



**Sri Lanka Institute of Information Technology
IE2012: System and Network Programming
Year 2 Semester 1**

Assignment

**IT23209534
A.A.I.Nethmika**

Table of Content

1.	Basic Linux Environments.....	3
1.1)	Virtual Machine Setup	3
1.2)	Basic Navigation Commands and functionalities.....	16
1.3)	File manipulation commands.....	17
1.4)	System Information Commands	18
1.5)	User management commands.	19
2.	DHCP, DNS and NTP Services	20
2.1)	DHCP (Dynamic Host Configuration Protocol)	20
2.2)	Installation and configuration	20
2.3)	DNS (Domain Name System).....	26
2.4)	Installation and Configuration	26
2.5)	NTP (Network Time Protocol)	32
2.6)	Installation and Configuration	32
3.	Shell Scripting and Security	35
3.1)	Shell Scripting.....	35
3.2)	SSH (Secure Shell)	46
3.3)	Iptables and ACLs.....	49
4.	Best Practices	53

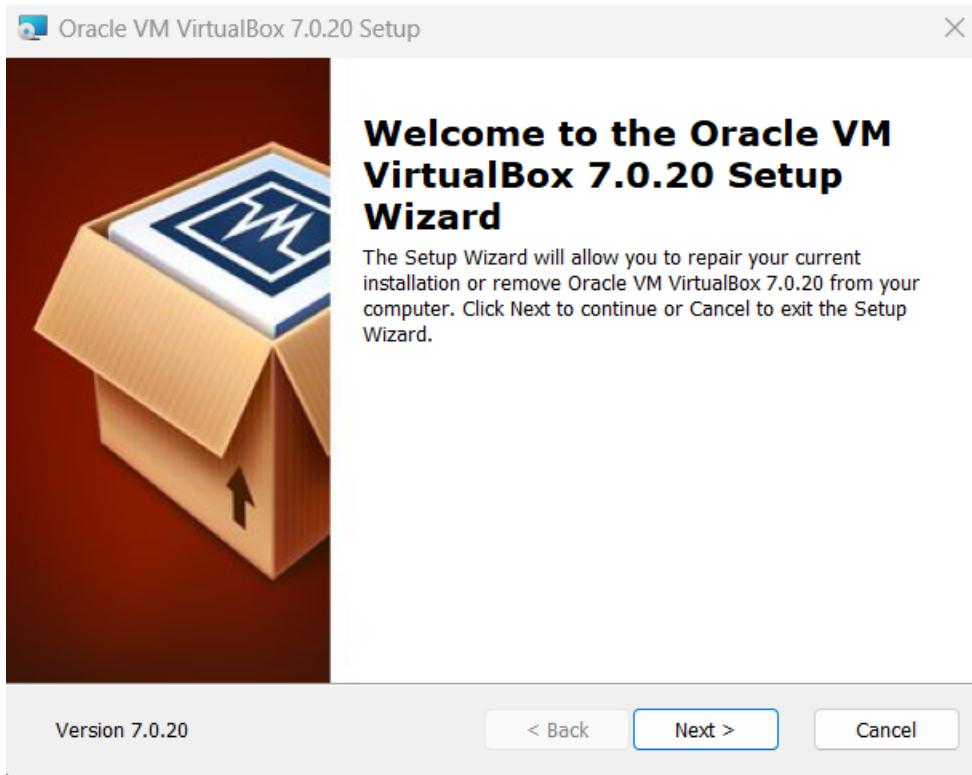
1. Basic Linux Environments

1.1) Virtual Machine Setup

Download Oracle VirtualBox using <https://www.virtualbox.org/wiki/Downloads>.

The screenshot shows the official Oracle VirtualBox download page. At the top, there's a navigation bar with links for Home, Download, Documentation, Community, and a search bar. The main heading is "Download VirtualBox". Below it, a note states: "The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license." A large button labeled "Accept and download" is visible. To the left, there's a section for "VirtualBox Platform Packages" listing various host operating systems. To the right, there's a section for the "VirtualBox Extension Pack" with a detailed description of the PUEL license. Below these sections are links for Change Log, File Checksums, User Guide, VirtualBox SDK, Source Code, and Previous Releases.

After downloading the windows host Oracle VirtualBox, Run the setup.

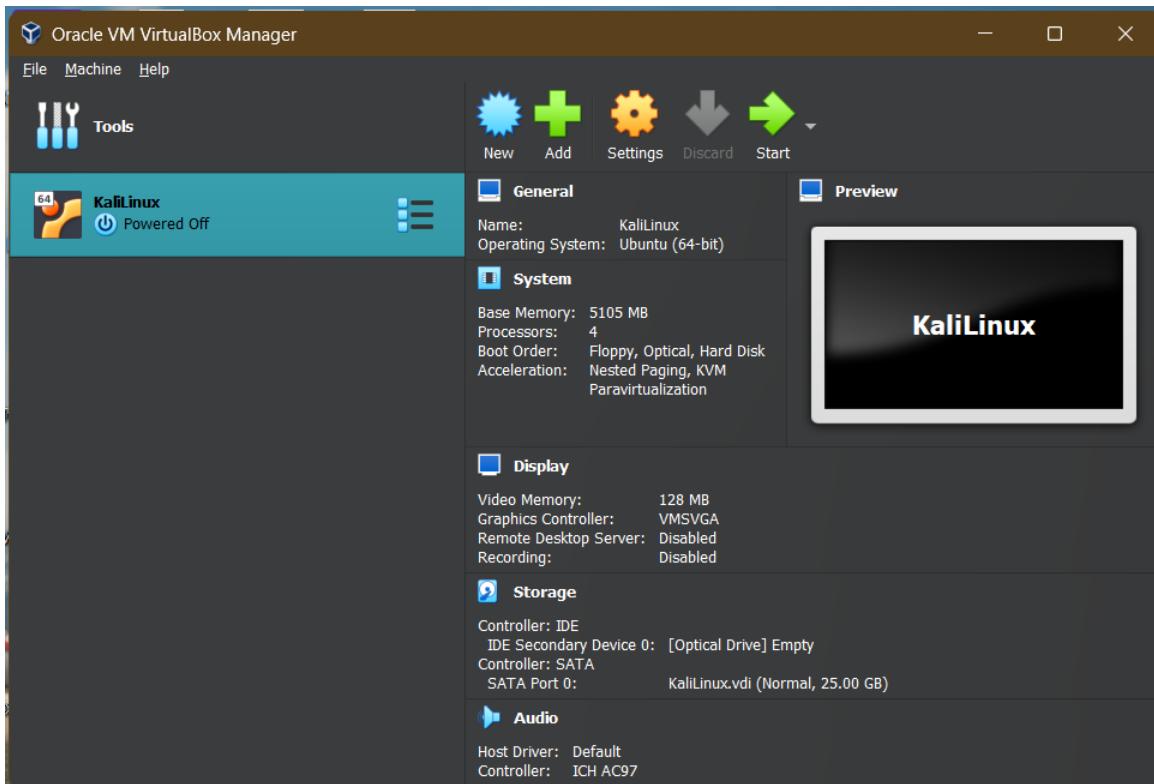


Select the preferred setting and install the VirtualBox. (VirtualBox software has already been installed in my computer)

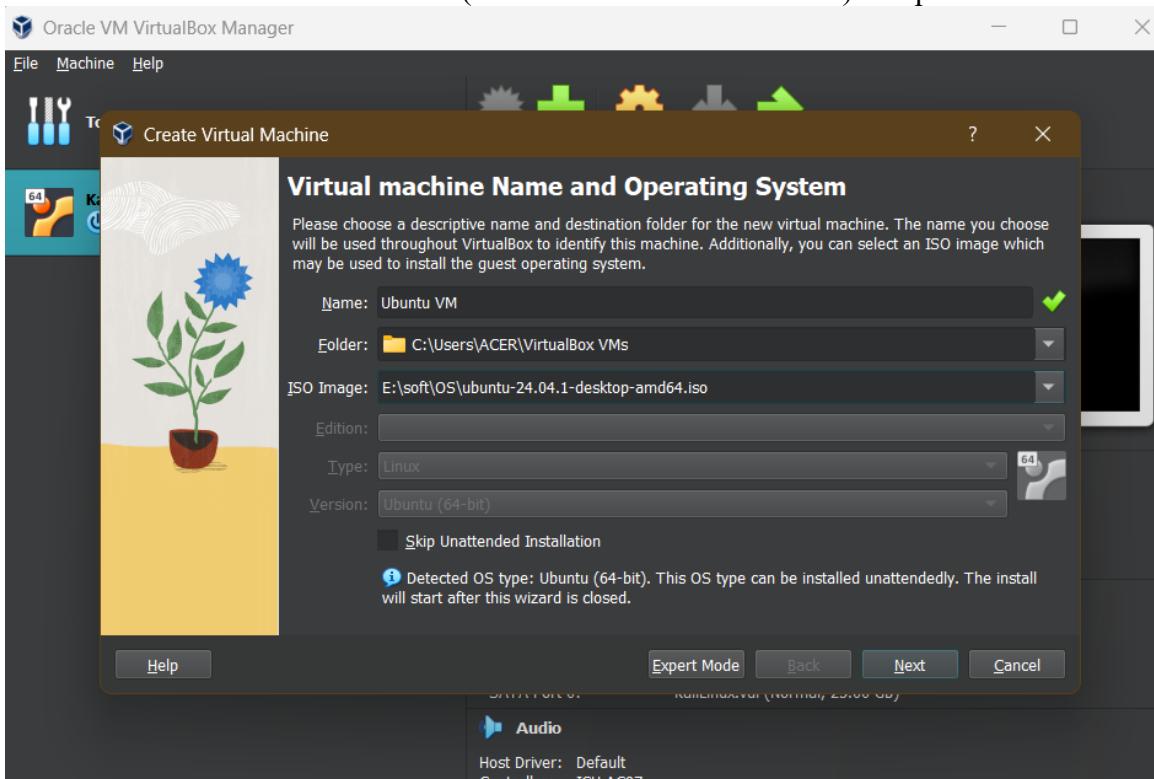
Download Ubuntu from <https://ubuntu.com/download/desktop>.

A screenshot of the Ubuntu 24.04.1 LTS download page. The page has a dark header with tabs for "Downloads", "Desktop", "Server", "Core", and "Cloud". The "Desktop" tab is selected. Below the header, there's a search bar with "Discover Ubuntu Desktop" and "Check out the blog". The main content area features a large image of a red crown icon with the text "Ubuntu 24.04.1 LTS" next to it. To the right, there's a paragraph about the LTS version and a "Download 24.04.1 LTS" button. Below the download button, there's a note about other download options and links to "What's new", "System requirements", and "How to install". A scrollable list of changes includes: "New Desktop installer with support for autoinstall", "New App Center and Firmware Updater applications", "GNOME 46 with support for quarter screen tiling", "Advanced Active Directory Group Policy Object support for Ubuntu Pro users", and "Experimental support for TPM-backed Full Disc Encryption and ZFS encryption". At the bottom, there's a link to the URL "https://ubuntu.com/download/desktop/thank-you?version=24.04.1&architecture=amd64&f...".

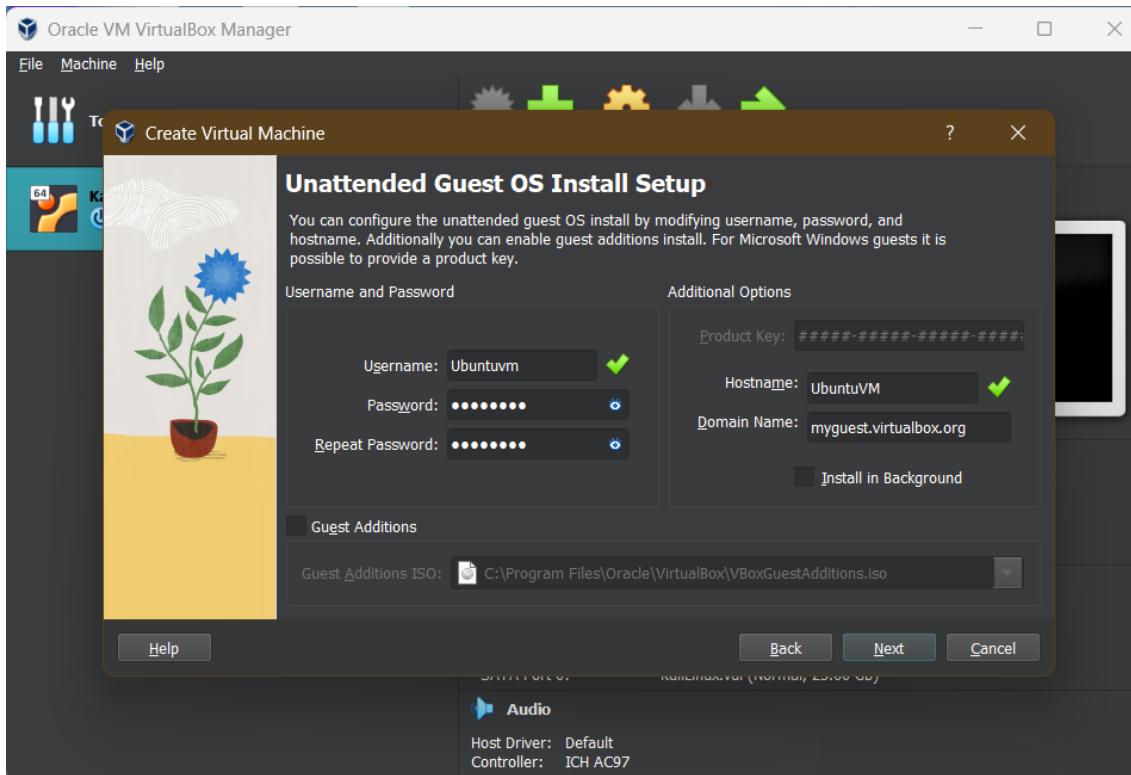
Run VirtualBox. Use new button to add new virtual machine.



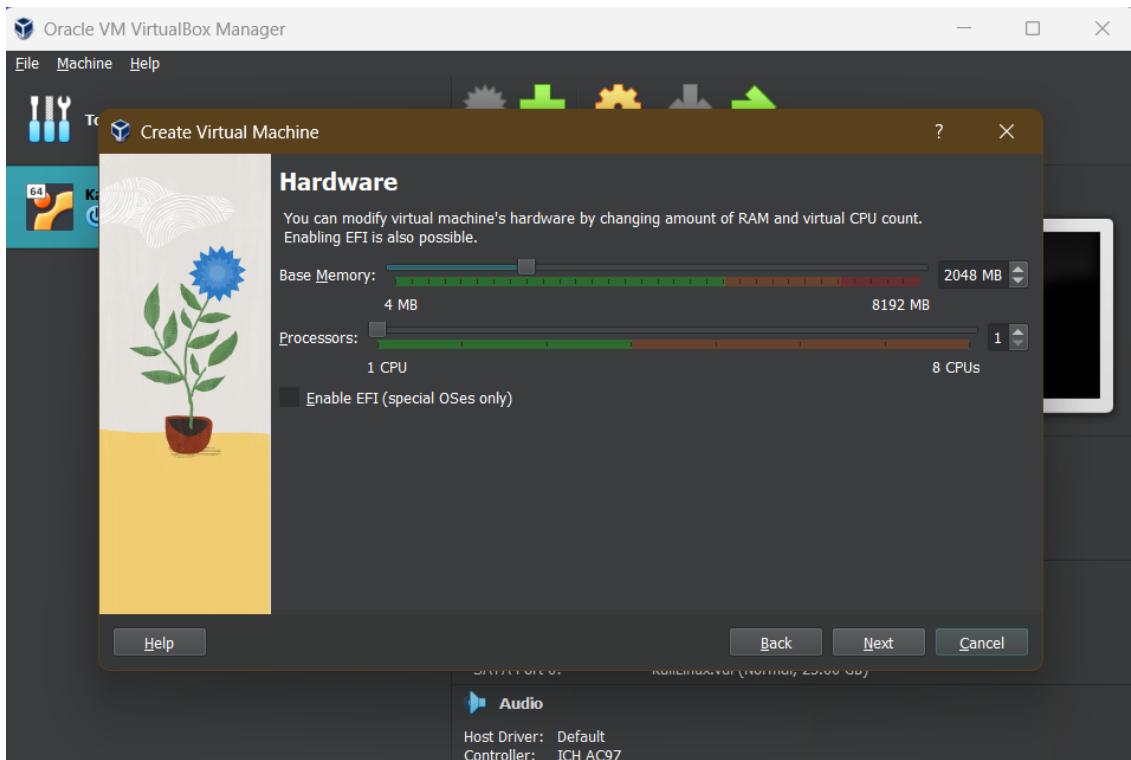
Enter a name and select the Iso file (Downloaded ubuntu ISO file) and press Next.



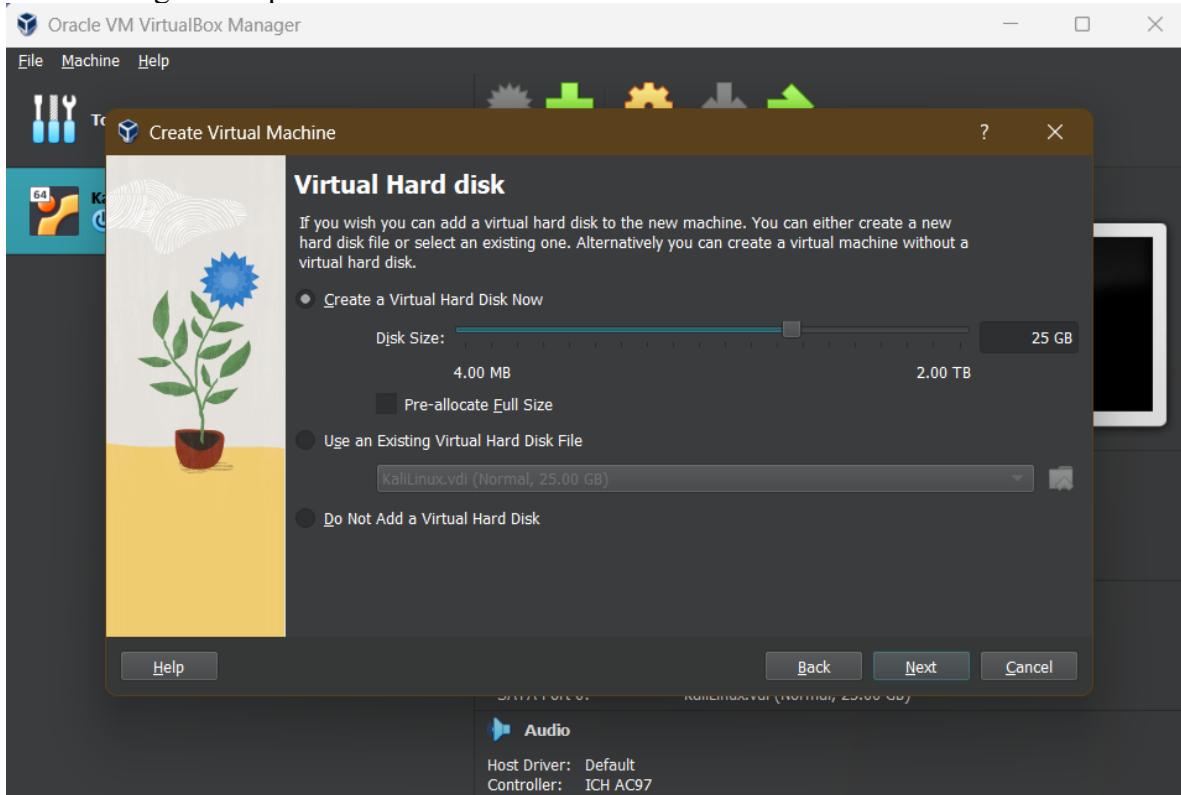
Then Enter a username and password



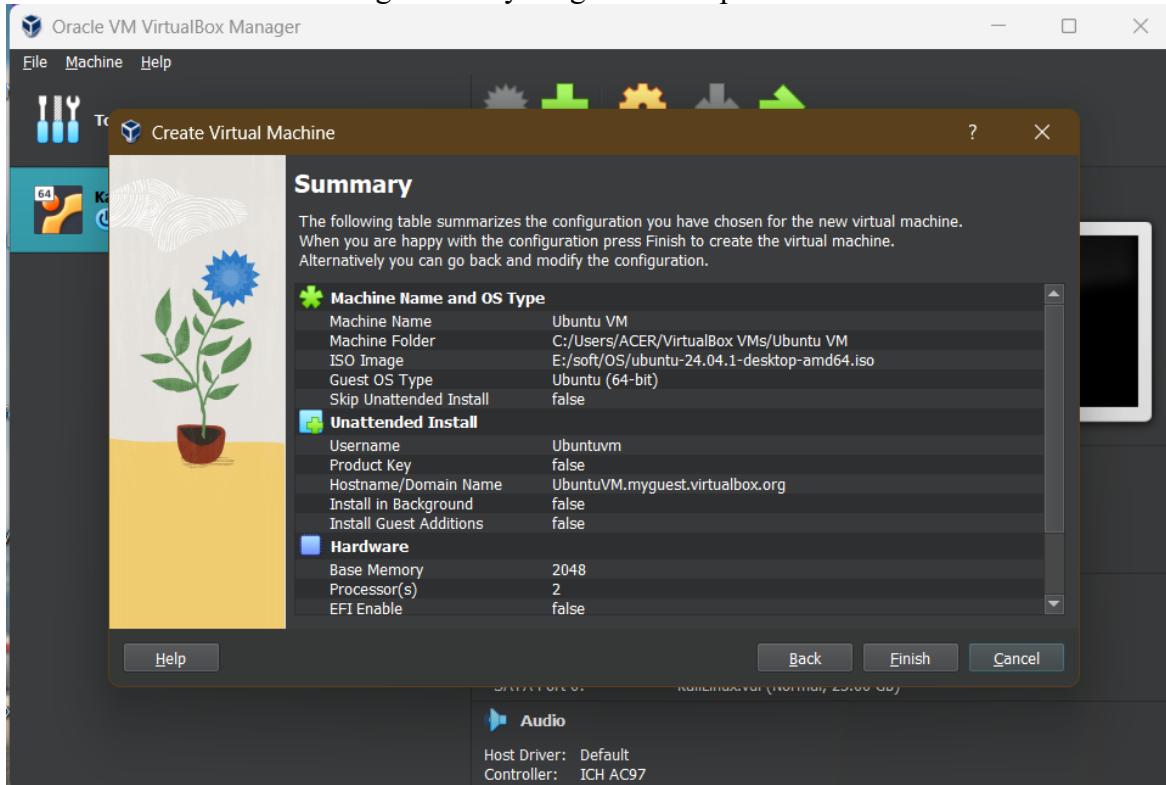
Select enough Base Memory space and Processors.



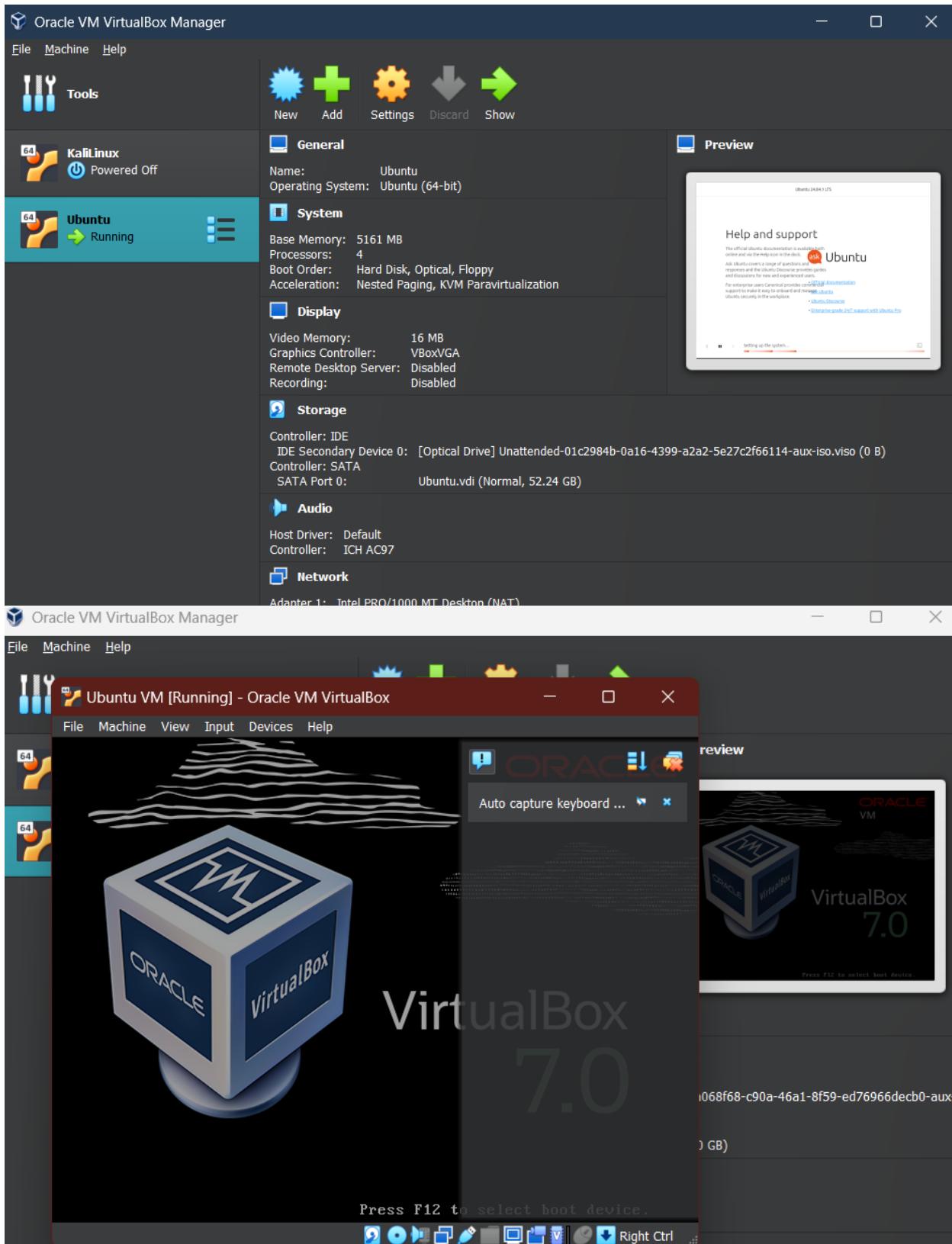
Select enough disk space for the virtual machine.



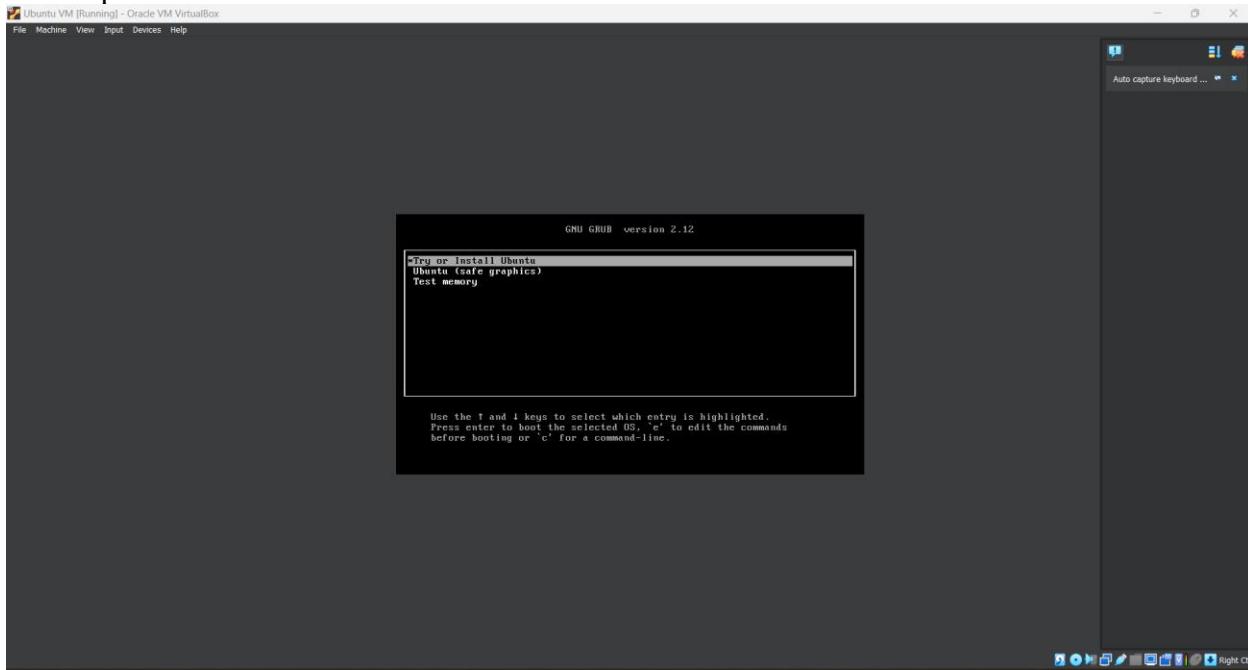
Check and confirm the settings. If everything is correct press finish.



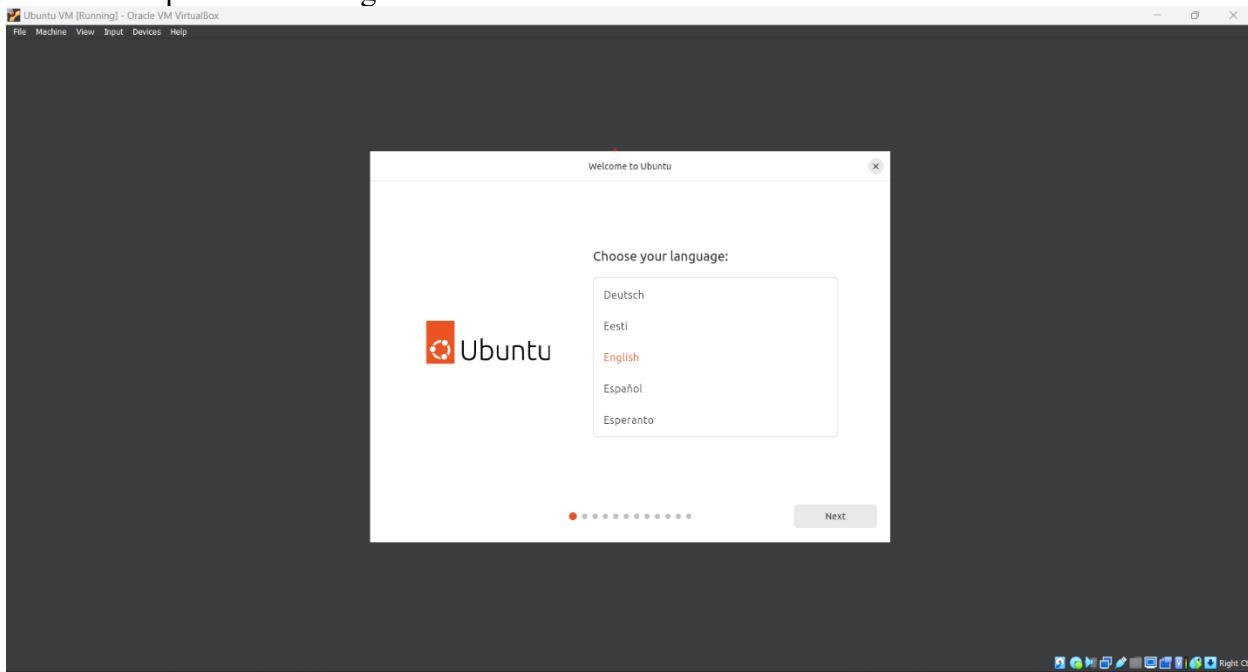
Now select the newly created virtual machine and click on start.

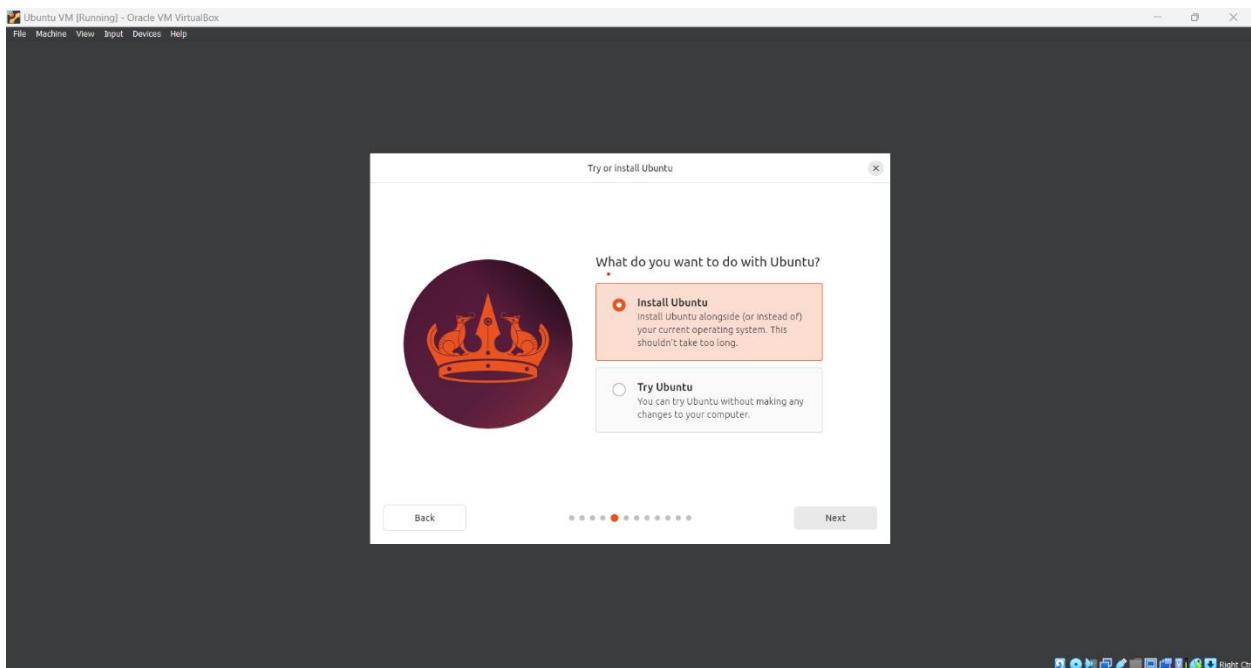
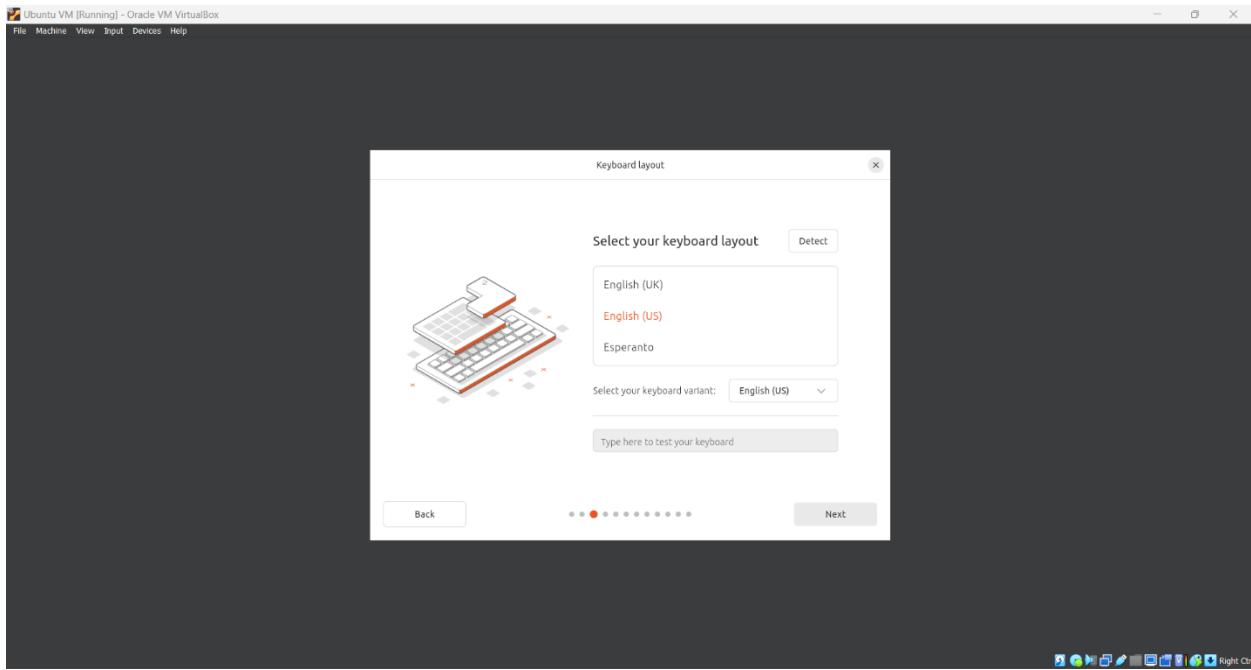


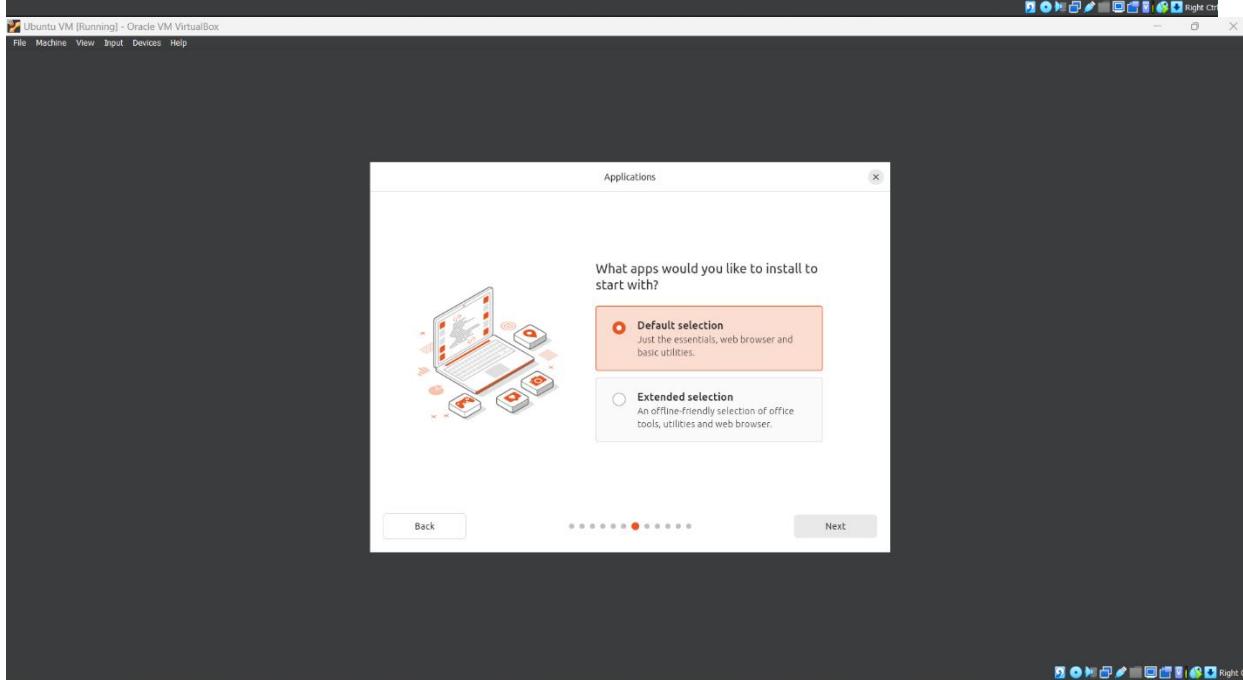
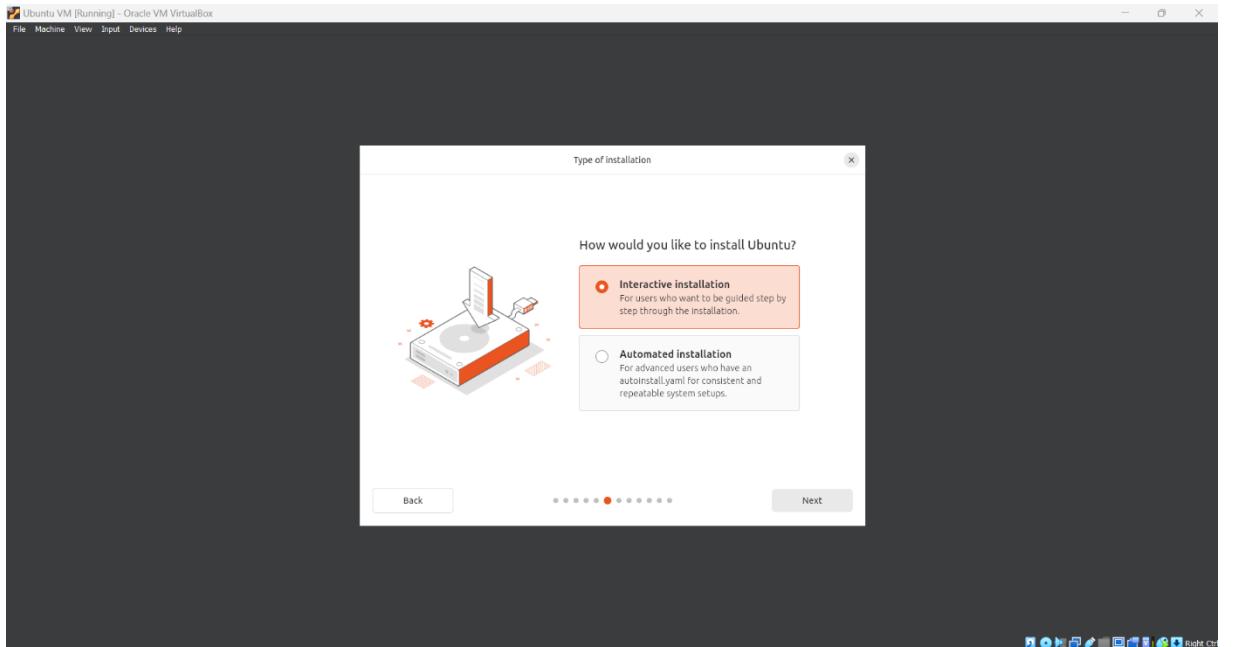
Select Try or install Ubuntu options (Highlighted option will be selected automatically after certain period.

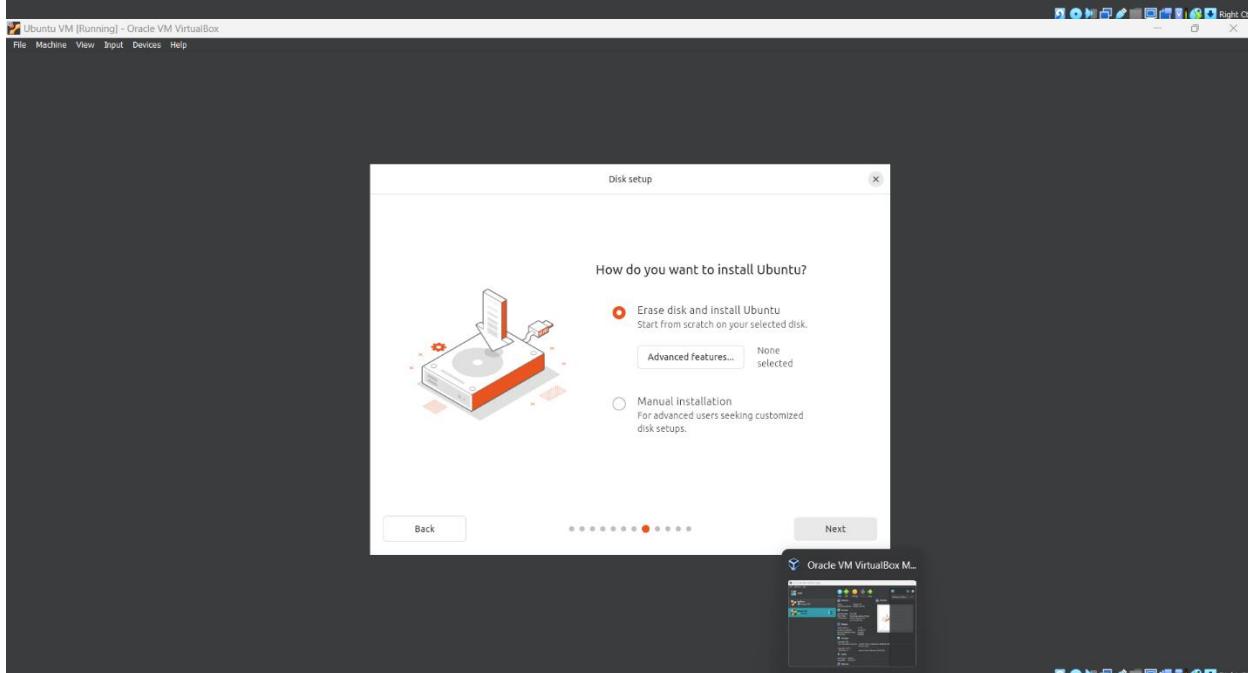
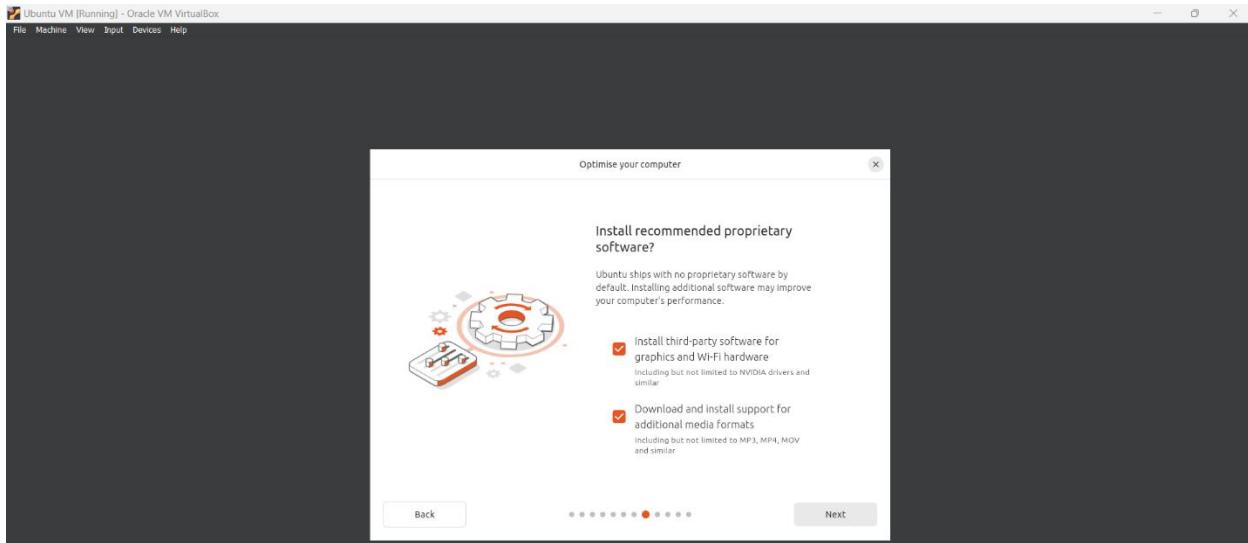


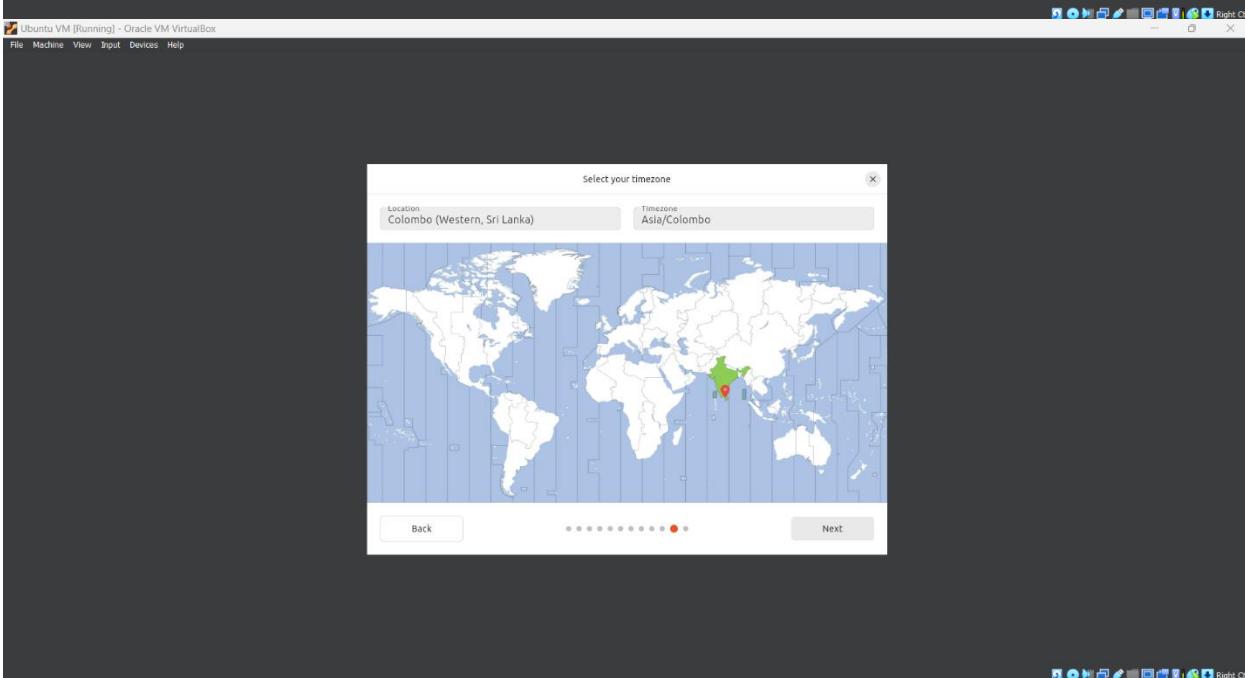
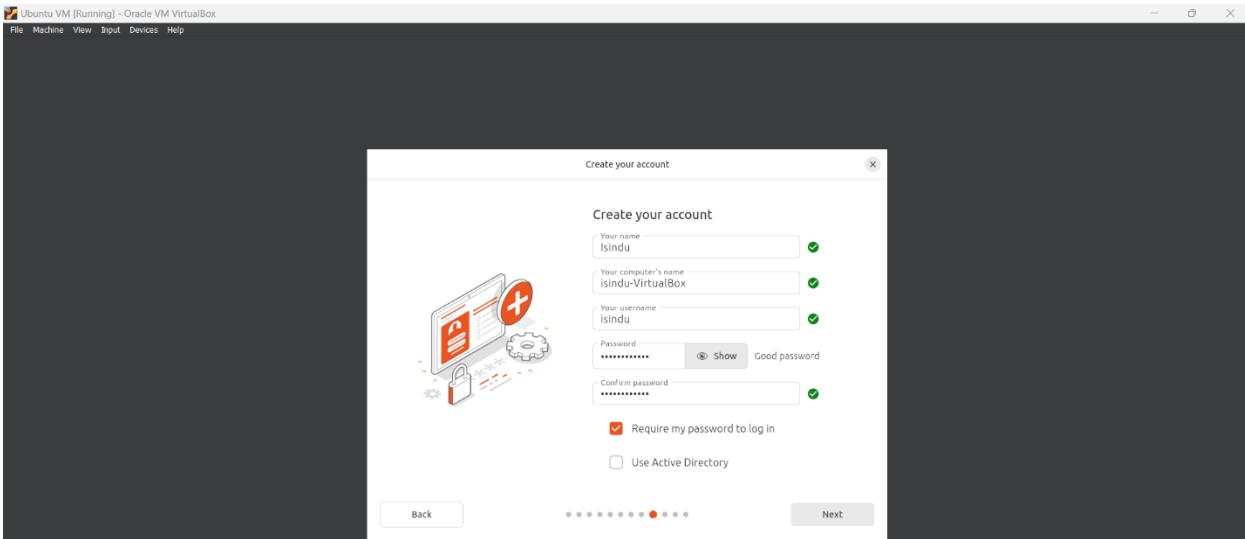
Then Select preferred settings and install Ubuntu.

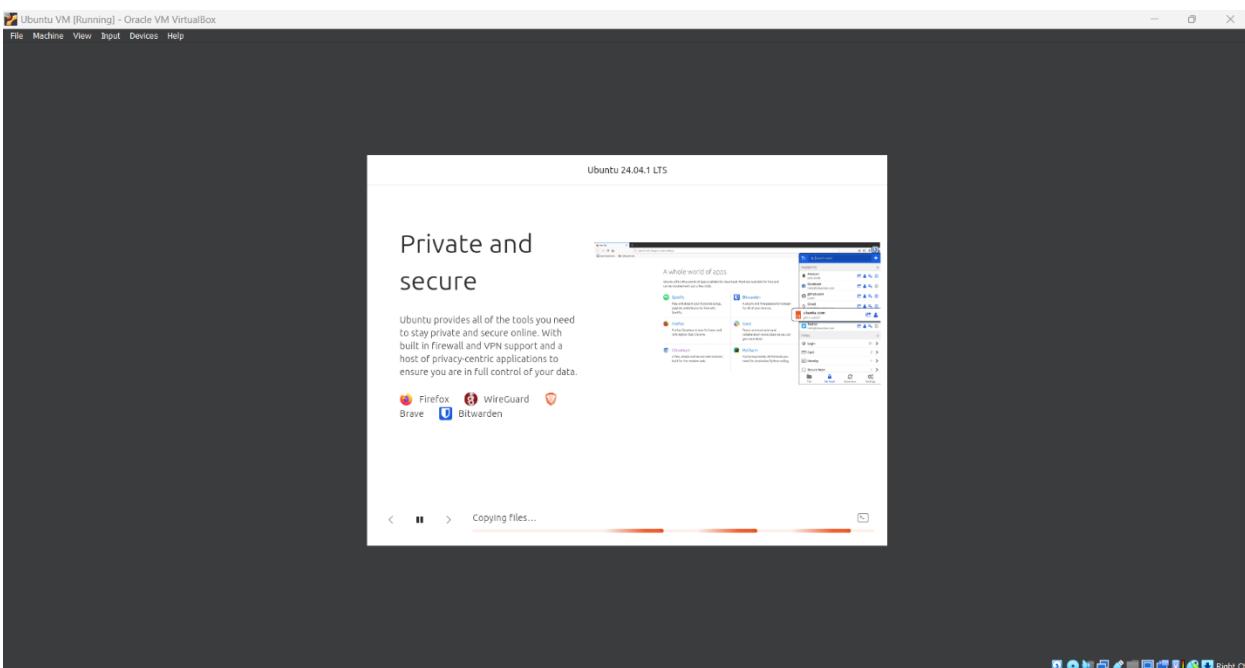
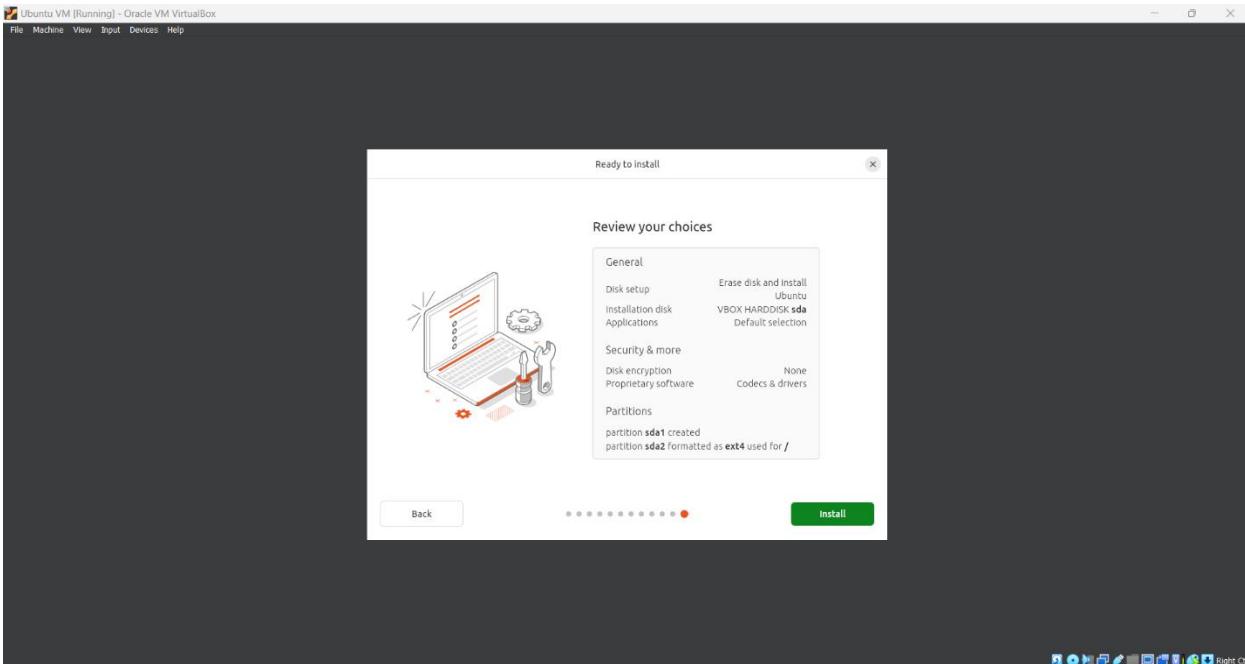




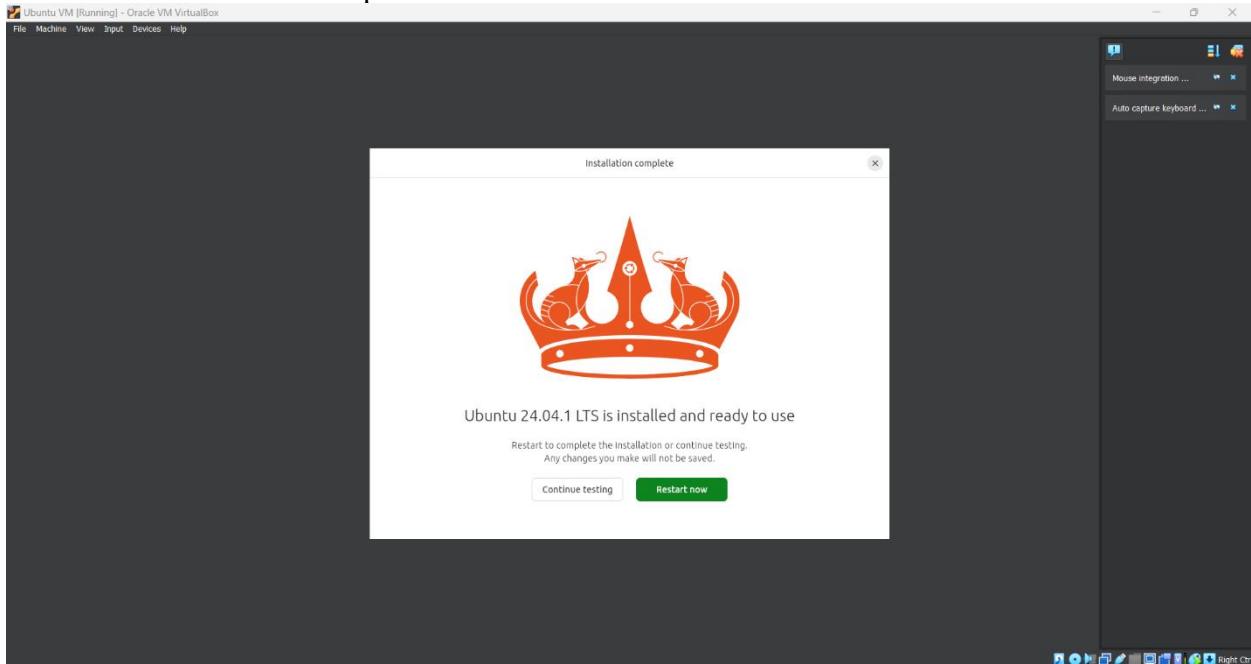






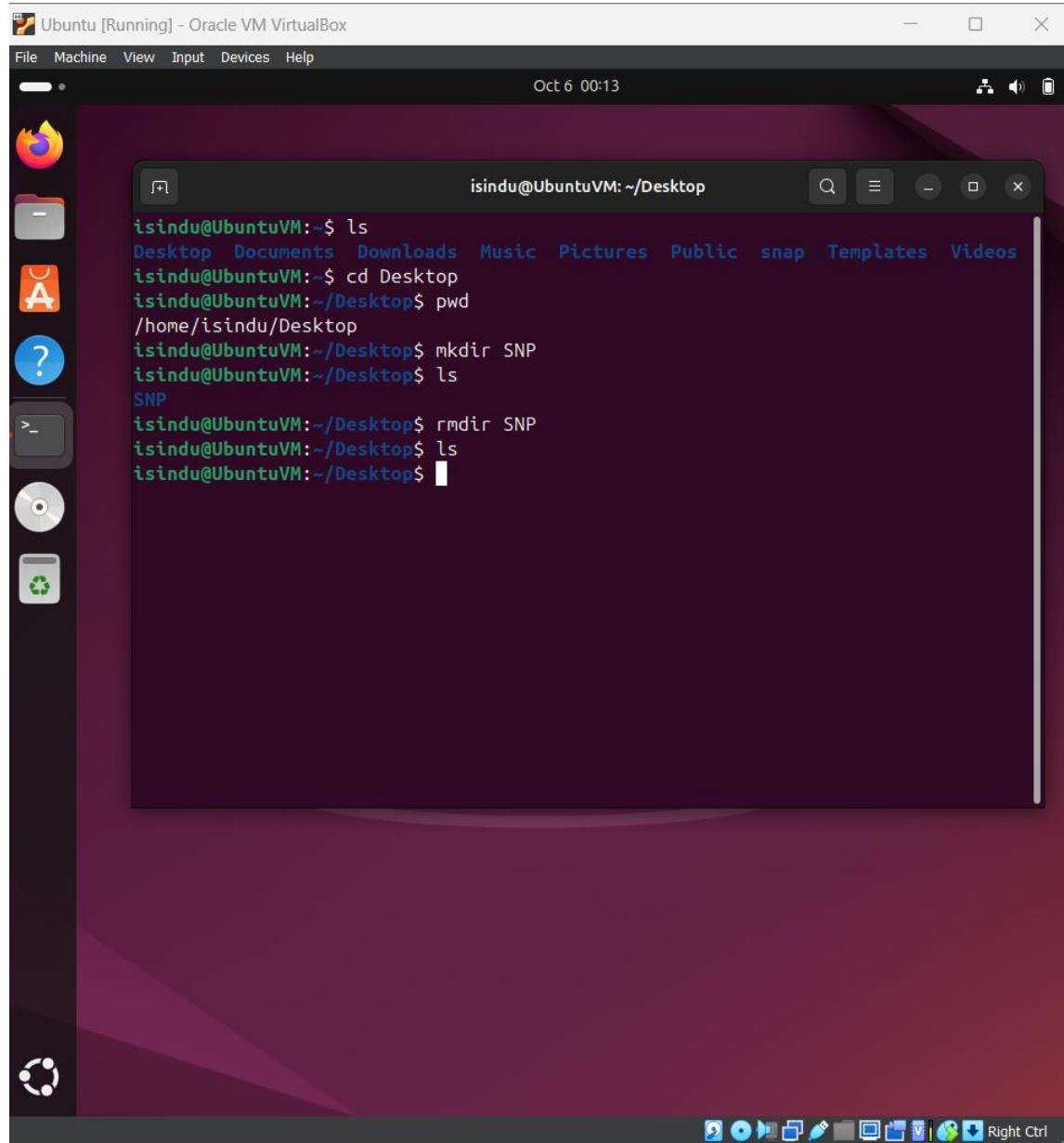


Once the installation is completed restart the virtual machine.



1.2) Basic Navigation Commands and functionalities.

Command	Functionality
ls	Listing items in the directory
cd	Change directory
pwd	Display the present working directory
mkdir	Create a directory
rmdir	Remove a directory



1.3) File manipulation commands

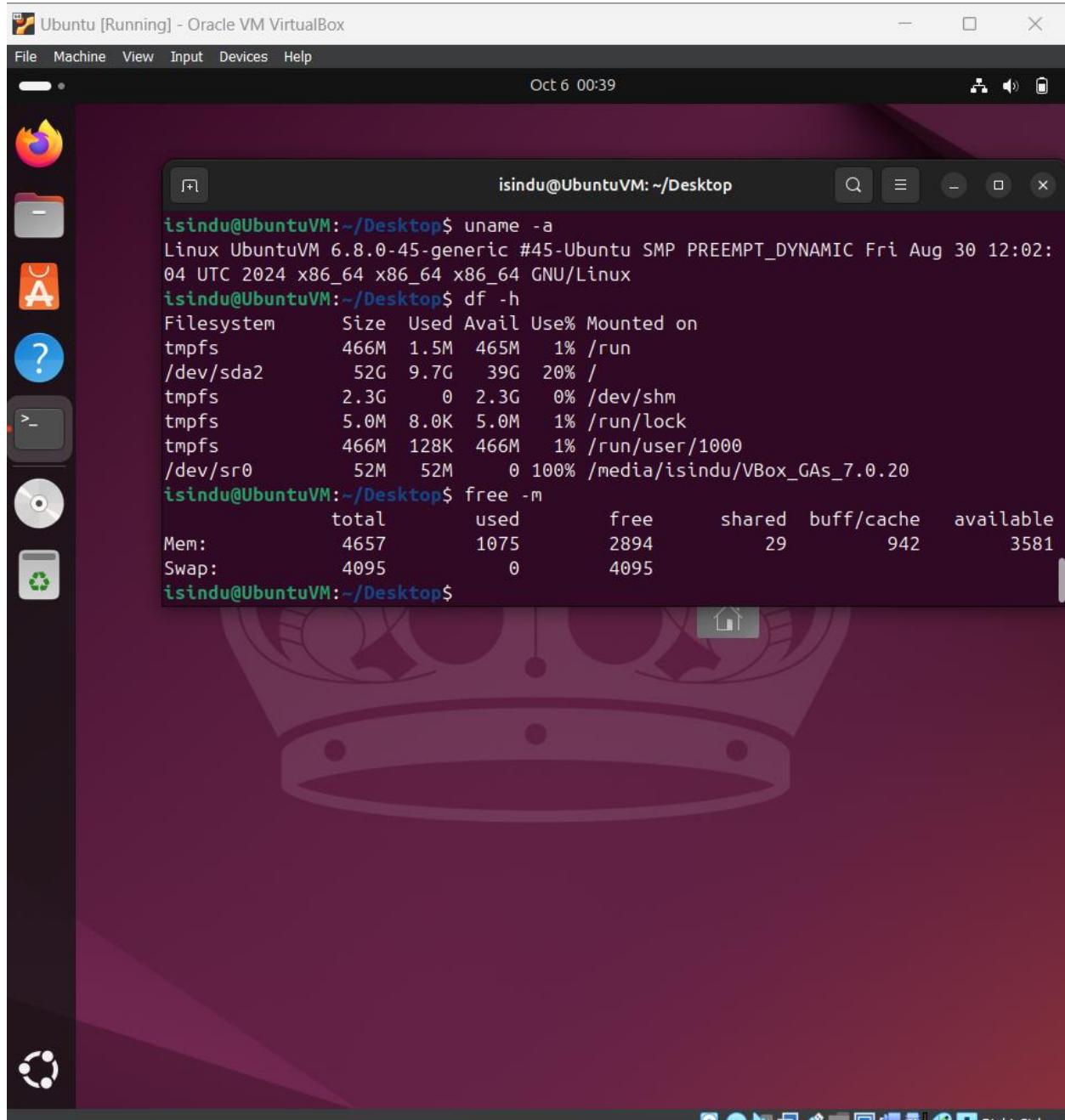
Command	Functionality
Touch	Creates an empty file
Nano	A text editor
Vim	A text editor
Cat	Displays file content
Chmod	Changes permissions of files / directories
Cp	Copy files / directories

The screenshot shows a virtual machine running Ubuntu. The desktop environment includes a dock at the bottom with icons for Dash, Home, Applications, and the Dash search bar. A terminal window is open, showing the following command history:

```
isindu@UbuntuVM:~/Desktop$ ls
SNP
isindu@UbuntuVM:~/Desktop$ touch test
isindu@UbuntuVM:~/Desktop$ nano test
isindu@UbuntuVM:~/Desktop$ cat test
Hello world
isindu@UbuntuVM:~/Desktop$ ls -l
total 8
drwxrwxr-x 2 isindu isindu 4096 Oct  6 00:16 SNP
-rw-rw-r-- 1 isindu isindu   12 Oct  6 00:29 test
isindu@UbuntuVM:~/Desktop$ chmod 777 test
isindu@UbuntuVM:~/Desktop$ cp test new.txt
isindu@UbuntuVM:~/Desktop$ cat new.txt
Hello world
```

1.4) System Information Commands

Command	Functionality
uname -a	Provide detailed information of the system
df -h	Displays the information about disk space usage in human readable format such as MB, GB.
free -m	Displays the information about system's memory usage in MB

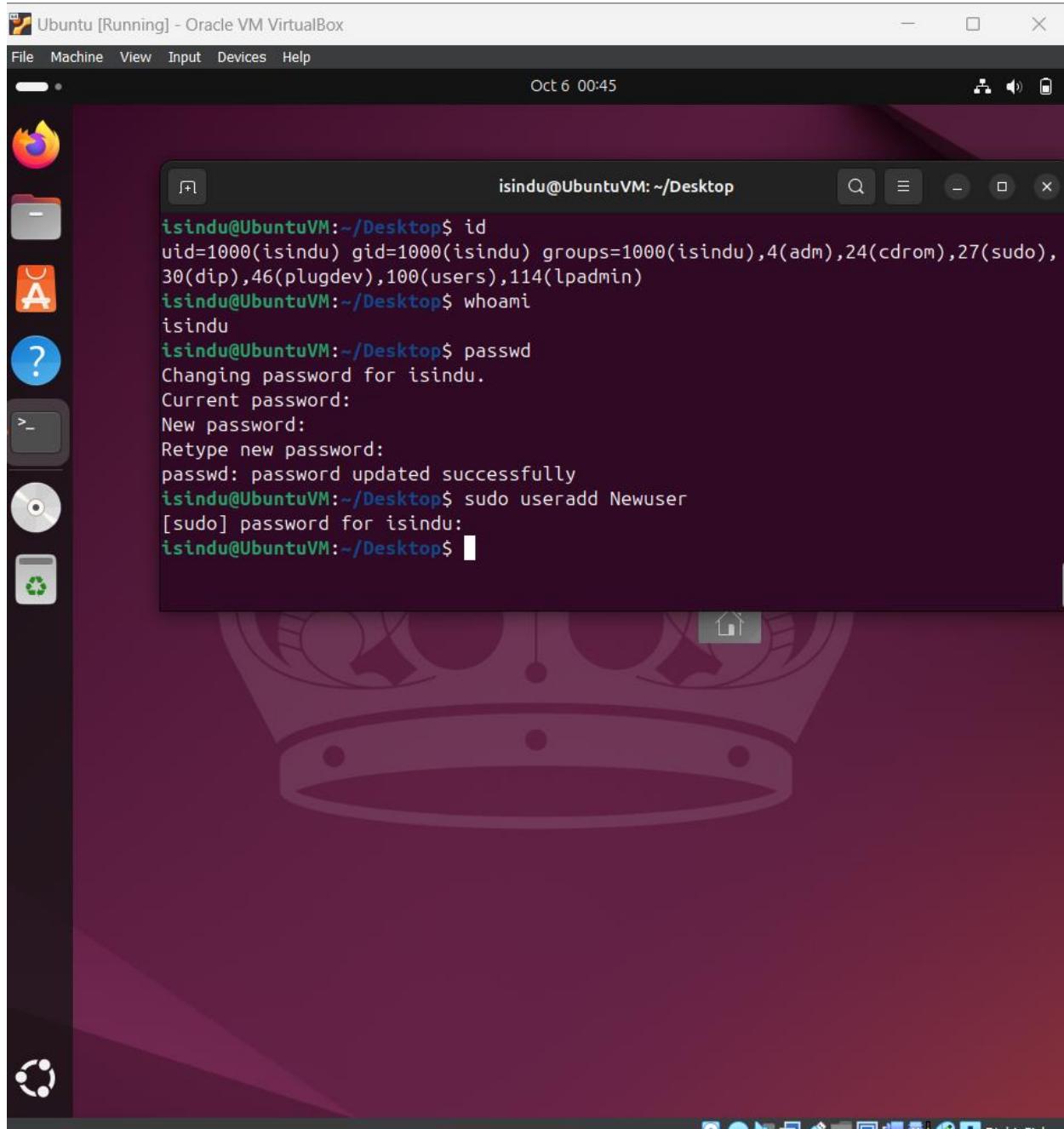


The screenshot shows a terminal window on an Ubuntu desktop. The terminal output is as follows:

```
isindu@UbuntuVM:~/Desktop$ uname -a
Linux UbuntuVM 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
isindu@UbuntuVM:~/Desktop$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            466M   1.5M  465M   1% /run
/dev/sda2         52G   9.7G   39G  20% /
tmpfs            2.3G     0  2.3G   0% /dev/shm
tmpfs            5.0M   8.0K  5.0M   1% /run/lock
tmpfs            466M  128K  466M   1% /run/user/1000
/dev/sr0          52M   52M     0 100% /media/isindu/VBox_GAs_7.0.20
isindu@UbuntuVM:~/Desktop$ free -m
              total        used        free      shared  buff/cache   available
Mem:       4657       1075       2894        29       942       3581
Swap:      4095           0       4095
isindu@UbuntuVM:~/Desktop$
```

1.5) User management commands.

Command	Functionality
id	Displays the user information and groups information of the user
whoami	Displays the username of the current user
passwd	Change the password of the user
useradd	Add a new user in to the system



The screenshot shows a terminal window on an Ubuntu desktop. The terminal output is as follows:

```
isindu@UbuntuVM:~/Desktop$ id
uid=1000(isindu) gid=1000(isindu) groups=1000(isindu),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),100(users),114(lpadmin)
isindu@UbuntuVM:~/Desktop$ whoami
isindu
isindu@UbuntuVM:~/Desktop$ passwd
Changing password for isindu.
Current password:
New password:
Retype new password:
passwd: password updated successfully
isindu@UbuntuVM:~/Desktop$ sudo useradd Newuser
[sudo] password for isindu:
isindu@UbuntuVM:~/Desktop$
```

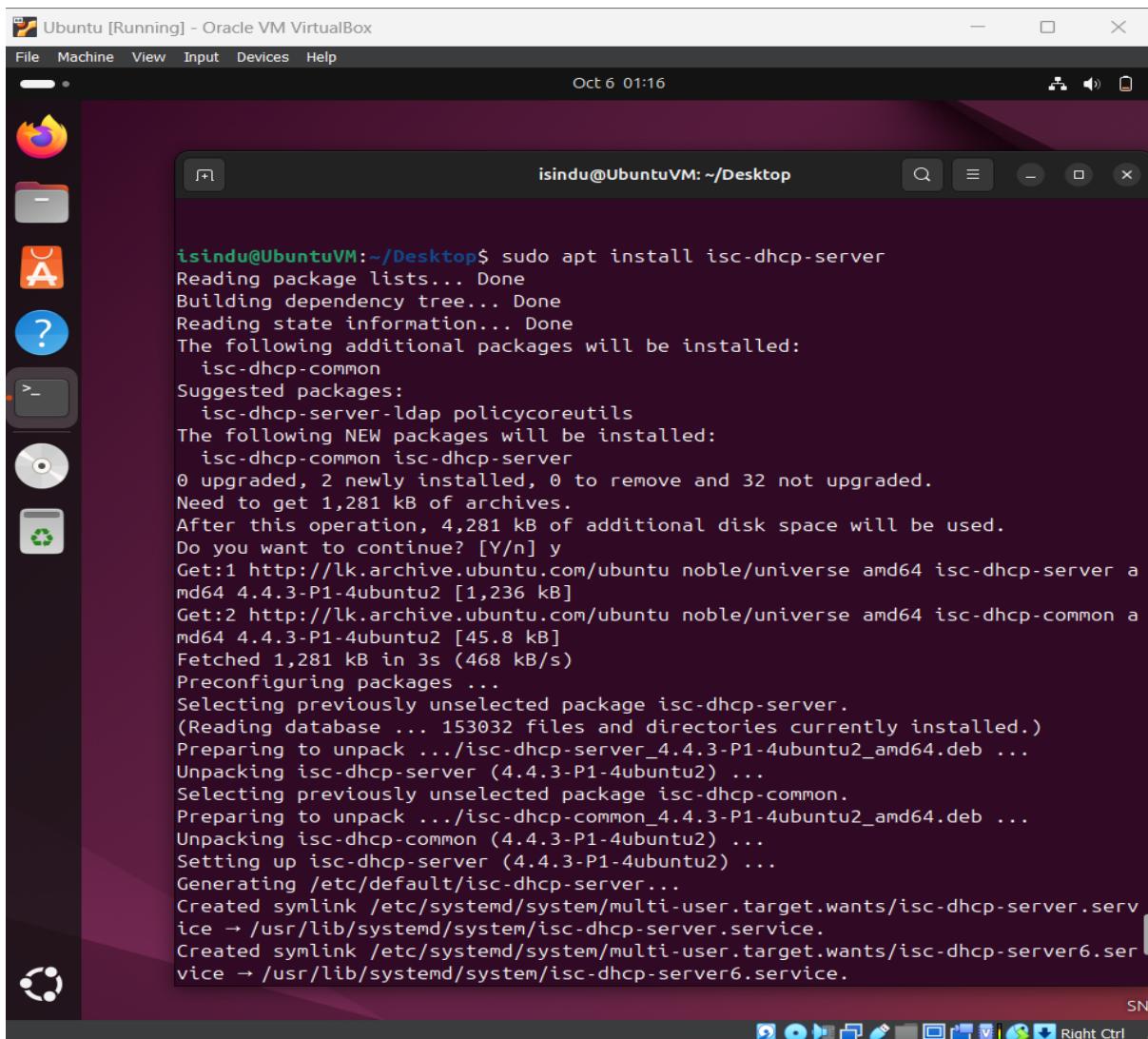
2. DHCP, DNS and NTP Services

2.1) DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is a protocol used to automatically assign IP addresses to devices on a network.

2.2) Installation and configuration

Open Terminal and install DHCP server package with “sudo apt install isc-dhcp-server” command.



The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
isindu@UbuntuVM:~/Desktop$ sudo apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  isc-dhcp-common
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-common isc-dhcp-server
0 upgraded, 2 newly installed, 0 to remove and 32 not upgraded.
Need to get 1,281 kB of archives.
After this operation, 4,281 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-server a
md64 4.4.3-P1-4ubuntu2 [1,236 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-common a
md64 4.4.3-P1-4ubuntu2 [45.8 kB]
Fetched 1,281 kB in 3s (468 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 153032 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Selecting previously unselected package isc-dhcp-common.
Preparing to unpack .../isc-dhcp-common_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Setting up isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Generating /etc/default/isc-dhcp-server...
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server.serv
ice → /usr/lib/systemd/system/isc-dhcp-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server6.ser
vice → /usr/lib/systemd/system/isc-dhcp-server6.service.
```

Use “sudo nano /etc/dhcp/dhcpd.conf” to open and edit DHCP configuration file and modify it do define the network settings for the DHCP server and save it.

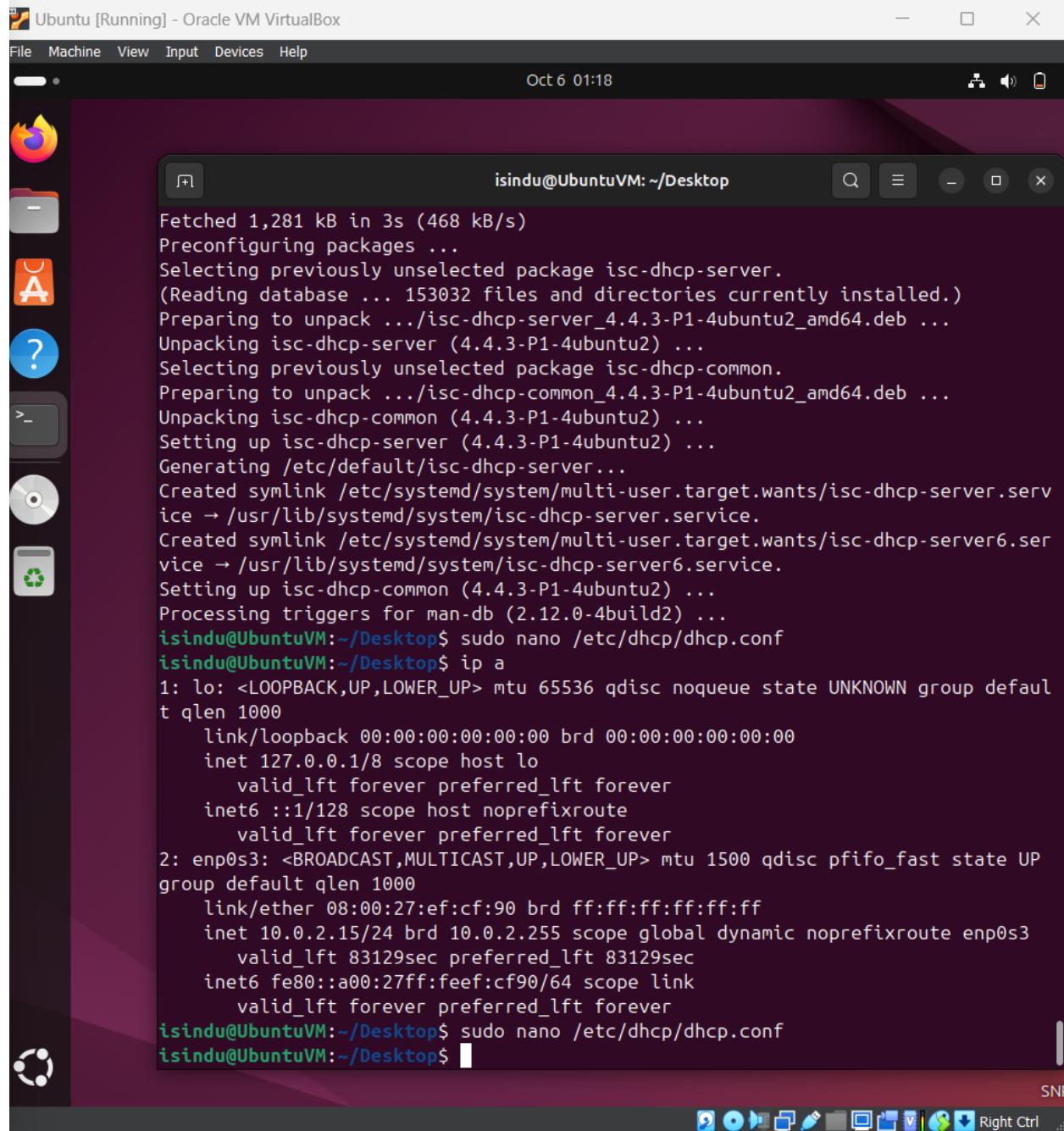
The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox" running on an Ubuntu desktop. The terminal is displaying the contents of the /etc/dhcp/dhcpd.conf file using the nano editor. The file contains configuration for a DHCP server, including options for domain name, lease times, and a subnet definition. The desktop background is dark purple, and there are icons for "new.txt", "test", and "SNP" on the desktop. The system tray at the bottom shows various application icons and system status information.

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
#
# Sample configuration file for ISC dhcpcd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
# option definitions common to all supported networks...
option domain-name "local";
option domain-name-servers 192.168.1.1;

default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.150;
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
    option subnet-mask 255.255.255.0;}
```

Use “sudo nano /etc/default/isc-dhcp-server” command to open and edit the DHCP server default file. Use “ip a” command to check network interface and make changes to the relevant interface.



The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
Fetched 1,281 kB in 3s (468 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 153032 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Selecting previously unselected package isc-dhcp-common.
Preparing to unpack .../isc-dhcp-common_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Setting up isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Generating /etc/default/isc-dhcp-server...
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server.service → /usr/lib/systemd/system/isc-dhcp-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server6.service → /usr/lib/systemd/system/isc-dhcp-server6.service.
Setting up isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Processing triggers for man-db (2.12.0-4build2) ...
isindu@UbuntuVM:~/Desktop$ sudo nano /etc/dhcp/dhcp.conf
isindu@UbuntuVM:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ef:cf:90 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 83129sec preferred_lft 83129sec
    inet6 fe80::a00:27ff:feef:cf90/64 scope link
        valid_lft forever preferred_lft forever
isindu@UbuntuVM:~/Desktop$ sudo nano /etc/dhcp/dhcp.conf
isindu@UbuntuVM:~/Desktop$
```

```
GNU nano 7.2          /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.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/dhcpcd6.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="enp0s3"
INTERFACESv6=""
```

Start the service with the command “`sudo systemctl start isc-dhcp-server`”. We can enable it to run on boot with the command “`sudo systemctl enable isc-dhcp-server`”.

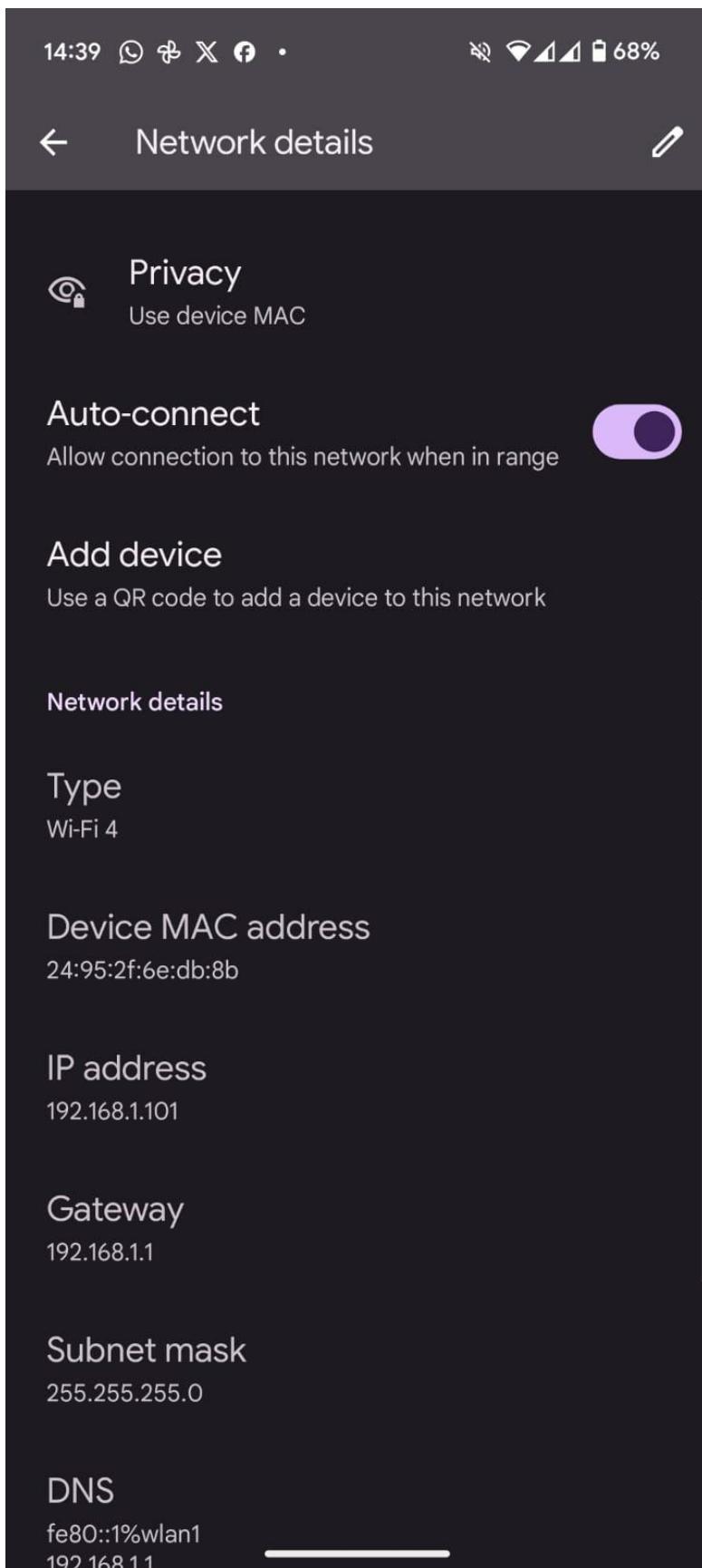
Then check the status of the service using “sudo systemctl status isc-dhcp-server. If it displays no errors and if its running, we can verify by connecting another device (with DHCP on) to the same network and check if it has a IP address within the range we designed.

The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
isindu@UbuntuVM:~$ sudo systemctl restart isc-dhcp-server
isindu@UbuntuVM:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; v
  Active: active (running) since Sun 2024-10-06 14:25:02 +0530; 9s ago
    Docs: man:dhcpd(8)
   Main PID: 11147 (dhcpd)
     Tasks: 1 (limit: 5504)
    Memory: 3.7M (peak: 4.1M)
       CPU: 8ms
      CGroup: /system.slice/isc-dhcp-server.service
              └─11147 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/>

Oct 06 14:25:02 UbuntuVM sh[11147]: Wrote 0 leases to leases file.
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: PID file: /run/dhcp-server/dhcpcd.pid
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: Wrote 0 leases to leases file.
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: Listening on LPF/enp0s3/08:00:27:ef:cf:9>
Oct 06 14:25:02 UbuntuVM sh[11147]: Listening on LPF/enp0s3/08:00:27:ef:cf:90/1>
Oct 06 14:25:02 UbuntuVM sh[11147]: Sending on   LPF/enp0s3/08:00:27:ef:cf:90/1>
Oct 06 14:25:02 UbuntuVM sh[11147]: Sending on   Socket/fallback/fallback-net
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: Sending on   LPF/enp0s3/08:00:27:ef:cf:9>
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: Sending on   Socket/fallback/fallback-net
Oct 06 14:25:02 UbuntuVM dhcpcd[11147]: Server starting service.
lines 1-21/21 (END)
```

The terminal window is part of a desktop environment, with icons for various applications like a browser, file manager, and terminal visible in the dock at the bottom. A file named "new.txt" is open in the background.

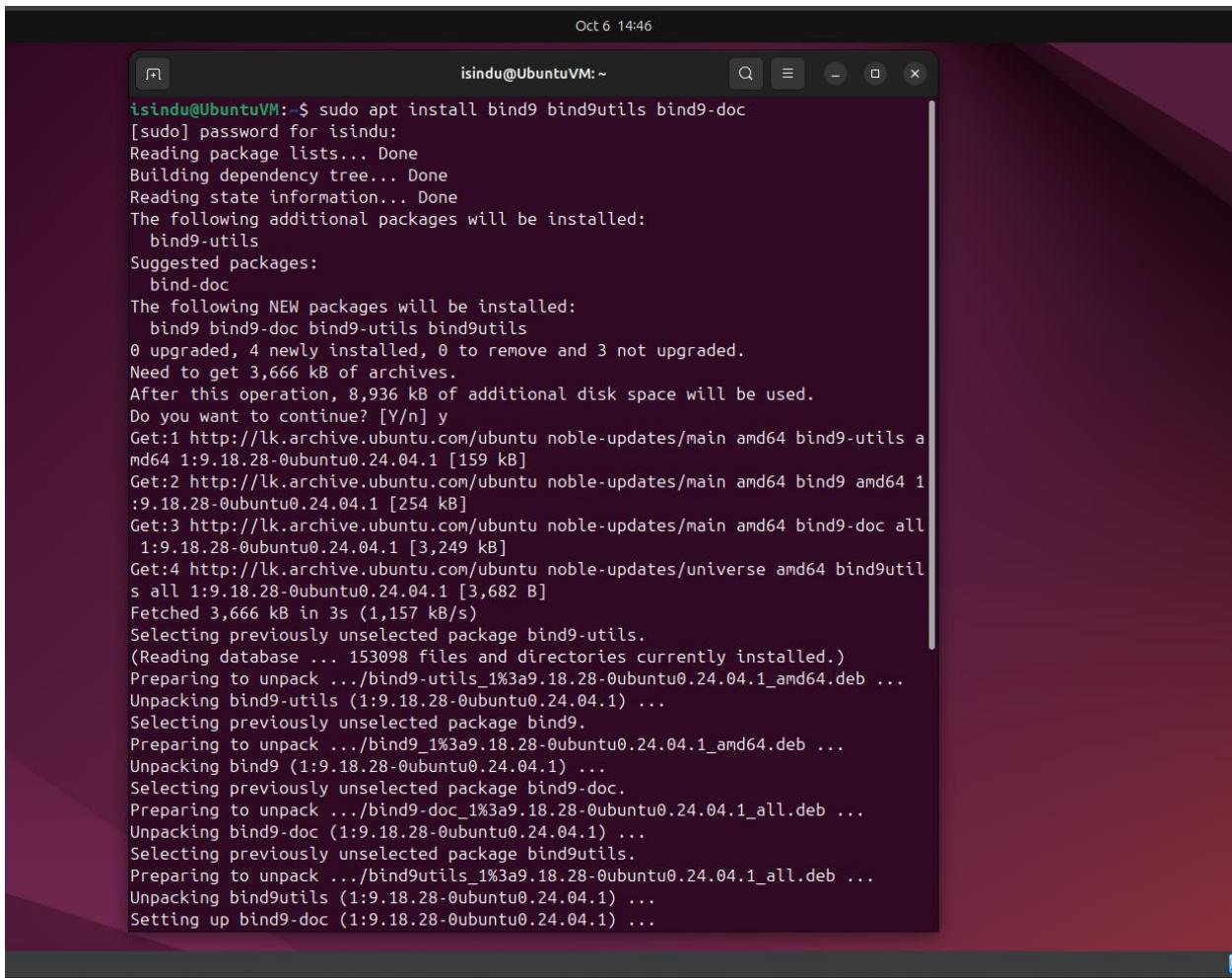


2.3) DNS (Domain Name System)

DNS (Domain Name System) plays a crucial role in translating human domains names to machine readable IP addresses which allows users to access websites with ease.

2.4) Installation and Configuration

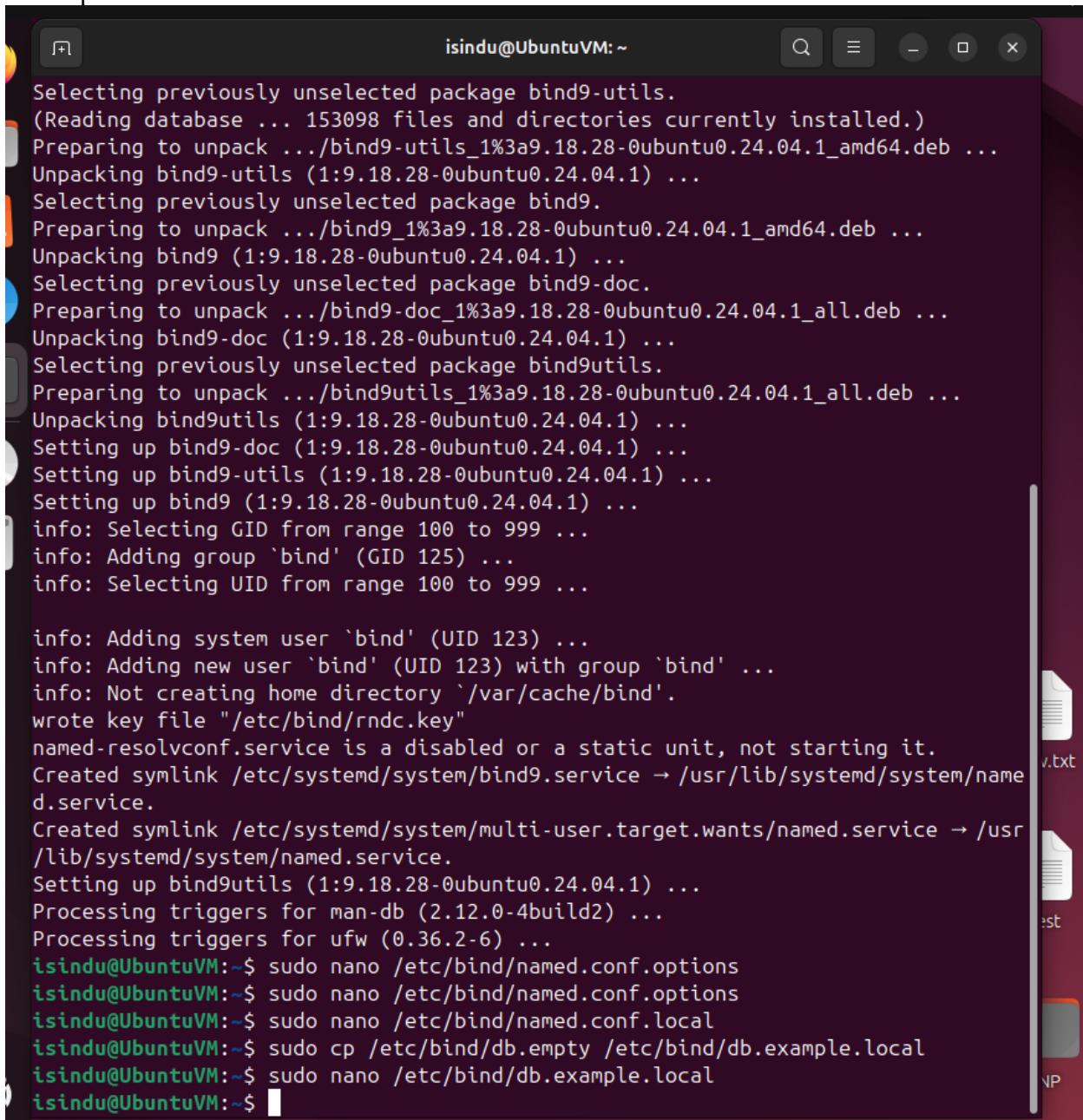
Install a DNS Server like BIND (Berkeley Internet Name Domain) and packages with “`sudo apt install bind9 bind9utils bind9-doc`” command.



The screenshot shows a terminal window titled "isindu@UbuntuVM:~". The command `sudo apt install bind9 bind9utils bind9-doc` is being run. The output shows the package manager reading lists, building dependency trees, and installing the specified packages. It lists "bind9-utils" as a suggested package and "bind9 bind9-doc bind9-utils bind9utils" as new packages. It shows the download of files from "lk.archive.ubuntu.com" and the unpacking of the downloaded packages. The process ends with the setting up of the "bind9-doc" package.

```
Oct 6 14:46
isindu@UbuntuVM:~$ sudo apt install bind9 bind9utils bind9-doc
[sudo] password for isindu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils
0 upgraded, 4 newly installed, 0 to remove and 3 not upgraded.
Need to get 3,666 kB of archives.
After this operation, 8,936 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-utils amd64 1:9.18.28-0ubuntu0.24.04.1 [159 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9 amd64 1:9.18.28-0ubuntu0.24.04.1 [254 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-doc all 1:9.18.28-0ubuntu0.24.04.1 [3,249 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 bind9utils all 1:9.18.28-0ubuntu0.24.04.1 [3,682 B]
Fetched 3,666 kB in 3s (1,157 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 153098 files and directories currently installed.)
Preparing to unpack .../bind9-utils_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9-utils (1:9.18.28-0ubuntu0.24.04.1) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9 (1:9.18.28-0ubuntu0.24.04.1) ...
Selecting previously unselected package bind9-doc.
Preparing to unpack .../bind9-doc_1%3a9.18.28-0ubuntu0.24.04.1_all.deb ...
Unpacking bind9-doc (1:9.18.28-0ubuntu0.24.04.1) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.18.28-0ubuntu0.24.04.1_all.deb ...
Unpacking bind9utils (1:9.18.28-0ubuntu0.24.04.1) ...
Setting up bind9-doc (1:9.18.28-0ubuntu0.24.04.1) ...
```

Open and edit BIND configuration file, zone configuration and copy the default zone file and edit copied zone file as well.



The screenshot shows a terminal window titled "isindu@UbuntuVM: ~". The window displays the following text:

```
Selecting previously unselected package bind9-utils.  
(Reading database ... 153098 files and directories currently installed.)  
Preparing to unpack .../bind9-utils_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...  
Unpacking bind9-utils (1:9.18.28-0ubuntu0.24.04.1) ...  
Selecting previously unselected package bind9.  
Preparing to unpack .../bind9_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...  
Unpacking bind9 (1:9.18.28-0ubuntu0.24.04.1) ...  
Selecting previously unselected package bind9-doc.  
Preparing to unpack .../bind9-doc_1%3a9.18.28-0ubuntu0.24.04.1_all.deb ...  
Unpacking bind9-doc (1:9.18.28-0ubuntu0.24.04.1) ...  
Selecting previously unselected package bind9utils.  
Preparing to unpack .../bind9utils_1%3a9.18.28-0ubuntu0.24.04.1_all.deb ...  
Unpacking bind9utils (1:9.18.28-0ubuntu0.24.04.1) ...  
Setting up bind9-doc (1:9.18.28-0ubuntu0.24.04.1) ...  
Setting up bind9-utils (1:9.18.28-0ubuntu0.24.04.1) ...  
Setting up bind9 (1:9.18.28-0ubuntu0.24.04.1) ...  
info: Selecting GID from range 100 to 999 ...  
info: Adding group `bind' (GID 125) ...  
info: Selecting UID from range 100 to 999 ...  
  
info: Adding system user `bind' (UID 123) ...  
info: Adding new user `bind' (UID 123) with group `bind' ...  
info: Not creating home directory `/var/cache/bind'.  
wrote key file "/etc/bind/rndc.key"  
named-resolvconf.service is a disabled or a static unit, not starting it.  
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.  
Setting up bind9utils (1:9.18.28-0ubuntu0.24.04.1) ...  
Processing triggers for man-db (2.12.0-4build2) ...  
Processing triggers for ufw (0.36.2-6) ...  
isindu@UbuntuVM:~$ sudo nano /etc/bind/named.conf.options  
isindu@UbuntuVM:~$ sudo nano /etc/bind/named.conf.options  
isindu@UbuntuVM:~$ sudo nano /etc/bind/named.conf.local  
isindu@UbuntuVM:~$ sudo cp /etc/bind/db.empty /etc/bind/db.example.local  
isindu@UbuntuVM:~$ sudo nano /etc/bind/db.example.local  
isindu@UbuntuVM:~$
```

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Oct 6 14:53

isindu@UbuntuVM:~

GNU nano 7.2 /etc/bind/named.conf.options

```
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

    allow-query {any;};

    // 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;

auth-nxdomain no;
listen-on-v6 { any; };
};
```

[Read 29 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

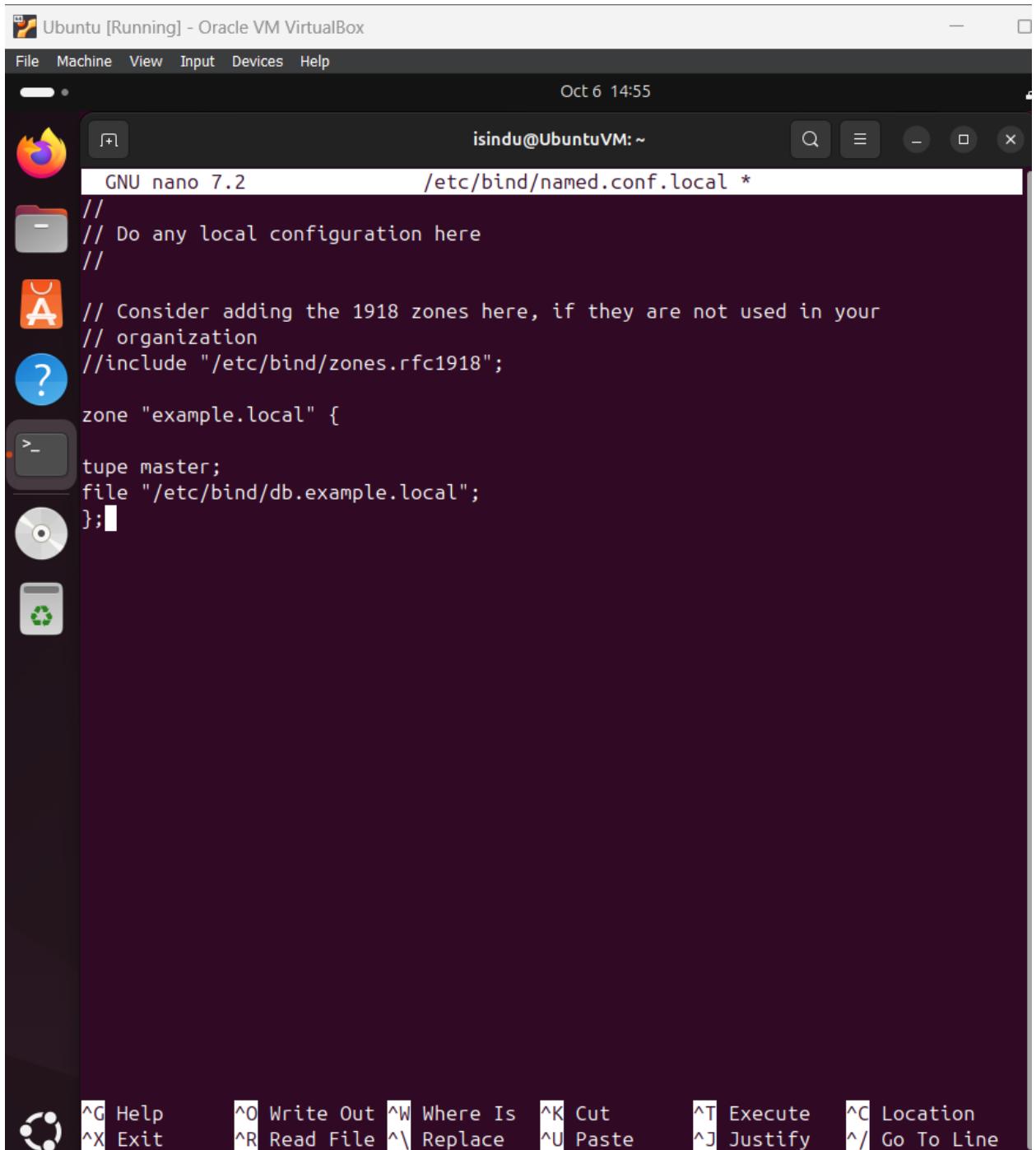
Oct 6 14:55

isindu@UbuntuVM: ~

GNU nano 7.2 /etc/bind/named.conf.local *

```
//  
// Do any local configuration here  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "example.local" {  
    type master;  
    file "/etc/bind/db.example.local";  
};
```

Help Write Out Where Is Cut Execute Location
Exit Read File Replace Paste Justify Go To Line



Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Oct 6 14:58

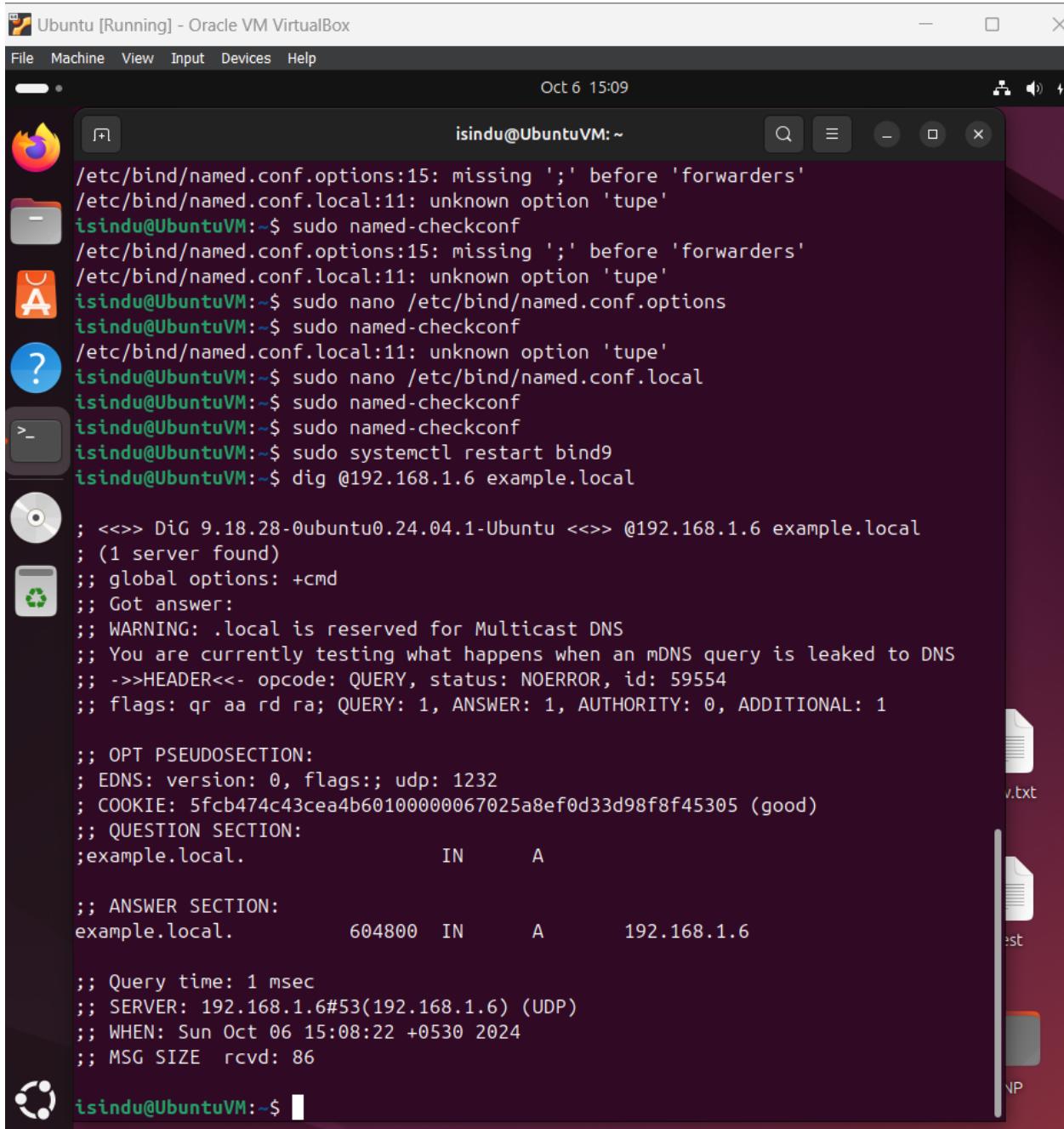
isindu@UbuntuVM:~

GNU nano 7.2 /etc/bind/db.example.local *

```
; BIND data file for example.local
;
$TTL    604800
@       IN      SOA     ns.example.local. admin.example.local. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@       IN      NS      ns.example.local.
ns      IN      A       192.168.1.6
@       IN      A       192.168.1.6
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

Check Bind configuration for errors with “sudo named-checkconf”. Then Restart the BIND and test the DNS server with “sudo systemctl restart bind9” and “dig” commands.



```
isindu@UbuntuVM:~$ sudo named-checkconf
/etc/bind/named.conf.options:15: missing ';' before 'forwarders'
/etc/bind/named.conf.local:11: unknown option 'tupe'
isindu@UbuntuVM:~$ sudo nano /etc/bind/named.conf.options
isindu@UbuntuVM:~$ sudo named-checkconf
/etc/bind/named.conf.local:11: unknown option 'tupe'
isindu@UbuntuVM:~$ sudo nano /etc/bind/named.conf.local
isindu@UbuntuVM:~$ sudo named-checkconf
isindu@UbuntuVM:~$ sudo named-checkconf
isindu@UbuntuVM:~$ sudo systemctl restart bind9
isindu@UbuntuVM:~$ dig @192.168.1.6 example.local

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> @192.168.1.6 example.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 59554
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5fcf474c43cea4b60100000067025a8ef0d33d98f8f45305 (good)
;; QUESTION SECTION:
;example.local.           IN      A

;; ANSWER SECTION:
example.local.        604800  IN      A      192.168.1.6

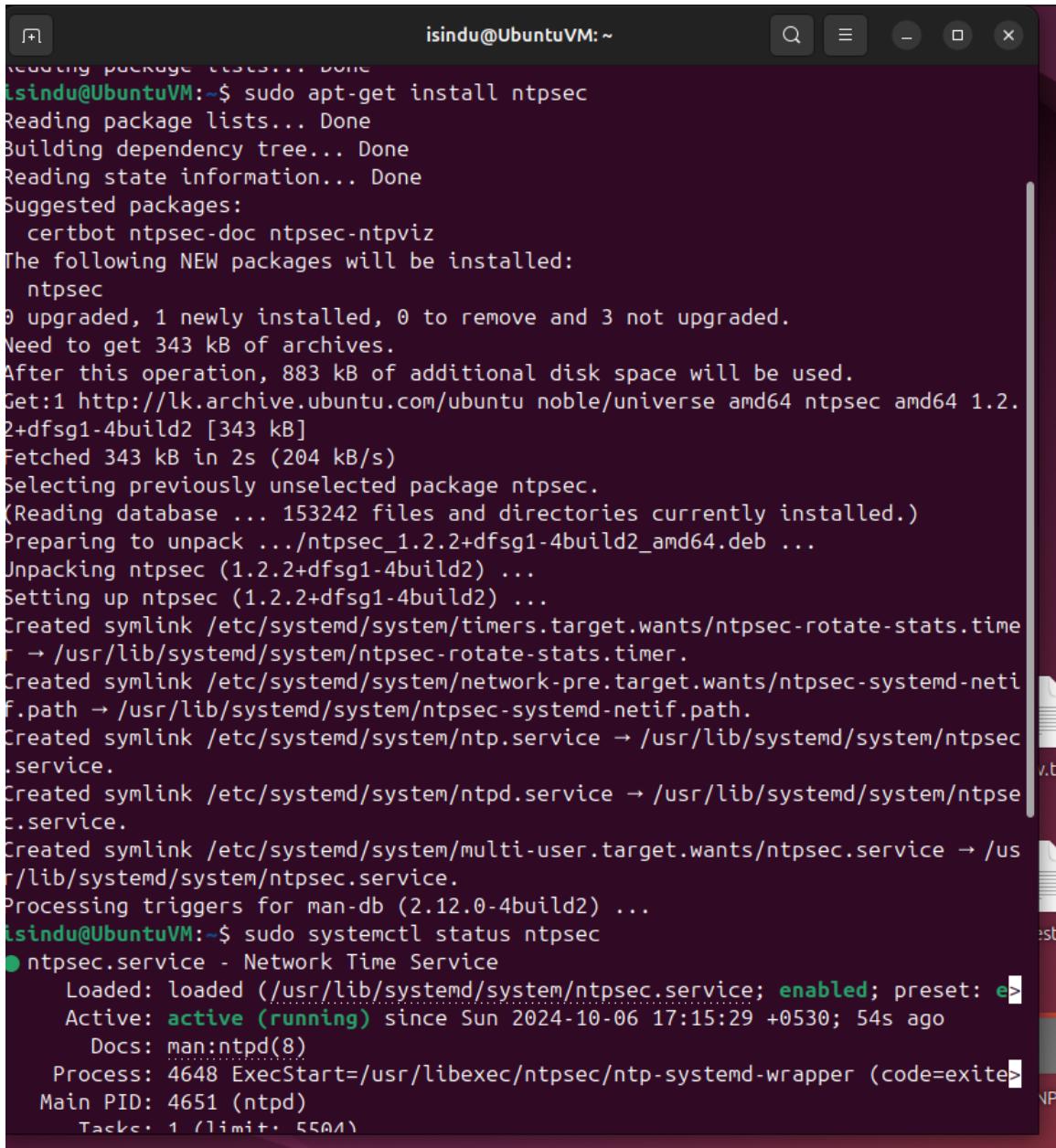
;; Query time: 1 msec
;; SERVER: 192.168.1.6#53(192.168.1.6) (UDP)
;; WHEN: Sun Oct 06 15:08:22 +0530 2024
;; MSG SIZE  rcvd: 86
```

2.5) NTP (Network Time Protocol)

NTP (Network Time Protocol) is a protocol designed to synchronize the clocks of computers in a network. IT ensures that all the computers on the network maintain the accurate time.

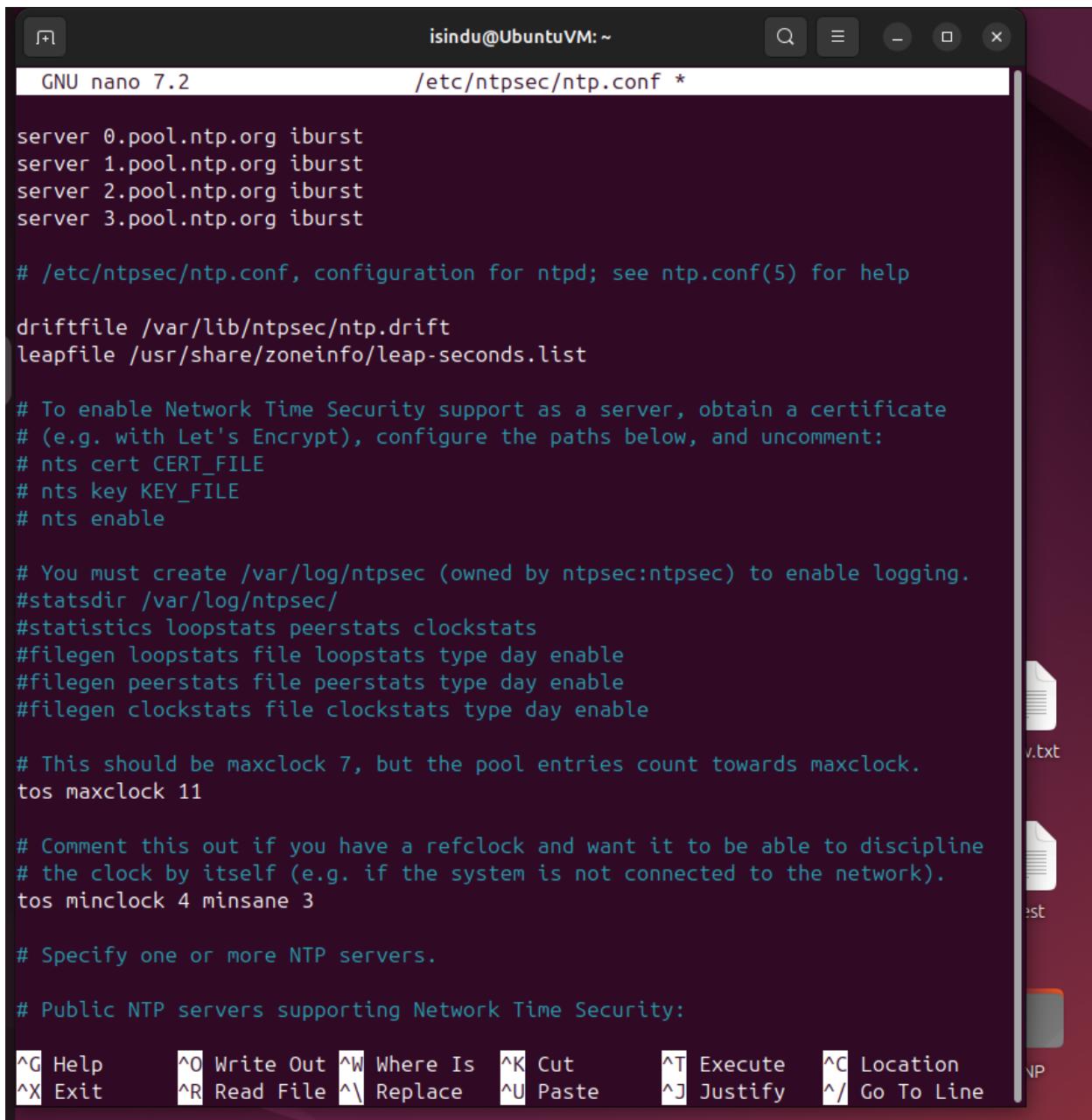
2.6) Installation and Configuration

Install the ntpsec package “sudo apt-get ins ntpsec” then verify the ins with “sudo systemctl status ntpsec”.



```
isindu@UbuntuVM:~$ sudo apt-get install ntpsec
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  certbot ntpsec-doc ntpsec-ntpviz
The following NEW packages will be installed:
  ntpsec
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 343 kB of archives.
After this operation, 883 kB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntpsec amd64 1.2.2+dfsg1-4build2 [343 kB]
Fetched 343 kB in 2s (204 kB/s)
Selecting previously unselected package ntpsec.
(Reading database ... 153242 files and directories currently installed.)
Preparing to unpack .../ntpsec_1.2.2+dfsg1-4build2_amd64.deb ...
Unpacking ntpsec (1.2.2+dfsg1-4build2) ...
Setting up ntpsec (1.2.2+dfsg1-4build2) ...
Created symlink /etc/systemd/system/timers.target.wants/ntpsec-rotate-stats.timer → /usr/lib/systemd/system/ntpsec-rotate-stats.timer.
Created symlink /etc/systemd/system/network-pre.target.wants/ntpsec-systemd-netif.path → /usr/lib/systemd/system/ntpsec-systemd-netif.path.
Created symlink /etc/systemd/system/ntp.service → /usr/lib/systemd/system/ntpsec.service.
Created symlink /etc/systemd/system/ntpd.service → /usr/lib/systemd/system/ntpsec.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ntpsec.service → /usr/lib/systemd/system/ntpsec.service.
Processing triggers for man-db (2.12.0-4build2) ...
isindu@UbuntuVM:~$ sudo systemctl status ntpsec
● ntpsec.service - Network Time Service
  Loaded: loaded (/usr/lib/systemd/system/ntpsec.service; enabled; preset: en>
  Active: active (running) since Sun 2024-10-06 17:15:29 +0530; 54s ago
    Docs: man:ntpd(8)
  Process: 4648 ExecStart=/usr/libexec/ntpsec/ntp-systemd-wrapper (code=exite>
 Main PID: 4651 (ntpd)
   Tasks: 1 (limit: 55001)
```

Open and edit the configuration file “sudo nano /etc/ntpsec/ntp.conf”



The screenshot shows a terminal window titled "isindu@UbuntuVM: ~" running the "GNU nano 7.2" editor. The file being edited is "/etc/ntpsec/ntp.conf". The content of the file is as follows:

```
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
server 3.pool.ntp.org iburst

# /etc/ntpsec/ntp.conf, configuration for ntpd; see ntp.conf(5) for help

driftfile /var/lib/ntpsec/ntp.drift
leapfile /usr/share/zoneinfo/leap-seconds.list

# To enable Network Time Security support as a server, obtain a certificate
# (e.g. with Let's Encrypt), configure the paths below, and uncomment:
# nts cert CERT_FILE
# nts key KEY_FILE
# nts enable

# You must create /var/log/ntpsec (owned by ntpsec:ntpsec) to enable logging.
#statsdir /var/log/ntpsec/
#statistics loopstats peerstats clockstats
#filegen loopstats file loopstats type day enable
#filegen peerstats file peerstats type day enable
#filegen clockstats file clockstats type day enable

# This should be maxclock 7, but the pool entries count towards maxclock.
tos maxclock 11

# Comment this out if you have a refclock and want it to be able to discipline
# the clock by itself (e.g. if the system is not connected to the network).
tos minclock 4 minsane 3

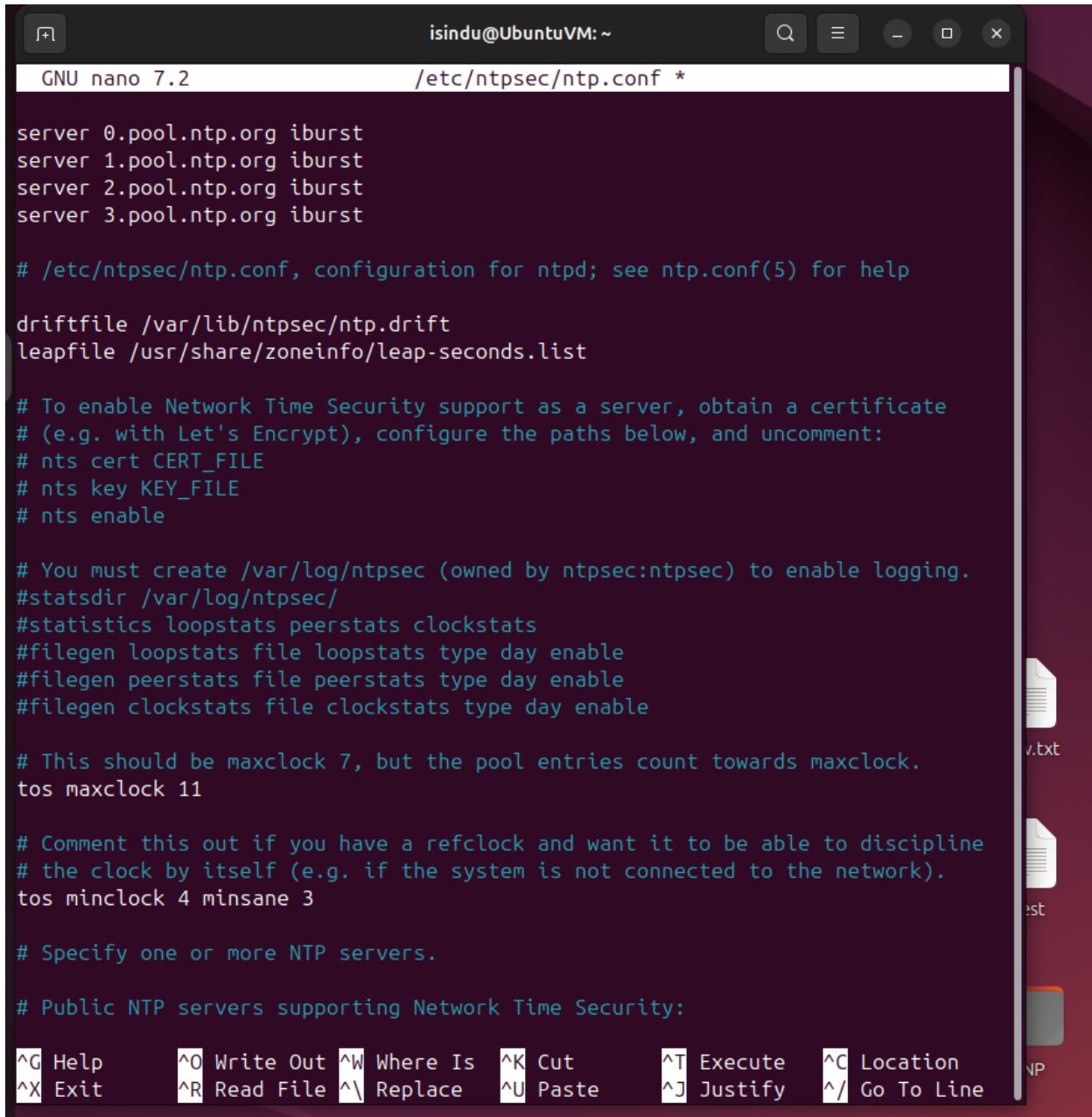
# Specify one or more NTP servers.

# Public NTP servers supporting Network Time Security:
```

At the bottom of the terminal window, there is a menu bar with the following options:

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^T Execute
- ^C Location
- ^X Exit
- ^R Read File
- ^\\ Replace
- ^U Paste
- ^J Justify
- ^/ Go To Line

Use “sudo systemctl start ntpsec” to start the service and “sudo systemctl enable ntpsec” to enable service start at boot. Check whether the service is running without any errors with “ sudo systemctl status ntpsec” and check if the NTP service is synchronizing with servers using “ntpq -p” command.



The screenshot shows a terminal window titled "isindu@UbuntuVM: ~" with the command "GNU nano 7.2" at the top. The file being edited is "/etc/ntpsec/ntp.conf *". The content of the file is as follows:

```
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
server 3.pool.ntp.org iburst

# /etc/ntpsec/ntp.conf, configuration for ntpd; see ntp.conf(5) for help

driftfile /var/lib/ntpsec/ntp.drift
leapfile /usr/share/zoneinfo/leap-seconds.list

# To enable Network Time Security support as a server, obtain a certificate
# (e.g. with Let's Encrypt), configure the paths below, and uncomment:
# nts cert CERT_FILE
# nts key KEY_FILE
# nts enable

# You must create /var/log/ntpsec (owned by ntpsec:ntpsec) to enable logging.
#statsdir /var/log/ntpsec/
#statistics loopstats peerstats clockstats
#filegen loopstats file loopstats type day enable
#filegen peerstats file peerstats type day enable
#filegen clockstats file clockstats type day enable

# This should be maxclock 7, but the pool entries count towards maxclock.
tos maxclock 11

# Comment this out if you have a refclock and want it to be able to discipline
# the clock by itself (e.g. if the system is not connected to the network).
tos minclock 4 minsane 3

# Specify one or more NTP servers.

# Public NTP servers supporting Network Time Security:
```

At the bottom of the terminal window, there is a menu of keyboard shortcuts:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^V Replace	^U Paste	^J Justify	/ Go To Line

3. Shell Scripting and Security

3.1) Shell Scripting

- i. Script to automate a report that captures system details every day.

Create a script file named system_report.sh and edit it using nano.

“nano system_report.sh”

Then Write the following script

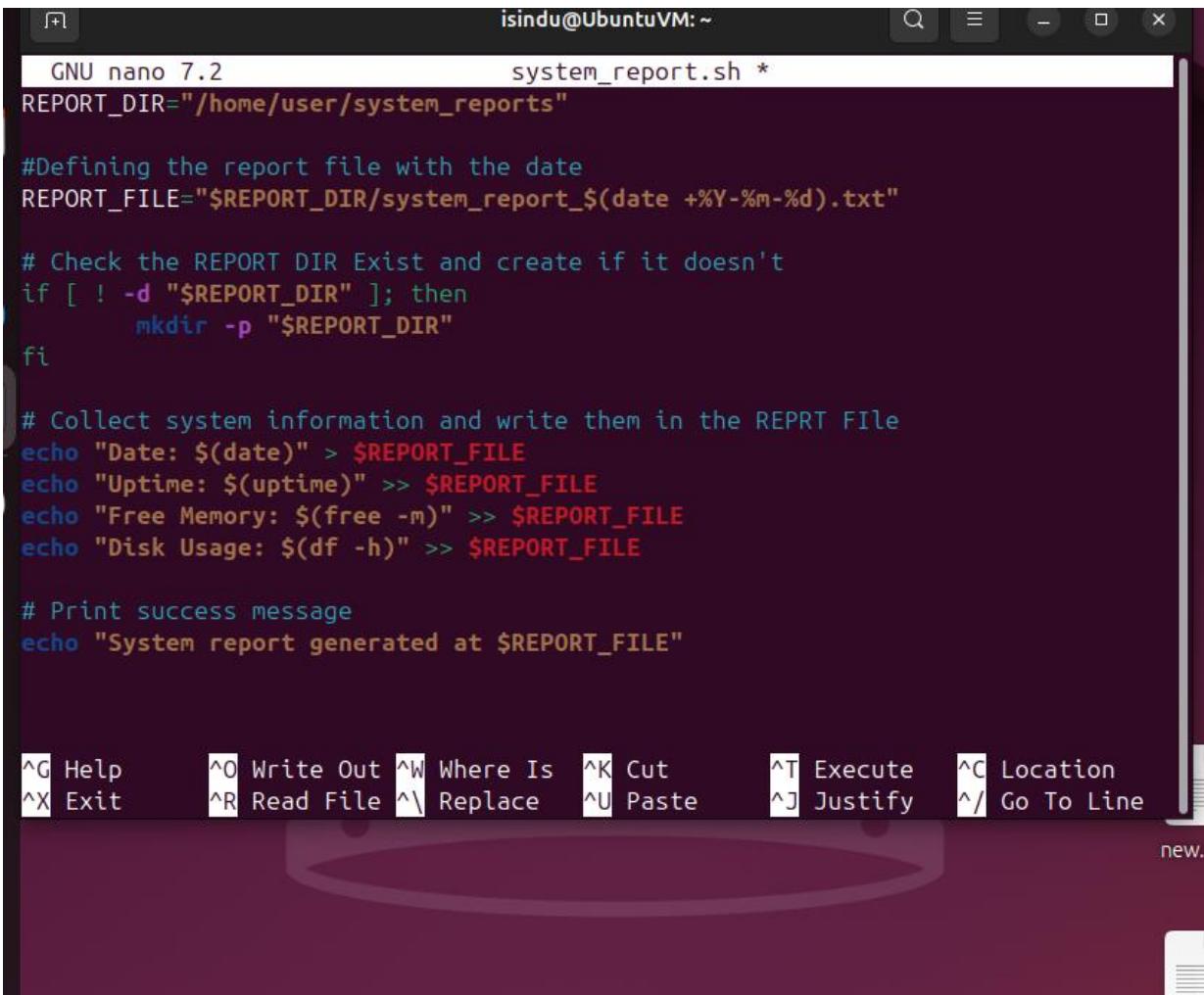
```
REPORT_DIR="/home/isindu/system_reports"

#Defining the report file with the date
REPORT_FILE="$REPORT_DIR/system_report_$(date +%Y-%m-%d).txt"

# Check the REPORT DIR Exist and create if it doesn't
if [ ! -d "$REPORT_DIR" ]; then
    mkdir -p "$REPORT_DIR"
fi

# Collect system information and write them in the REPRT FIle
echo "Date: $(date)" > $REPORT_FILE
echo "Uptime: $(uptime)" >> $REPORT_FILE
echo "Free Memory: $(free -m)" >> $REPORT_FILE
echo "Disk Usage: $(df -h)" >> $REPORT_FILE

# Print success message
echo "System report generated at $REPORT_FILE"
```



```
isindu@UbuntuVM:~$ nano 7.2 system_report.sh *
REPORT_DIR="/home/user/system_reports"

#Defining the report file with the date
REPORT_FILE="$REPORT_DIR/system_report_$(date +%Y-%m-%d).txt"

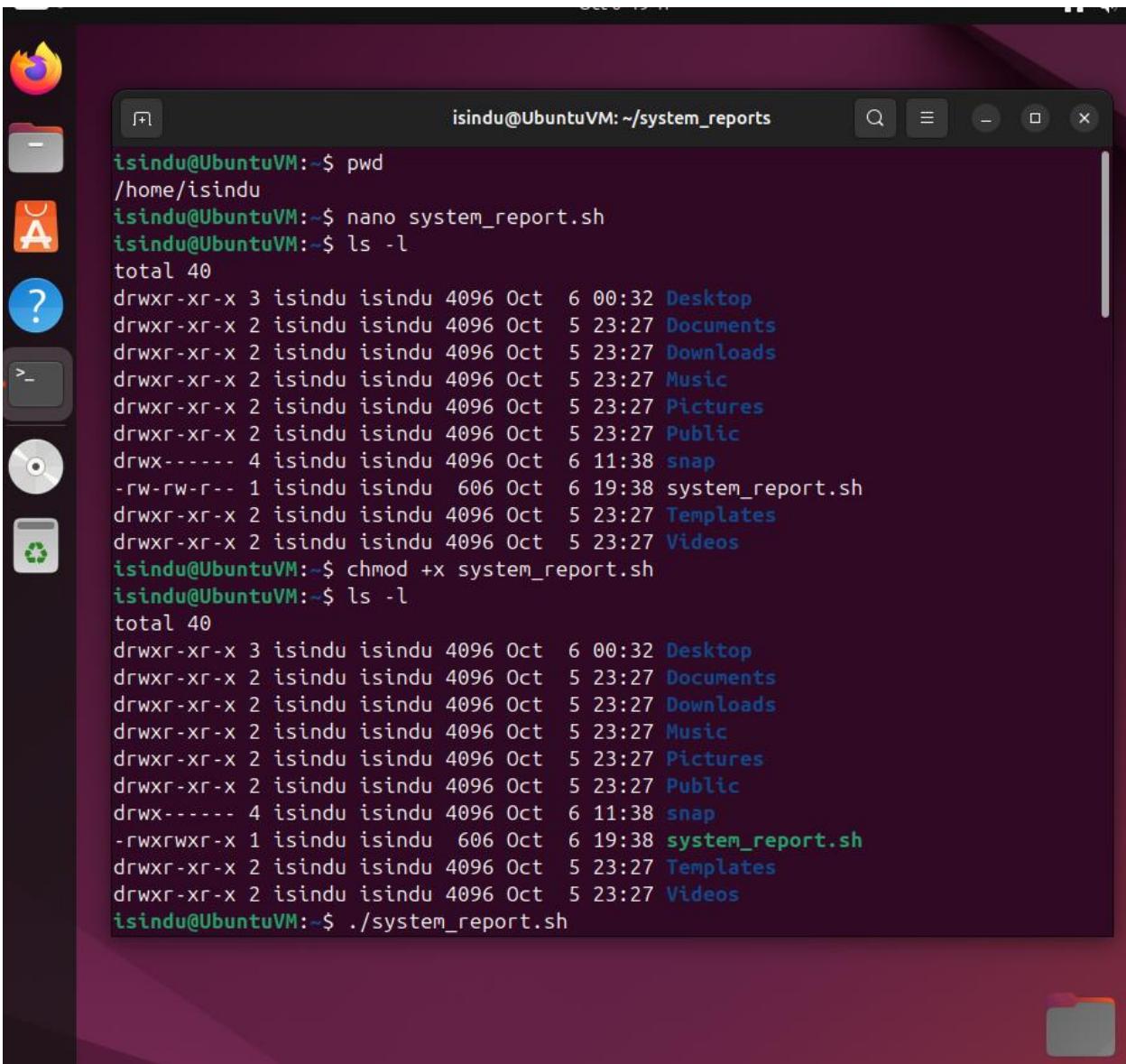
# Check the REPORT DIR Exist and create if it doesn't
if [ ! -d "$REPORT_DIR" ]; then
    mkdir -p "$REPORT_DIR"
fi

# Collect system information and write them in the REPRT FILE
echo "Date: $(date)" > $REPORT_FILE
echo "Uptime: $(uptime)" >> $REPORT_FILE
echo "Free Memory: $(free -m)" >> $REPORT_FILE
echo "Disk Usage: $(df -h)" >> $REPORT_FILE

# Print success message
echo "System report generated at $REPORT_FILE"

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line
```

Make the script executable with “chmod +x system_report.sh”



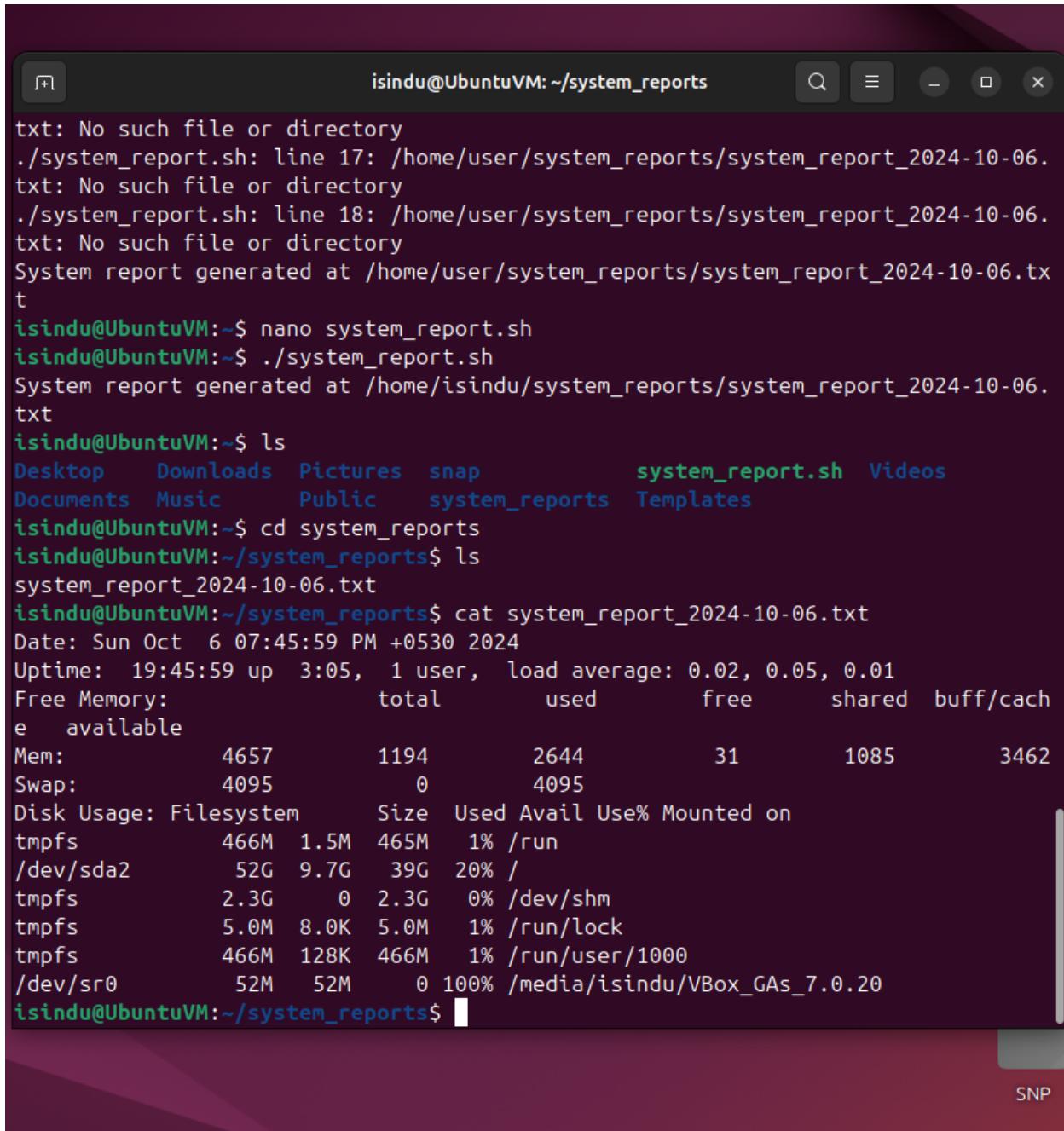
A screenshot of a Ubuntu desktop environment. On the left is a dock with icons for the Dash, Home, Applications, and Files. A terminal window is open in the center, showing the following command-line session:

```
isindu@UbuntuVM:~/system_reports$ pwd
/home/isindu
isindu@UbuntuVM:~$ nano system_report.sh
isindu@UbuntuVM:~$ ls -l
total 40
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
-rw-rw-r-- 1 isindu isindu 606 Oct  6 19:38 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$ chmod +x system_report.sh
isindu@UbuntuVM:~$ ls -l
total 40
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
-rwxrwxr-x 1 isindu isindu 606 Oct  6 19:38 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$ ./system_report.sh
```

Test the script by running it manually. “./system_report.sh”

```
isindu@UbuntuVM:~$ ls -l
total 40
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
-rwxrwxr-x 1 isindu isindu 606 Oct  6 19:38 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$ ./system_report.sh
mkdir: cannot create directory '/home/user': Permission denied
./system_report.sh: line 15: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
./system_report.sh: line 16: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
./system_report.sh: line 17: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
./system_report.sh: line 18: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
System report generated at /home/user/system_reports/system_report_2024-10-06.tx
t
isindu@UbuntuVM:~$ nano system_report.sh
isindu@UbuntuVM:~$ ./system_report.sh
System report generated at /home/isindu/system_reports/system_report_2024-10-06.
txt
isindu@UbuntuVM:~$ ls
Desktop  Downloads  Pictures  snap          system_report.sh  Videos
Documents  Music    Public    system_reports  Templates
isindu@UbuntuVM:~$ cd system_reports
```

Read and check the contents of the file with “cat /system_reports/ system_report_2024-10-06.txt”



The screenshot shows a terminal window titled "isindu@UbuntuVM: ~/system_reports". The terminal displays the following command-line session:

```
txt: No such file or directory
./system_report.sh: line 17: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
./system_report.sh: line 18: /home/user/system_reports/system_report_2024-10-06.
txt: No such file or directory
System report generated at /home/user/system_reports/system_report_2024-10-06.txt
isindu@UbuntuVM:~$ nano system_report.sh
isindu@UbuntuVM:~$ ./system_report.sh
System report generated at /home/isindu/system_reports/system_report_2024-10-06.txt
isindu@UbuntuVM:~$ ls
Desktop  Downloads  Pictures  snap      system_report.sh  Videos
Documents  Music    Public    system_reports  Templates
isindu@UbuntuVM:~$ cd system_reports
isindu@UbuntuVM:~/system_reports$ ls
system_report_2024-10-06.txt
isindu@UbuntuVM:~/system_reports$ cat system_report_2024-10-06.txt
Date: Sun Oct  6 07:45:59 PM +0530 2024
Uptime: 19:45:59 up 3:05, 1 user, load average: 0.02, 0.05, 0.01
Free Memory: total        used        free        shared   buff/cach
e available
Mem:       4657          1194         2644          31        1085        3462
Swap:      4095            0          4095
Disk Usage: Filesystem      Size  Used Avail Use% Mounted on
tmpfs        466M  1.5M  465M   1% /run
/dev/sda2     52G  9.7G  39G  20% /
tmpfs        2.3G    0    2.3G   0% /dev/shm
tmpfs        5.0M  8.0K  5.0M   1% /run/lock
tmpfs        466M  128K  466M   1% /run/user/1000
/dev/sr0       52M   52M    0 100% /media/isindu/VBox_GAs_7.0.20
isindu@UbuntuVM:~/system_reports$
```

This report contains current date, system uptime, number of users, Memory details, disk usage etc.

To automate the script open the crontab file. “crontab -e” and select a editor. Following command tells cron to run the script at 8.00 AM everyday.

```
0 8 * * * /home/isindy/system_report.sh
```

The screenshot shows a terminal window titled "isindu@UbuntuVM: ~/system_reports". The user runs several commands to generate a system report and then edit the crontab:

```
isindu@UbuntuVM:~$ cd system_reports
isindu@UbuntuVM:~/system_reports$ ls
system_report_2024-10-06.txt
isindu@UbuntuVM:~/system_reports$ cat system_report_2024-10-06.txt
Date: Sun Oct 6 07:45:59 PM +0530 2024
Uptime: 19:45:59 up 3:05, 1 user, load average: 0.02, 0.05, 0.01
Free Memory: total used free shared buff/cach
e available
Mem: 4657 1194 2644 31 1085 3462
Swap: 4095 0 4095
Disk Usage: Filesystem Size Used Avail Use% Mounted on
tmpfs 466M 1.5M 465M 1% /run
/dev/sda2 52G 9.7G 39G 20% /
tmpfs 2.3G 0 2.3G 0% /dev/shm
tmpfs 5.0M 8.0K 5.0M 1% /run/lock
tmpfs 466M 128K 466M 1% /run/user/1000
/dev/sr0 52M 52M 0 100% /media/isindu/VBox_GAs_7.0.20
isindu@UbuntuVM:~/system_reports$ crontab -e
no crontab for isindu - using an empty one

Select an editor. To change later, run 'select-editor'.
1. /bin/nano      <---- easiest
2. /usr/bin/vim.basic
3. /usr/bin/vim.tiny
4. /bin/ed

Choose 1-4 [1]: 1
No modification made
isindu@UbuntuVM:~/system_reports$ crontab -e
no crontab for isindu - using an empty one
crontab: installing new crontab
isindu@UbuntuVM:~/system_reports$
```

Oct 8 20:02

The screenshot shows a terminal window titled "isindu@UbuntuVM: ~/system_reports". The window contains the crontab file, which is a configuration file for cron. The file includes comments explaining the syntax and fields, and a specific command to run a script every minute. The bottom of the window shows the nano editor's command key mappings.

```
GNU nano 7.2          /tmp/crontab.5plcBU/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# 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 timezones.
#
# 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 8 * * * /home/isindy/system_report.sh
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

SNP

ii. Script to automate the backup of the Documents directory

Create and edit a script file named backup_script.sh using nano.

“nano backup_script.sh”

Insert the following script and save the file.

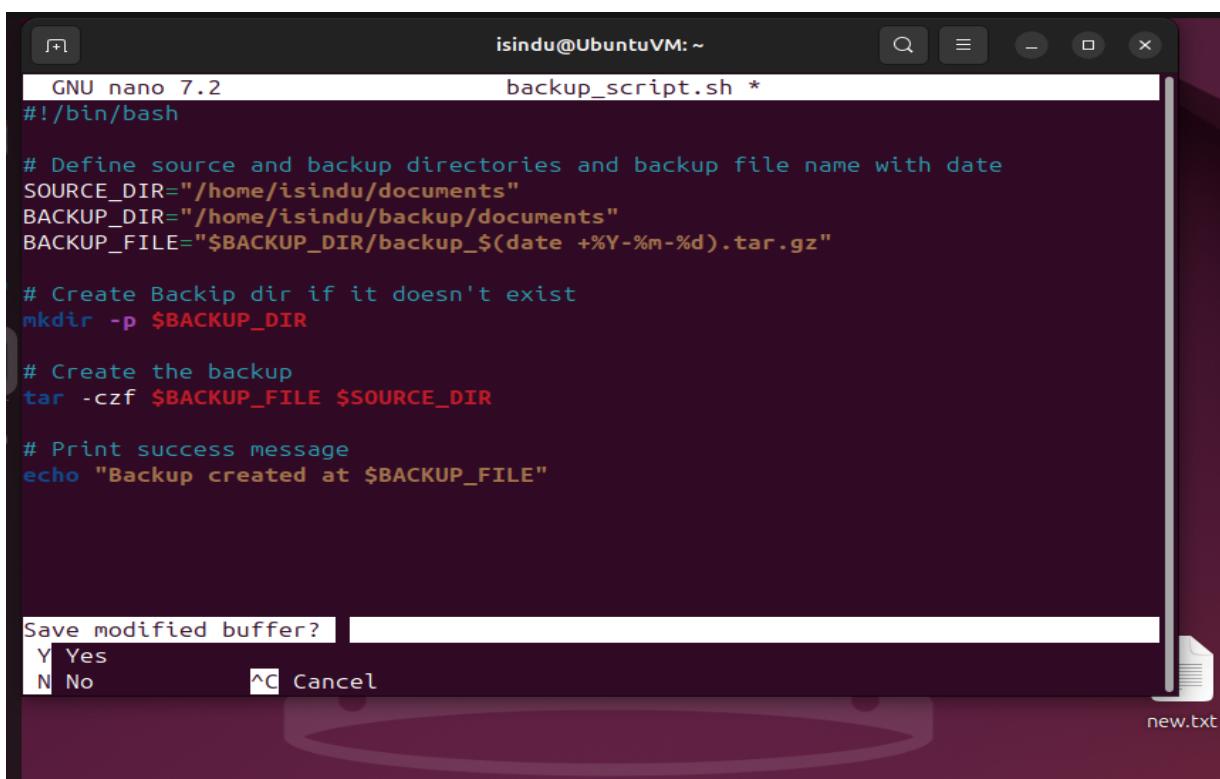
```
#!/bin/bash

# Define source and backup directories and backup file name with date
SOURCE_DIR="/home/isindu/Documents"
BACKUP_DIR="/home/isindu/backup/Documents"
BACKUP_FILE="$BACKUP_DIR/backup_$(date +%Y-%m-%d).tar.gz"

# Create Backup dir if it doesn't exist
mkdir -p $BACKUP_DIR

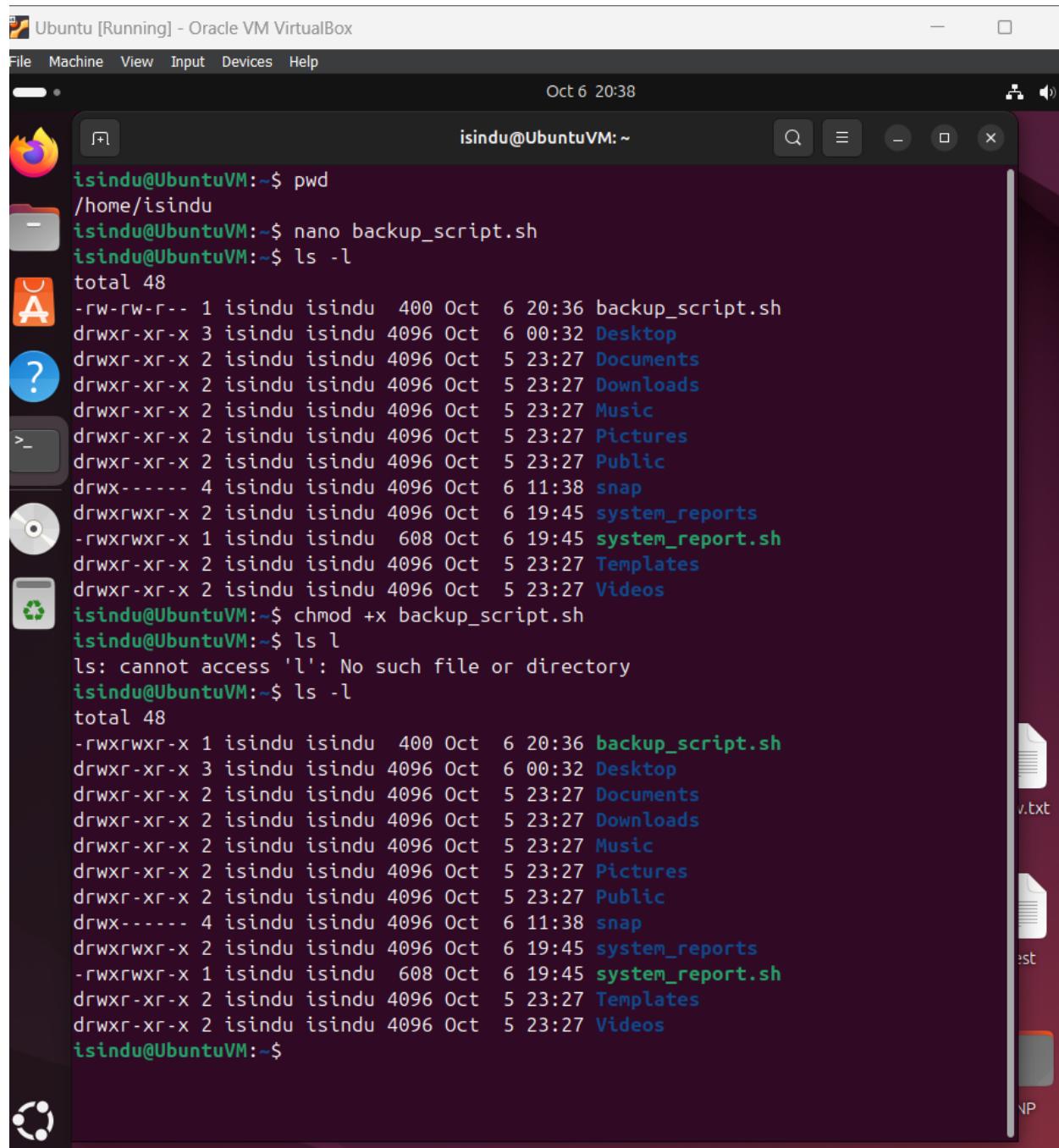
# Create the backup
tar -czf $BACKUP_FILE $SOURCE_DIR

# Print success message
echo "Backup created at $BACKUP_FILE"
```



Make the script executable.

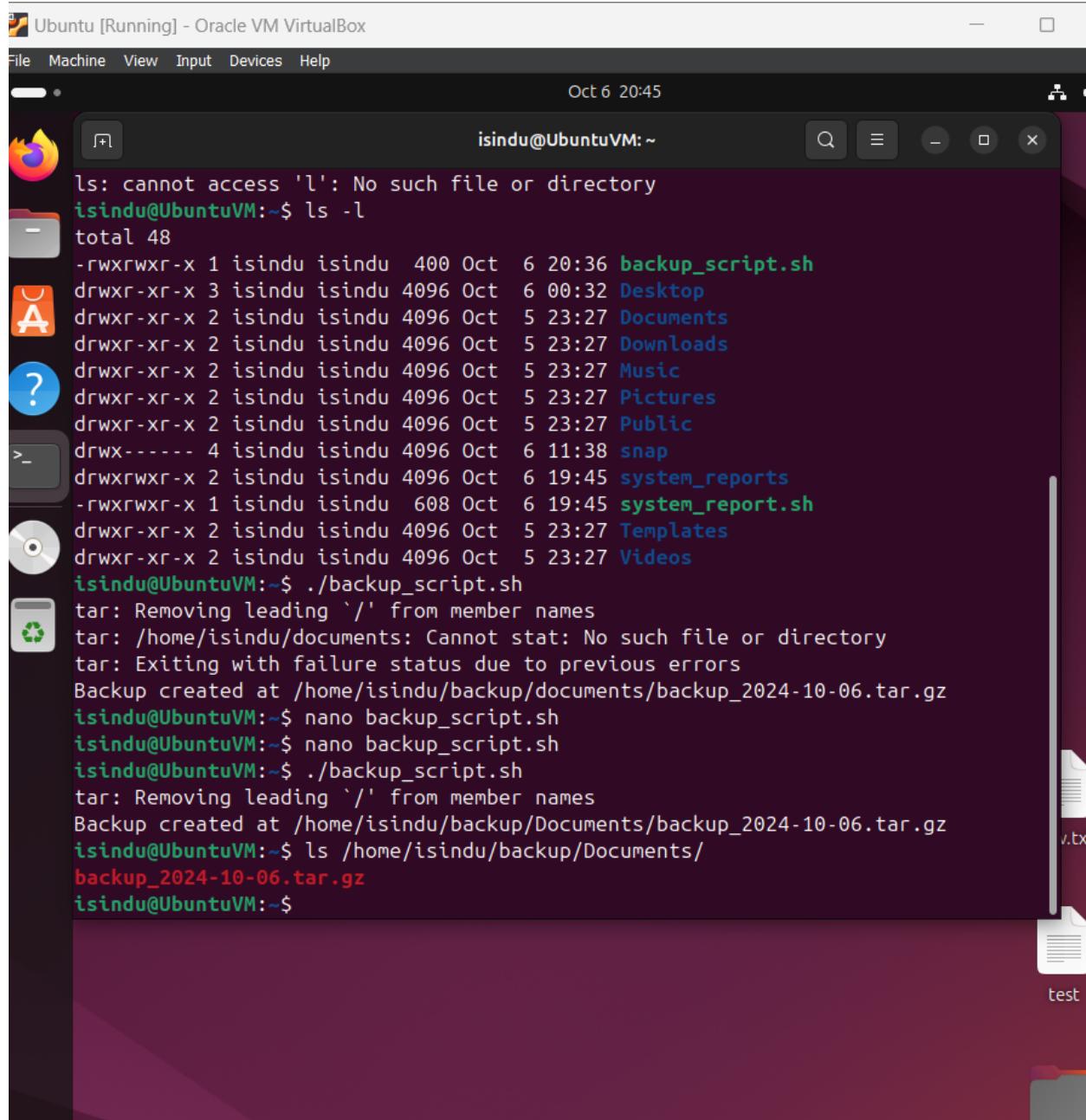
“Chmod +x backup_script.sh”



The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
isindu@UbuntuVM:~$ pwd
/home/isindu
isindu@UbuntuVM:~$ nano backup_script.sh
isindu@UbuntuVM:~$ ls -l
total 48
-rw-rw-r-- 1 isindu isindu 400 Oct  6 20:36 backup_script.sh
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
drwxrwxr-x 2 isindu isindu 4096 Oct  6 19:45 system_reports
-rwxrwxr-x 1 isindu isindu 608 Oct  6 19:45 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$ chmod +x backup_script.sh
isindu@UbuntuVM:~$ ls l
ls: cannot access 'l': No such file or directory
isindu@UbuntuVM:~$ ls -l
total 48
-rwxrwxr-x 1 isindu isindu 400 Oct  6 20:36 backup_script.sh
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
drwxrwxr-x 2 isindu isindu 4096 Oct  6 19:45 system_reports
-rwxrwxr-x 1 isindu isindu 608 Oct  6 19:45 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$
```

Run the script manually to check whether its work.
“backup_script.sh”



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "isindu@UbuntuVM: ~". The terminal content shows the execution of a backup script:

```
ls: cannot access 'l': No such file or directory
isindu@UbuntuVM:~$ ls -l
total 48
-rwxrwxr-x 1 isindu isindu 400 Oct  6 20:36 backup_script.sh
drwxr-xr-x 3 isindu isindu 4096 Oct  6 00:32 Desktop
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Documents
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Downloads
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Music
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Pictures
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Public
drwx----- 4 isindu isindu 4096 Oct  6 11:38 snap
drwxrwxr-x 2 isindu isindu 4096 Oct  6 19:45 system_reports
-rwxrwxr-x 1 isindu isindu 608 Oct  6 19:45 system_report.sh
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Templates
drwxr-xr-x 2 isindu isindu 4096 Oct  5 23:27 Videos
isindu@UbuntuVM:~$ ./backup_script.sh
tar: Removing leading '/' from member names
tar: /home/isindu/documents: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
Backup created at /home/isindu/backup/documents/backup_2024-10-06.tar.gz
isindu@UbuntuVM:~$ nano backup_script.sh
isindu@UbuntuVM:~$ nano backup_script.sh
isindu@UbuntuVM:~$ ./backup_script.sh
tar: Removing leading '/' from member names
Backup created at /home/isindu/backup/Documents/backup_2024-10-06.tar.gz
isindu@UbuntuVM:~$ ls /home/isindu/backup/Documents/
backup_2024-10-06.tar.gz
isindu@UbuntuVM:~$
```

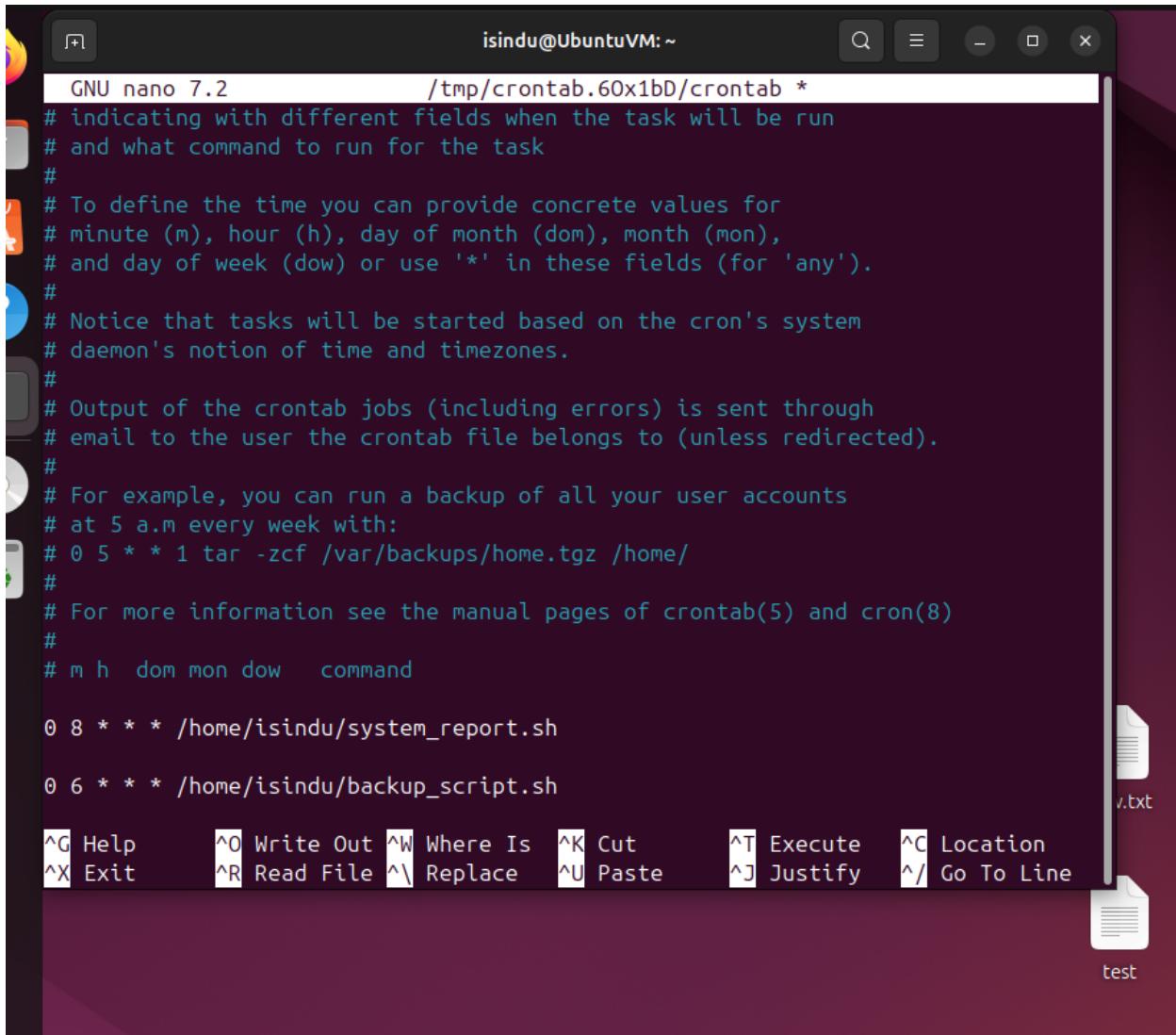
If you got the successful message check the Documents directory for the backup file.

To automate the backup script, open Crontab file.

“Crontab -e”

Edit and add Cron job to run the script periodically.

```
0 6 * * * /home/isindu/backup_script.sh
```



```
GNU nano 7.2          /tmp/crontab.60x1bD/crontab *
# indicating with different fields when the task will be run
# and what command to run for the task
#
# 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 timezones.
#
# 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 8 * * * /home/isindu/system_report.sh

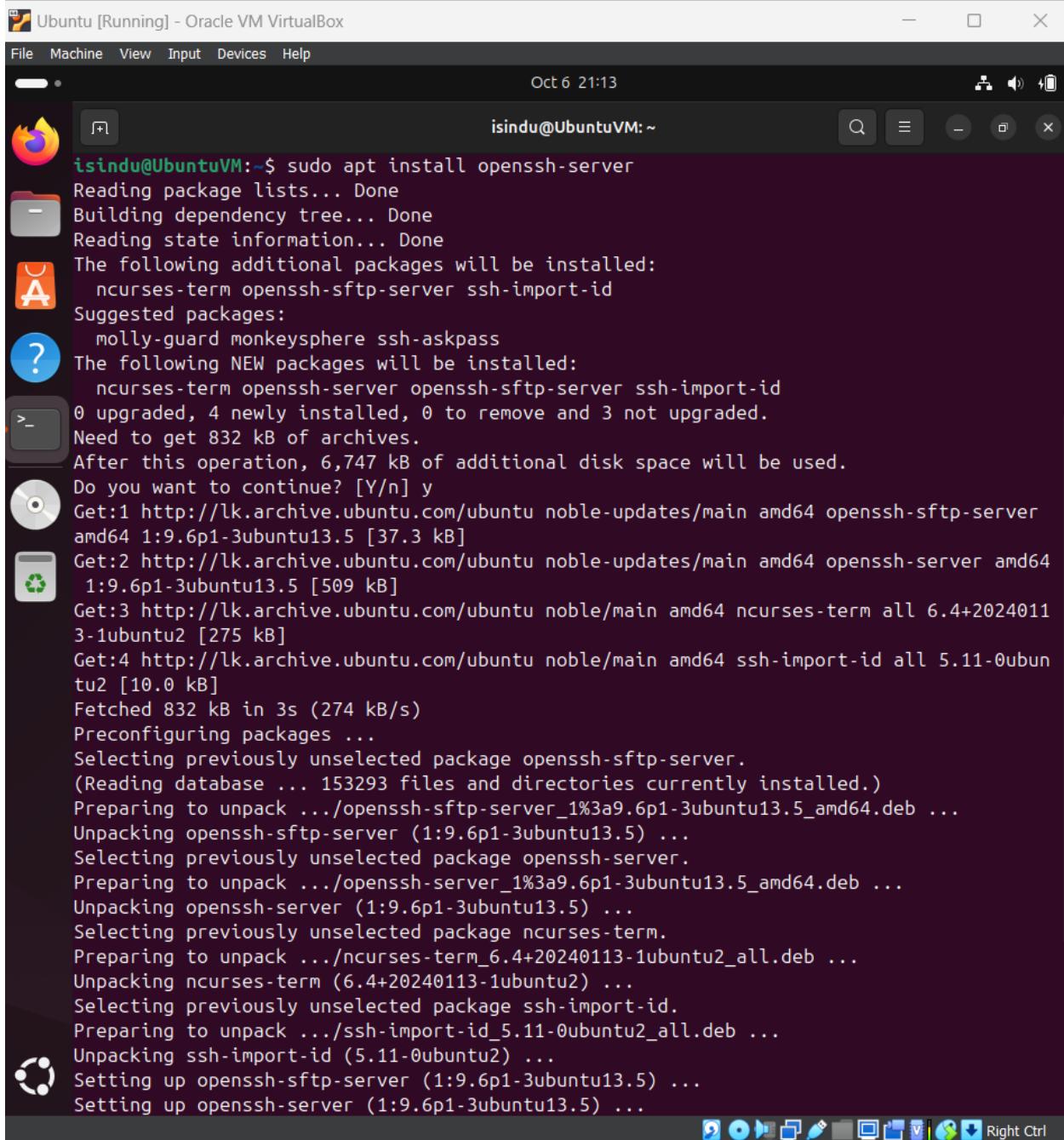
0 6 * * * /home/isindu/backup_script.sh
```

This tells Cron to run the script every day at 6.00 am

3.2) SSH (Secure Shell)

Install the ssh server.

“sudo apt install openssh-server”



```
isindu@UbuntuVM:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 3 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,747 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.5 [37.3 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.5 [509 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 ssh-import-id all 5.11-0ubuntu2 [10.0 kB]
Fetched 832 kB in 3s (274 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 153293 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.6p1-3ubuntu13.5_amd64.deb ...
Unpacking openssh-sftp-server (1:9.6p1-3ubuntu13.5) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.6p1-3ubuntu13.5_amd64.deb ...
Unpacking openssh-server (1:9.6p1-3ubuntu13.5) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.4+20240113-1ubuntu2_all.deb ...
Unpacking ncurses-term (6.4+20240113-1ubuntu2) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu2_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu2) ...
Setting up openssh-sftp-server (1:9.6p1-3ubuntu13.5) ...
Setting up openssh-server (1:9.6p1-3ubuntu13.5) ...
```

After installation start the SSH service with following command.

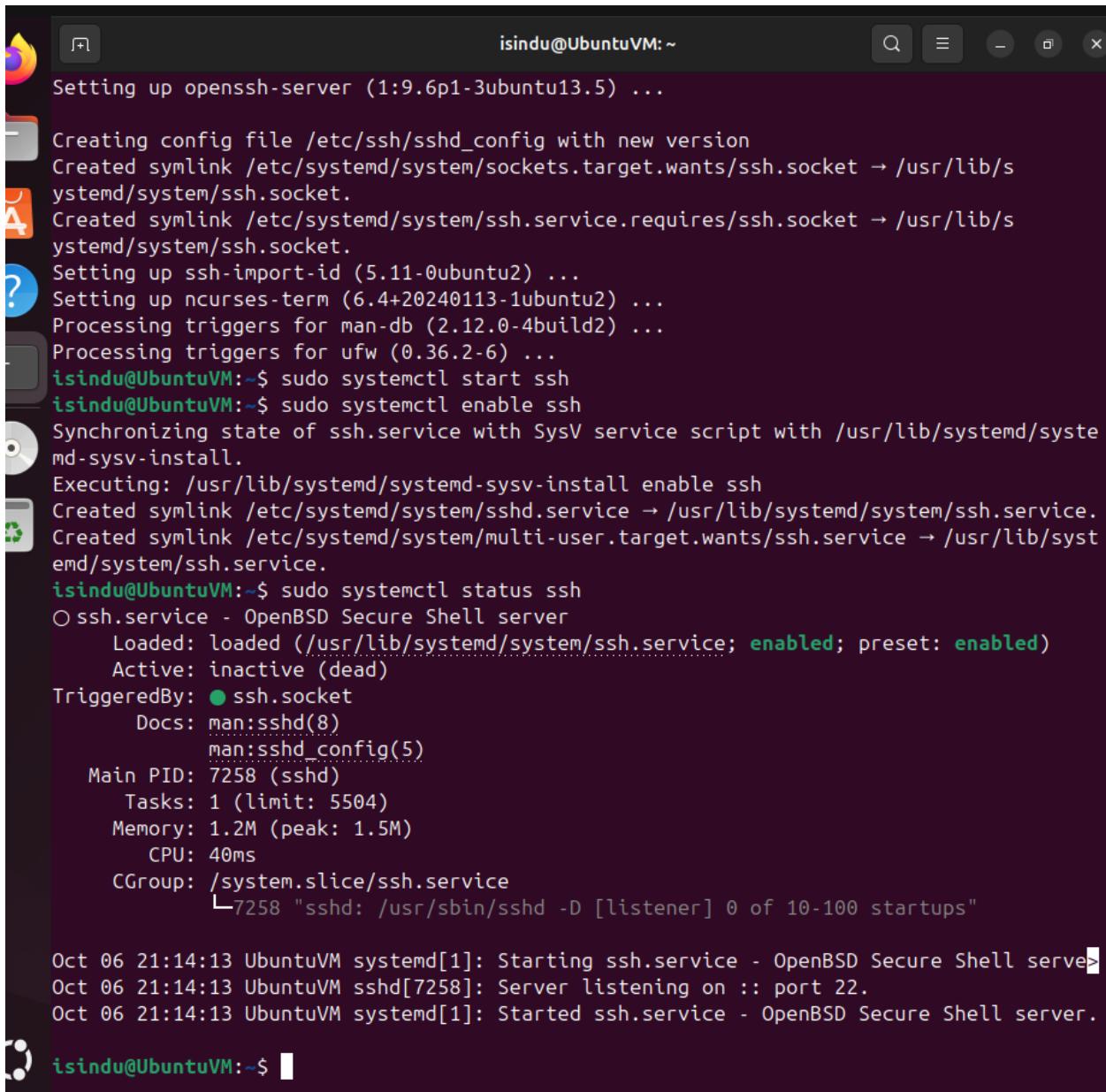
“sudo systemctl start ssh”

Make the service auto start at boot.

“sudo systemctl enable ssh”

Check the status of the system.

“sudo systemctl status ssh”



```
isindu@UbuntuVM: ~
Setting up openssh-server (1:9.6p1-3ubuntu13.5) ...
Creating config file /etc/ssh/sshd_config with new version
Created symlink /etc/systemd/system/sockets.target.wants/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Created symlink /etc/systemd/system/ssh.service.requires/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Setting up ssh-import-id (5.11-0ubuntu2) ...
Setting up ncurses-term (6.4+20240113-1ubuntu2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for ufw (0.36.2-6) ...
isindu@UbuntuVM:~$ sudo systemctl start ssh
isindu@UbuntuVM:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
isindu@UbuntuVM:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
      Active: inactive (dead)
 TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
              man:sshd_config(5)
     Main PID: 7258 (sshd)
        Tasks: 1 (limit: 5504)
      Memory: 1.2M (peak: 1.5M)
         CPU: 40ms
      CGroup: /system.slice/ssh.service
              └─7258 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 06 21:14:13 UbuntuVM systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 06 21:14:13 UbuntuVM sshd[7258]: Server listening on :: port 22.
Oct 06 21:14:13 UbuntuVM systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

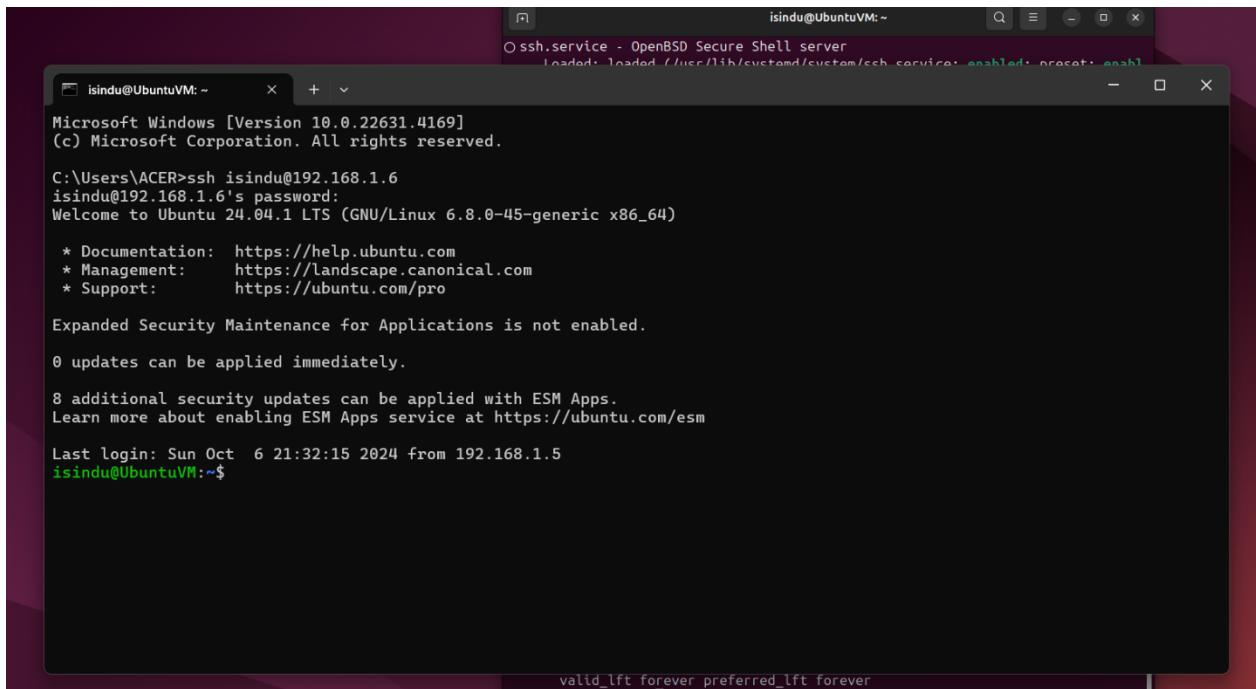
isindu@UbuntuVM:~$
```

Find the ip address of the virtual machine.

“ip a”

```
isindu@UbuntuVM:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
  qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
      inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
      inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
  qlen 1000
    link/ether 08:00:27:ef:cf:90 brd ff:ff:ff:ff:ff:ff
      inet 192.168.1.6/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 71290sec preferred_lft 71290sec
      inet6 fe80::a00:27ff:feef:cf90/64 scope link
        valid_lft forever preferred_lft forever
isindu@UbuntuVM:~$
```

Then use the client computer’s terminal and enter “ssh isindu@192.168.1.6” to connect to the virtual machine.



3.3) Iptables and ACLs

i. Web Sever Security

Install iptables

“Sudo apt install iptables”

Set default policies

“sudo iptables -P INPUT DROP”

“sudo iptables -P FORWARD DROP”

“sudo iptables -P OUTPUT ACCEPT”

Allow incoming traffic on port 80 (HTTP)

“sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT”

Allow incoming traffic on port 443 (HTTP)

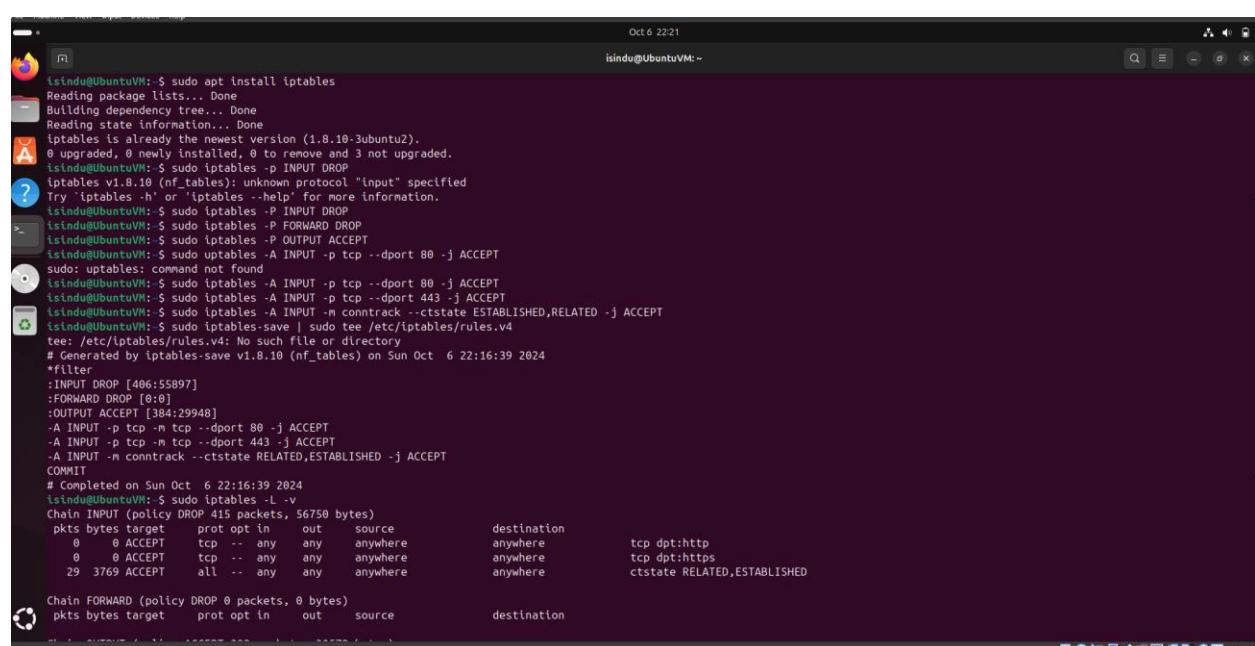
“sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT”

Allow established and related connections

“sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT”

Save set rules.

“sudo iptables-save | sudo tee /etc/iptables/rules.v4”

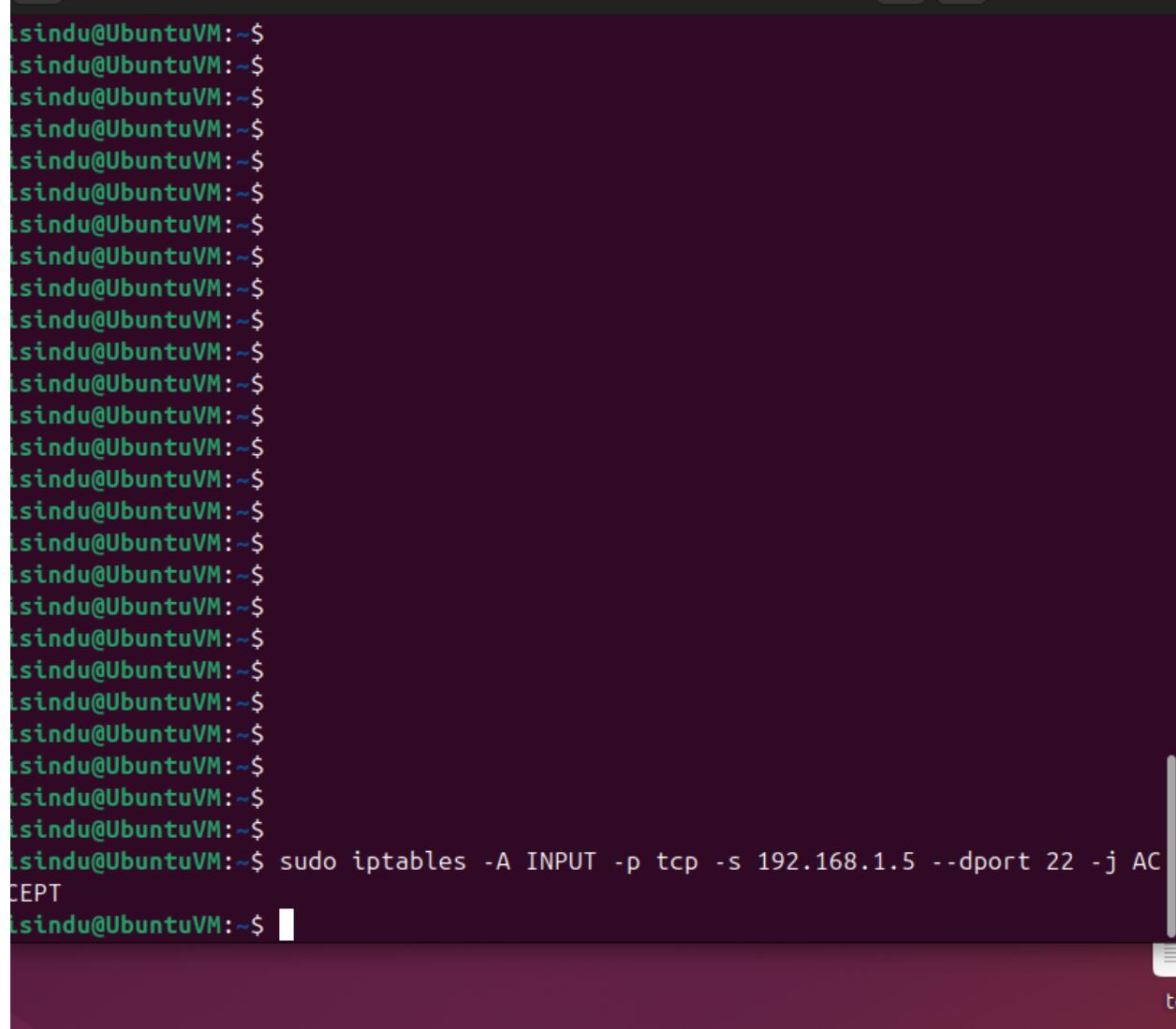


```
lsindu@UbuntuVM:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
lsindu@UbuntuVM:~$ sudo iptables -P INPUT DROP
iptables v1.8.10 (nf_tables): unknown protocol "input" specified
Try 'iptables -h' or 'iptables --help' for more information.
lsindu@UbuntuVM:~$ sudo iptables -P INPUT DROP
lsindu@UbuntuVM:~$ sudo iptables -P FORWARD DROP
lsindu@UbuntuVM:~$ sudo iptables -P OUTPUT ACCEPT
lsindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo: iptables: command not found
lsindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
lsindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
lsindu@UbuntuVM:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
lsindu@UbuntuVM:~$ sudo iptables-save | sudo tee /etc/iptables/rules.v4
tee: /etc/iptables/rules.v4: No such file or directory
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Oct 6 22:16:39 2024
*filter
:INPUT DROP [406:55897]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [384:29948]
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Sun Oct 6 22:16:39 2024
lsindu@UbuntuVM:~$ sudo iptables -L -v
Chain INPUT (policy DROP 415 packets, 56750 bytes)
 pkts bytes target  prot opt in     out    source               destination
      0     0 ACCEPT   tcp  --  any    any   anywhere             anywhere
      0     0 ACCEPT   tcp  --  any    any   anywhere             anywhere
      29  3769 ACCEPT  all  --  any    any   anywhere             anywhere
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target  prot opt in     out    source               destination
```

ii. Remote Administration Access

Use the following command to ALLOW SSH access (port 22) only from 192.168.1.5 used for administration.

“sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 22 -j ACCEPT”

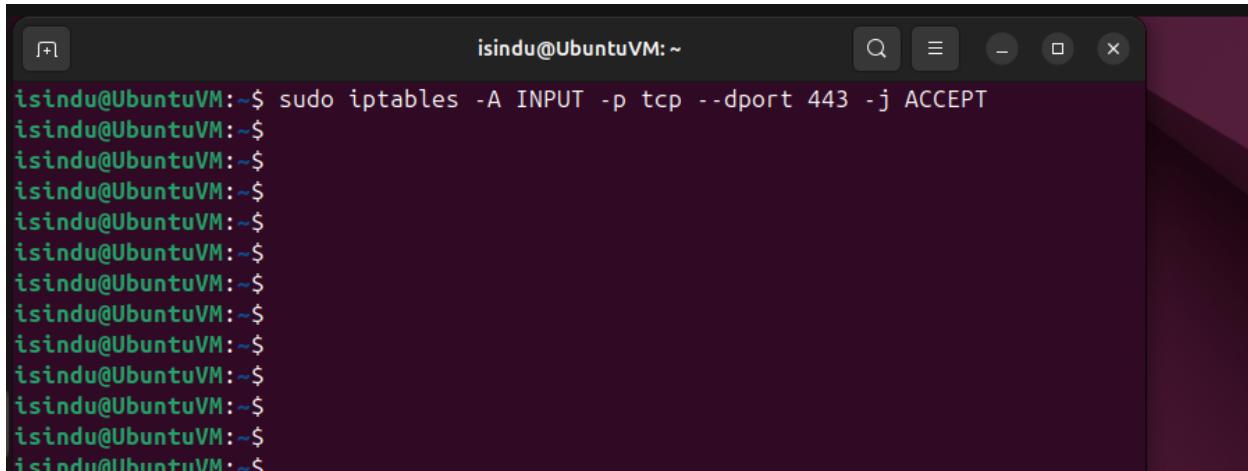


The screenshot shows a terminal window with a dark background and light-colored text. The text is a series of identical entries starting with 'lsindu@UbuntuVM:~\$' followed by a blank line. At the bottom of the window, the command 'sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 22 -j ACCEPT' is typed, and the text 'ACCEPT' is visible, indicating the command was successfully executed. The terminal window has a scroll bar on the right side.

iii. Allow Specific Application

Use the following command to allow specific application.

“sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT”

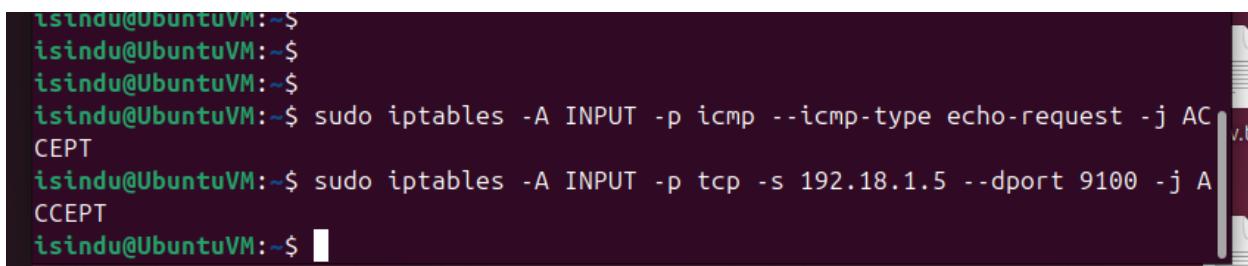


```
isindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
isindu@UbuntuVM:~$
```

iv. Allow Pings (ICMP Echo Requests)

Use the following commands to allow ping request (ICMP Echo Request)

“sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT”

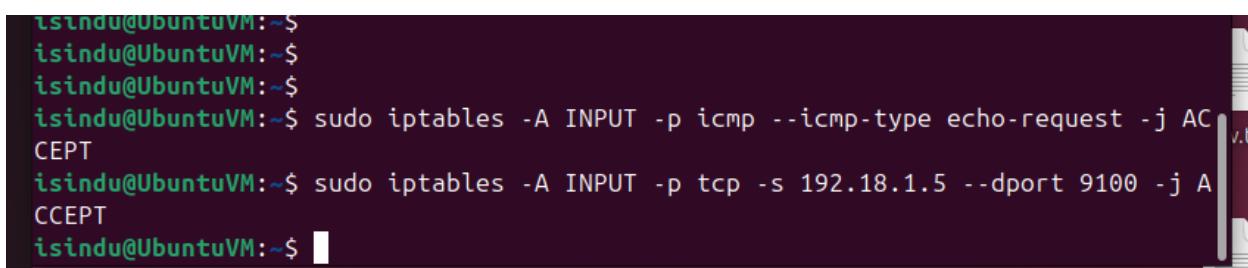


```
isindu@UbuntuVM:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
isindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 9100 -j ACCEPT
isindu@UbuntuVM:~$
```

v. Printer Server Access

Use the following command to allow printing traffic only from 192.168.1.5

“sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 9100 -j ACCEPT”



```
isindu@UbuntuVM:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
isindu@UbuntuVM:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 9100 -j ACCEPT
isindu@UbuntuVM:~$
```

```
isindu@UbuntuVM:~$ sudo iptables -L
[sudo] password for isindu:
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT    tcp  --  anywhere        anywhere       tcp dpt:http
ACCEPT    tcp  --  anywhere        anywhere       tcp dpt:https
ACCEPT    all  --  anywhere        anywhere      ctstate RELATED,ESTABLISH
ED
ACCEPT    tcp  --  192.168.1.5    anywhere       tcp dpt:ssh
ACCEPT    tcp  --  anywhere        anywhere       tcp dpt:https
ACCEPT    icmp --  anywhere       anywhere      icmp echo-request
ACCEPT    tcp  --  192.18.1.5    anywhere       tcp dpt:9100

Chain FORWARD (policy DROP)
target     prot opt source          destination

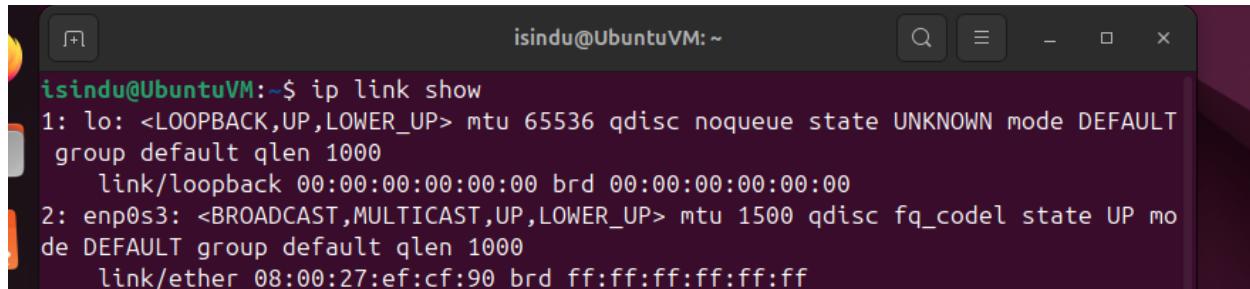
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
isindu@UbuntuVM:~$
```

4. Best Practices

1) Disable Unnecessary Network Interfaces

Some of the interfaces that comes with the system may not be required. Leaving unused interfaces active can expose the system to unnecessary risk.

“ip link show” command lists out the interfaces in the system.



```
isindu@UbuntuVM:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:ef:cf:90 brd ff:ff:ff:ff:ff:ff
```

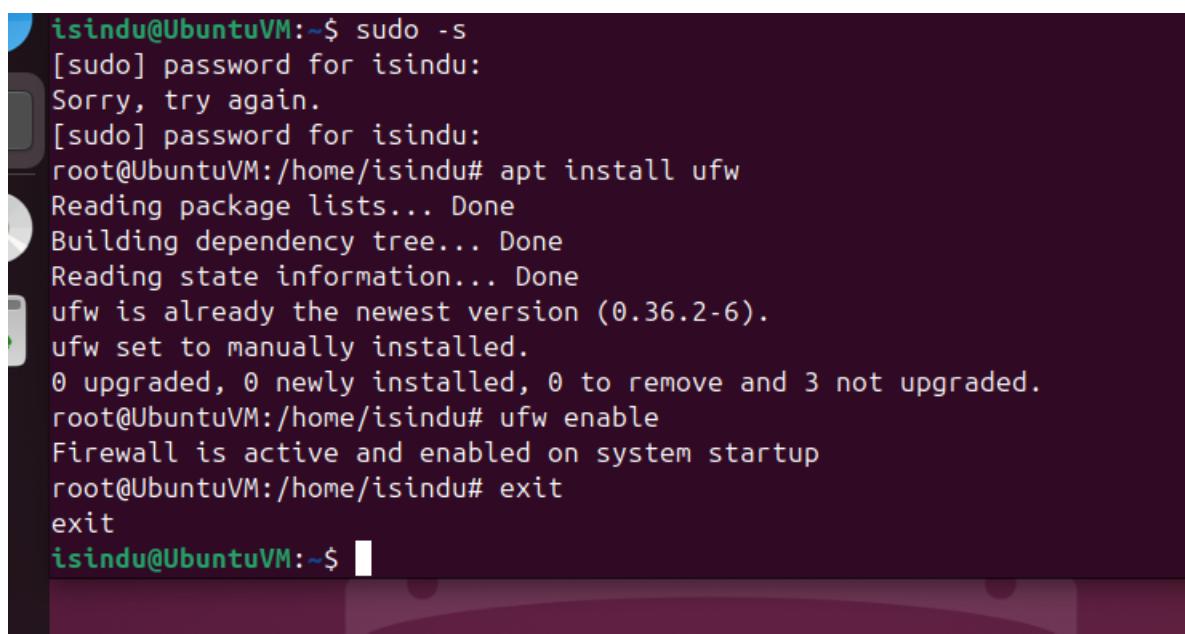
Use “sudo ip link set [interface] down” to disable unnecessary interfaces. (I do not have any unnecessary interfaces)

2) Enable and configure firewall

Configured firewall controls the flow of traffic to the system and from the system which will help to prevent the system.

To install and enable firewall use

“apt install ufw” and “ufw enable” commands



```
isindu@UbuntuVM:~$ sudo -s
[sudo] password for isindu:
Sorry, try again.
[sudo] password for isindu:
root@UbuntuVM:/home/isindu# apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@UbuntuVM:/home/isindu# ufw enable
Firewall is active and enabled on system startup
root@UbuntuVM:/home/isindu# exit
exit
isindu@UbuntuVM:~$
```

You can configure firewall using iptables rules.

3) Disable IP Forwarding

IP forwarding is the process of forwarding packets between different network interfaces. It is unnecessary to the server configuration unless the machine is acting as a router.

You can check the status of IP fording.

“`sysctl net.ipv4.ip_forward`”

```
exll
isindu@UbuntuVM:~$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
isindu@UbuntuVM:~$
```



If IP forwarding is on disable it by editing syctl configuration file and modifying `net.ipv4.ip_forward = 0`

4) Configure NTP Securely

Exposing NTP services without securing them can allow an attacker to manipulate time or use the system in a DDoS amplification attack.

5) Use Secure DNS Configurations

DNS configurations can be exploited to redirect traffic or eavesdrop on communication. Secure DNS setups prevent DNS spoofing, cache poisoning, and other DNS-related attacks.