Sri Lanka Institute of Information Technology

IE2012 - Systems and Network Programming

Final Assignment

Name: Peiris W.S.S.N

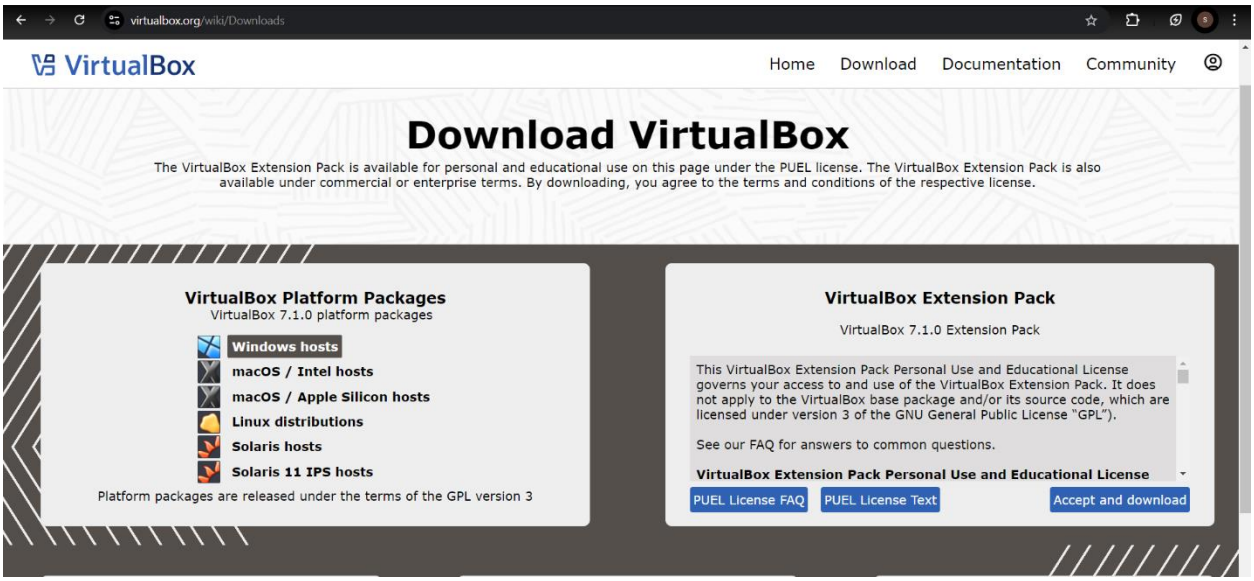
Registration Number: IT23227286

Table of Contents

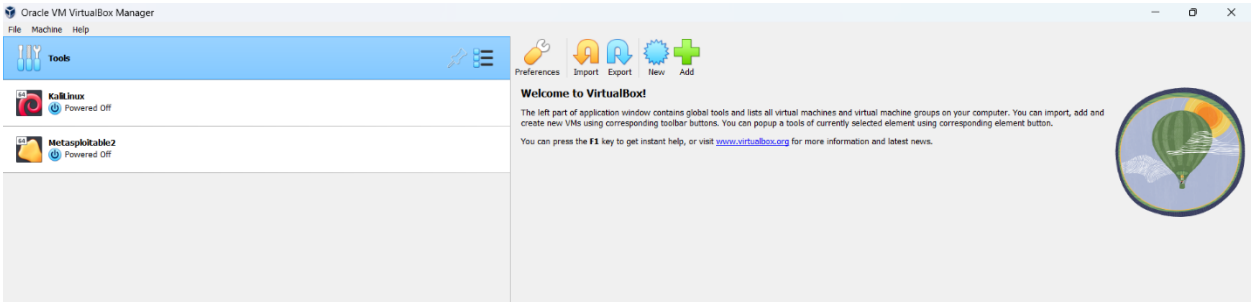
1 Basics of Linux Environments

1.1 Virtual Machine Setup

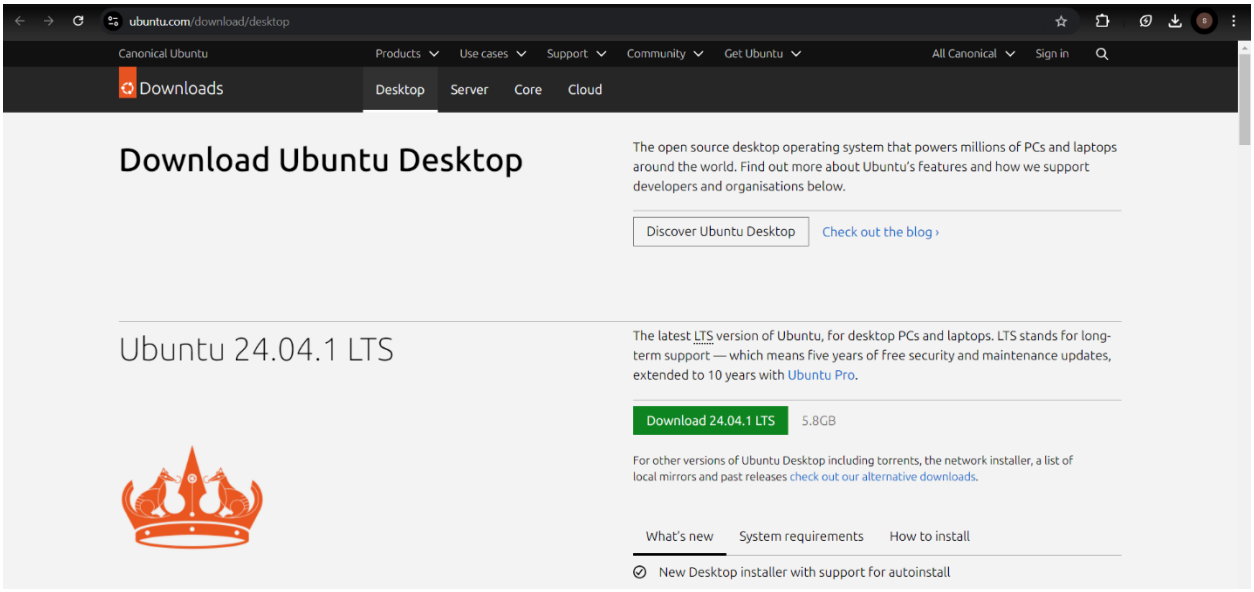
Go to this link https://www.virtualbox.org/wiki/Downloads and download virtual machine setup and go through the setup.



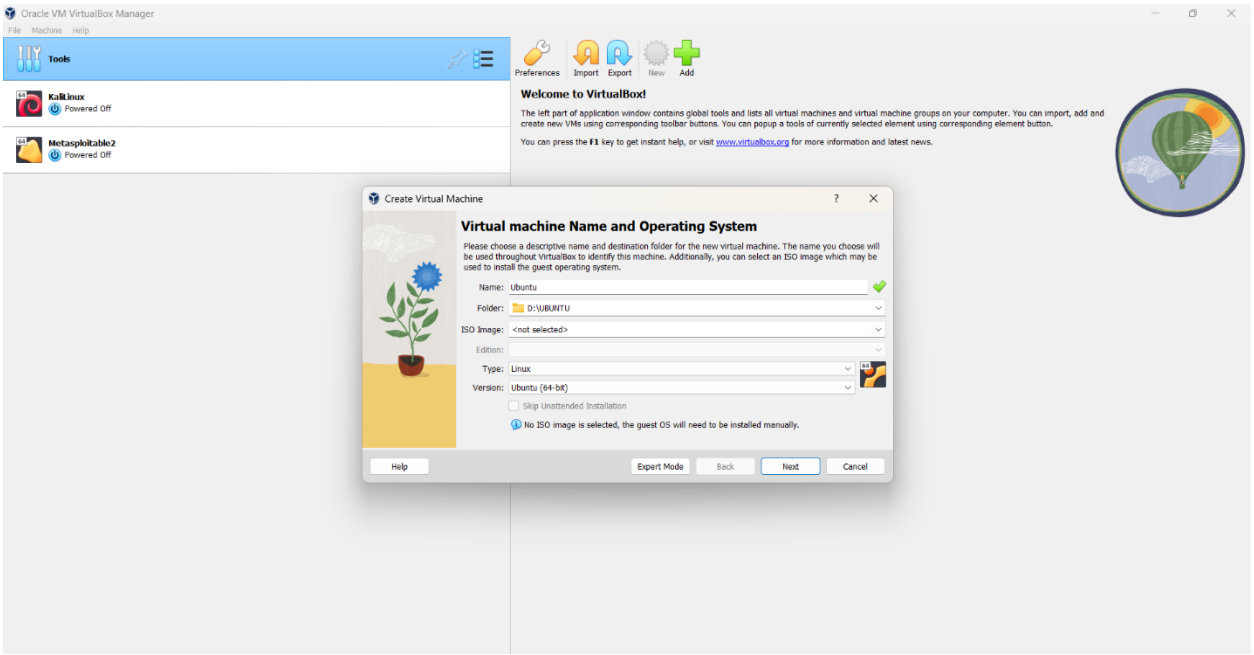
Below screenshot shows VirtualBox software after installation. I have already installed VirtualBox and added Kali Linux and Metasploitable2.



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.



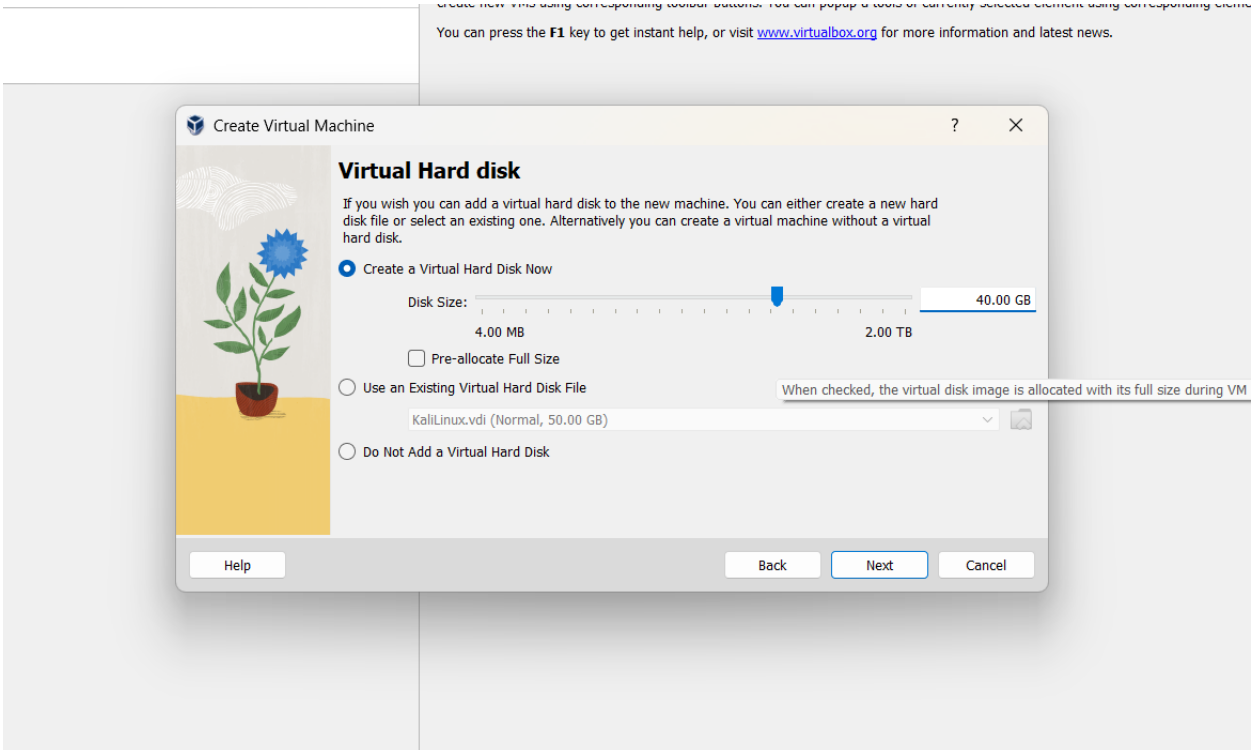
After downloading the iso file open virtualbox and press new button. In the create virtual machine window put a name and a folder to install Ubuntu. Automatically type will be selected to Linux and the version to Ubuntu (64-bit). Then select next to configure hardware.



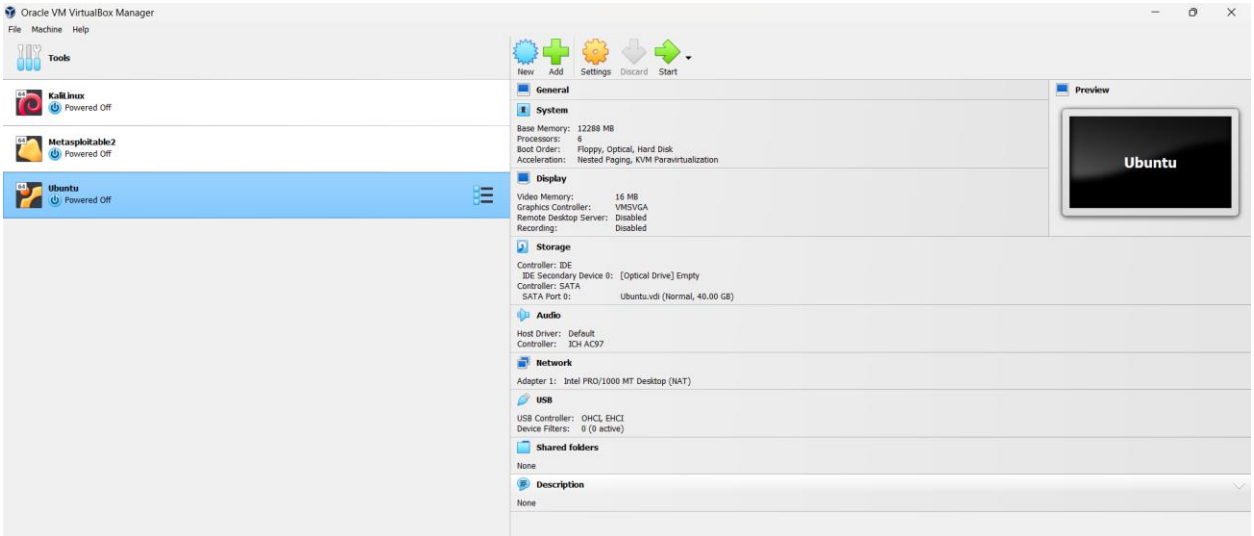
In the hardware section select a suitable base memory for Ubuntu considering the amount of RAM installed in your device. I have selected 12GB ram for faster installation. Then select the amount of CPUs you want to allocate for Ubuntu I have selected 6 CPUs. In both base memory

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

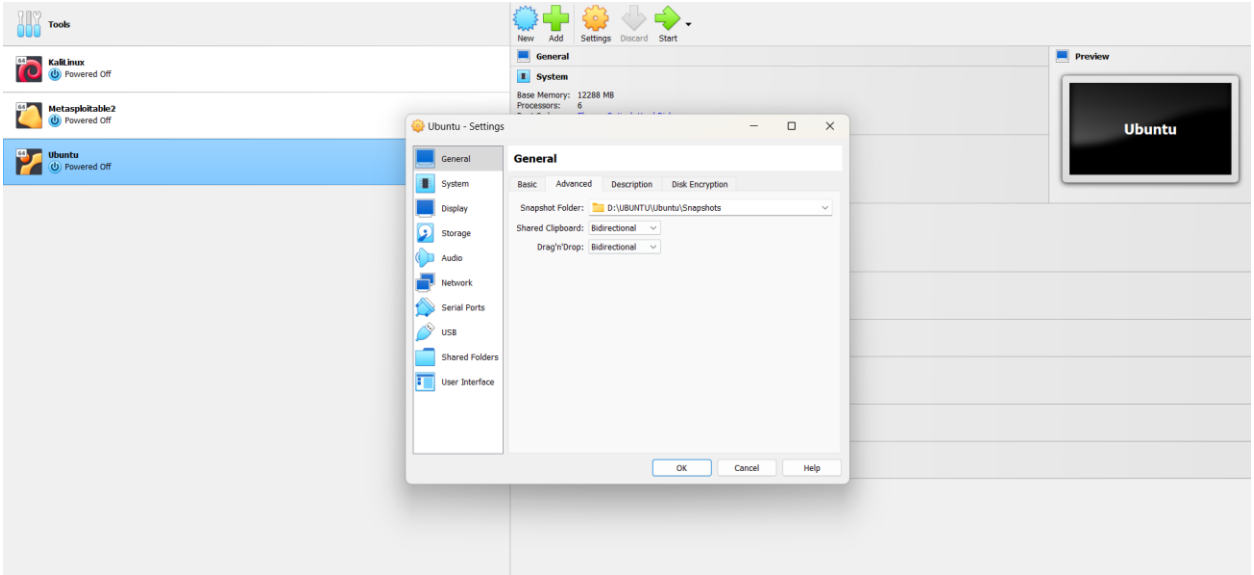
Select create a virtual hard disk now. Then select enough disk size to accommodate the Ubuntu OS. I chose to give 40GB.



Select next to see the summary and press finish.

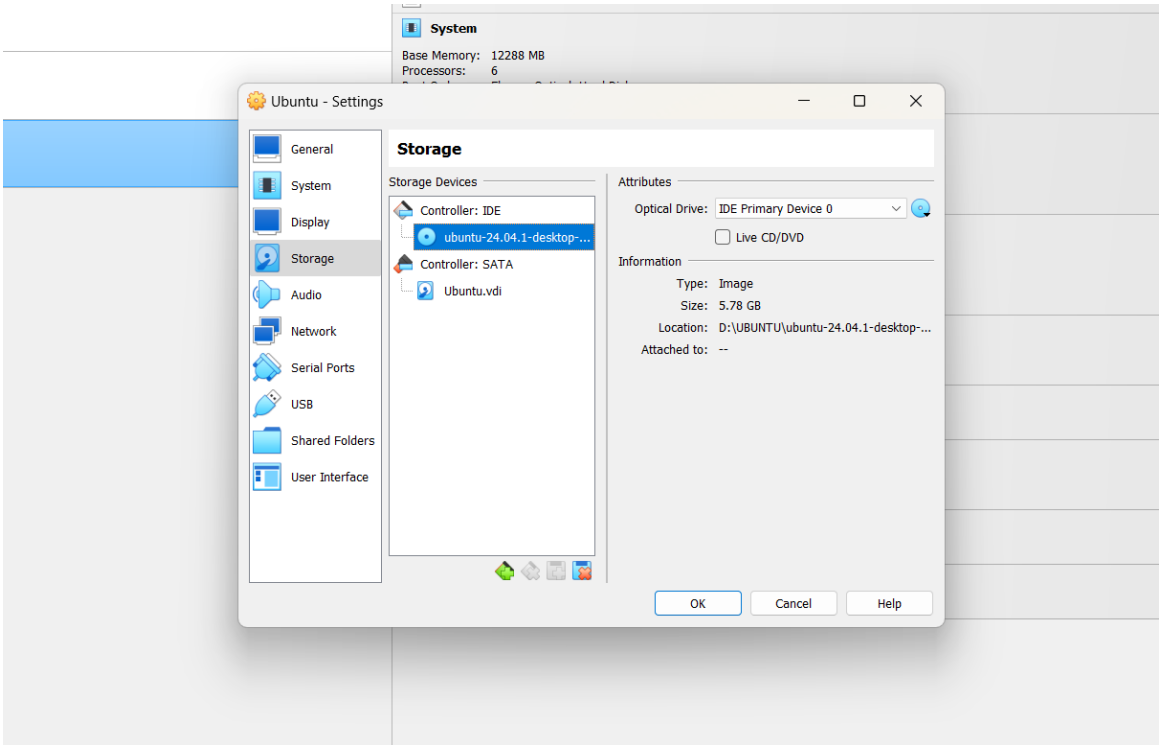


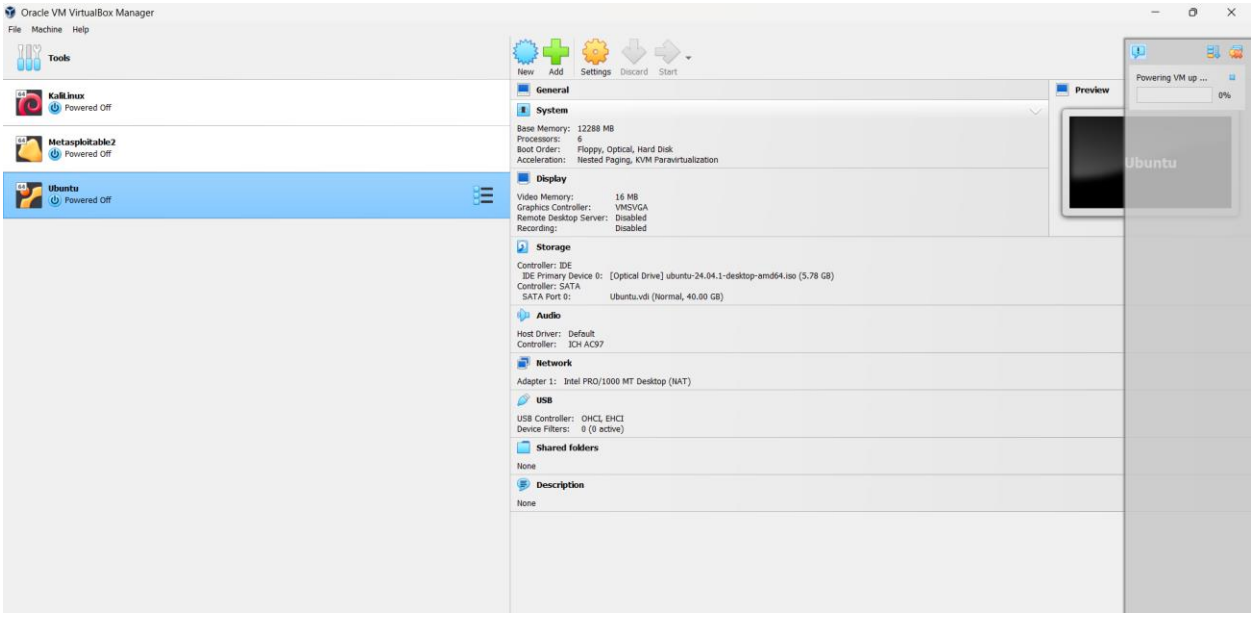
Go to settings of Ubuntu by selecting Ubuntu and pressing settings icon. In “General” section select Advanced tab change shared clipboard and Drag’n’Drop to Bidirectional from Disabled.



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.

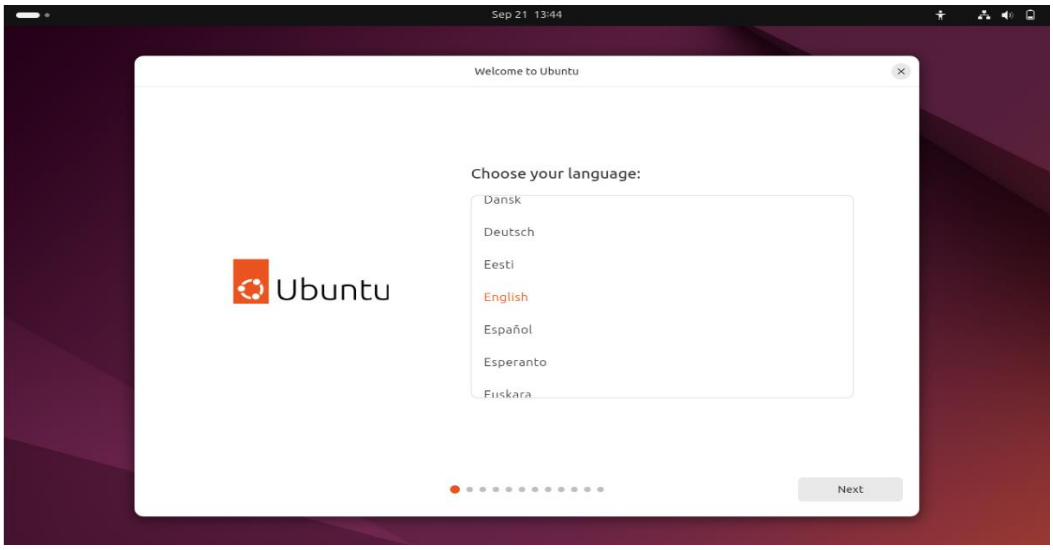

System
Base Memory: 12288 MB
Processors: 6
Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
ubuntu-24.04.1-desktop-...
Controller: SATA
Ubuntu.vdi
Attributes
Optical Drive: IDE Primary Device 0
Live CD/DVD
Information
Type: Image
Size: 5.78 GB
Location: D:\UBUNTU\ubuntu-24.04.1-desktop-...
Attached to: --
OK
Cancel
Help


Oracle VM VirtualBox Manager
File Machine Help
Tools
KaliLinux
Powered Off
Metasploitable2
Powered Off
Ubuntu
Powered Off
New Add Settings Discard Start
General
System
Base Memory: 12288 MB
Processors: 6
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] ubuntu-24.04.1-desktop-amd64.iso (5.78 GB)
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 40.00 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Preview
Powering VM up ...
0%
Ubuntu

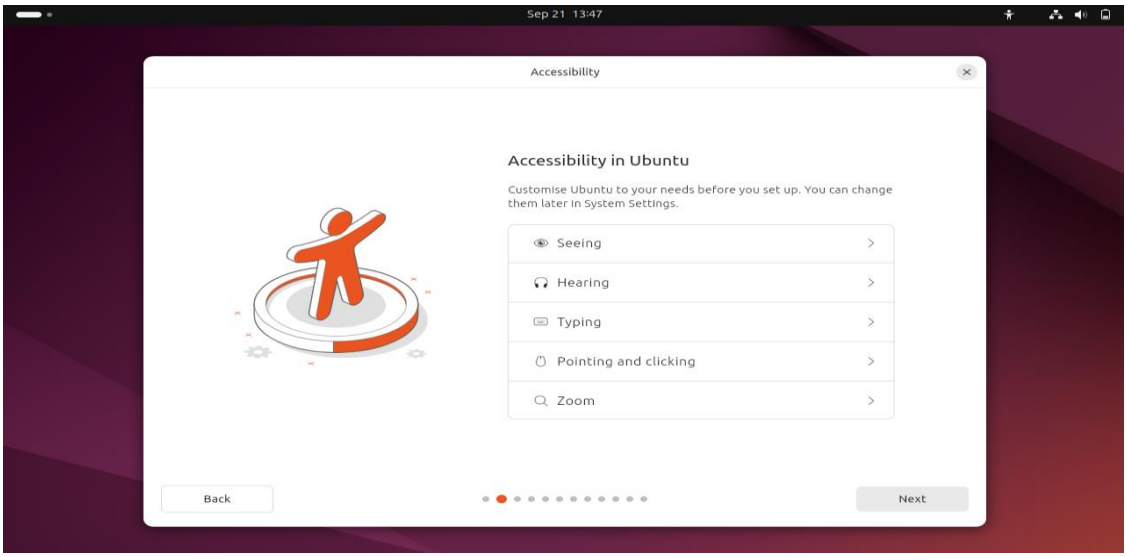
After selecting Ubuntu press start. Below steps will lead to a successful install.

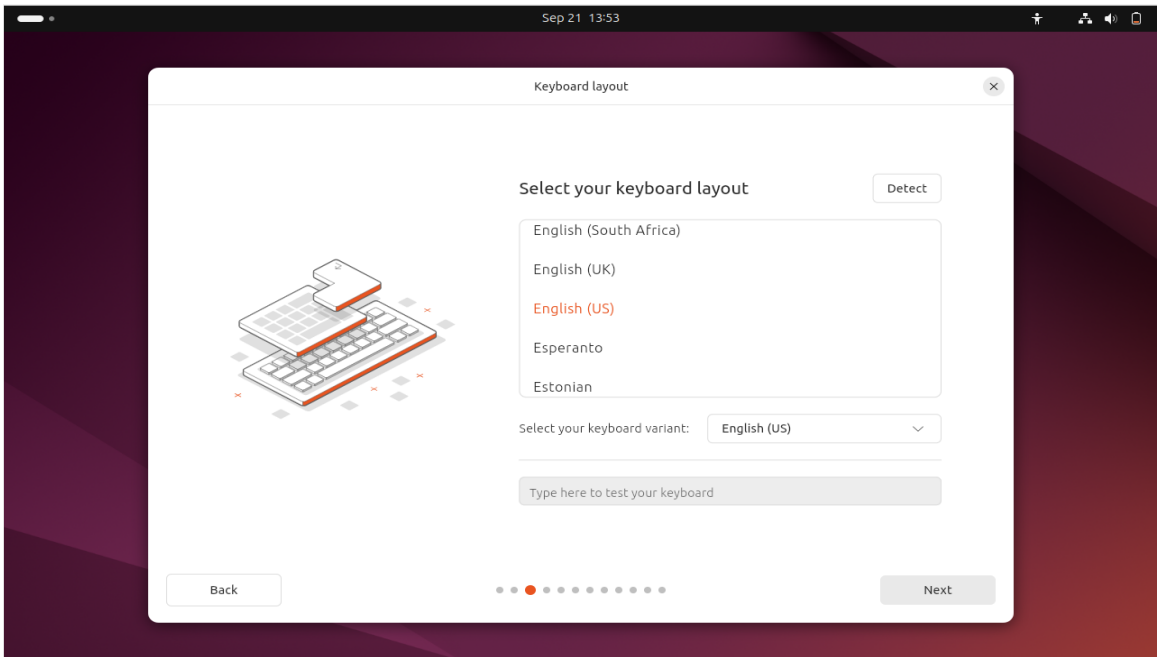
Select Try or Install Ubuntu here by pressing enter.

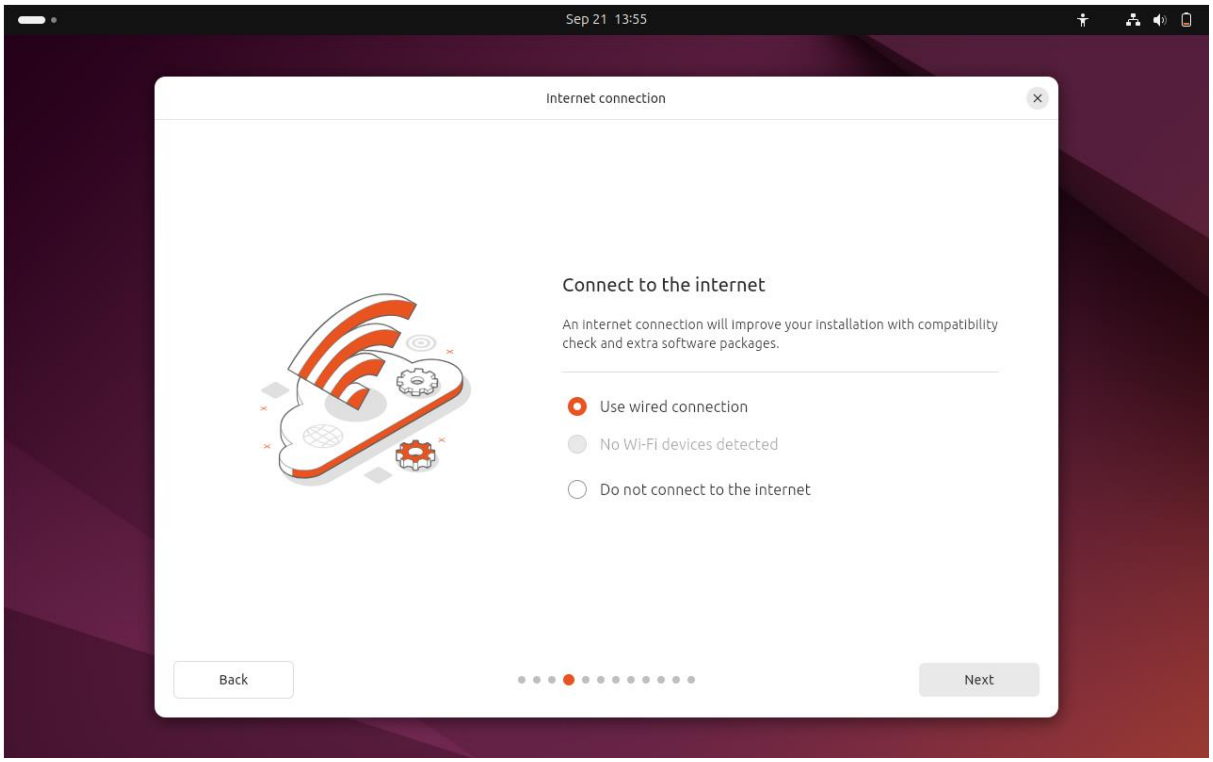
Select English and press next.

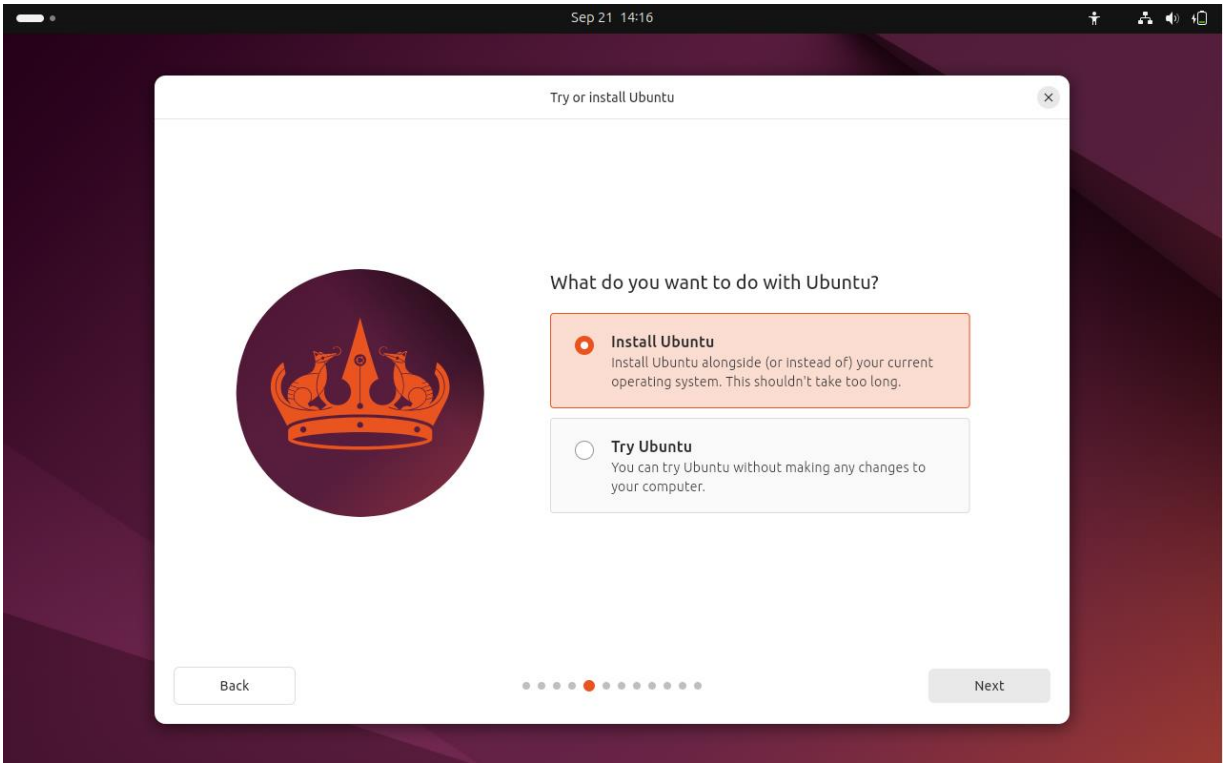


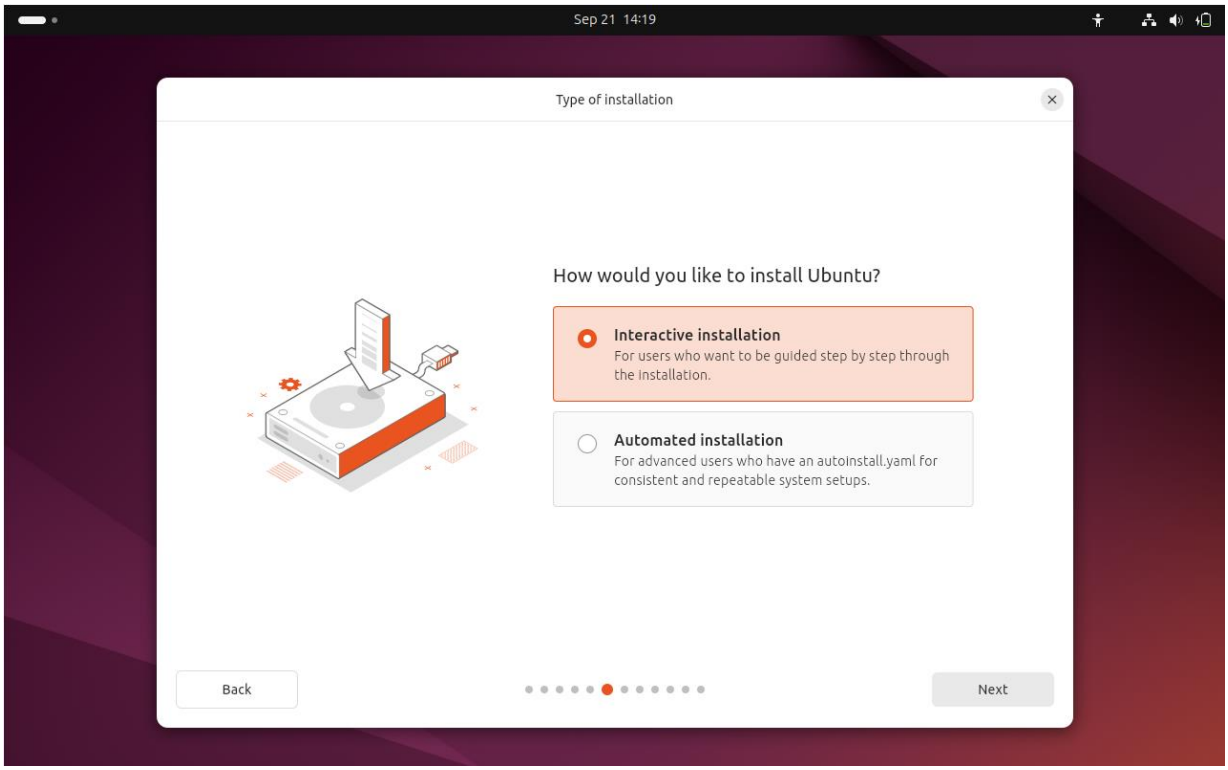
Select the accessibility settings to your liking. I didn't change anything here because everything is according to my preference here.

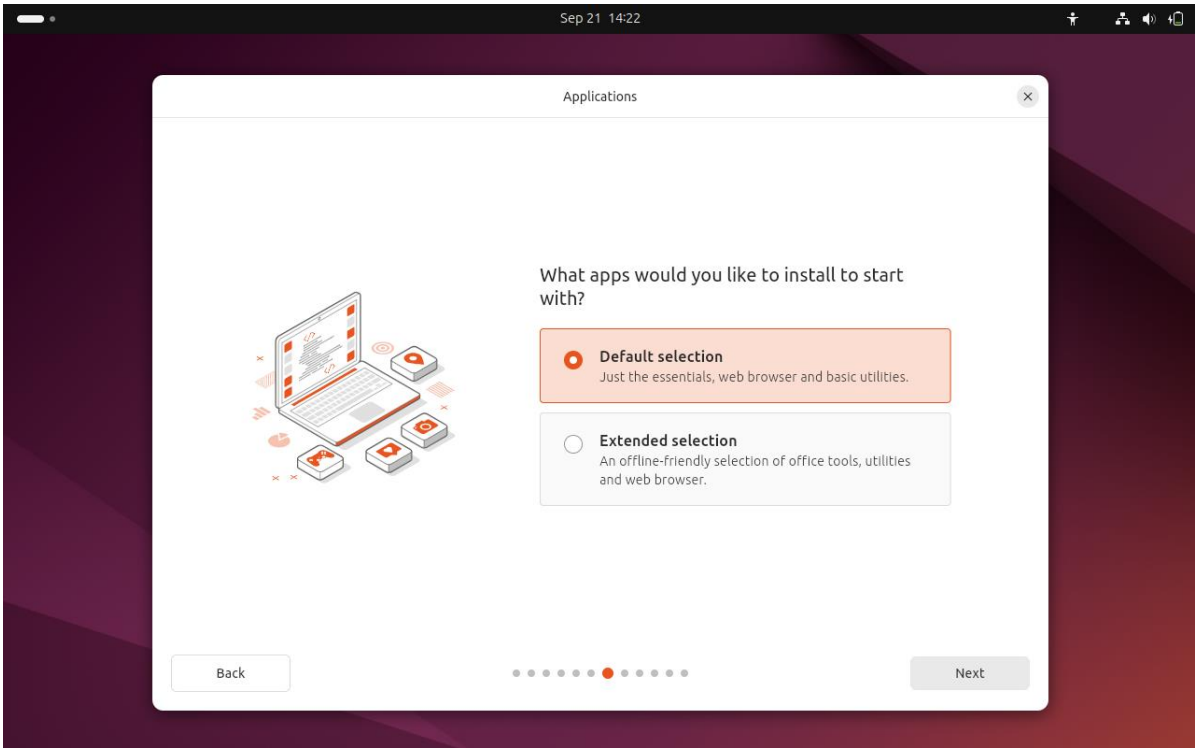

Sep 21 13:47
Accessibility
Accessibility in Ubuntu
Customise Ubuntu to your needs before you set up. You can change them later in System Settings.
Seeing
Hearing
Typing
Pointing and clicking
Zoom
Back
Next


Sep 21 13:53
Keyboard layout
Select your keyboard layout
Detect
English (South Africa)
English (UK)
English (US)
Esperanto
Estonian
Select your keyboard variant:
English (US)
Type here to test your keyboard
Back
Next

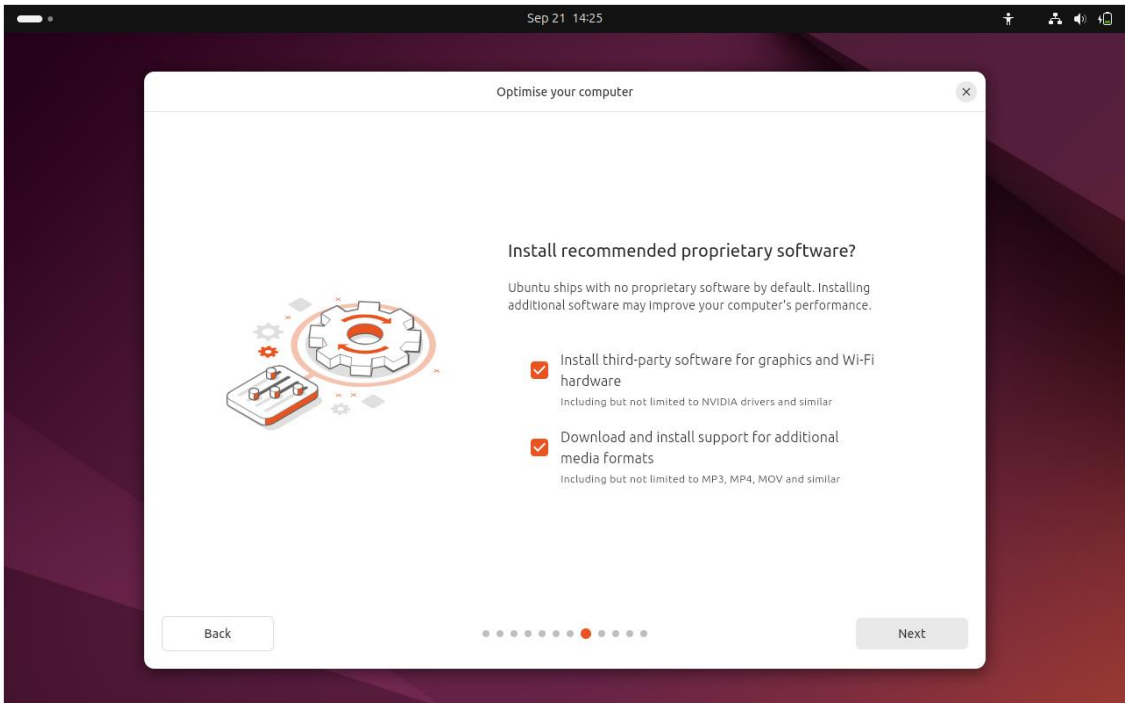

Sep 21 13:55
Internet connection
Connect to the internet
An internet connection will improve your installation with compatibility check and extra software packages.
Use wired connection
No Wi-Fi devices detected
Do not connect to the internet
Back
Next


Sep 21 14:16
Try or install Ubuntu
What do you want to do with Ubuntu?
Install Ubuntu
Install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.
Try Ubuntu
You can try Ubuntu without making any changes to your computer.
Back
Next

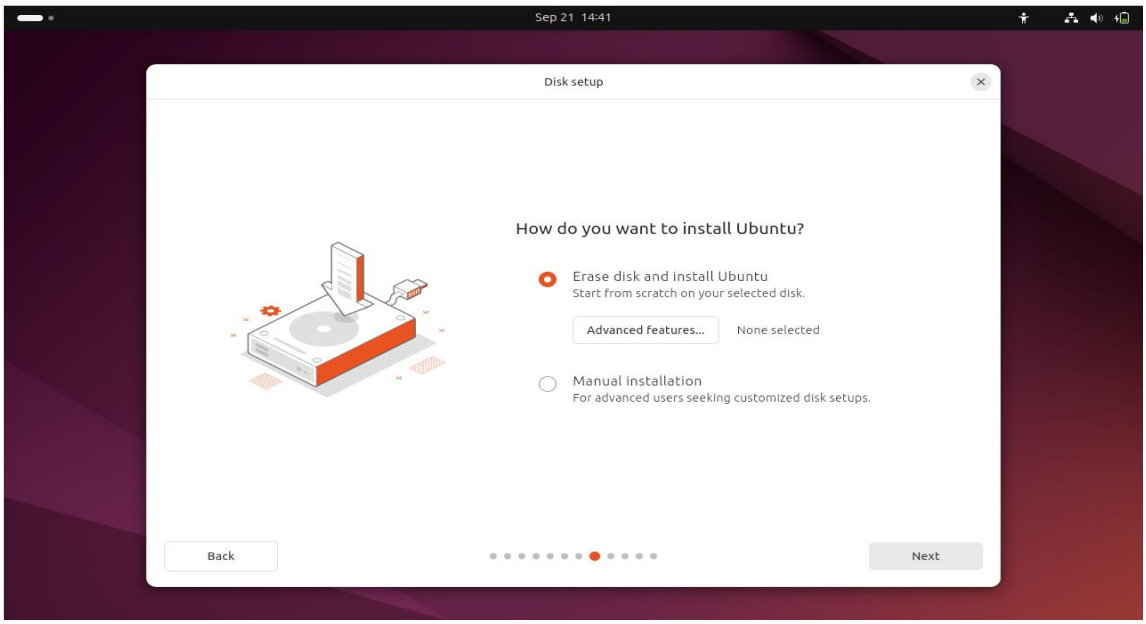

Sep 21 14:19
Type of installation
How would you like to install Ubuntu?
Interactive installation
For users who want to be guided step by step through the installation.
Automated installation
For advanced users who have an autoinstall.yaml for consistent and repeatable system setups.
Back
Next


Sep 21 14:22
Applications
What apps would you like to install to start with?
Default selection
Just the essentials, web browser and basic utilities.
Extended selection
An offline-friendly selection of office tools, utilities and web browser.
Back
Next

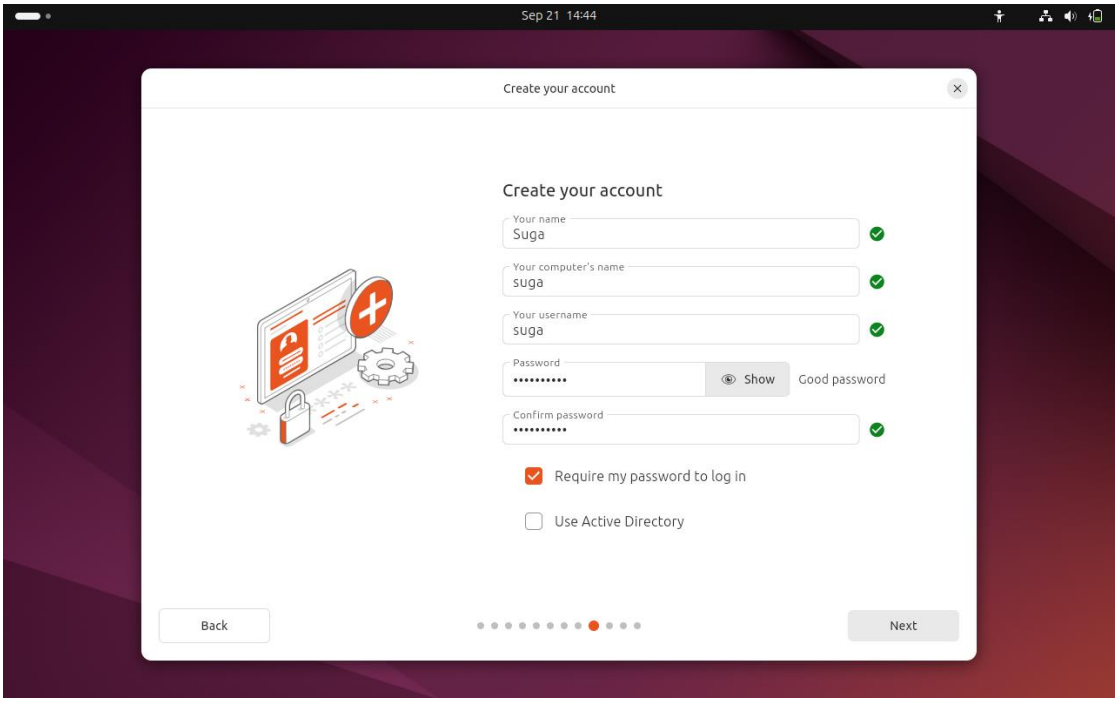
Check both of these checkboxes to install third-party software for graphics and WIFI hardware and to download and install support for additional media formats.



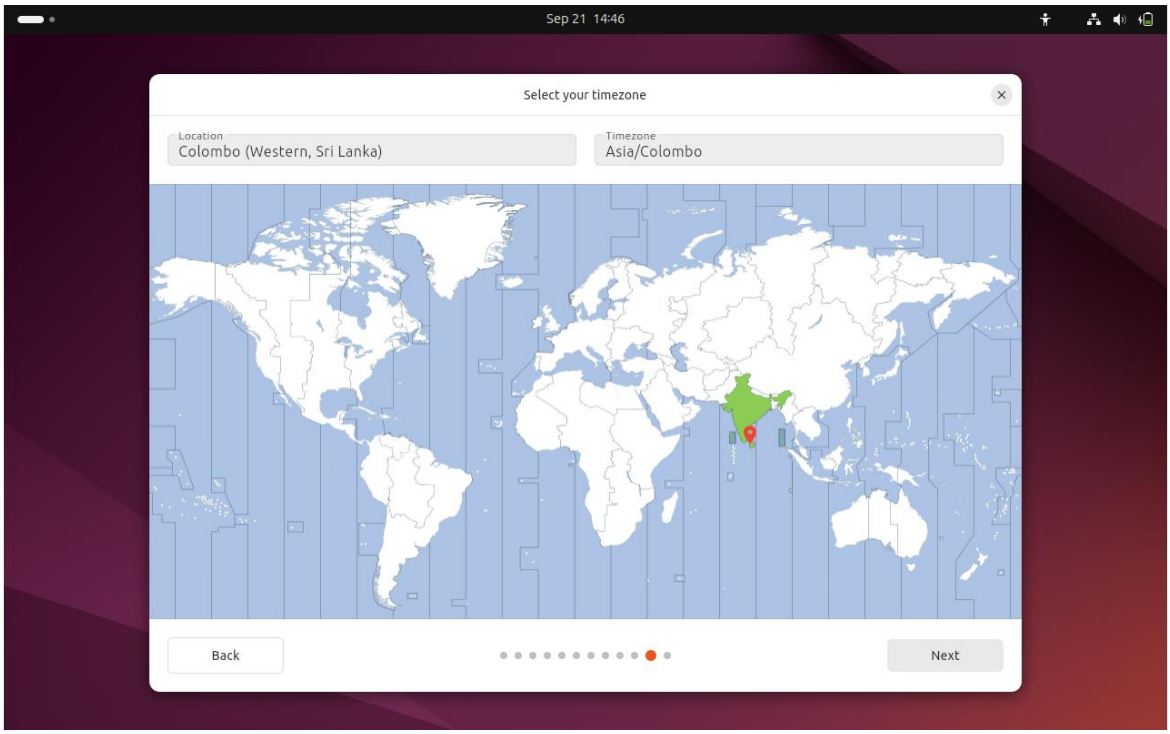
Below configuration will only clear the virtual disk space I allocated previously.



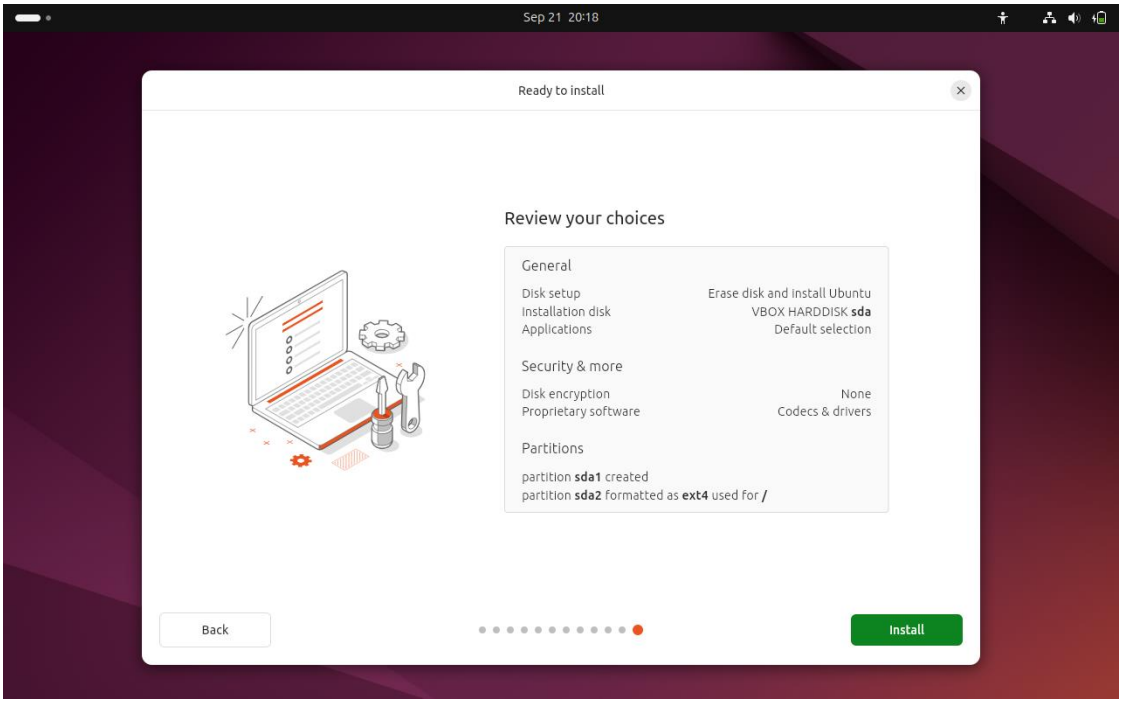
Set credentials for the user account.



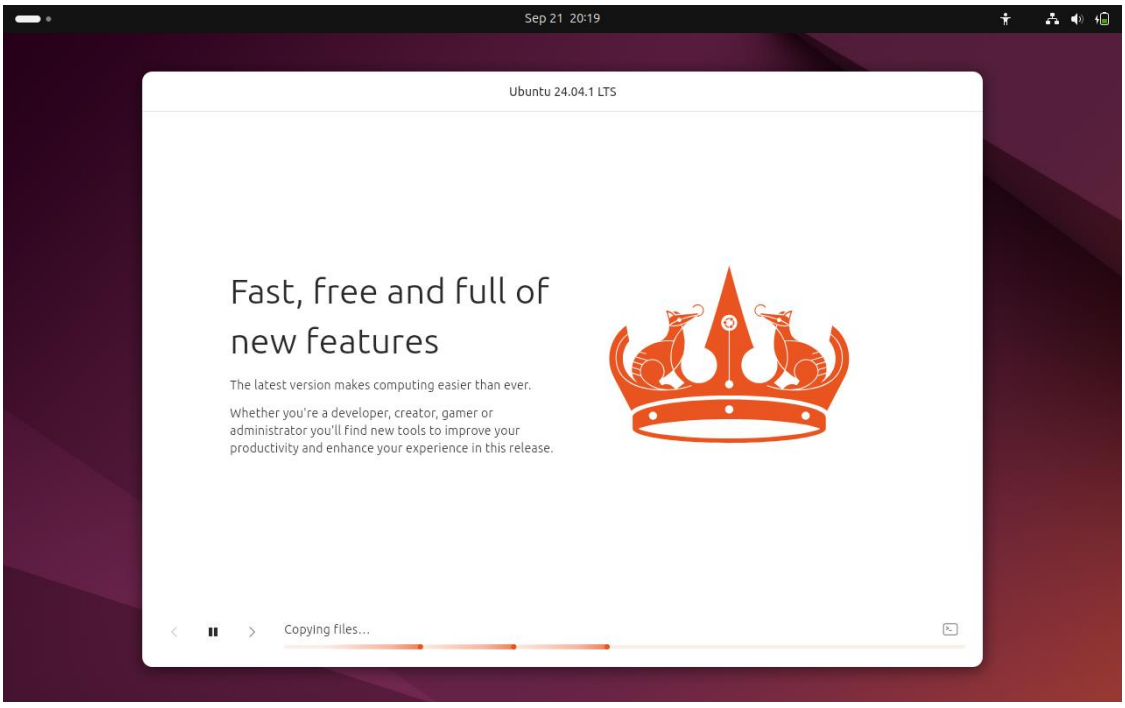
Region will be automatically detected. If not select it manually.



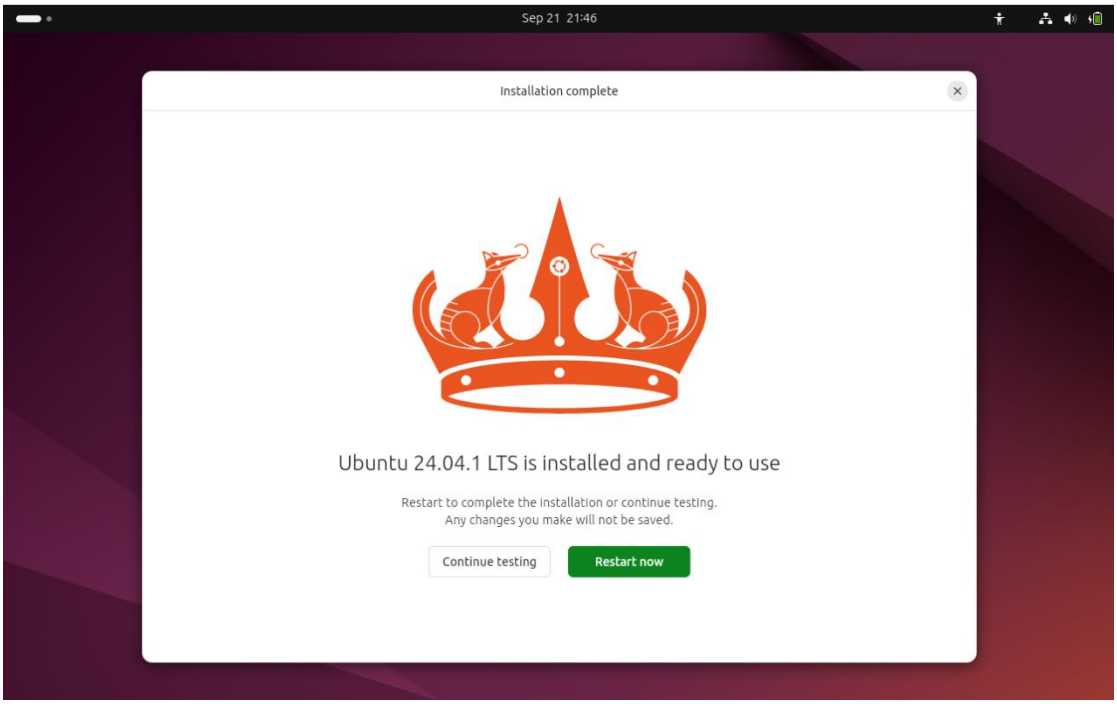
Check the summary to make sure everything is alright.



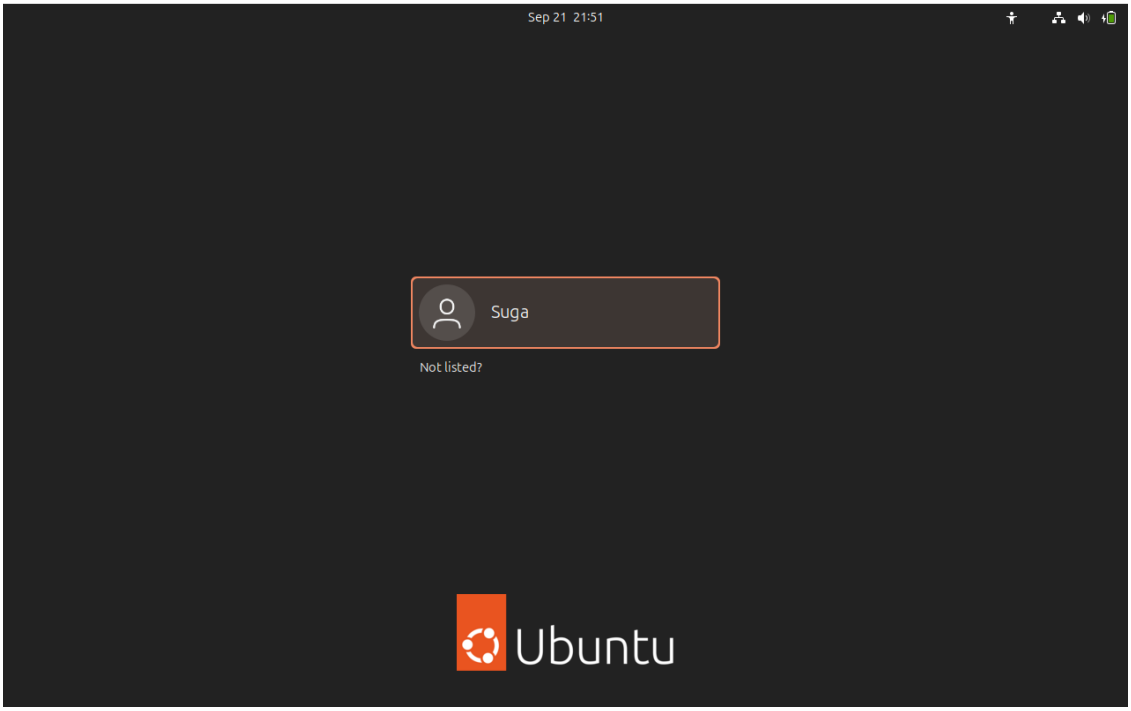
Below process will take few minuts.



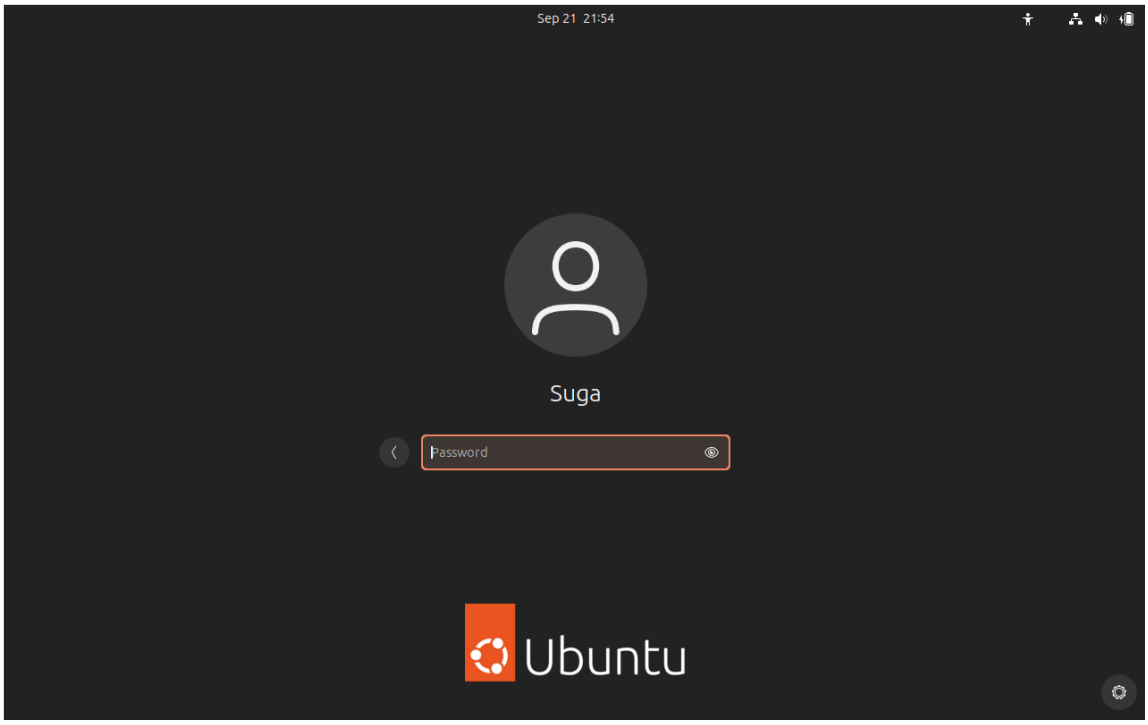
After the installation system will ask to restart.

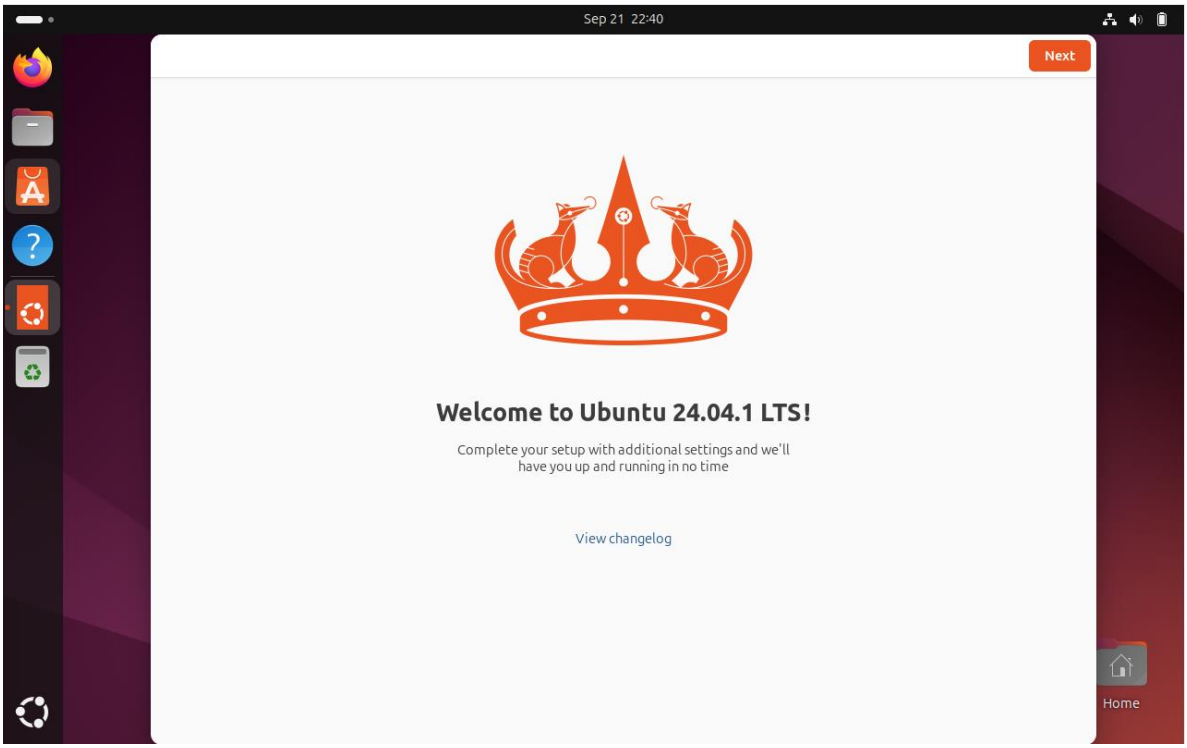


Select your account and press enter.

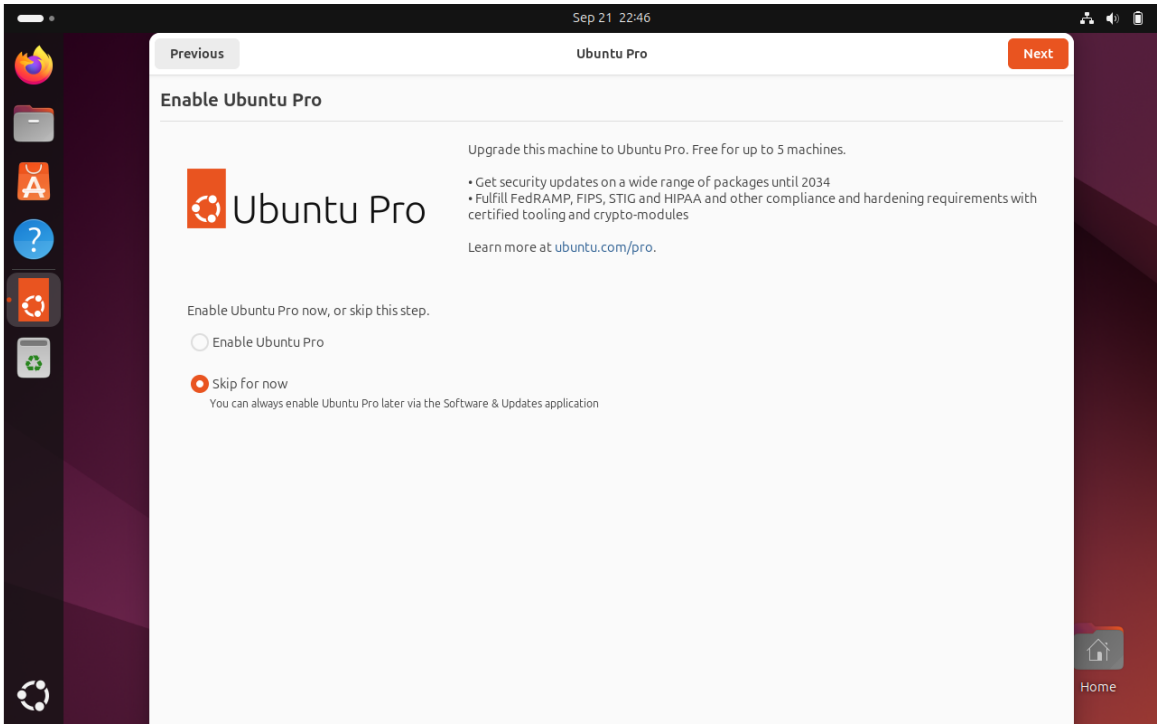


Entered the password I provided earlier.

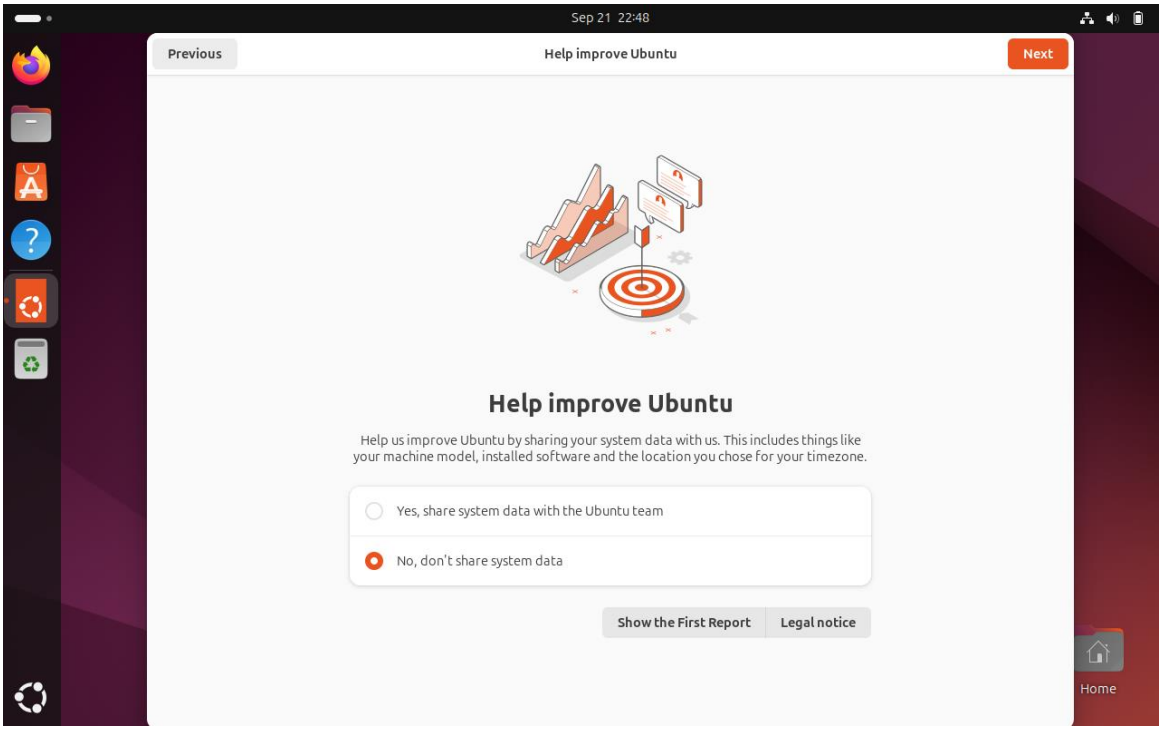




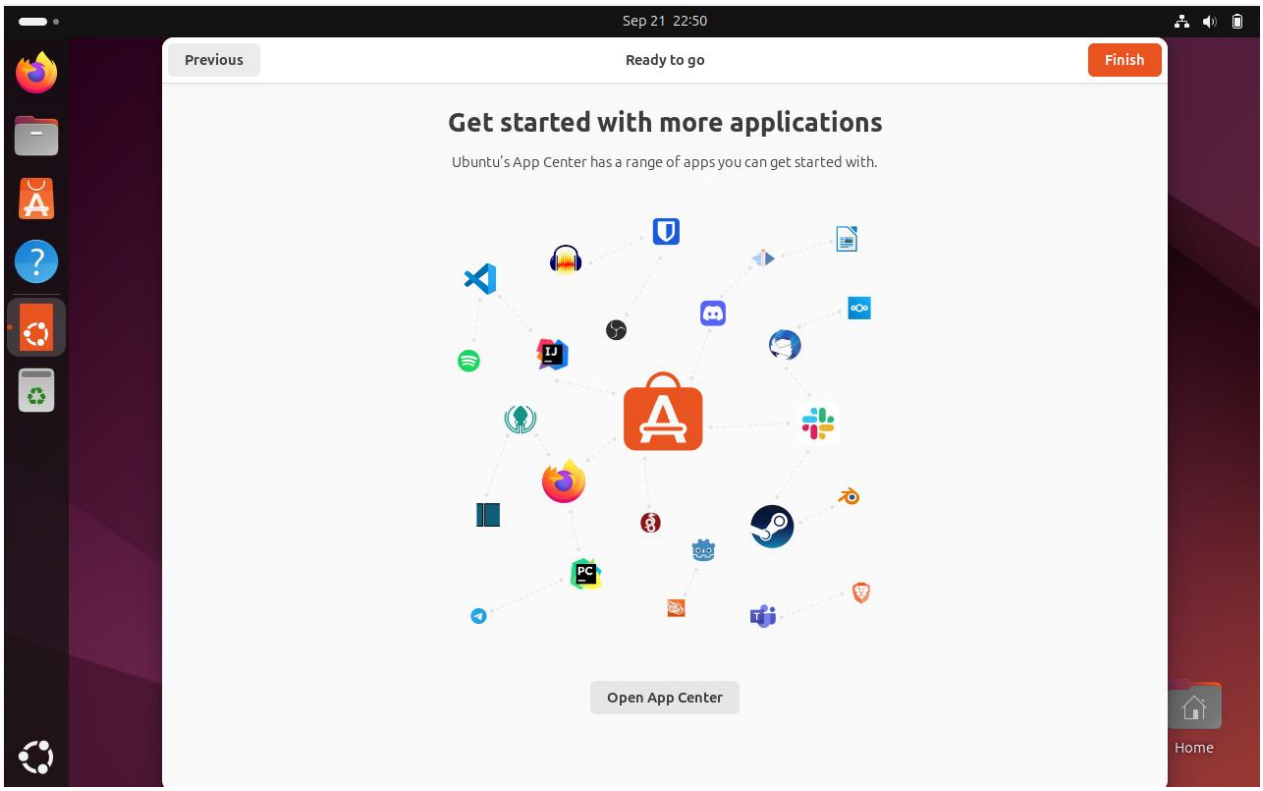
Chose skip for now below for this demonstration.



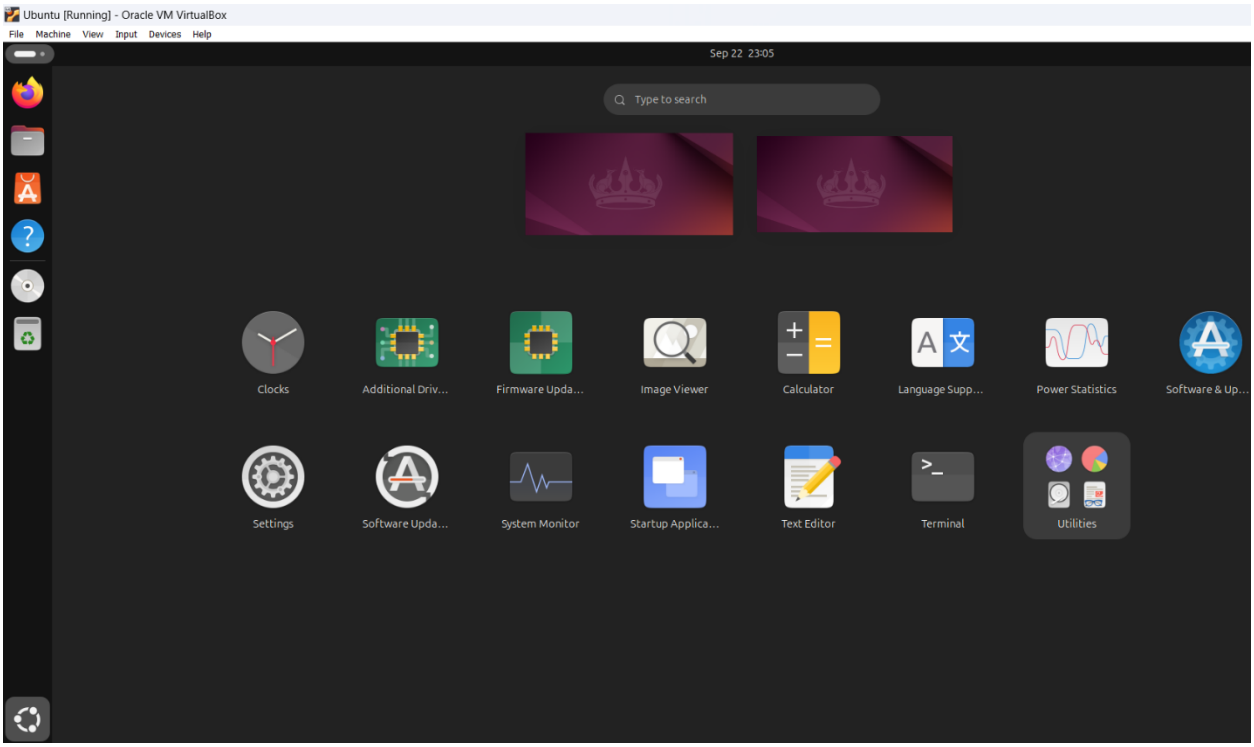
Chose no below because of privacy concerns.



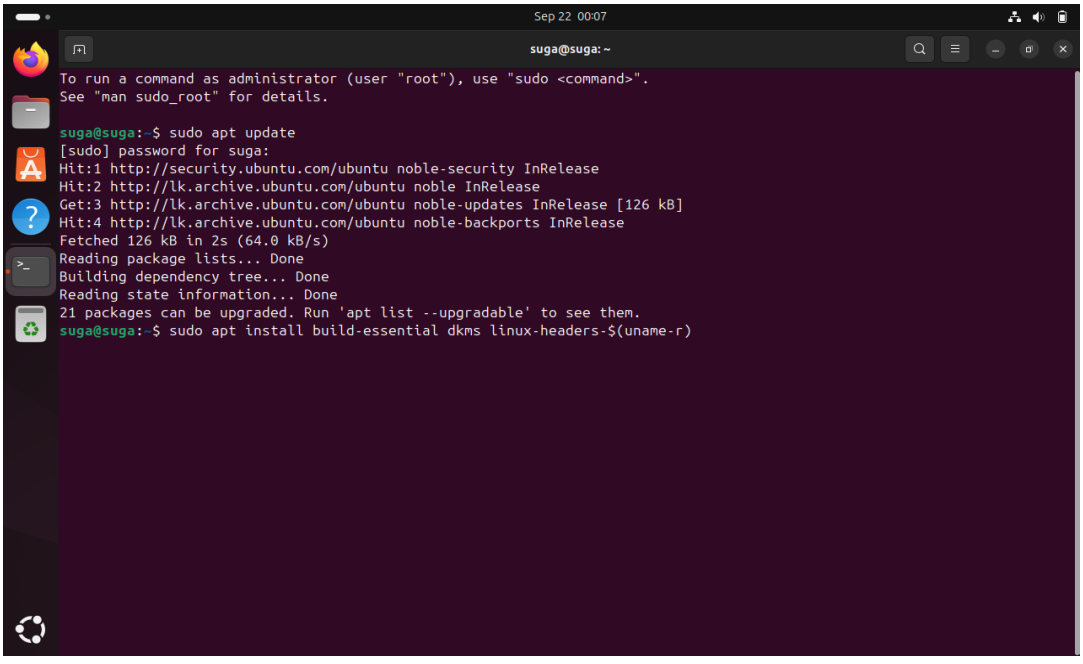
Press finish to end initial setting up process.



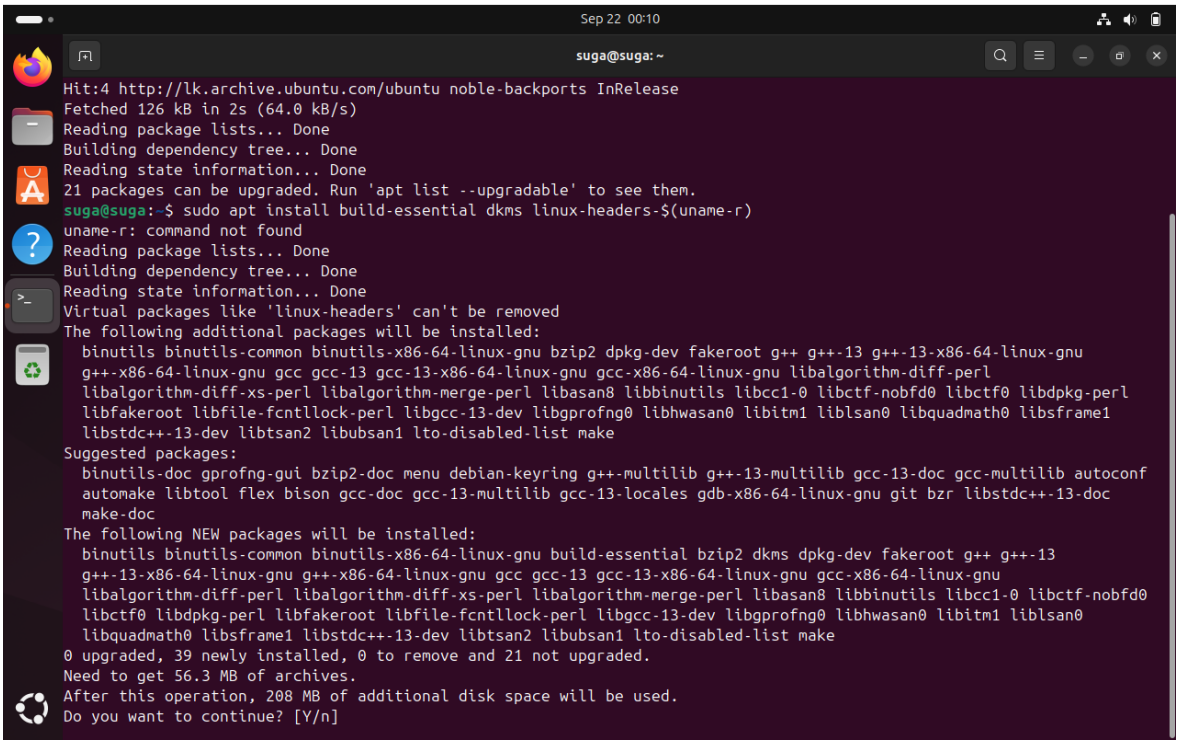
After installation VirtualBox doesn't give Ubuntu on full screen. That issue can be solved by installing VirtualBox guest editions through Ubuntu terminal. To access the terminal press the show apps button in the bottom left corner and then select terminal.

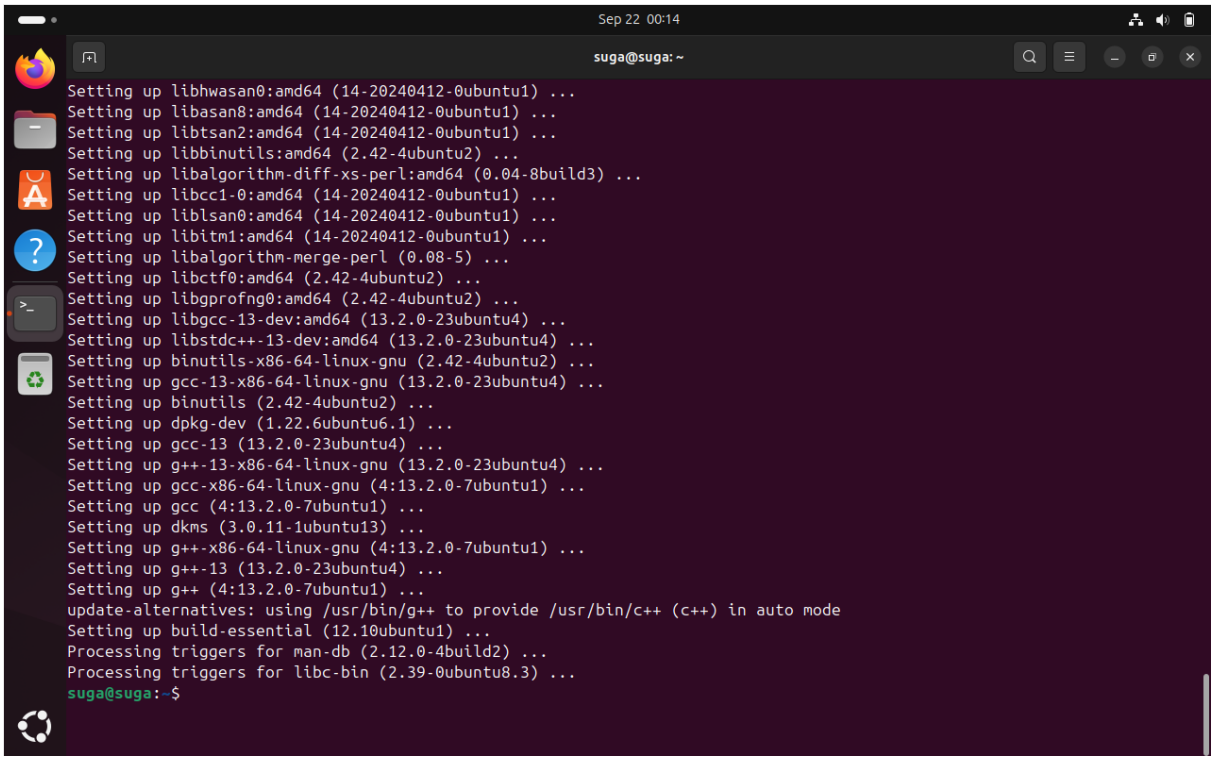


First run sudo apt update command on Ubuntu terminal. Enter the password to commence. This will update packages and repository information. Then run sudo apt install build-essential dkms linux-headers-$(uname -r) command. This command will install build essentials, dkms and Linux headers.

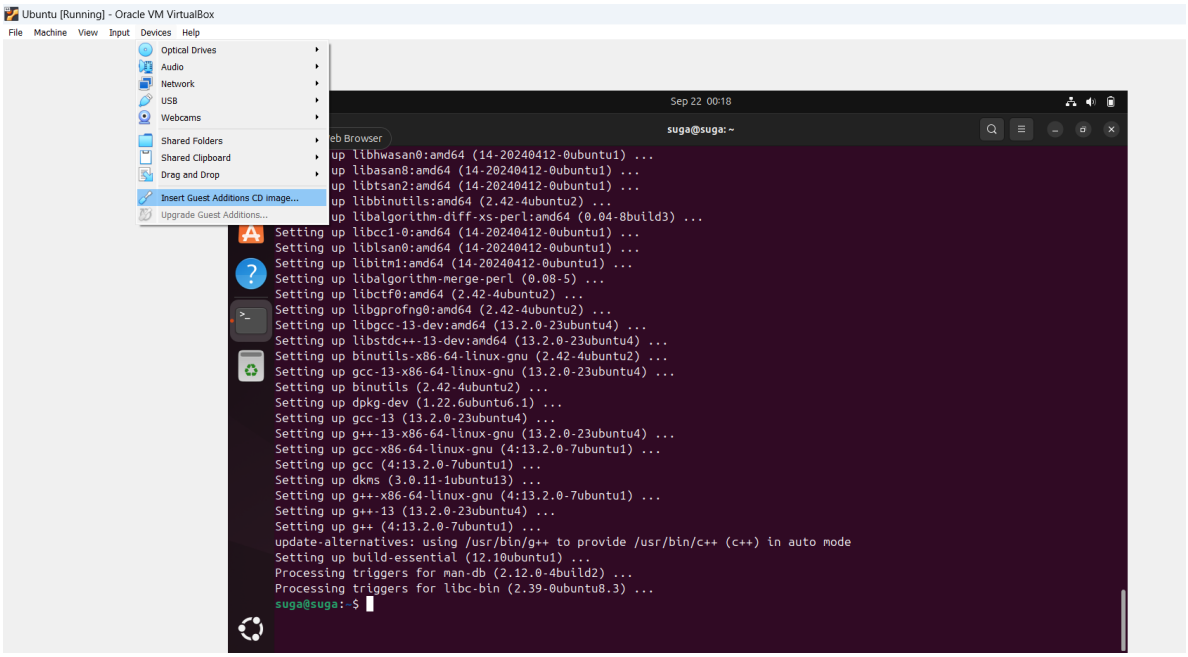


Pess Y to continue.

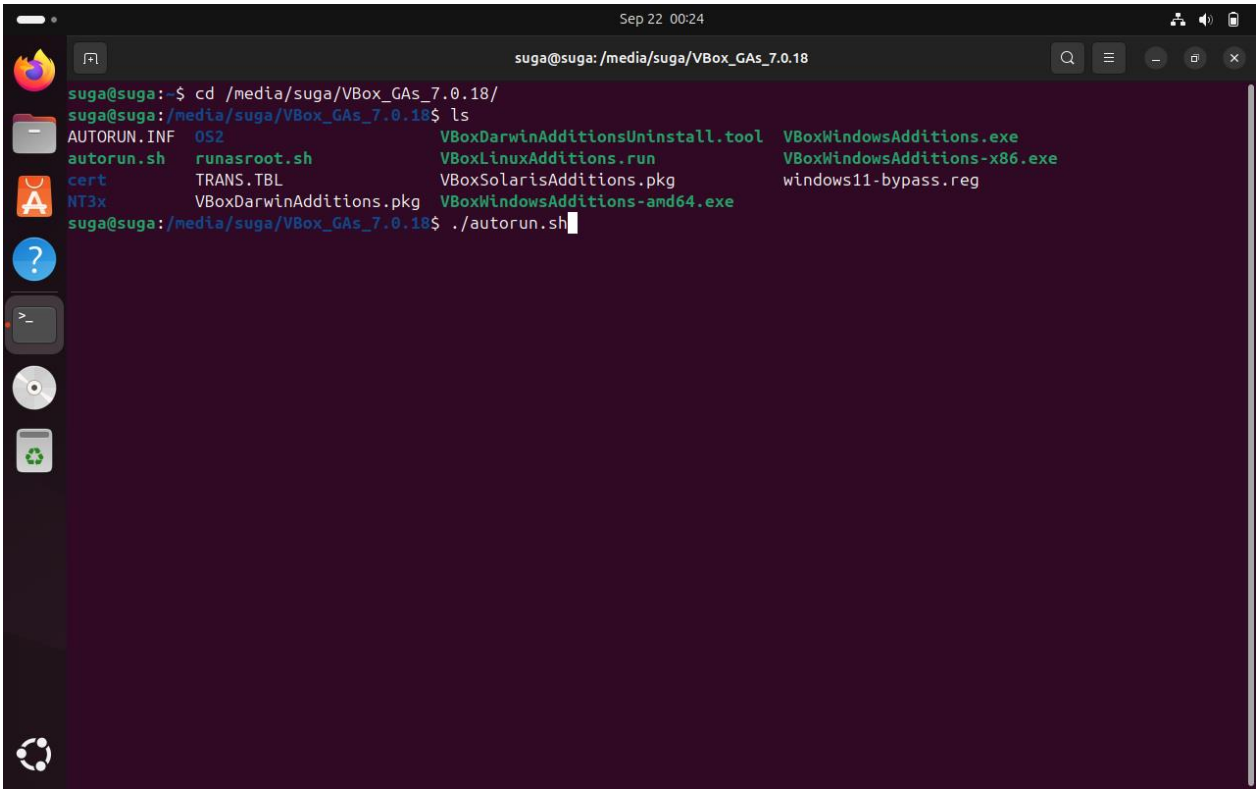




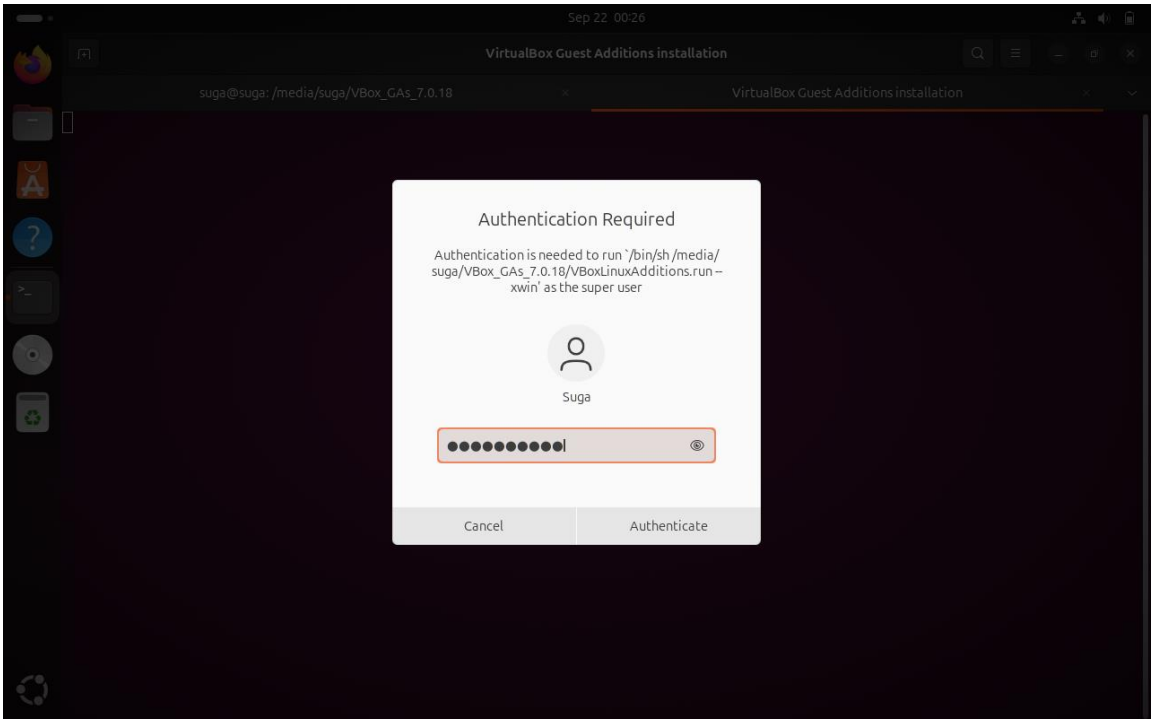
After installation click on devices option on the top left VirtualBox menu and select insert guest additions CD image. It will mount guest additions to Ubuntu OS.



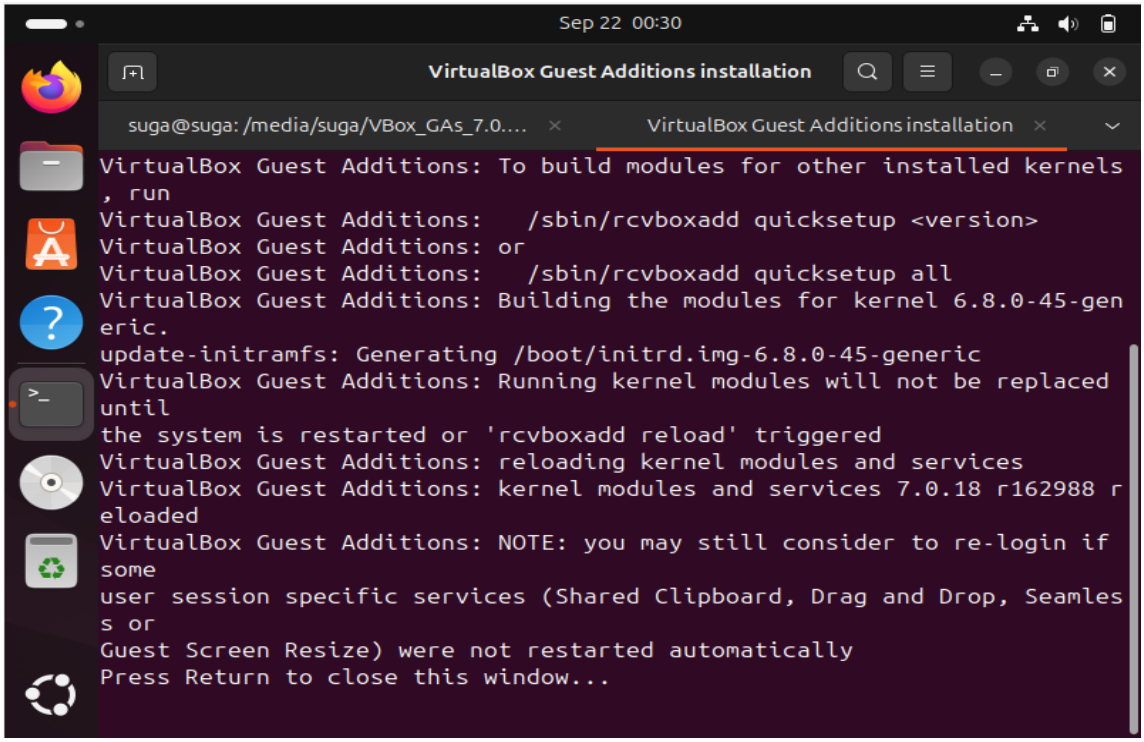
Then navigate in to /media/suga/VBox_Gas_7.0.18/ folder and look for autorun.sh file.



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



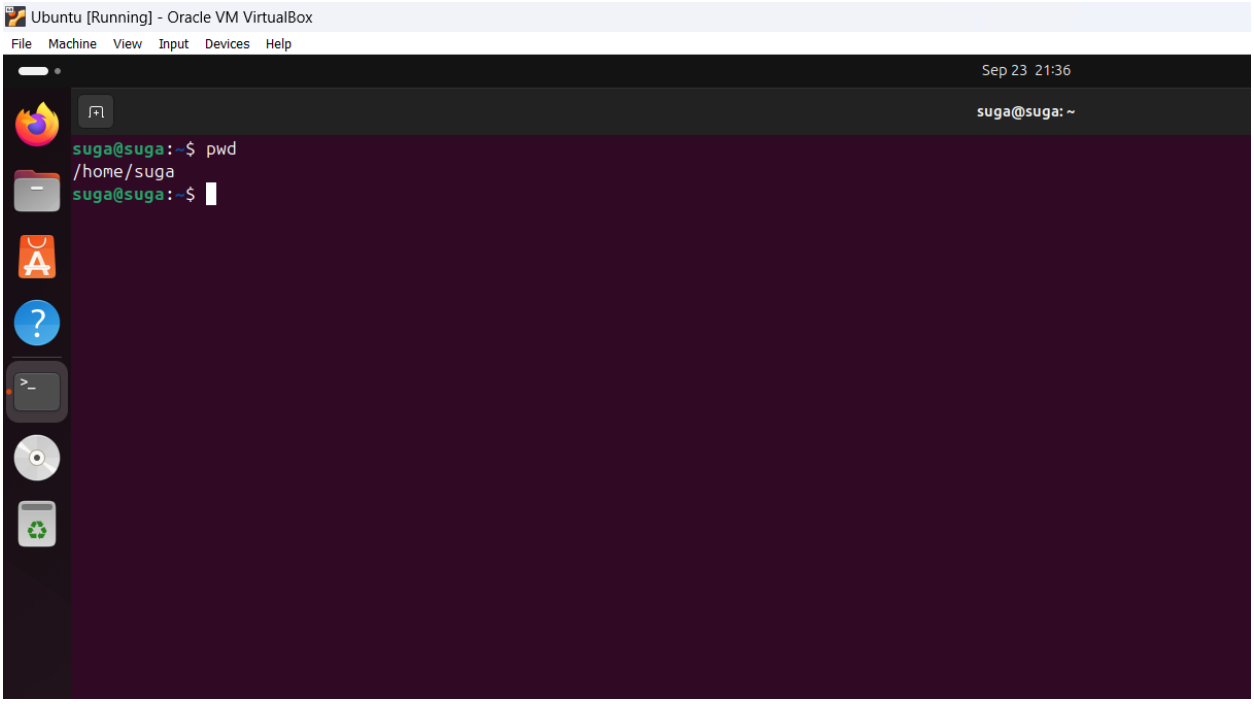
It will start installing guest additions in VirtualBox.



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

1.2 Command Line Introduction

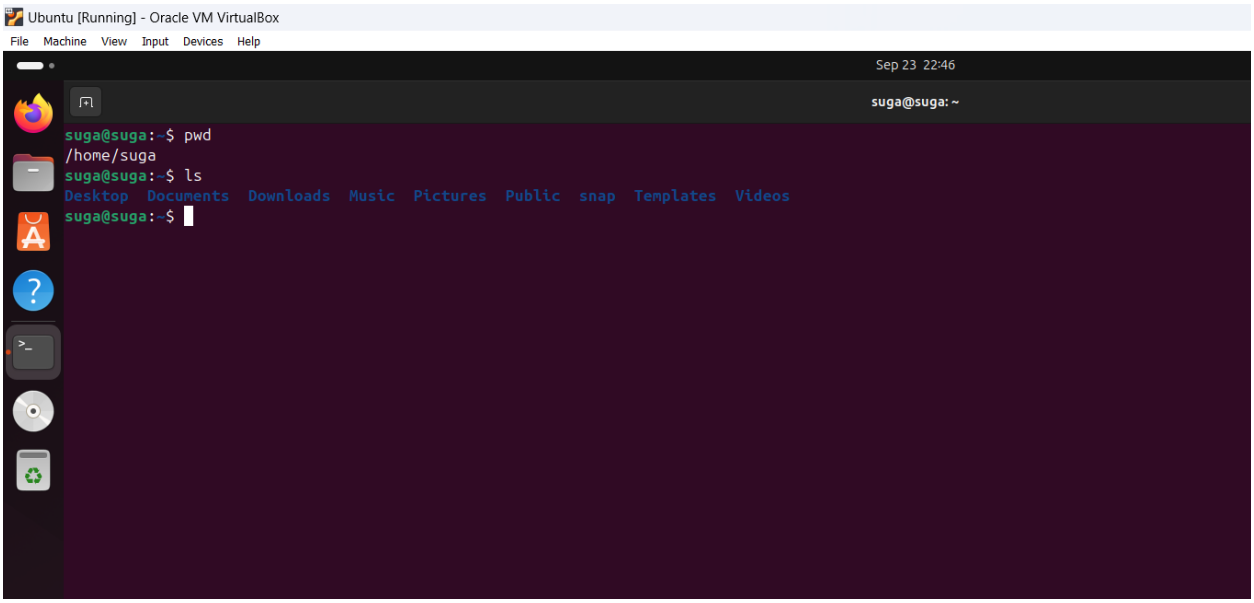
1.pwd



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 though 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 shows 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.

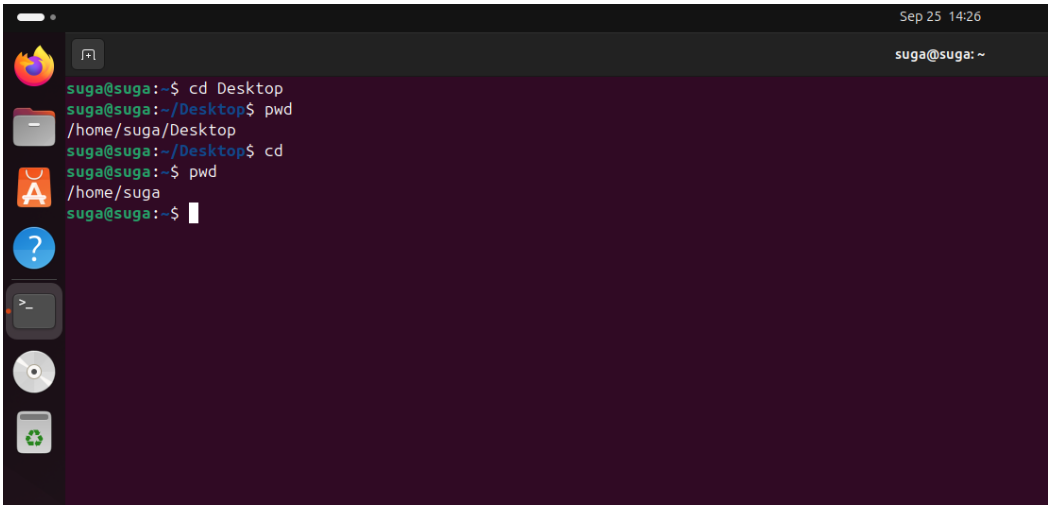
```
suga@suga:~$ ls -l
total 36
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Desktop
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Documents
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Downloads
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Music
drwxr-xr-x 2 suga suga 4096 Sep 21 21:56 Pictures
drwxr-xr-x 2 suga suga 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.

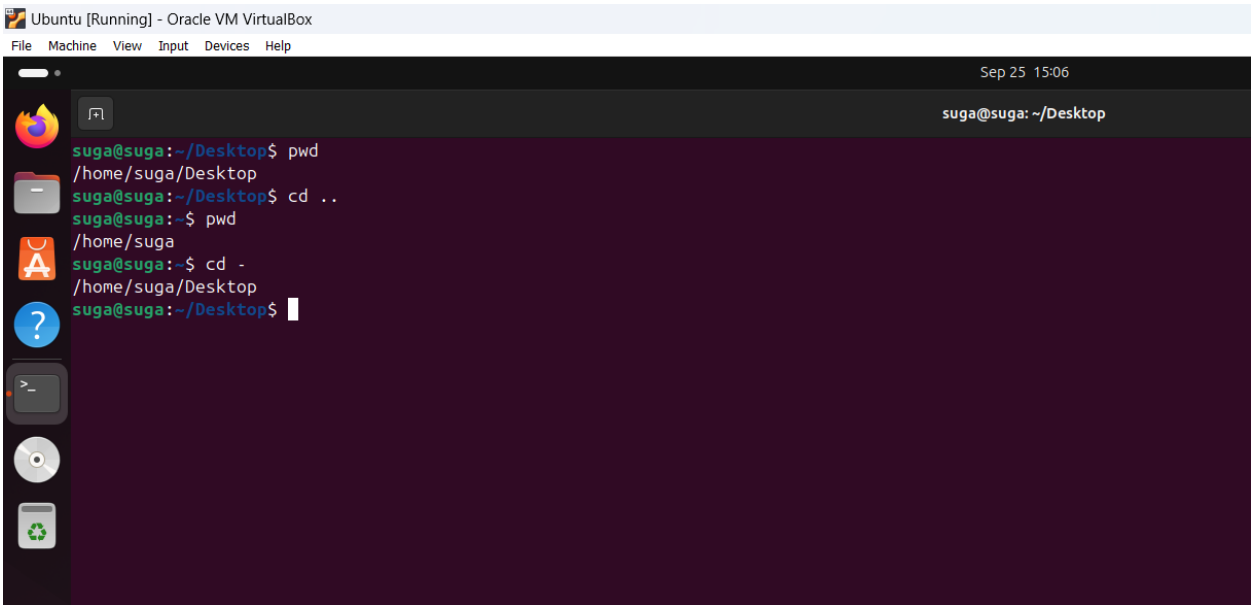
```
suga@suga:~$ ls -R
.:
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos

./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.

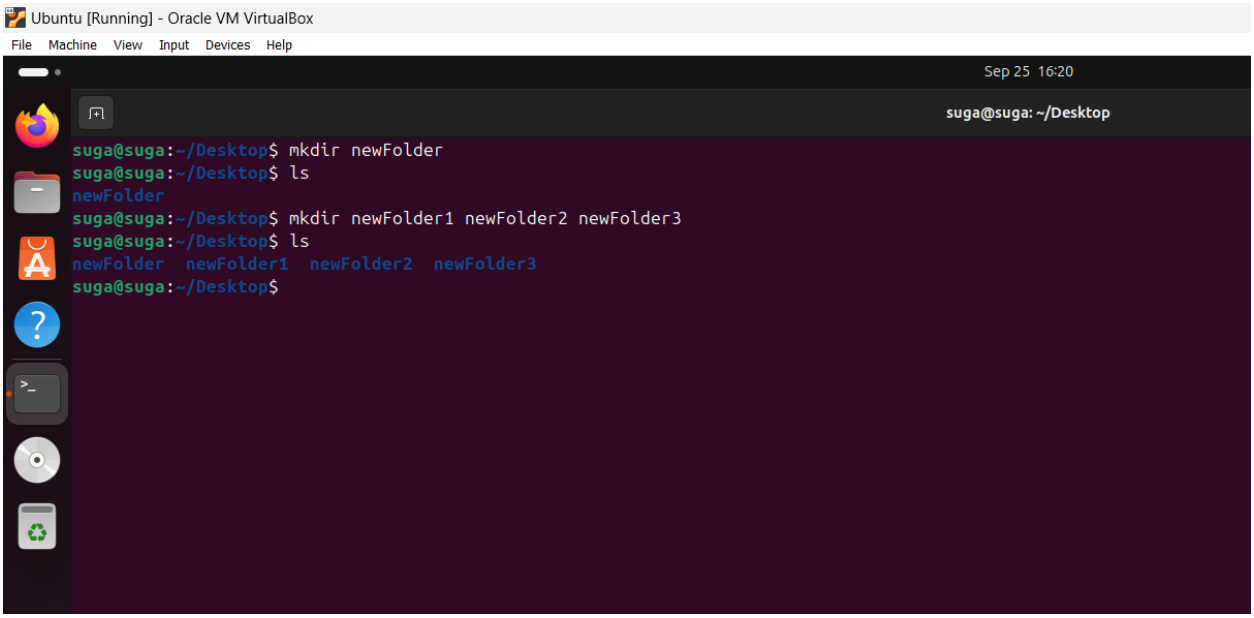


If you use cd .. command terminal will take you to parent directory. The command cd – will take you to previous directory.



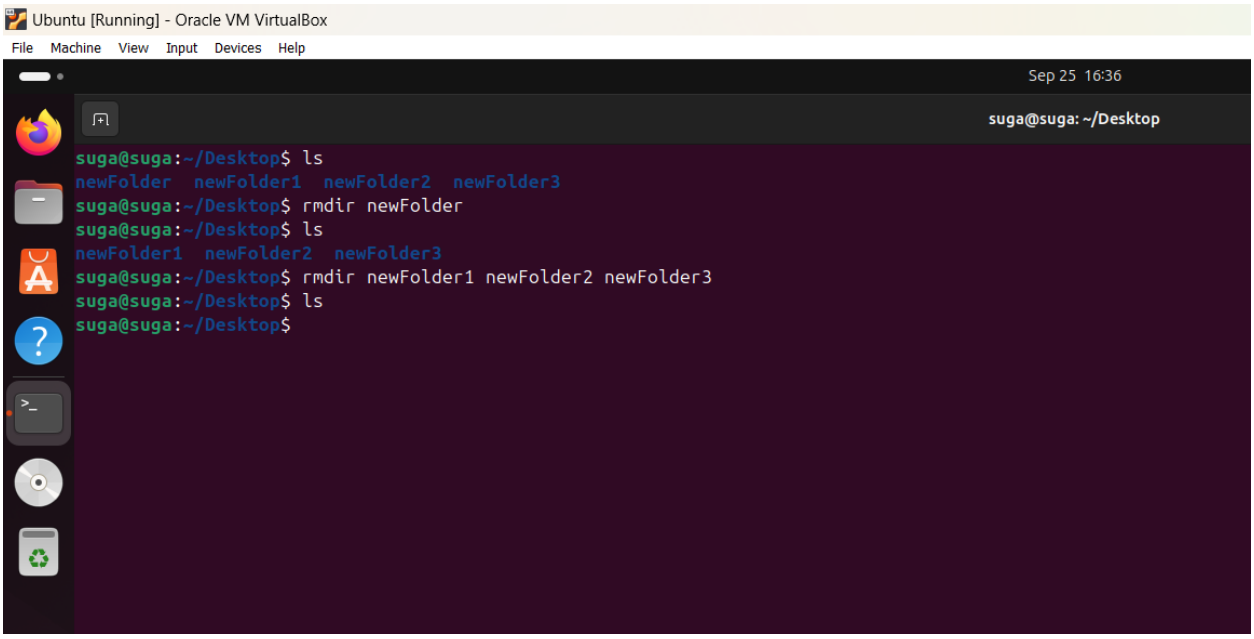
4.mkdir

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



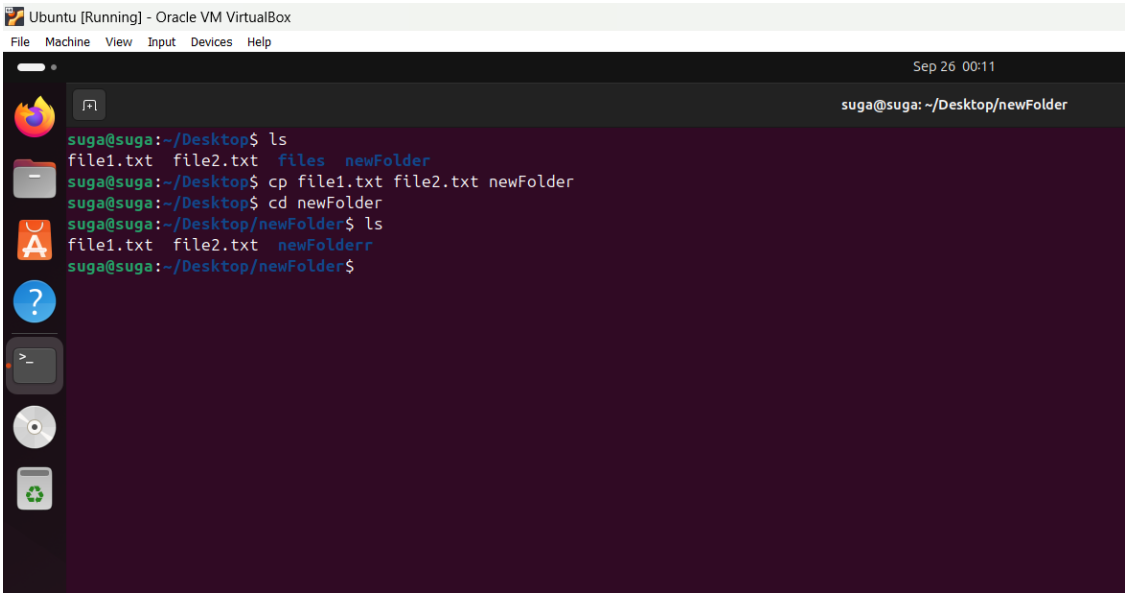
5.rmdir

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



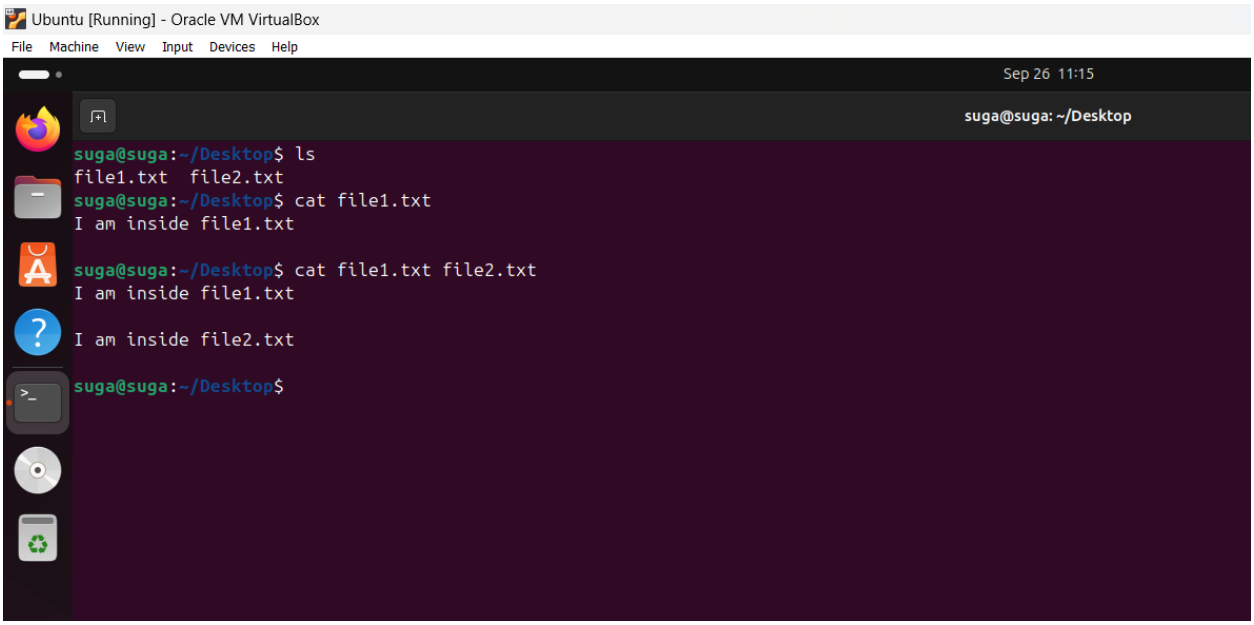
6.cp

The cp command is used to copy files and directories.



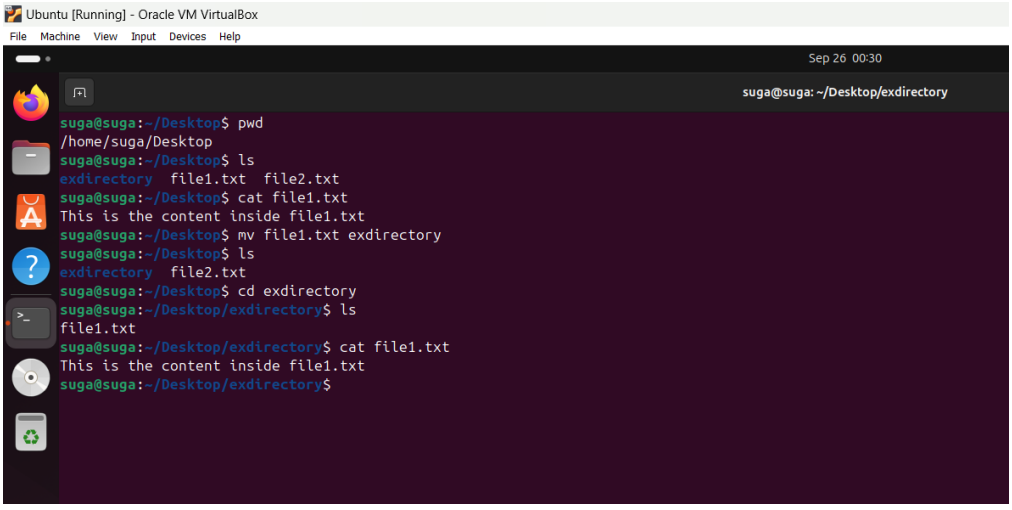
7.cat

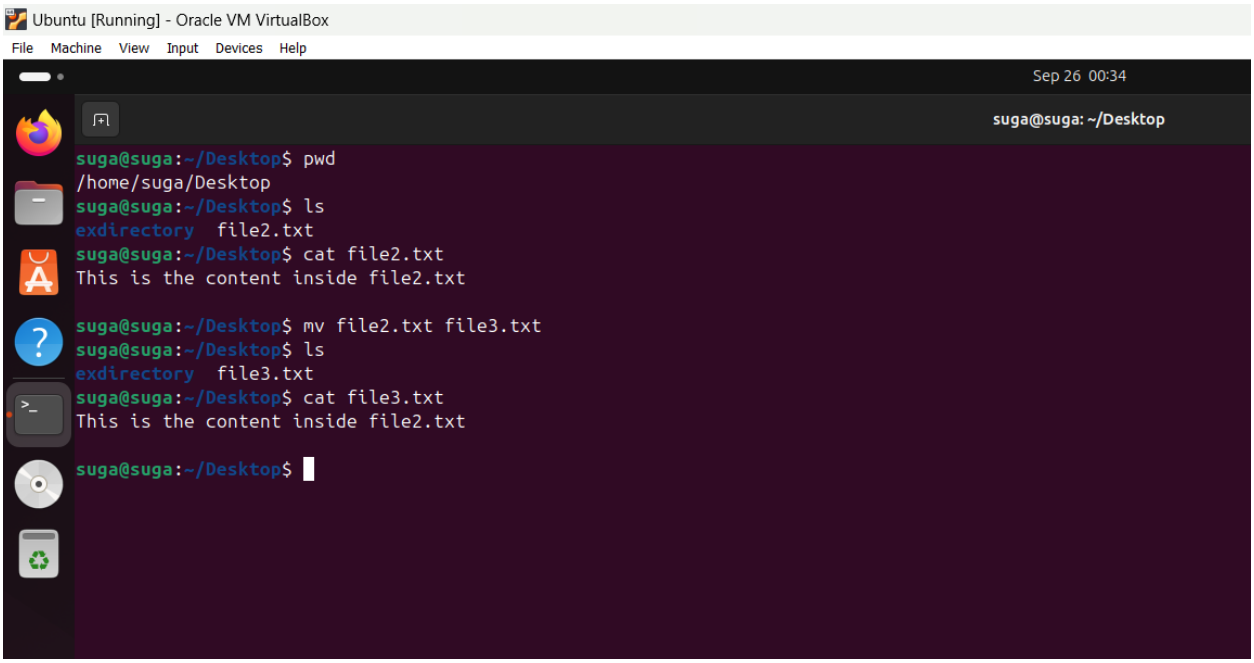
The cat command is used to display the content of a file or concatenate multiple files and print their output.



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.

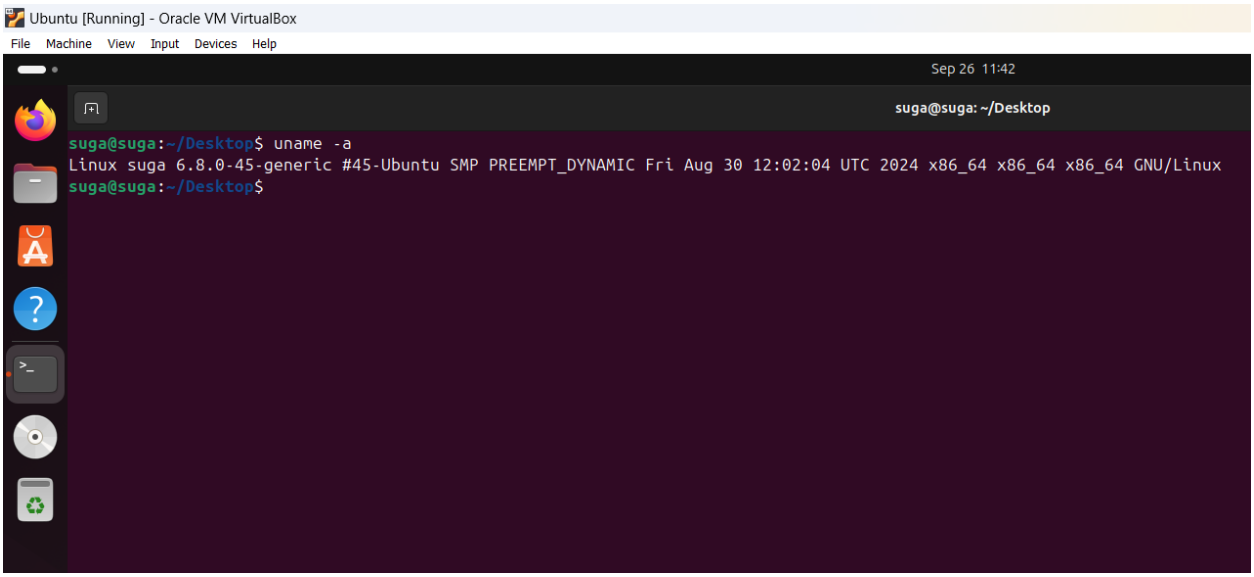




1.3 System Information and User Management

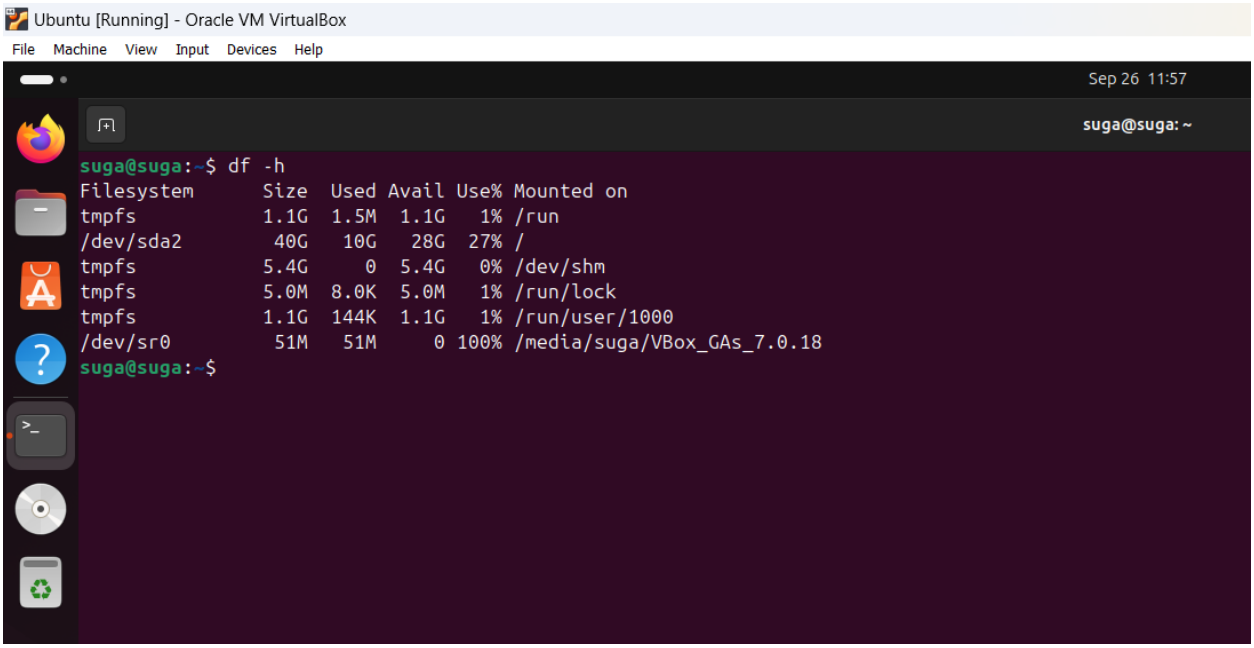
9.uname -a

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.



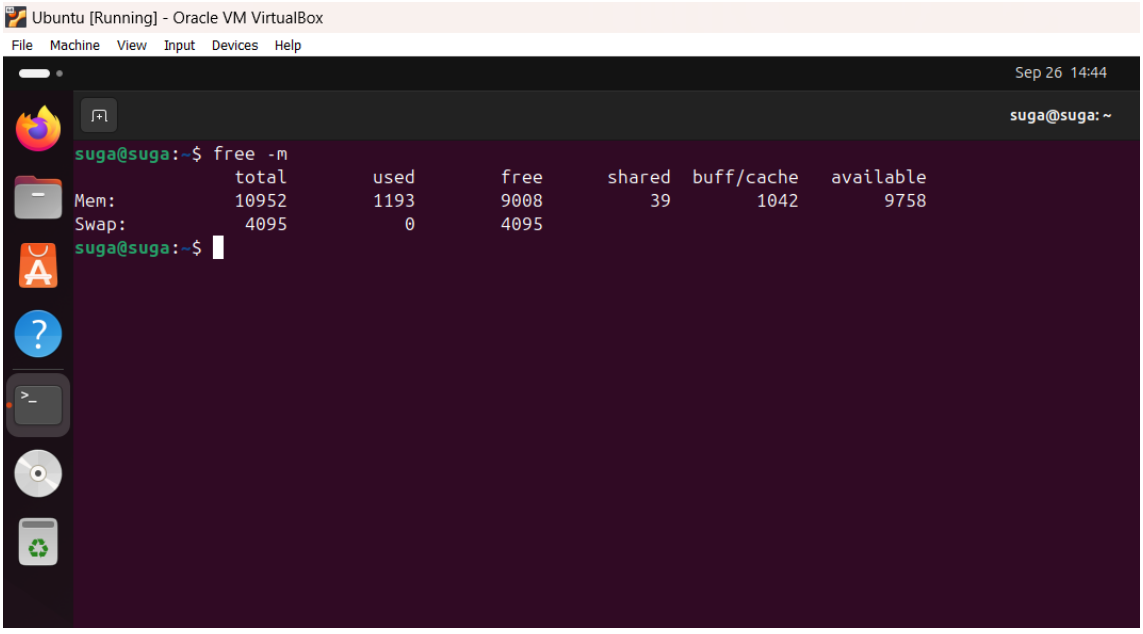
10.df -h

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



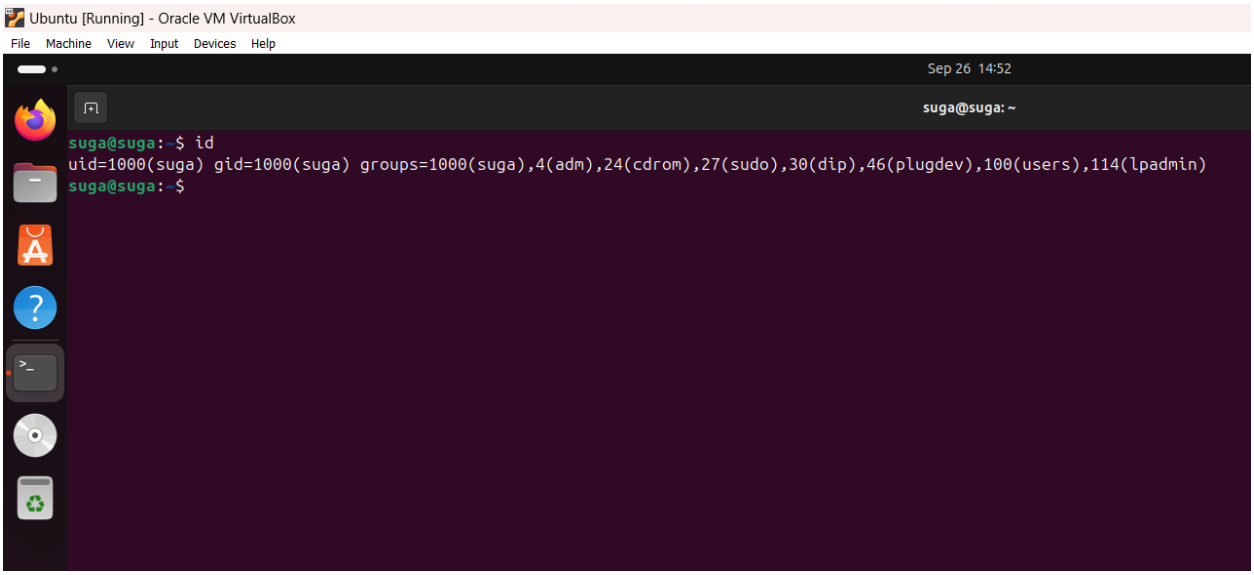
11.free -m

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



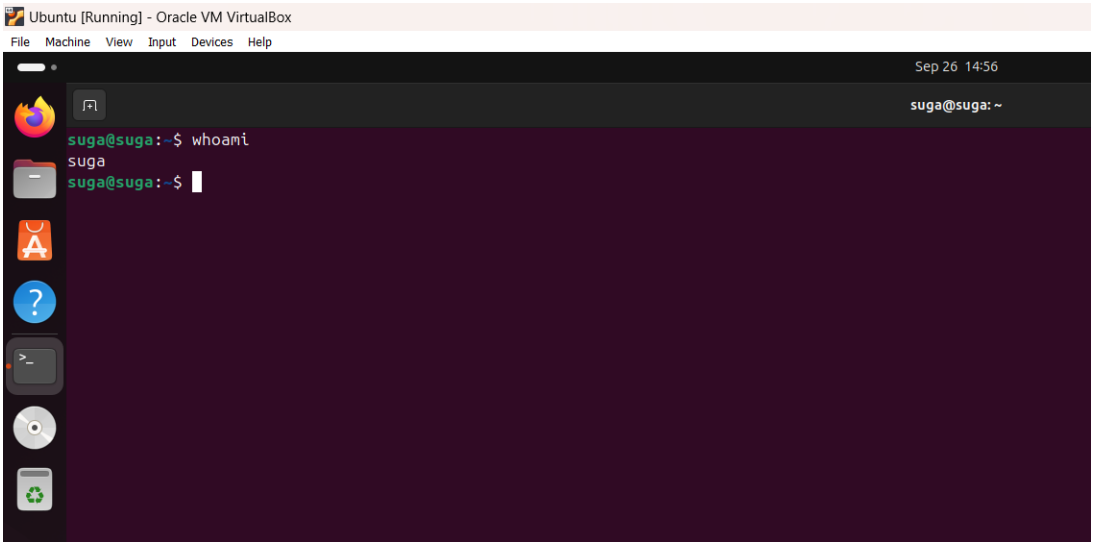
12.id

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



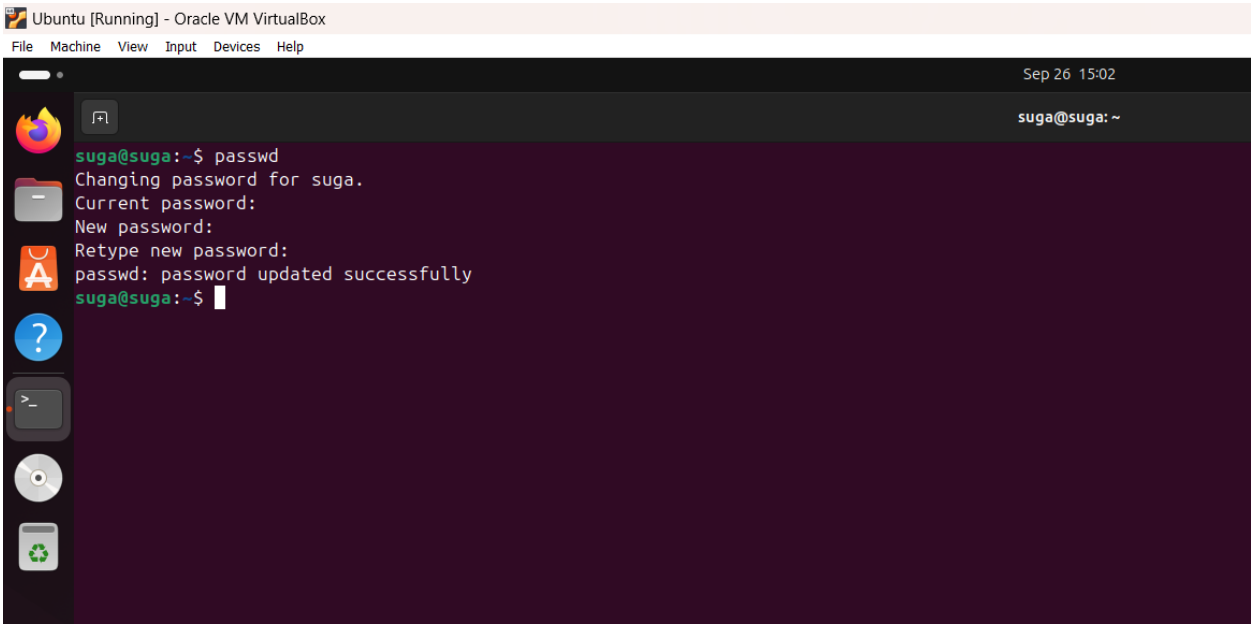
13. whoami

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.



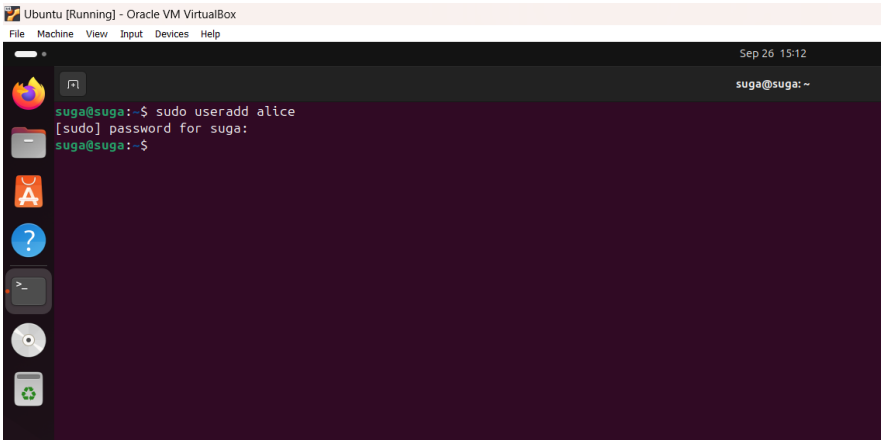
14. passwd

The passwd command in 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).



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.



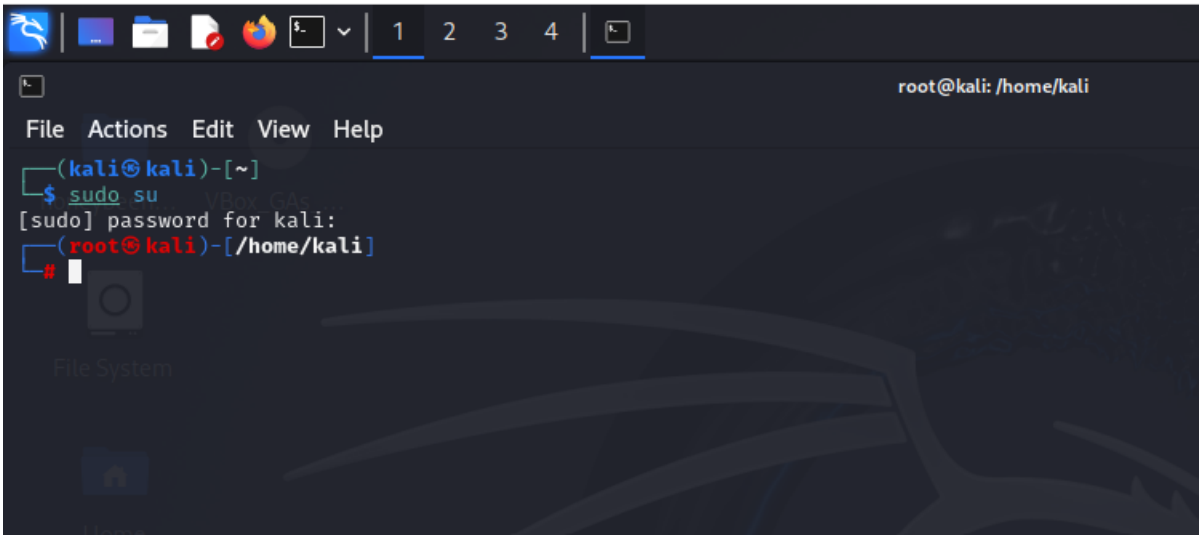
2 DHCP, DNS and NTP Services

2.1 DHCP (Dynamic Host Configuration Protocol)

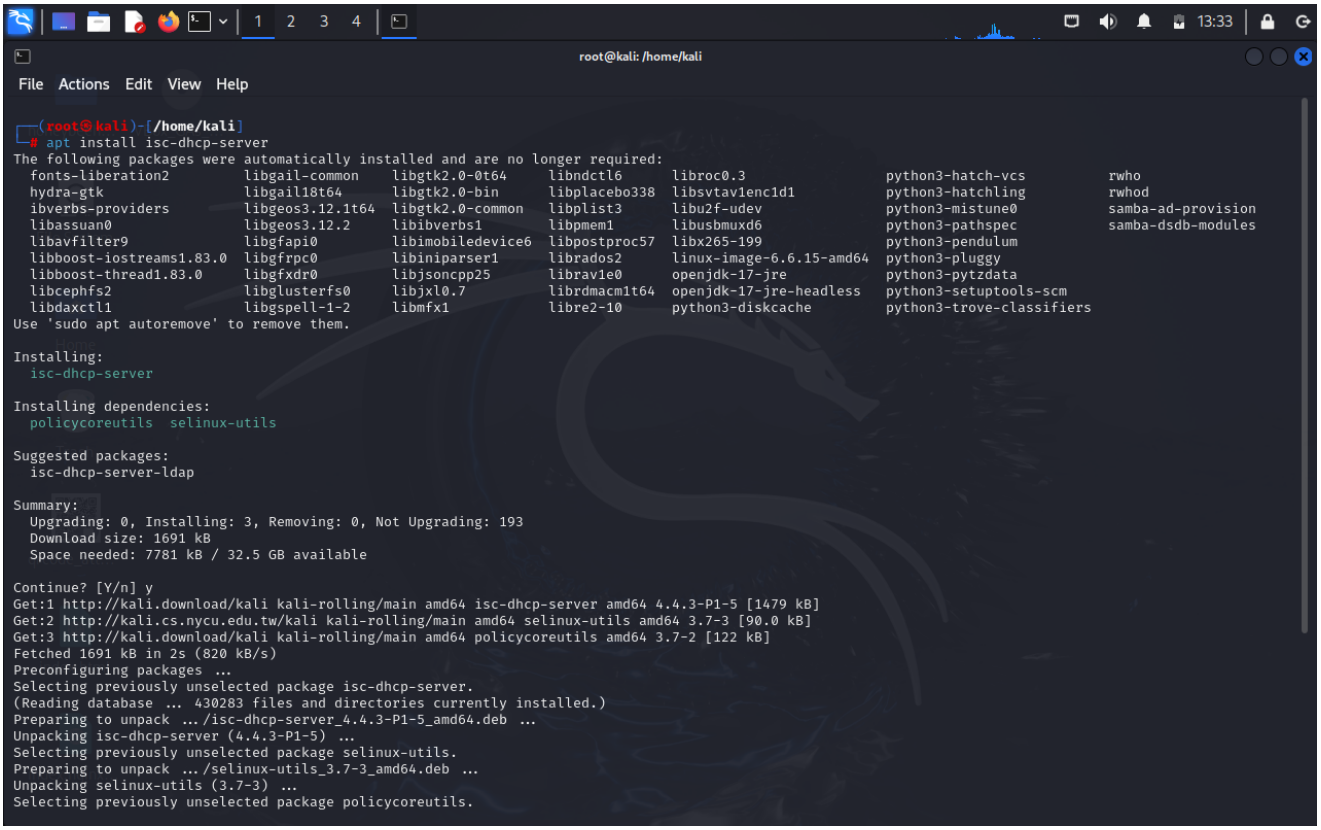
My Ubuntu VM started to be so buggy to the point I couldn't use it anymore. So I switched to Kali.

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.

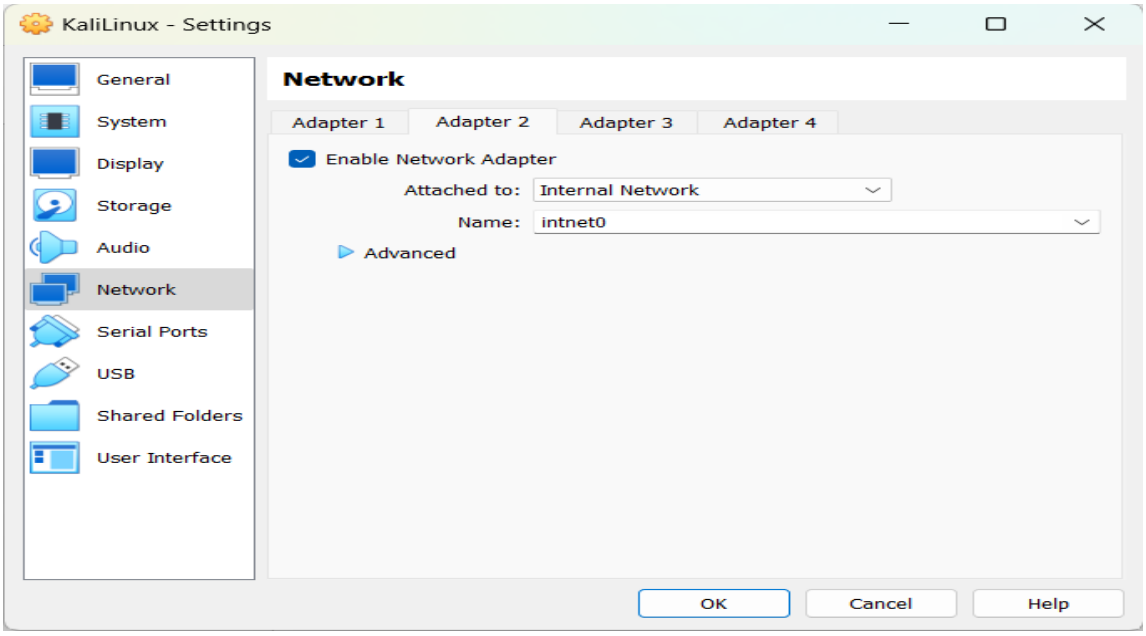
First login as root by giving the command sudo su and enter the password.



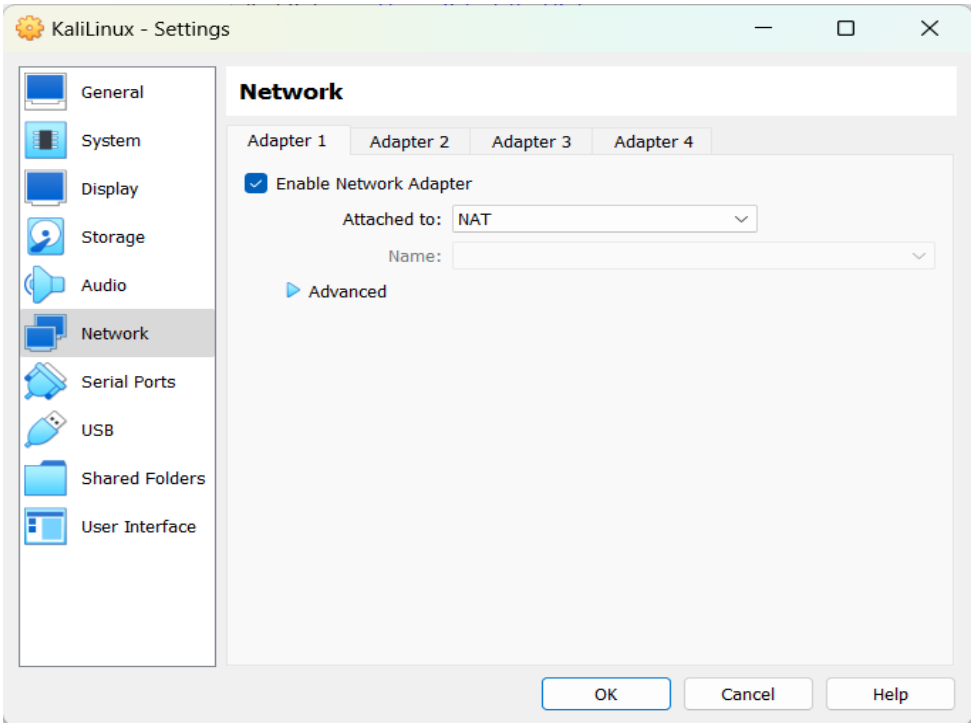
To install DHCP server open Kali terminal and give the command apt install isc-dhcp-server.



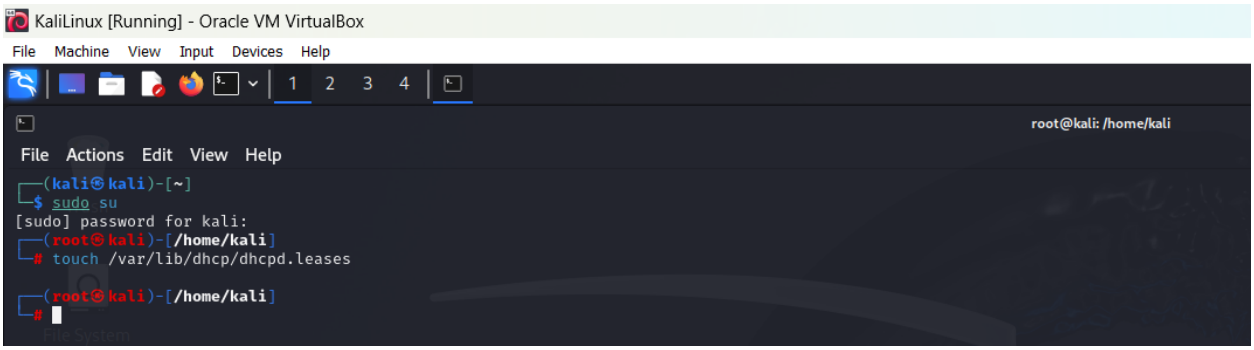
After installation go to setting of Kali VM and select network. Then press adopter 2 tab and tick enable network adopter and change “attached to:” option to internal network. And I have changed the name to intnet0 for easier identification.



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

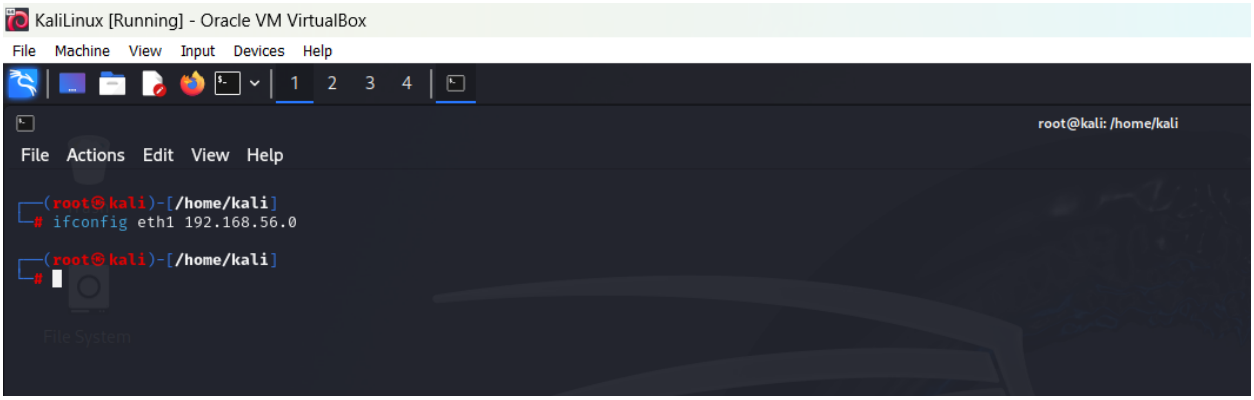


Then type dhcpd you can initiate the DHCP server and test the server configuration.

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

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:ca:3b:65  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

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:0d:00:1b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 284  bytes 47219 (46.1 KiB)
        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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(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.

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.

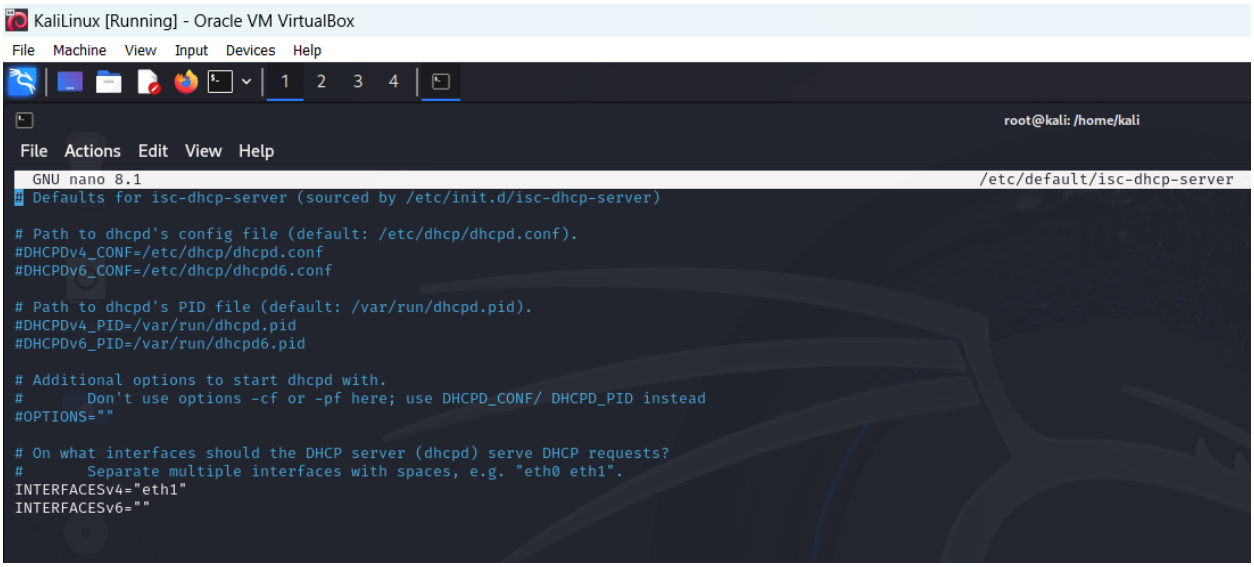
range 192.168.56.10 192.168.56.100 – This is the range that the DHCP can assign clients to

option routers 192.168.56.1 – Defines the default gateway

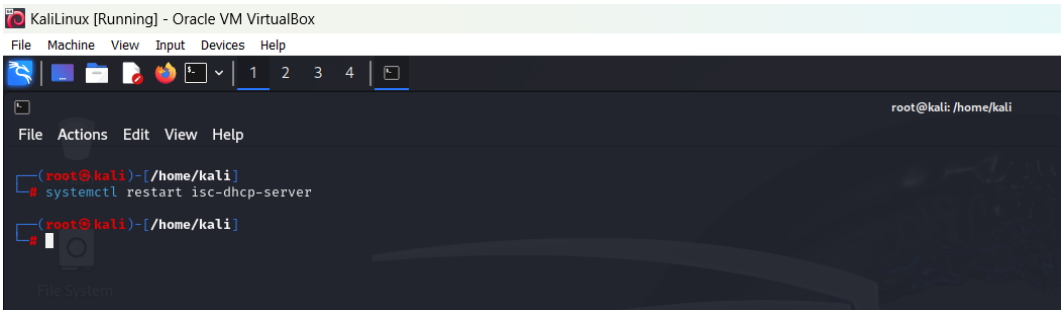
option domain-name-servers 192.168.1.1 192.168.1.2 – DNS servers clients should use

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

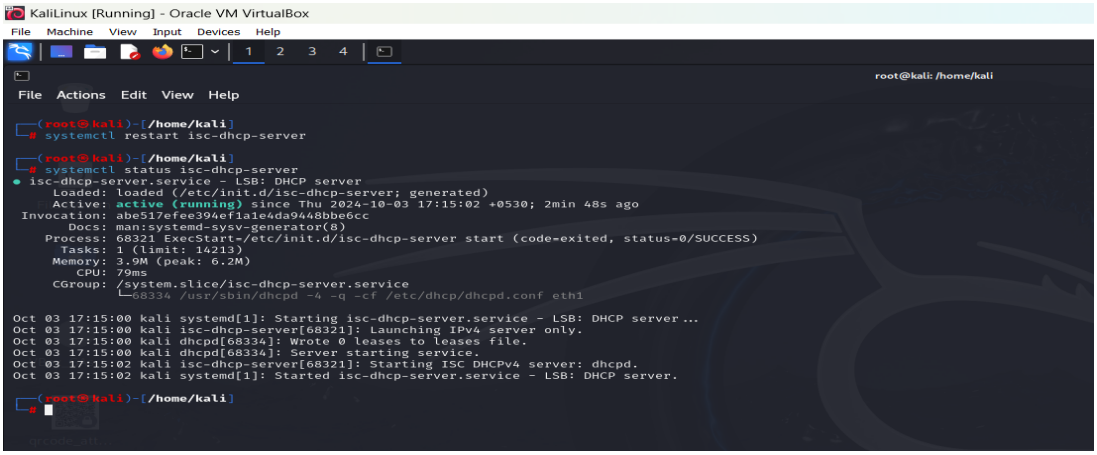
Go to /etc/default/isc-dhcp-server and change INTERFACESv4 to eth1.

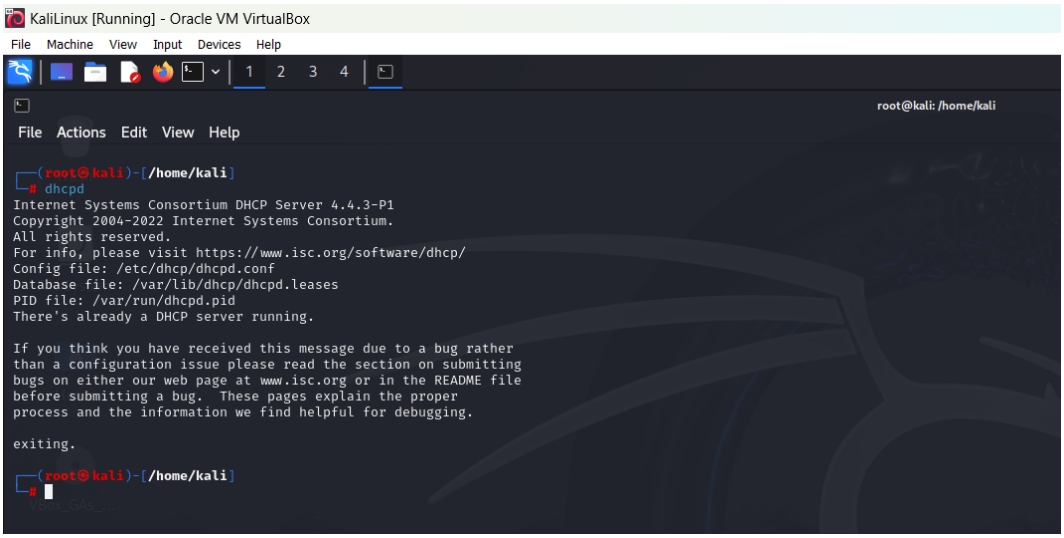


Then use the command systemctl restart isc-dhcp-server to restart the server.

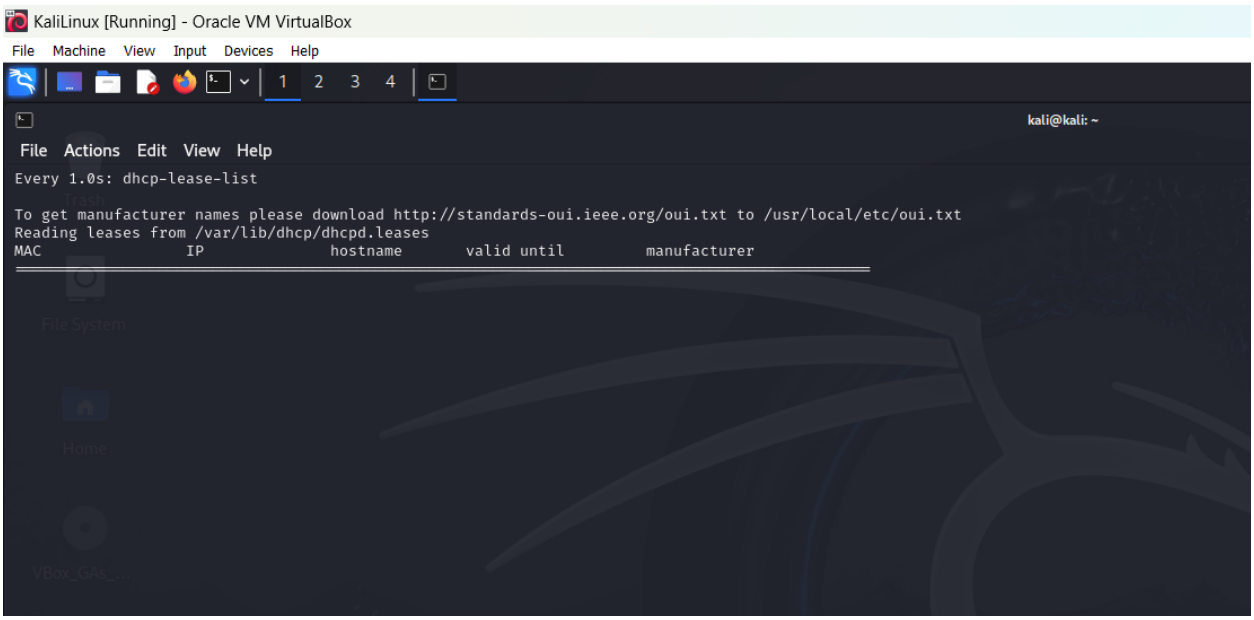


To check the status of the server type systemctl status isc-dhcp-server and dhcpd





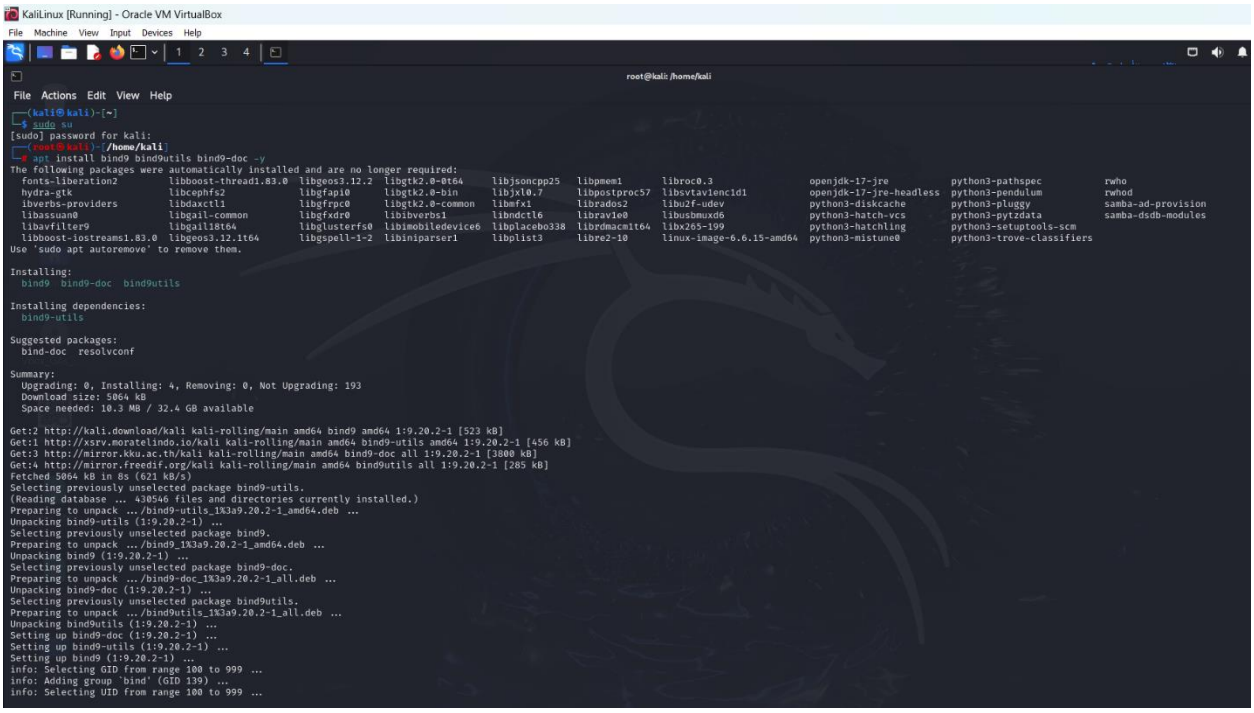
Use the command watch -n 1 dhcp-lease-list to view how devices get assigned IP addresses.



2.2 DNS (Domain Name System)

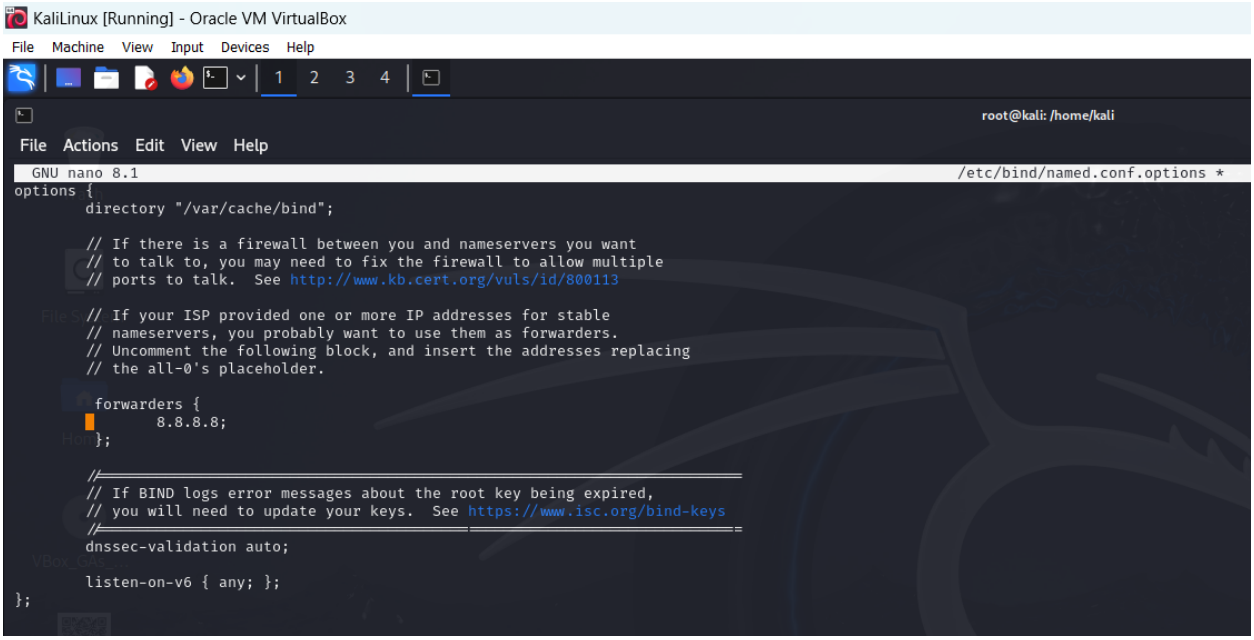
DNS is a very important component of the internet. It translates human-readable domain names into IP addresses which computers use to communicate with each other.

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

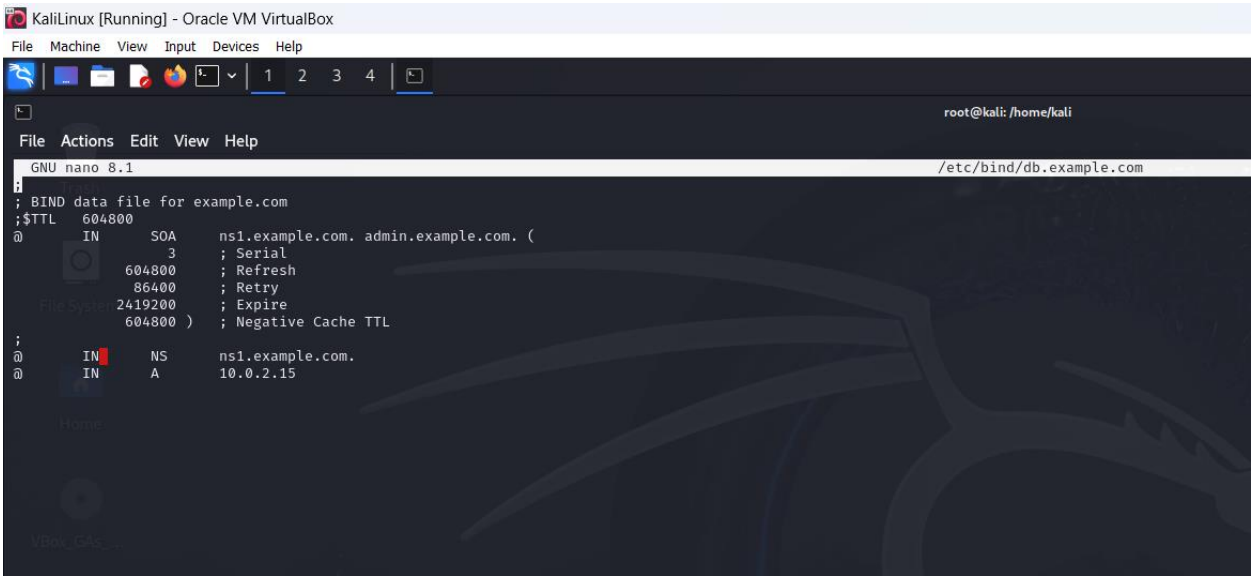


Then we need to install net tools. For that we'll use the command apt install net-tools

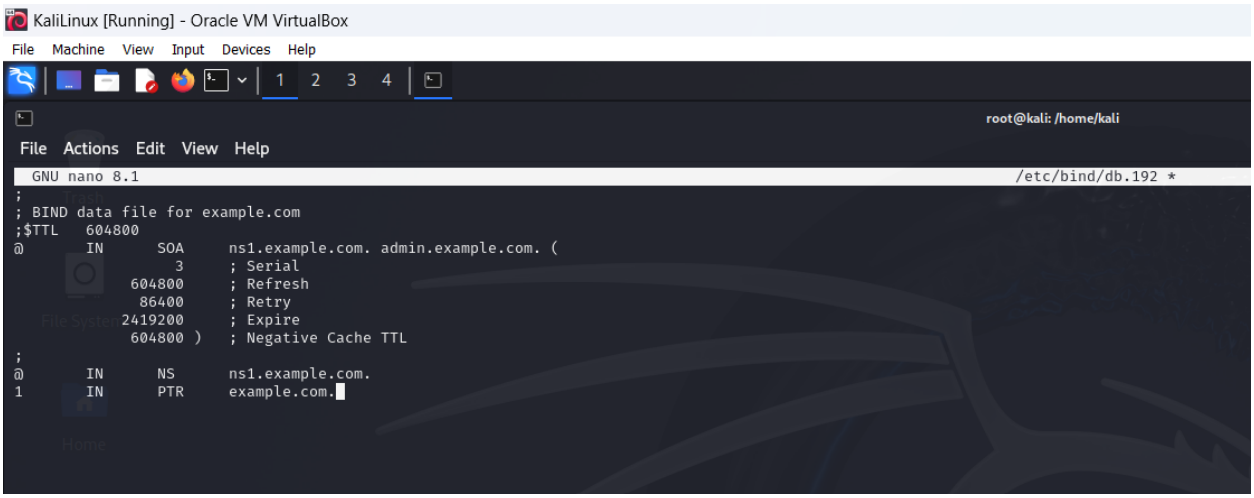
Next we'll use the command nano /etc/bind/named.conf.options to edit the file named.conf.options. Uncomment the forwarders and change it to 8.8.8.8(google DNS). Then save the changes made.



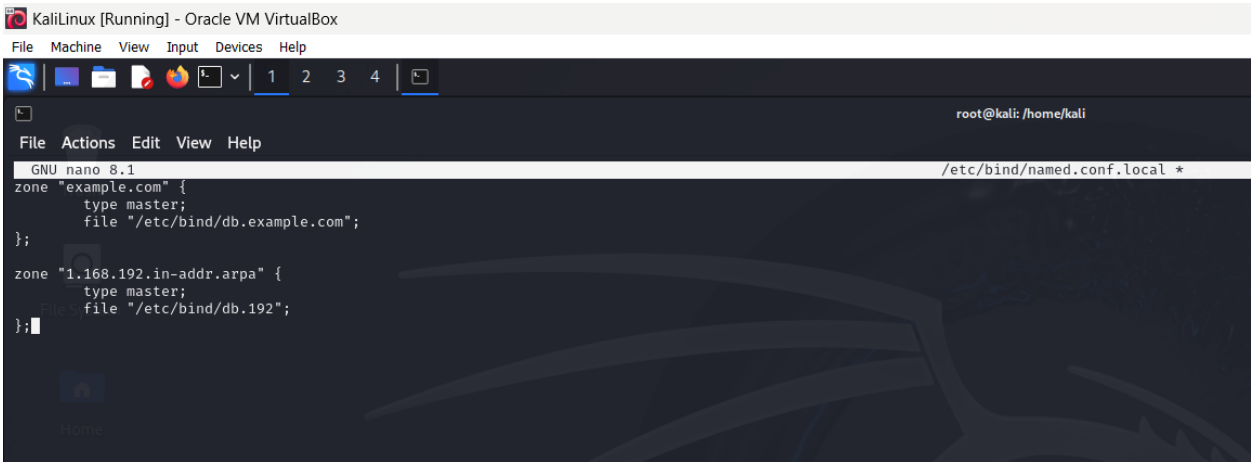
Next we'll use the command nano /etc/bind/db.example.com to edit the file db.example.com. Add the below information(I have added my current IP address below) and then save the changes made.



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.



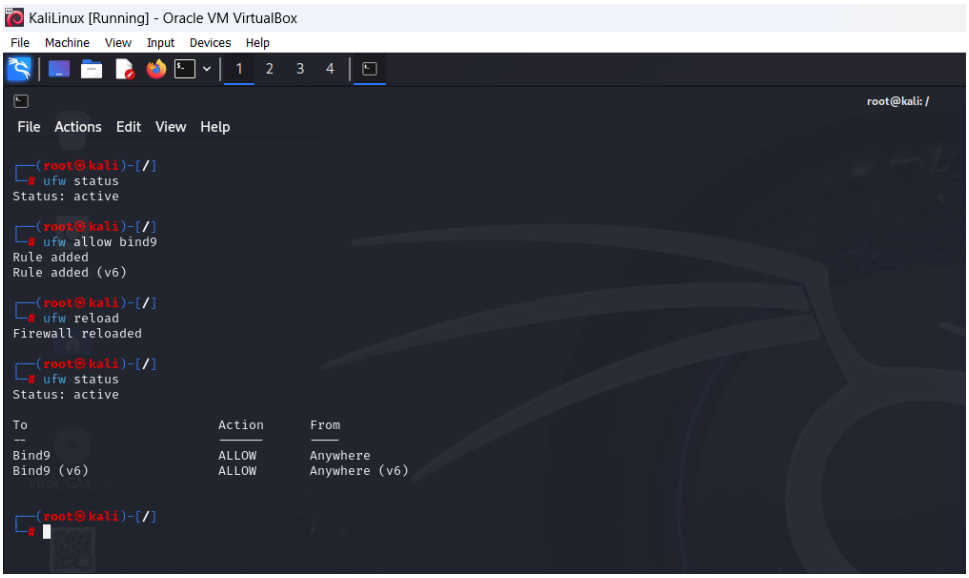
Next we'll use the command nano /etc/bind/named.conf.local to edit the file named.conf.local. Add the below information and then save the changes made.



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: cdc1442583a547db8e11e9670dda11cd
       Docs: man:named(8)
   Main PID: 60001 (named)
     Status: "running"
      Tasks: 26 (limit: 14213)
     Memory: 46M (peak: 47.1M)
        CPU: 121ms
     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::c#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.



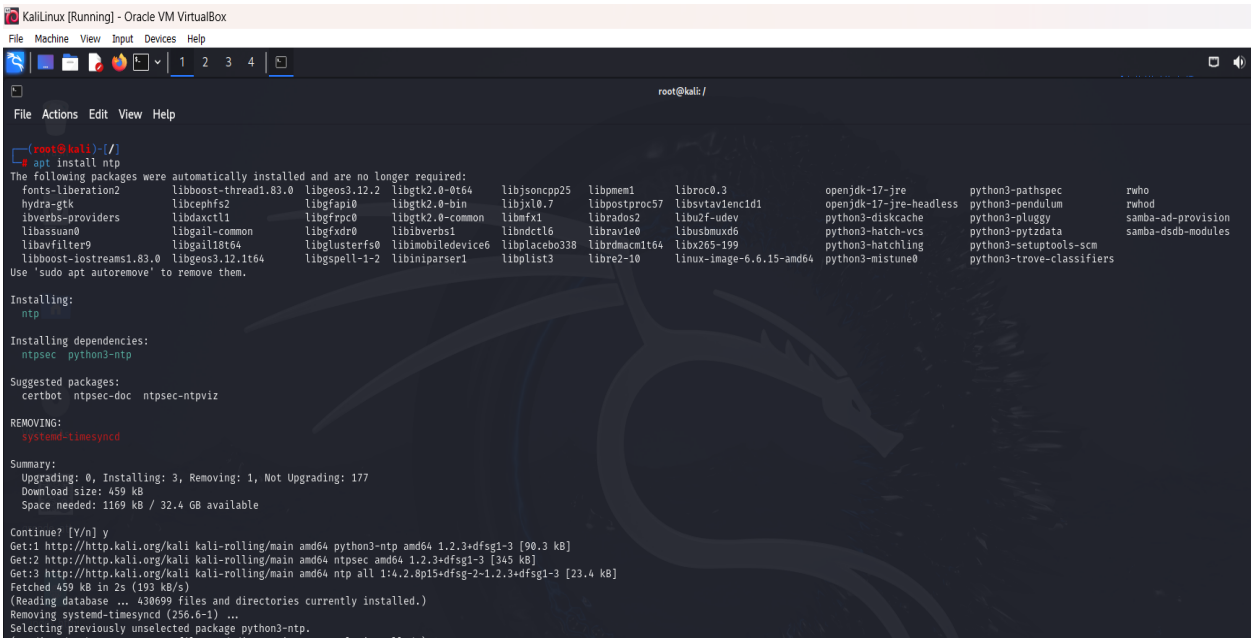
Then go to windows OS and open command prompt. In the command prompt type ping www.example.com. If we get a response that means the DNS is up and running.

```
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>
```

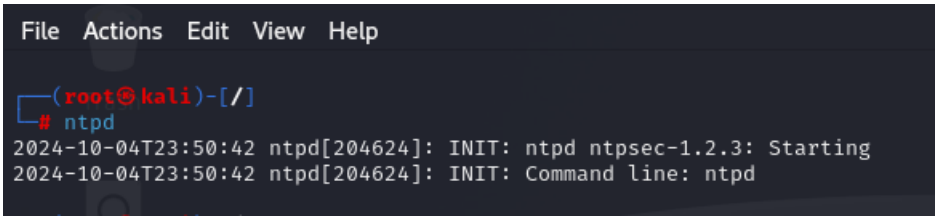
2.3 NTP (Network Time Protocol)

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.

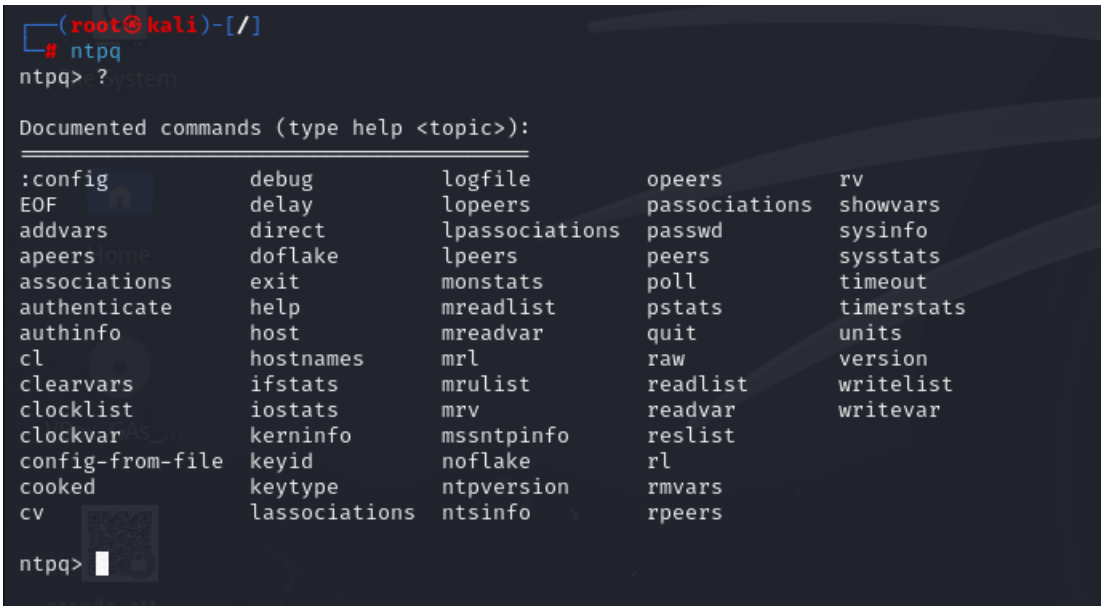
In order to install NTP use the command apt install ntp.



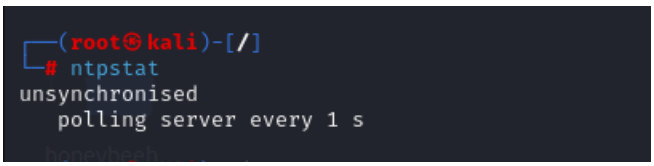
Startup the NTP service with ntpd command.



Type the command ntpq to test the server.



The command ntpstat will display the synchronization status.



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-liberation2         libboost-thread1.83.0  libgeos3.12.2  libgtk2.0-0t64     libjsoncpp25   libpmem1       libroc0.3               openjdk-17-jre          python3-pathspec          rwho
  hydra-gtk                 libcephfs2             libgfapi0      libgtk2.0-bin      libjxl0.7      libpostproc57  libsvtav1enc1d1         openjdk-17-jre-headless python3-pendulum          rwhod
  ibverbs-providers         libdaxctl1             libgfrpc0      libgtk2.0-common   libmfx1        librados2      libu2f-udev             python3-diskcache       python3-pluggy            samba-ad-provision
  libassuan0                libgail-common         libgfxdr0      libibverbs1        libndctl6      libravle0      libusbmuxd6             python3-hatch-vcs       python3-pytzdata          samba-dsdb-modules
  libavfilter9              libgail18t64           libglusterfs0  libimobiledevice6  libplacebo338  librdmacm1t64  libx265-199             python3-hatchling       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 'sudo apt autoremove' to remove them.

Installing:
  systemd-timesyncd

REMOVING:
  ntpsec

Summary:
  Upgrading: 0, Installing: 1, Removing: 1, Not Upgrading: 177
  Download size: 85.4 kB
  Freed 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, source configuration file or drop-ins of ntpsec-rotate-stats.timer changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of ntpsec-systemd-netif.path changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of 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) ...
```

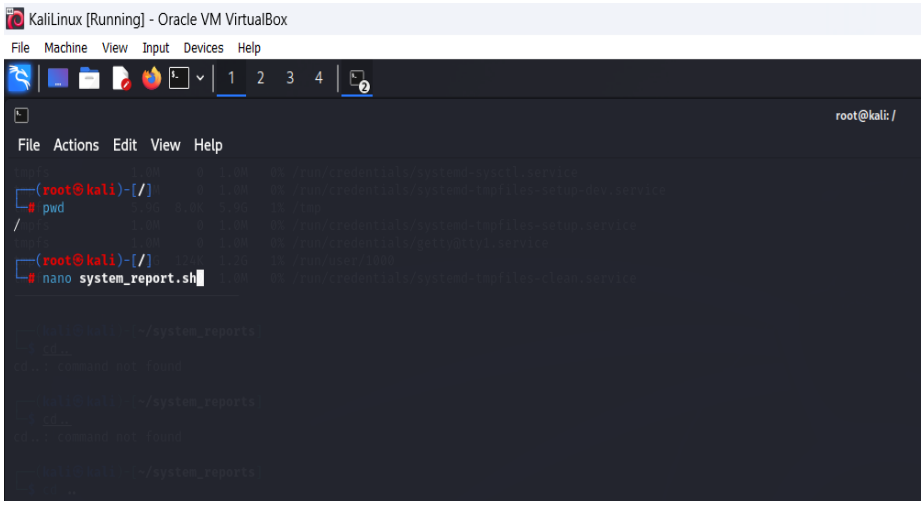
After that run the command timedatectl status to check the status of the NTP.

```
┌──(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
              NTP service: active
          RTC in local TZ: no

┌──(root㉿kali)-[/]
└─#
```

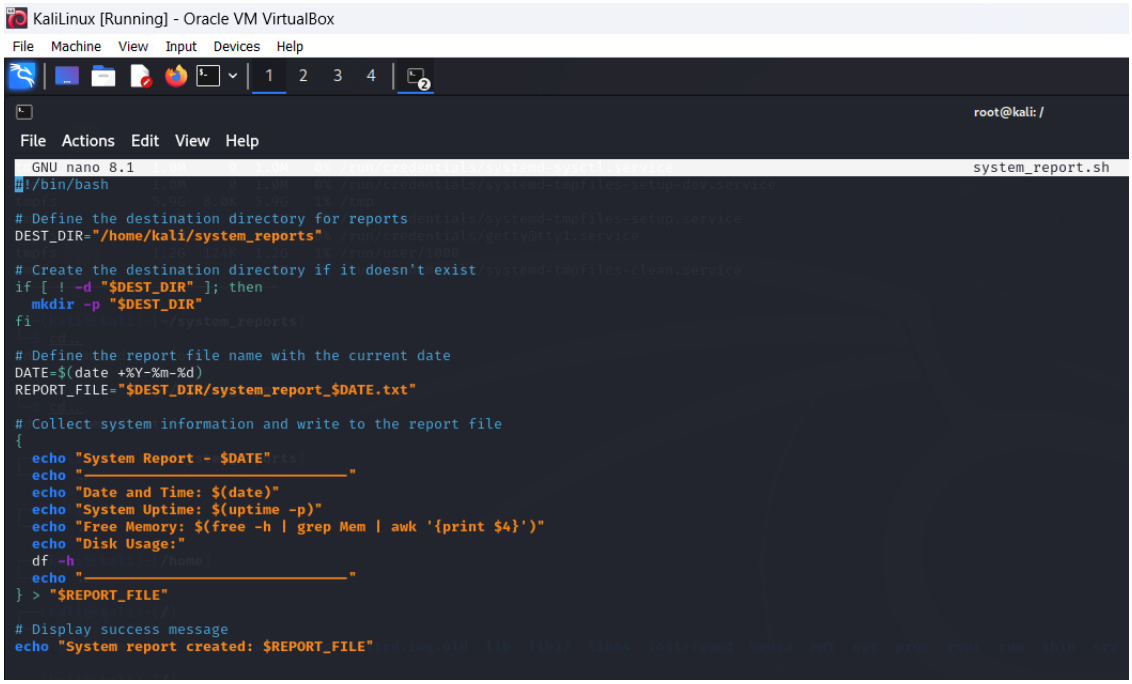
3 Shell Scripting and Security

3.1 Shell Scripting

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



Then write the below script inside the system_report.sh.



```
#!/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:

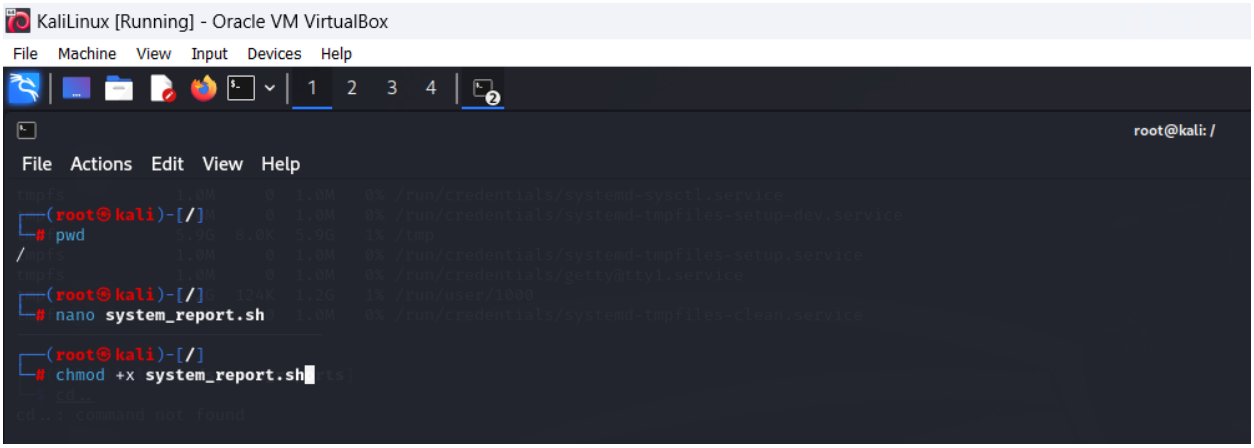
Date and Time: Using the $DATE command.

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

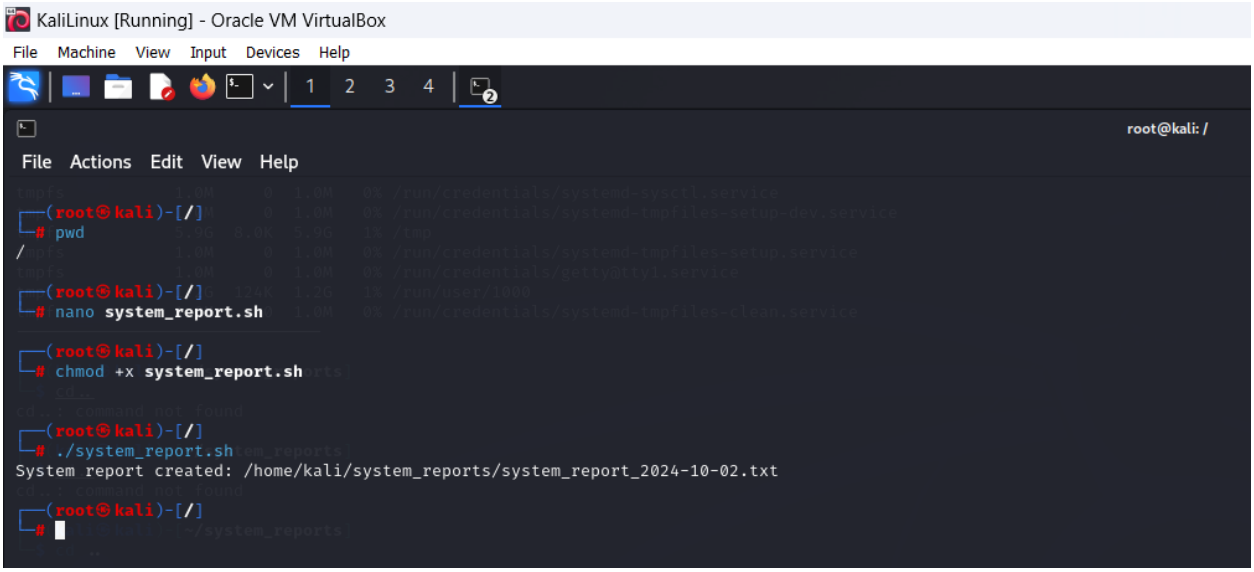
Free Memory: free -h will show the amount of free memory in human-readable format.

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

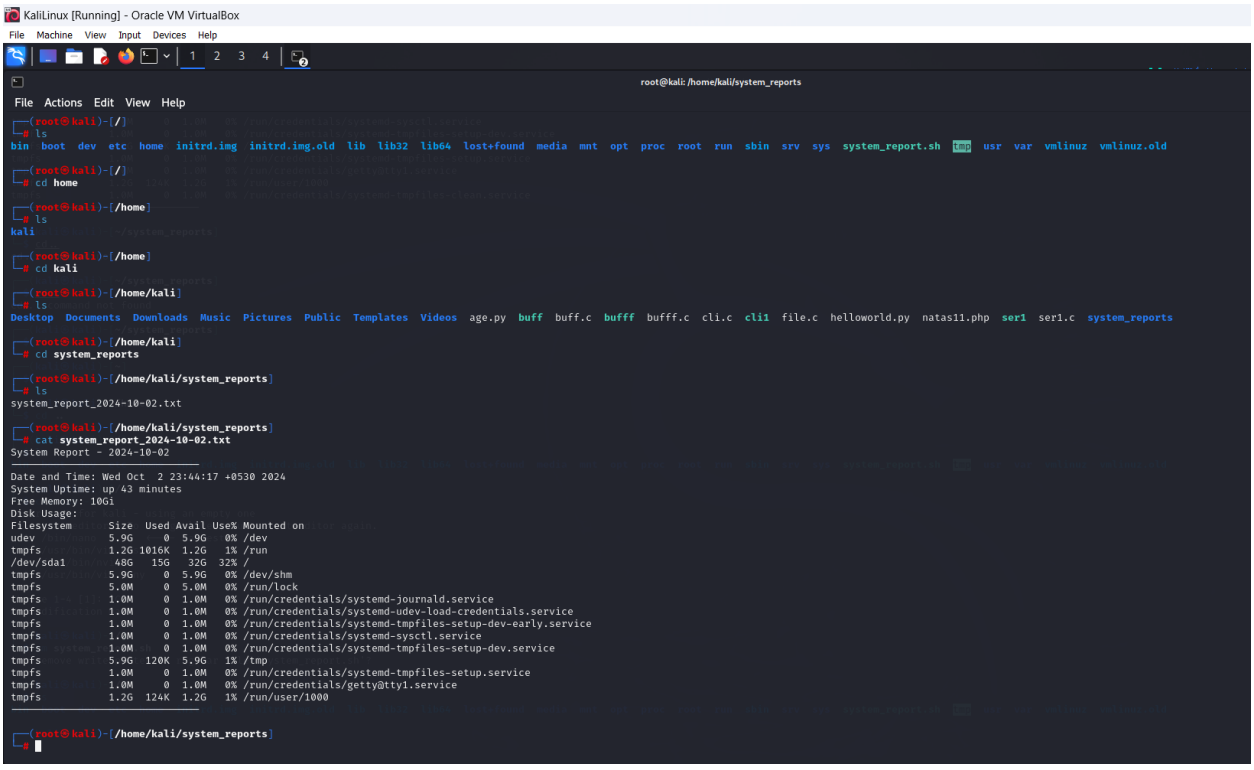
After writing the script we need to give executable permissions.



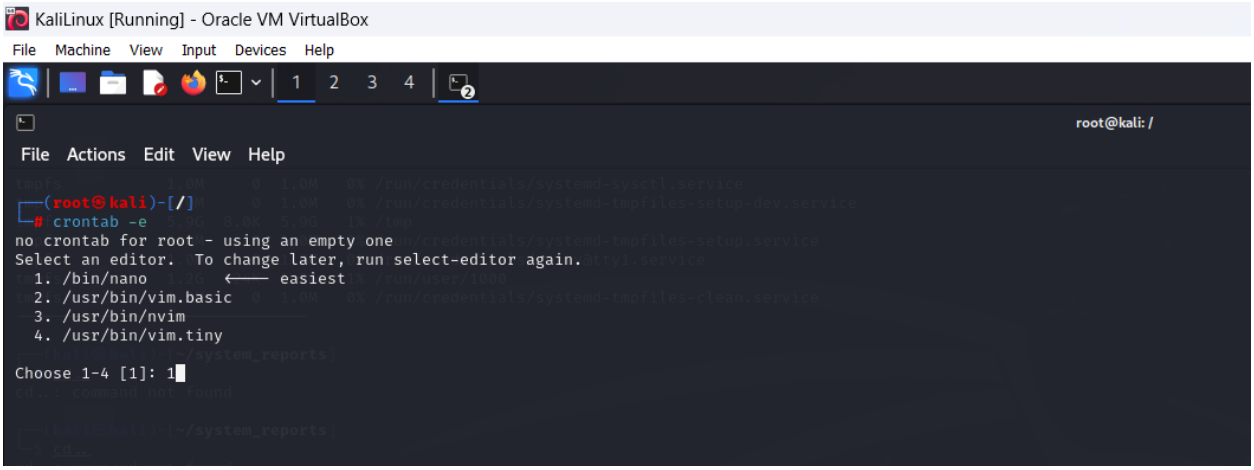
After that lets run the script file.



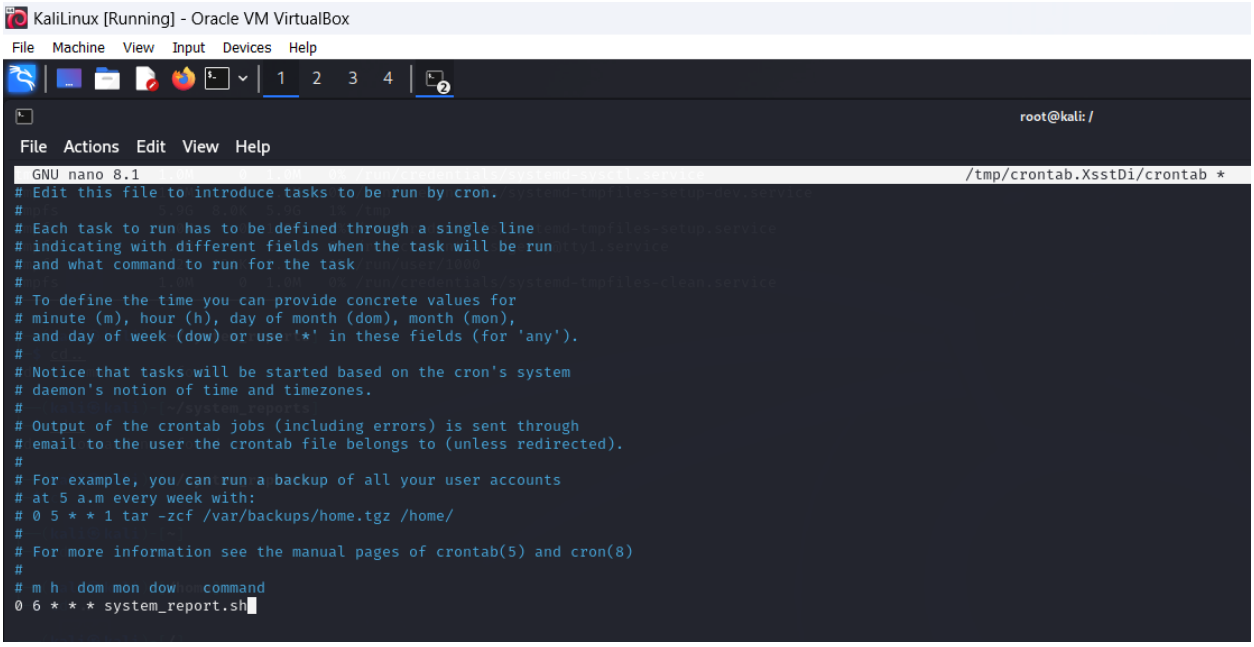
Then we will see the content of the resulted file at /home/kali/system_reports/.



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

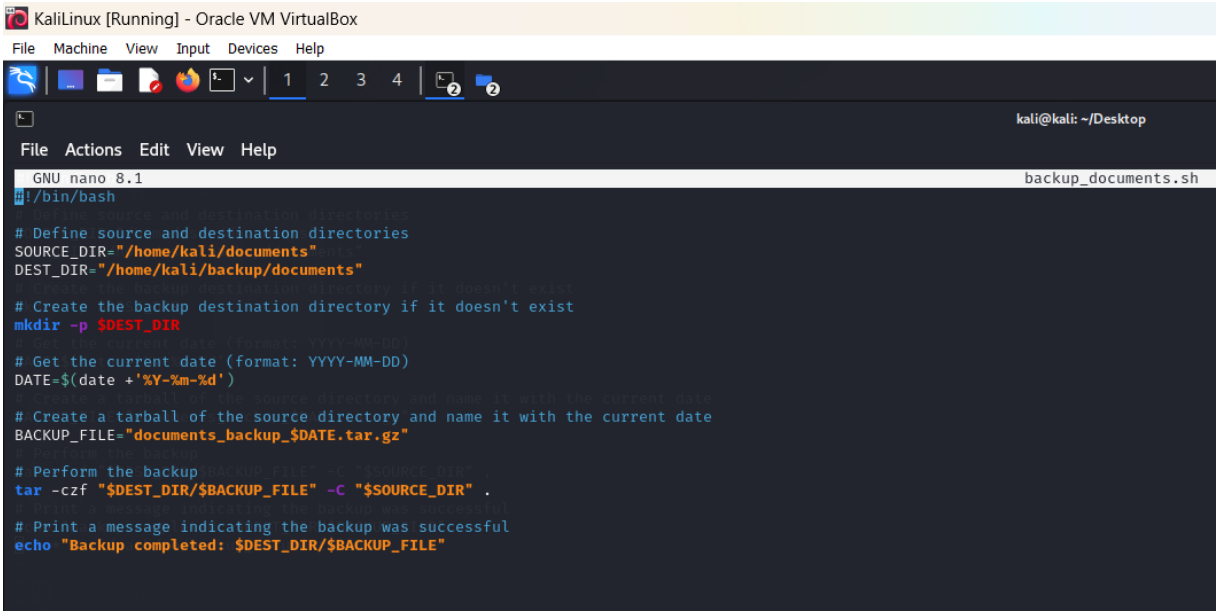


Inside the crontab write following code and save.



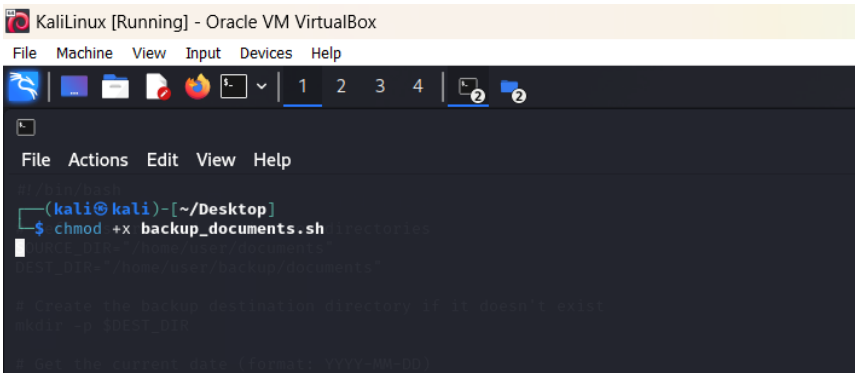
This tells cron to run the command at 6:00 AM every day

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.

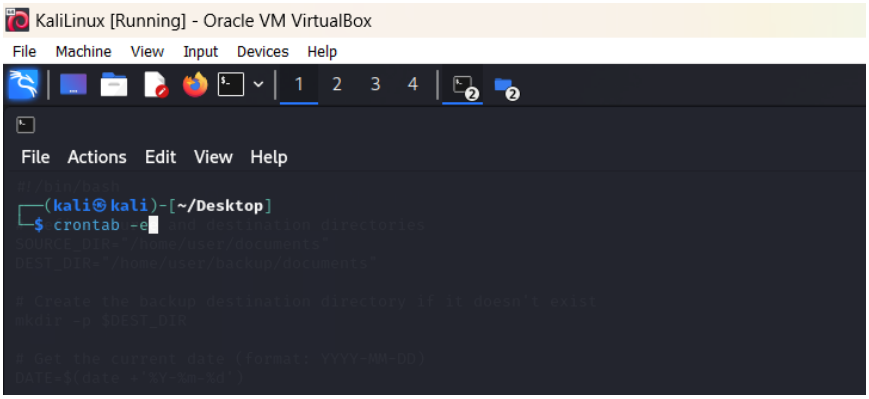



```
#!/bin/bash

# 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"
```

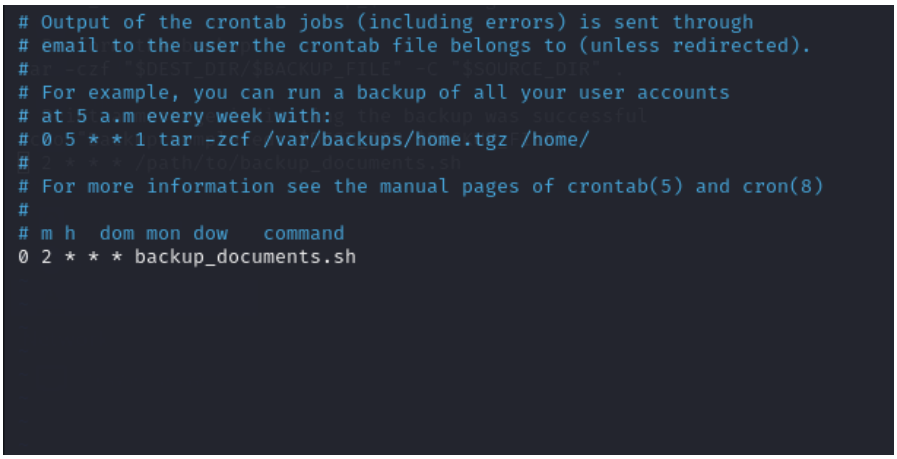
Then we'll make the script executable by using the command chmod +x backup_documents.sh.



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

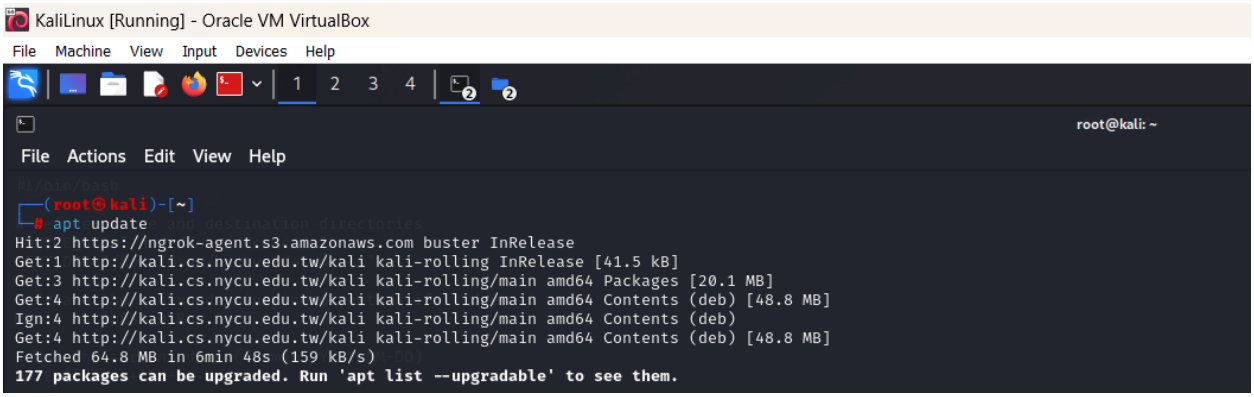


Next add a cron job to run the script daily. For that type below code inside the crontab.

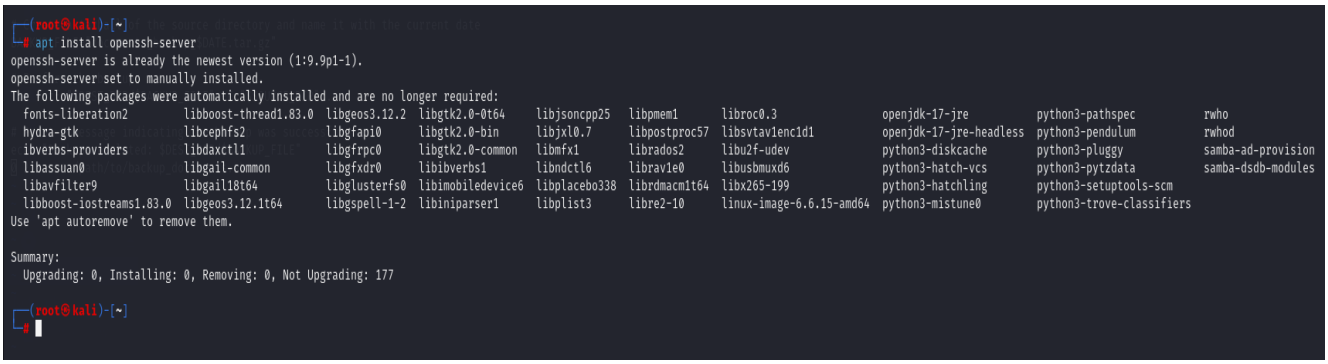


3.2 SSH (Secure Shell)

First run the apt update command and download packages.



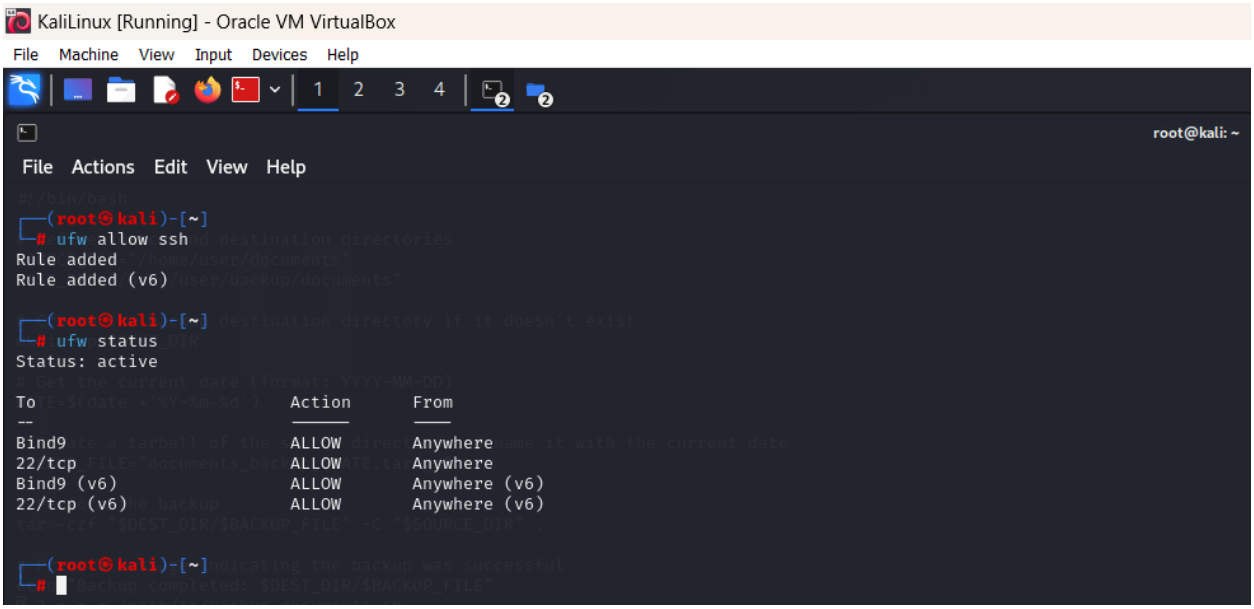
Then we need to install open ssh server. To do that run the command apt install openssh-server.



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.
```

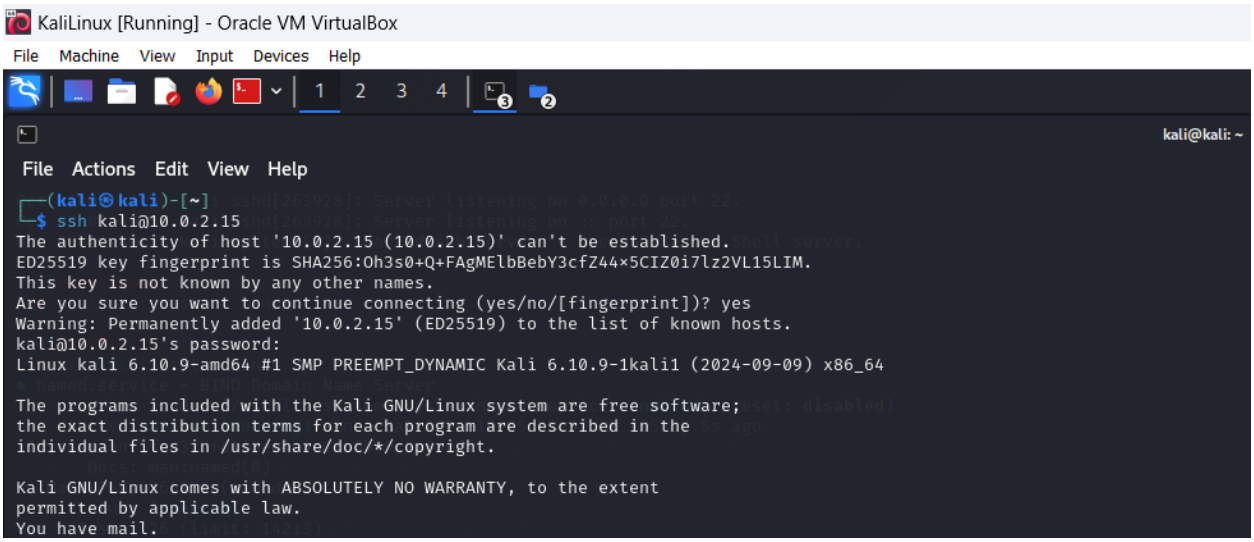
To allow ssh through the firewall with which it can listen for incoming requests. Run below commands.



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.

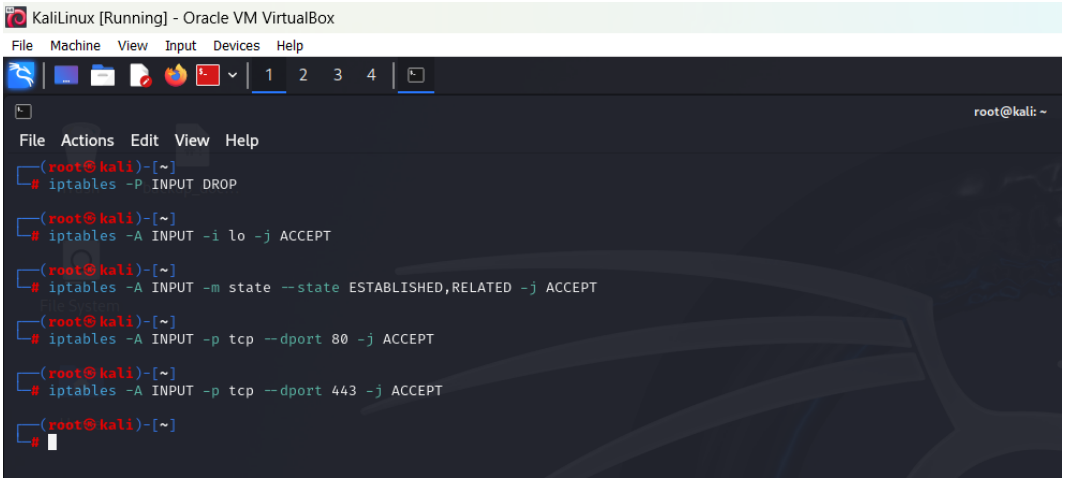
```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe42:3e52  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:3e:52  txqueuelen 1000  (Ethernet)
        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.



3.3 IP tables and ACLs

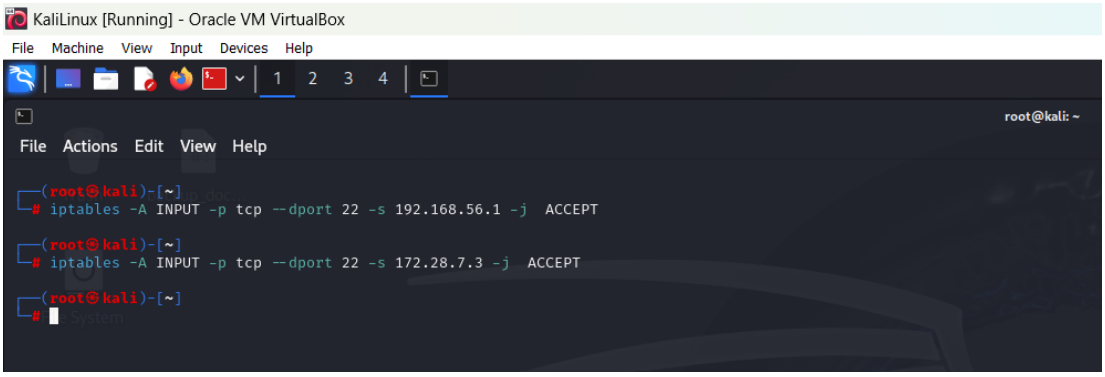
3.3.1 Web Server Security



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.

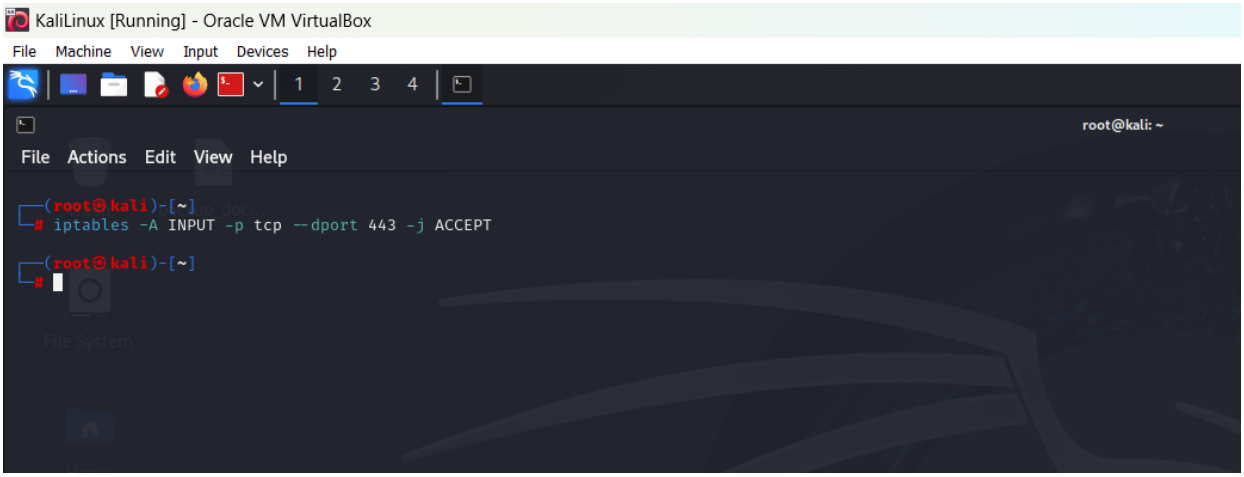
3.3.2 Remote Administration Access

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.



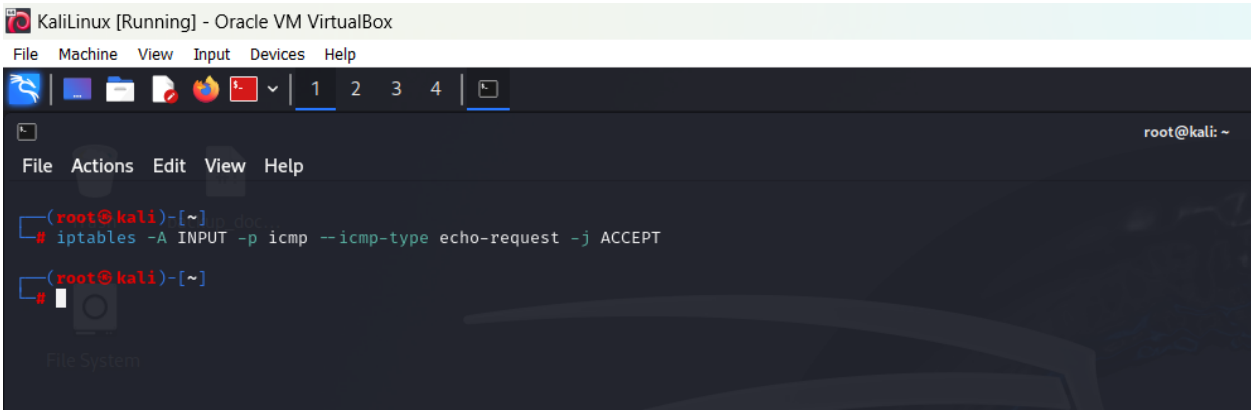
3.3.3 Allow Specific Applications

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



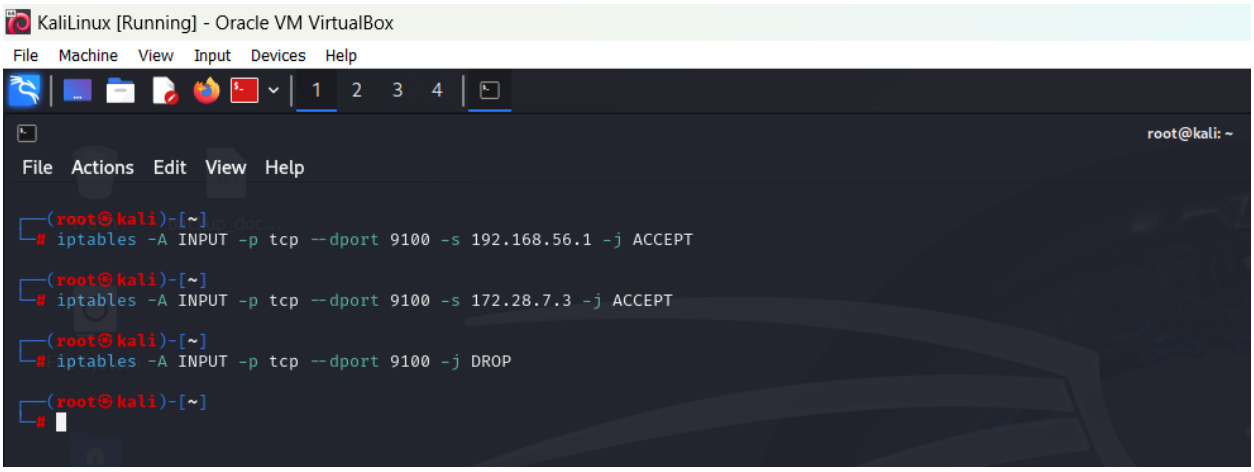
3.3.4 Allow Pings

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.



3.3.5 Printer Server Access

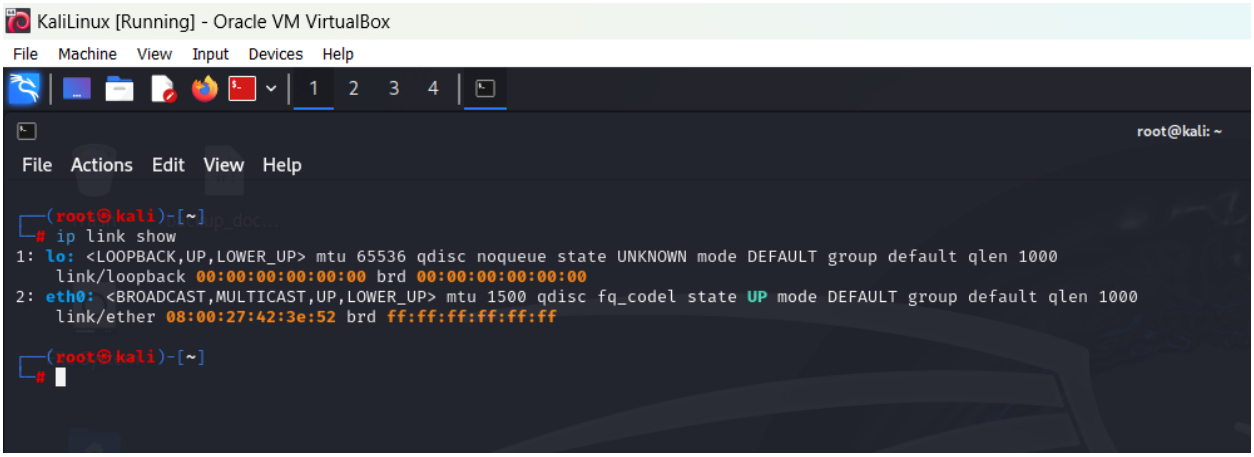
To allow traffic to the printer server only from specific IP addresses within our local network use iptables -A INPUT -p tcp --dport 9100 -s <trusted IP> -j ACCEPT command. To block external access to printer server use the command iptables -A INPUT -p tcp --dport 9100 -j DROP.



4 Best practices

4.1 Disable Unused Network Interfaces

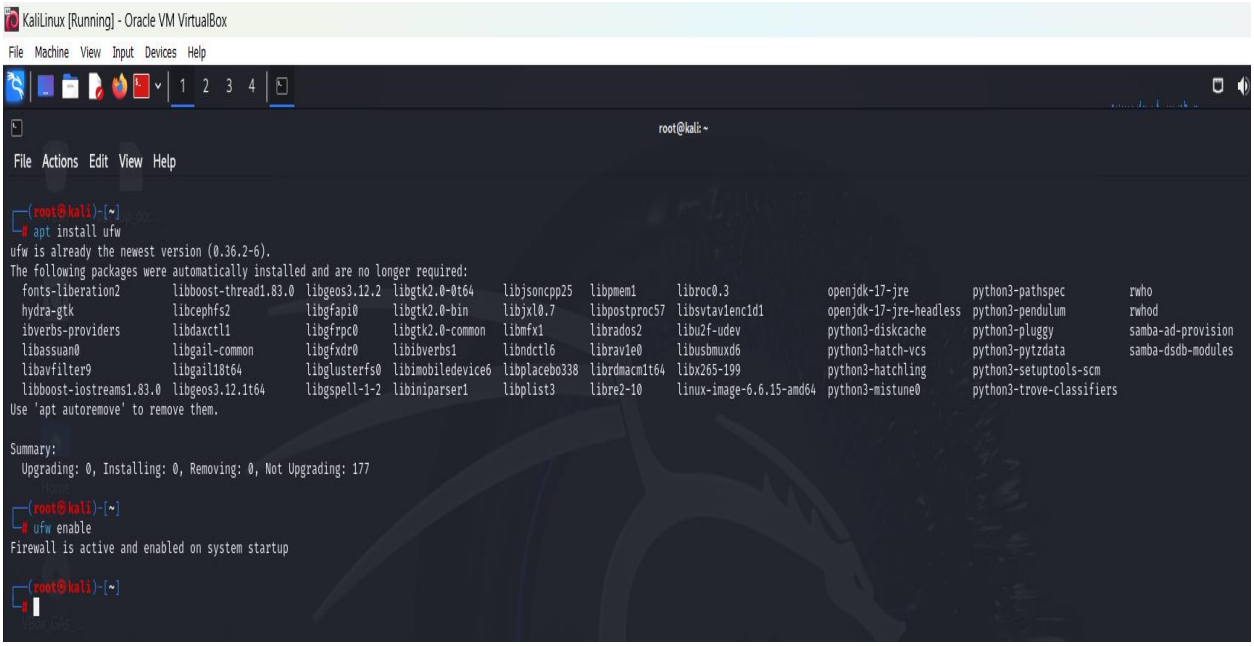
Your Linux machine has multiple network interfaces. If they are not being used it's a good security practice to disable or shut down any unused network interfaces. These interfaces can act as attack surfaces if not properly secured. Use the ip link show command to list all interfaces. If there are unused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



4.2 Enable a Firewall

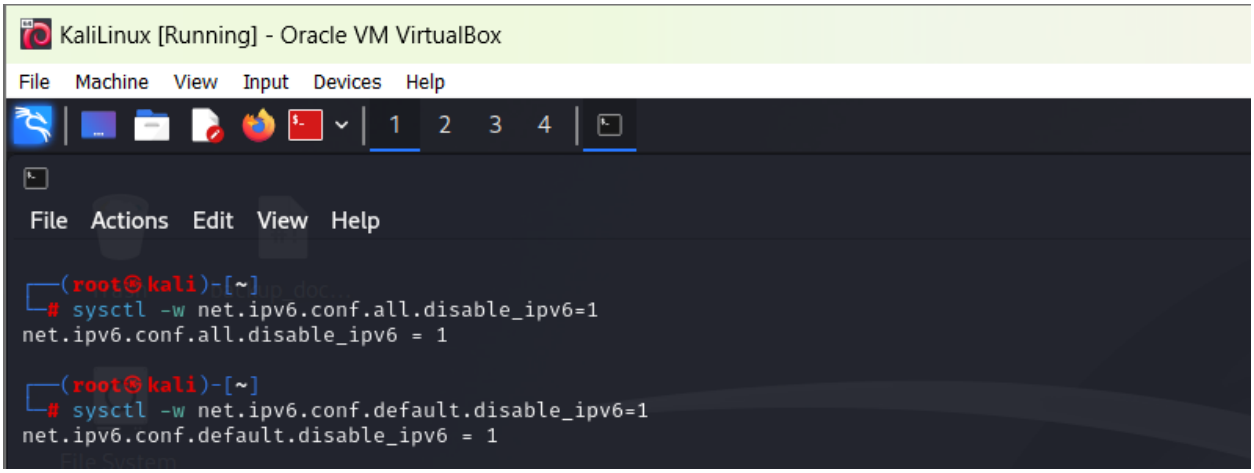
Firewalls help filter and control network traffic based on predefined rules and it will protect our system from unauthorized access and potential attacks.

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



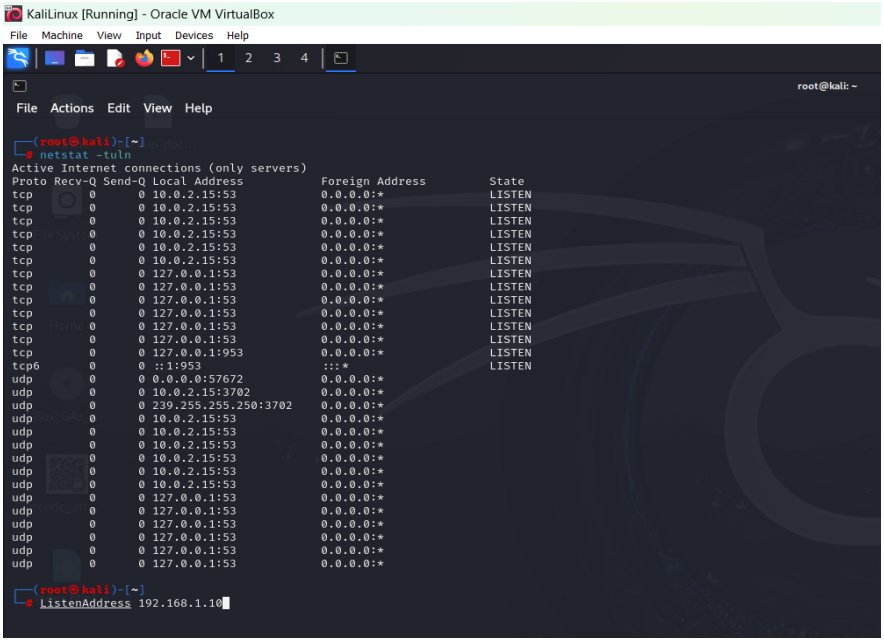
4.3 Disable IPv6 if Not Needed

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.

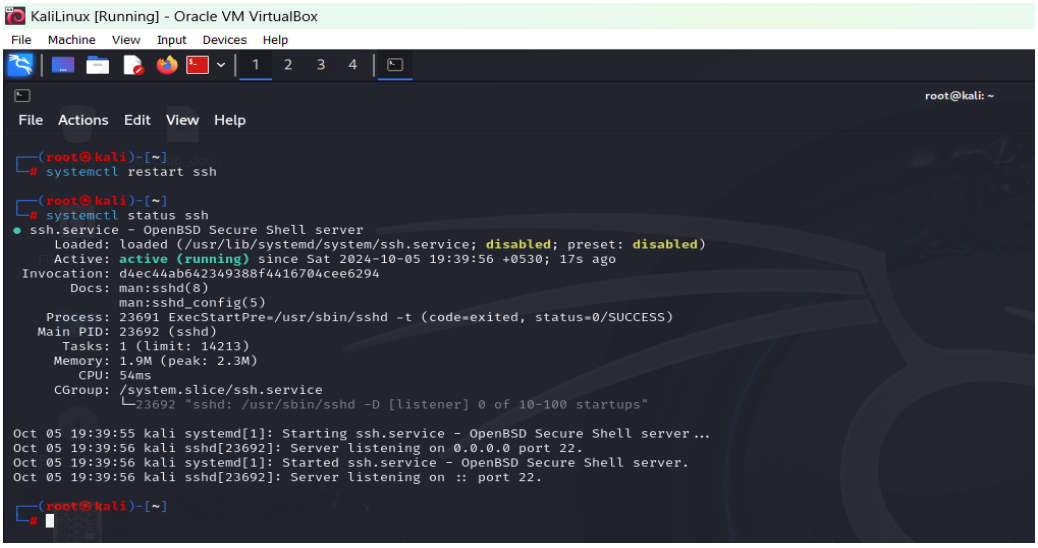


4.4 Limit Network Service Exposure

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.



Restart the service to apply the changes



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.