only from specific IP addresses of trusted machines by **iptables -A INPUT -p tcp --dport 22 -s <trusted ip address> -j ACCEPT** command.



```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# iptables -A INPUT -p tcp --dport 22 -s 192.168.56.1 -j ACCEPT
(root@kali)-[~]
# iptables -A INPUT -p tcp --dport 22 -s 172.28.7.3 -j ACCEPT
(root@kali)-[~]
#
```

3.3.3 Allow Specific Applications

To allow video conferencing app using port 443 its going to be same as HTTPS rule.



KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

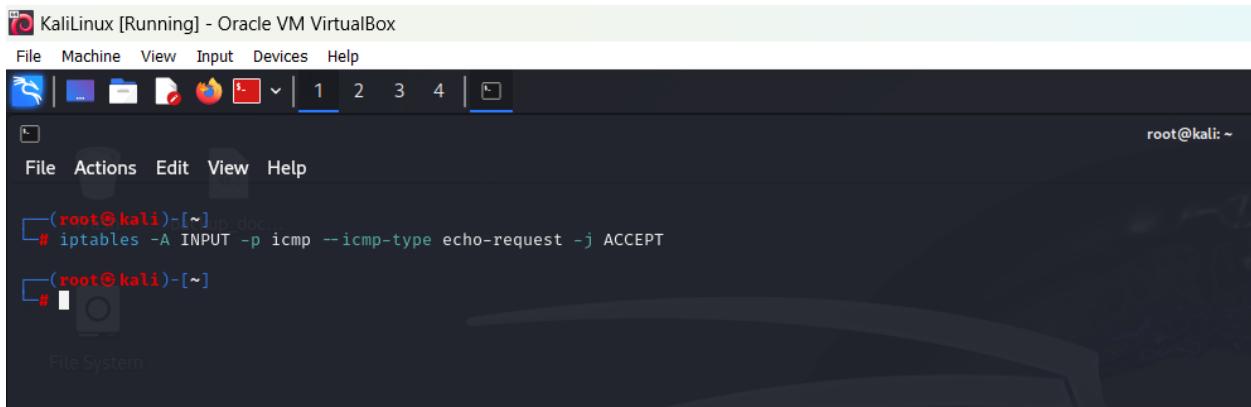
```
(root@kali)-[~] # iptables -A INPUT -p tcp --dport 443 -j ACCEPT
[root@kali: ~]
```

File System

This screenshot shows a terminal window on Kali Linux. The user is root, as indicated by the prompt '(root@kali)-[~]'. The user has run the command 'iptables -A INPUT -p tcp --dport 443 -j ACCEPT' to allow traffic on port 443. The terminal also shows a file browser interface with tabs 1, 2, 3, and 4 at the top.

3.3.4 Allow Pings

To allow ping requests to our server to help with the network diagnostic we can run the command **iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT**.



KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
(root@kali)-[~] # iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
[root@kali: ~]
```

File System

This screenshot shows a terminal window on Kali Linux. The user is root, as indicated by the prompt '(root@kali)-[~]'. The user has run the command 'iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT' to allow ICMP echo requests. The terminal also shows a file browser interface with tabs 1, 2, 3, and 4 at the top.

3.3.5 Printer Server Access

To allow traffic to the printer server only from specific IP addresses within our local network use **iptables -A INPUT -p tcp --dport 9100 -s <trusted IP> -j ACCEPT** command. To block external access to printer server use the **command iptables -A INPUT -p tcp --dport 9100 -j DROP**.

```
(root㉿kali)-[~] ~ doc
# iptables -A INPUT -p tcp --dport 9100 -s 192.168.56.1 -j ACCEPT
(root㉿kali)-[~]
# iptables -A INPUT -p tcp --dport 9100 -s 172.28.7.3 -j ACCEPT
(root㉿kali)-[~]
# iptables -A INPUT -p tcp --dport 9100 -j DROP
(root㉿kali)-[~]
```

4 Best practices

4.1 Disable Unused Network Interfaces

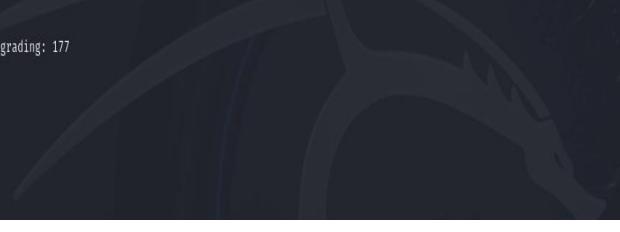
Your Linux machine has multiple network interfaces. If they are not being used it's a good security practice to disable or shut down any unused network interfaces. These interfaces can act as attack surfaces if not properly secured. Use the `ip link show` command to list all interfaces. If there are unused interfaces disable them using the command `ip link set <interface> down`.

```
(root㉿kali)-[~] ~ ip_doc...
# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:42:3e:52 brd ff:ff:ff:ff:ff:ff
(root㉿kali)-[~]
```

4.2 Enable a Firewall

Firewalls help filter and control network traffic based on predefined rules and it will protect our system from unauthorized access and potential attacks.

To install and enable a firewall type `apt install ufw` and `ufw enable` commands.



```

KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# apt install ufw
ufw is already the newest version (0.36.2-6).
The following packages were automatically installed and are no longer required:
fonts-liberation2 libboost-thread1.83.0 libgeos3.12.2 libgtk2.0-0t64 libjsoncpp25 libpmem1 libroc0.3 openjdk-17-jre python3-pathspec rwho
hydra-gtk libcephfs2 libgfaio libgtk2.0-bin libjxl0.7 libpostproc57 libsvtavenc1d1 openjdk-17-jre-headless python3-pendulum rwtmp
ibverbs-providers libdaxctl1 libgfrpc0 libgtk2.0-common libmfx1 librados2 libu2f-udev python3-diskcache python3-pluggy samba-ad-provision
libasan0 libgail-common libgfrx0 libibverbs1 libndctl6 libravie0 libusmuxd python3-hatch-vcs python3-ptzdata samba-dsdb-modules
libavfilter9 libgail18t64 libglusterfs0 libimobiledevice6 libplacebo338 librdmcam1t64 libx265-199 python3-hatching python3-setuptools-scm
libboost-iostreams1.83.0 libgeos3.12.1t64 libgspell-1-2 libimparser1 libplist3 libre2-10 linux-image-6.6.15-amd64 python3-mistune0 python3-trove-classifiers
Use 'apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 177

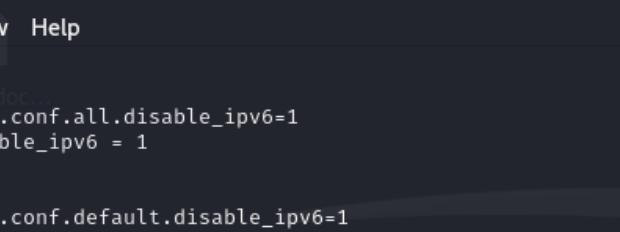
[root@kali)-[~]
# ufw enable
Firewall is active and enabled on system startup

[root@kali)-[~]

```

4.3 Disable IPv6 if Not Needed

If our network environment does not use IPv6, temporarily disabling it can help reduce the attack surface because attackers cannot exploit IPv6-related vulnerabilities if it is disabled. In order to do that run the following commands `sysctl -w net.ipv6.conf.all.disable_ipv6=1` and `sysctl -w net.ipv6.conf.default.disable_ipv6=1`.



```

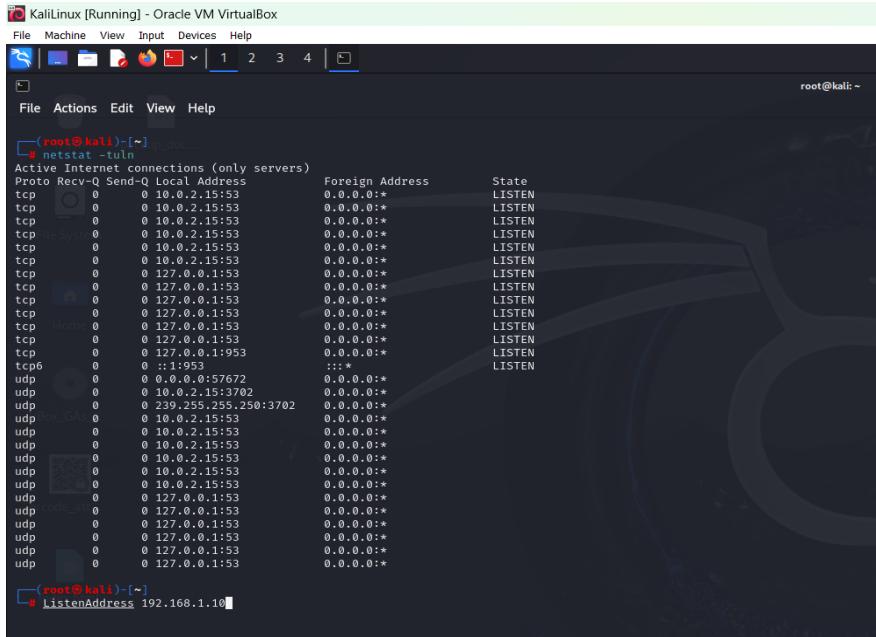
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# sysctl -w net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.all.disable_ipv6 = 1

[root@kali)-[~]
# sysctl -w net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6 = 1

```

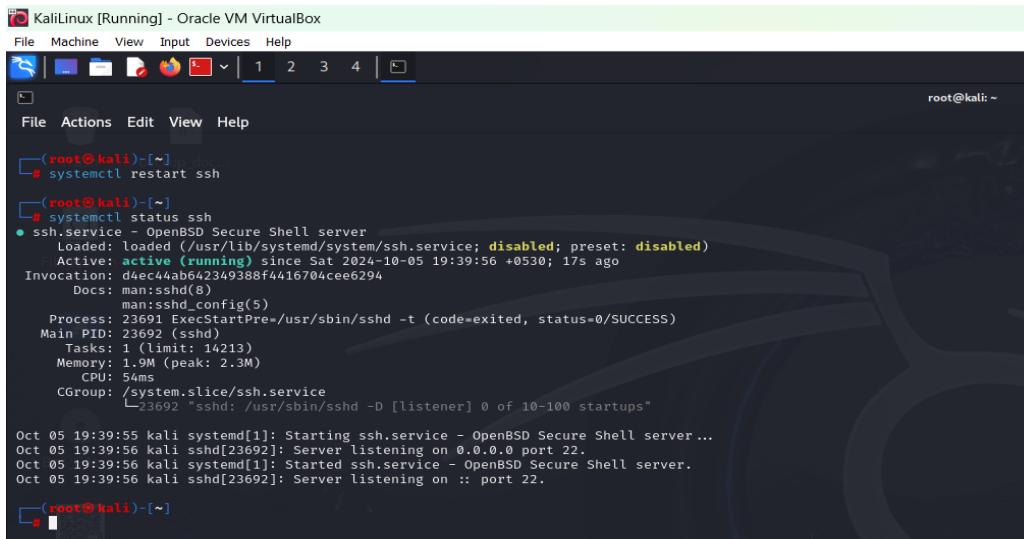
4.4 Limit Network Service Exposure

Only run network services that are necessary, and bind them to specific network interfaces if possible. This helps in reducing unnecessary network exposure and limits the services that attackers can target. Use the command `netstat -tuln` to check active connections. Next use `ListenAddress <Preferred ip>` and hit enter.



```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@kali] ~]# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0      10.0.2.15:53          0.0.0.0:*
                                         LISTEN
tcp     0      0      127.0.0.1:53          0.0.0.0:*
                                         LISTEN
tcp     0      0      ::1:953               ::*:*
                                         LISTEN
udp    0      0      0.0.0.0:57672        0.0.0.0:*
                                         LISTEN
udp    0      0      10.0.2.15:3702       0.0.0.0:*
                                         LISTEN
udp    0      0      239.255.255.250:3702  0.0.0.0:*
                                         LISTEN
udp    0      0      10.0.2.15:53          0.0.0.0:*
                                         LISTEN
udp    0      0      127.0.0.1:53          0.0.0.0:*
                                         LISTEN
[root@kali] ~]# ListenAddress 192.168.1.10
```

Restart the service to apply the changes



```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@kali] ~]# systemctl restart ssh
[root@kali] ~]# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-10-05 19:39:56 +0530; 17s ago
   Invocation: d4ec44ab642349388f4416704cee6294
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 23691 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 23692 (sshd)
   Tasks: 1 (limit: 14213)
  Memory: 1.9M (peak: 2.3M)
    CPU: 54ms
   CGroup: /system.slice/ssh.service
           └─23692 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 05 19:39:55 Kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 05 19:39:56 Kali sshd[23692]: Server listening on 0.0.0.0 port 22.
Oct 05 19:39:56 Kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Oct 05 19:39:56 Kali sshd[23692]: Server listening on :: port 22.

[root@kali] ~]
```

4.5 Configure Network Interface Security Settings

Configuring security settings for network interfaces, such as enabling secure protocols, configuring static IP addresses, and limiting promiscuous mode, can prevent unauthorized access and data interception.

To use static ip addresses edit the network configuration file (e.g., /etc/network/interfaces, /etc/netplan/, or NetworkManager configuration) to set a static IP.

Promiscuous mode allows an interface to capture all traffic, not just the traffic intended for it, which could be a security risk. To check for it type `ip link`. If necessary disable it with `ip link set <interface> promisc off`.

```
(root@kali)-[~/home/kali]
# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:42:3e:52 brd ff:ff:ff:ff:ff:ff

(root@kali)-[~/home/kali]
# ip link set eth0 promisc off
```