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

Assignment

IT23209534
A.A.I.Nethmika

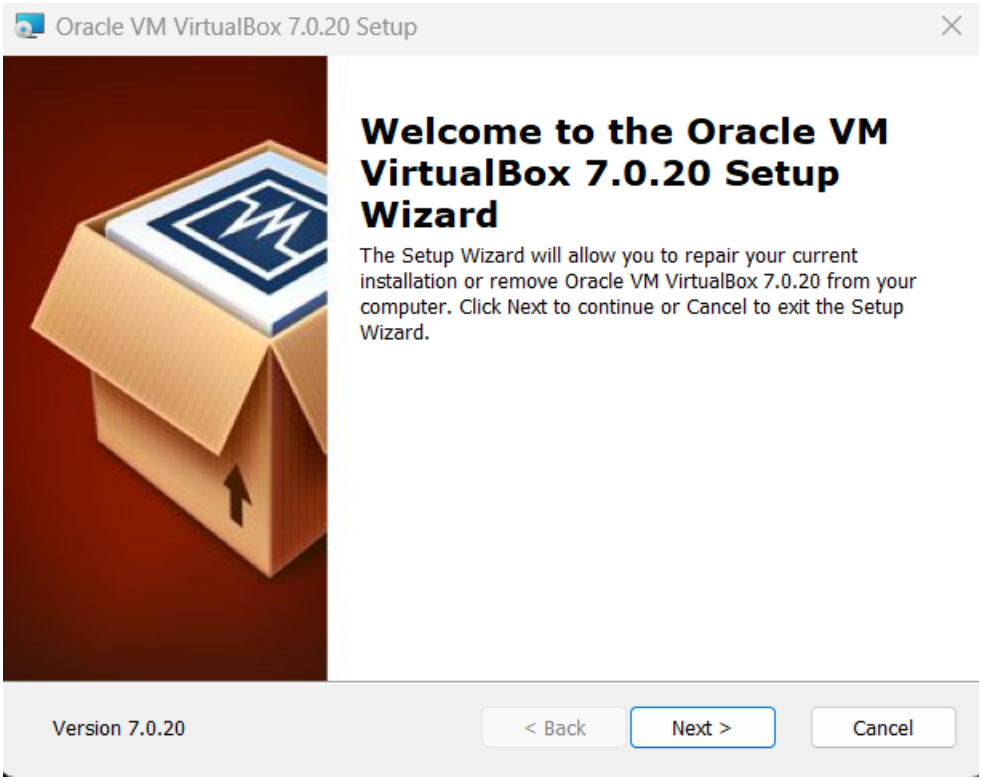
Table of Content

1. Basic Linux Environments

1.1) Virtual Machine Setup

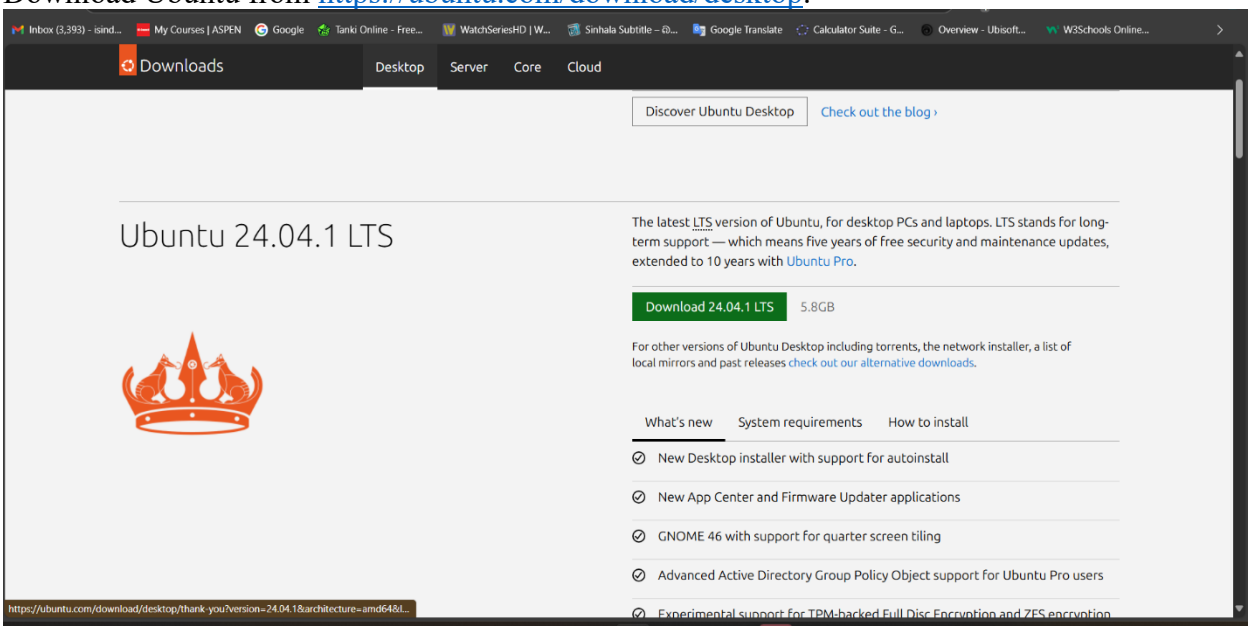
Download Oracle VirtualBox using https://www.virtualbox.org/wiki/Downloads.

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

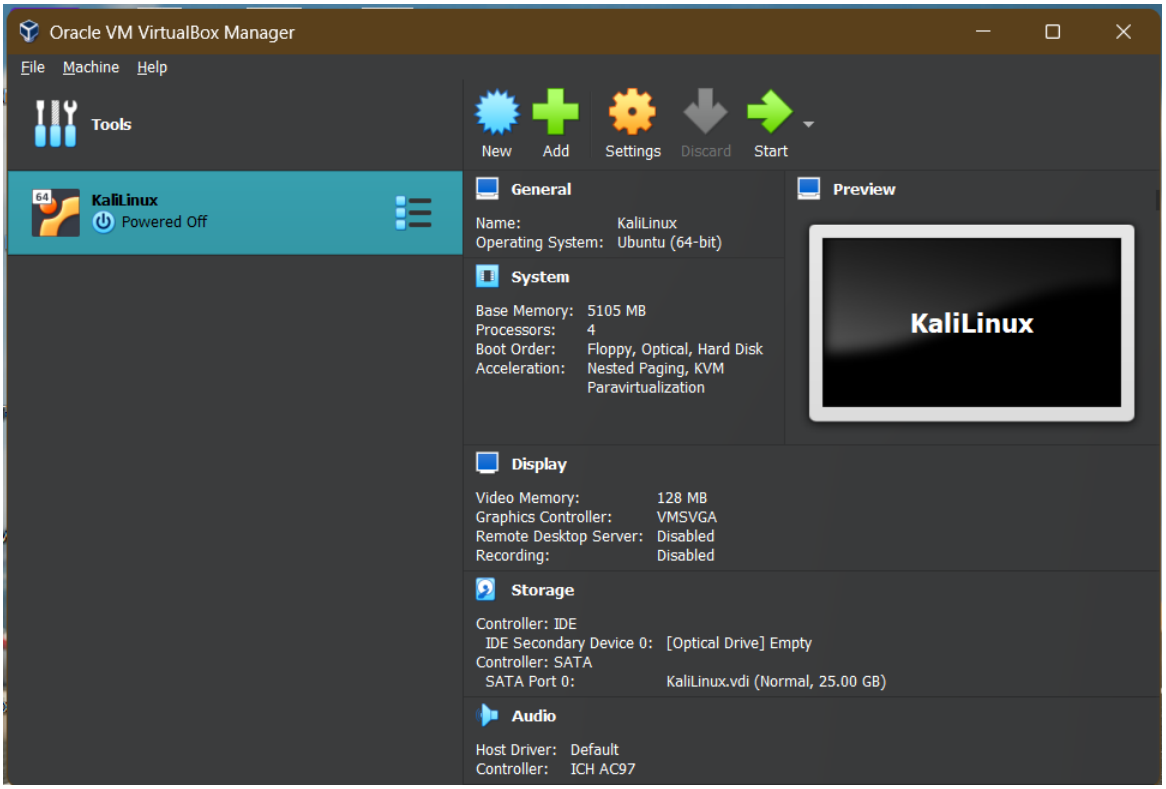


Select the preferred setting and install the VirtualBox. (VirtualBox software has already been installed in my computer)

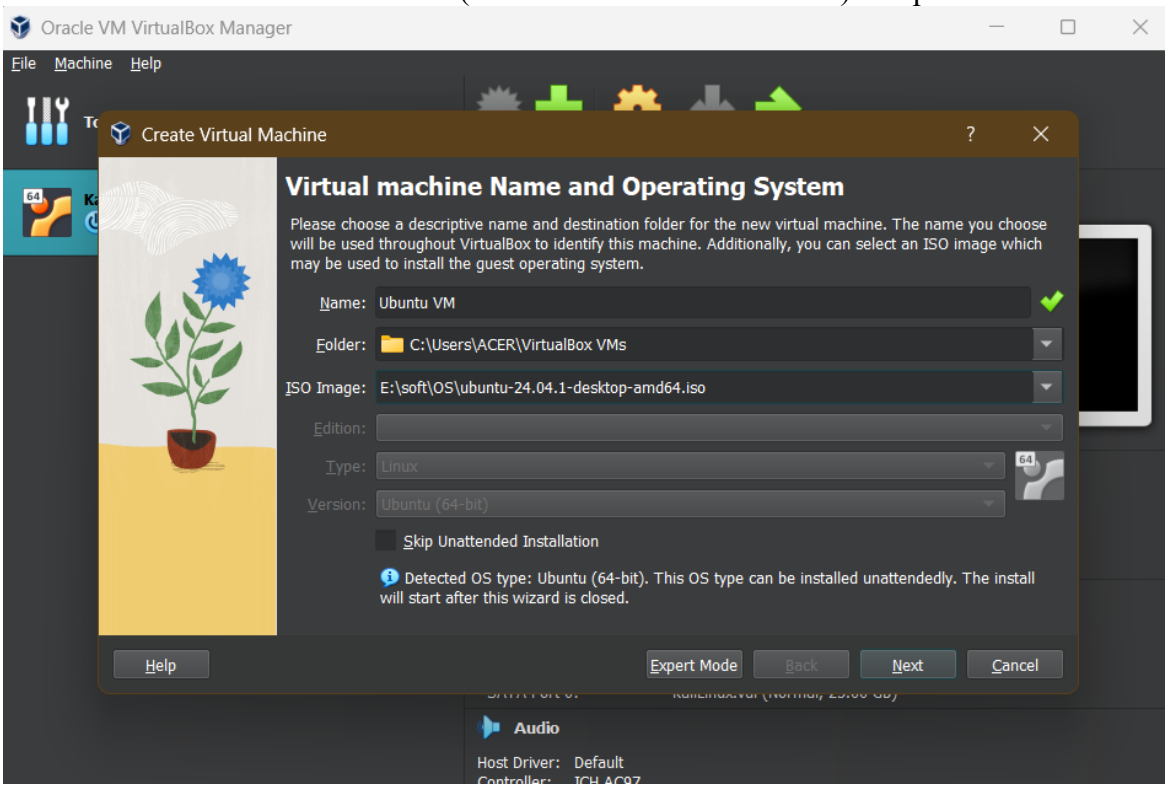
Download Ubuntu from https://ubuntu.com/download/desktop.



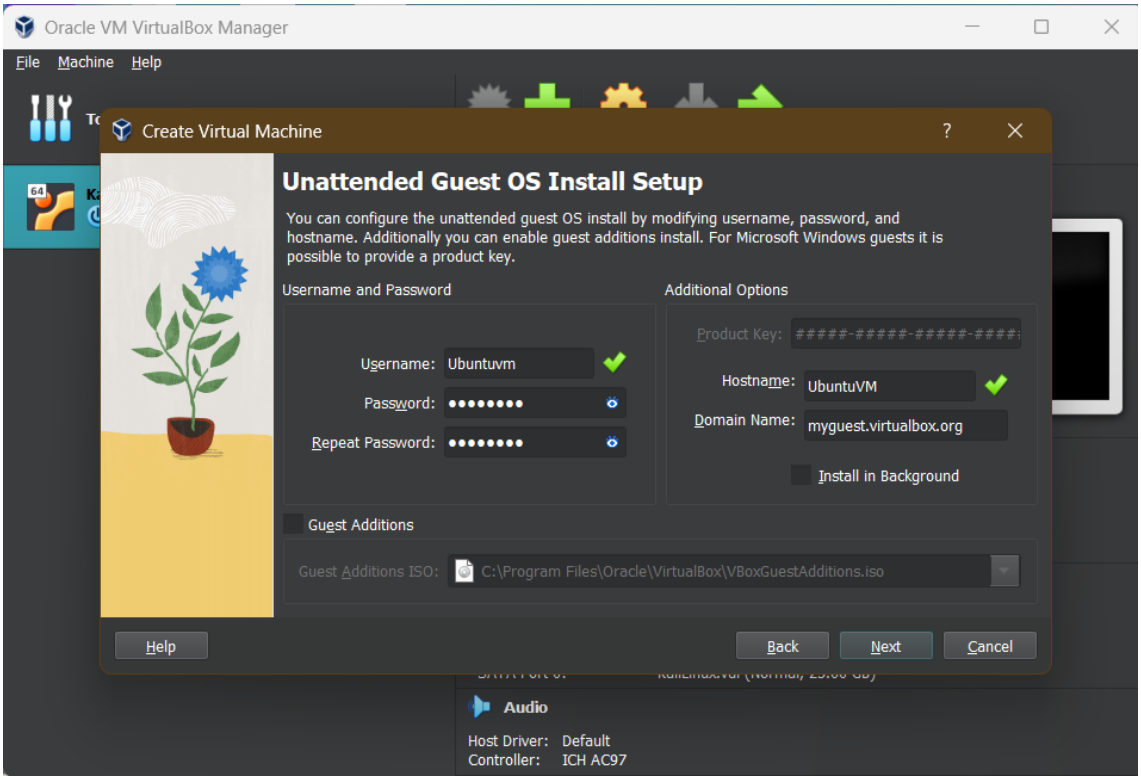
Run VirtualBox. Use new button to add new virtual machine.



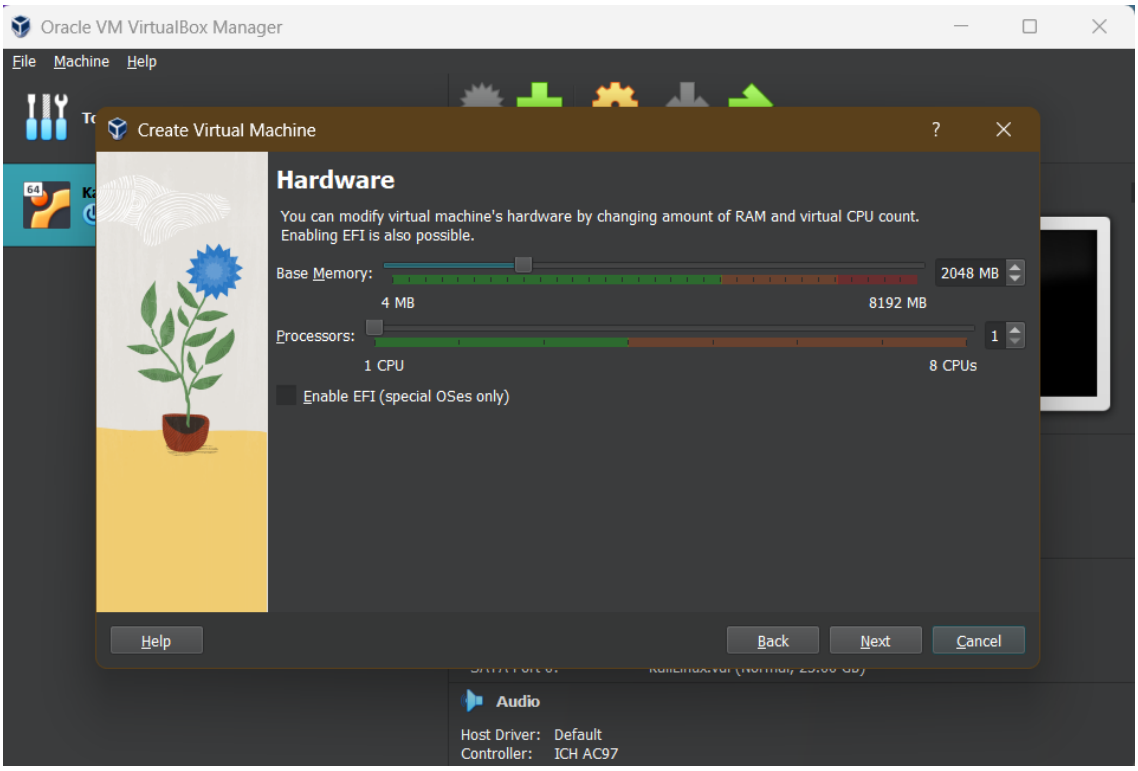
Enter a name and select the Iso file (Downloaded ubuntu ISO file) and press Next.



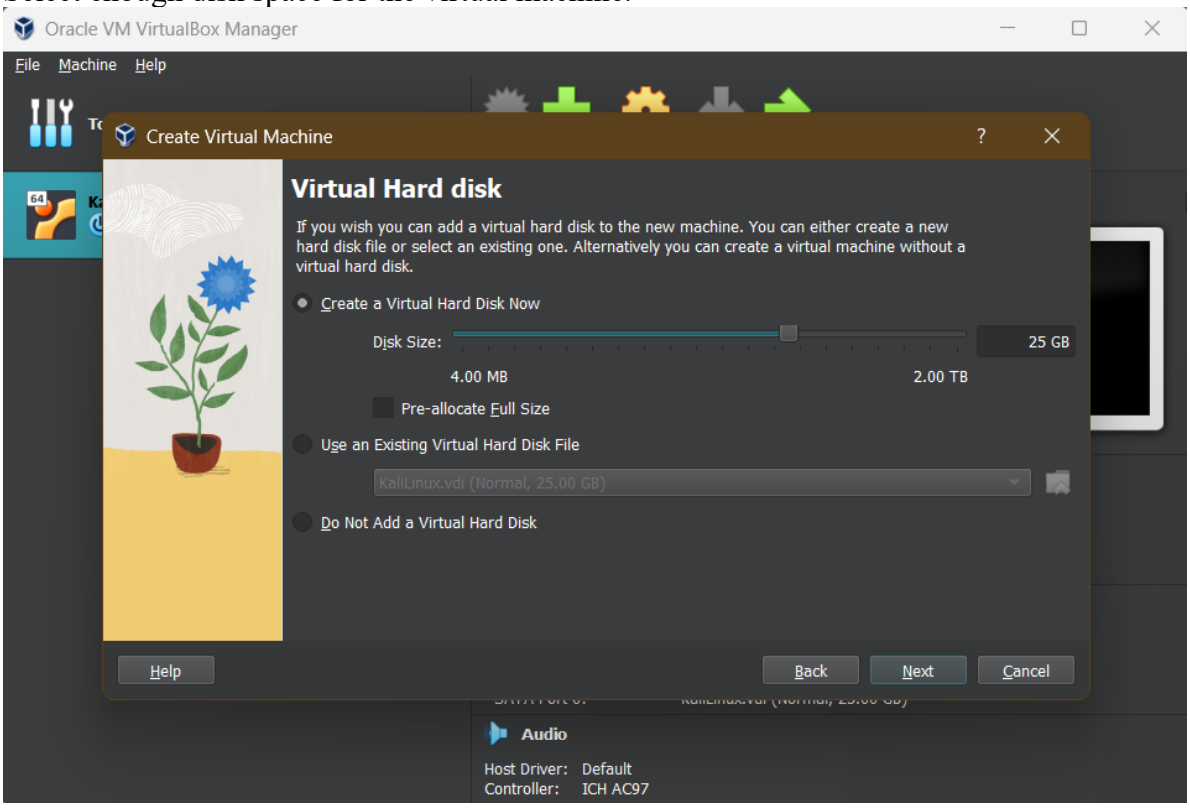
Then Enter a username and password



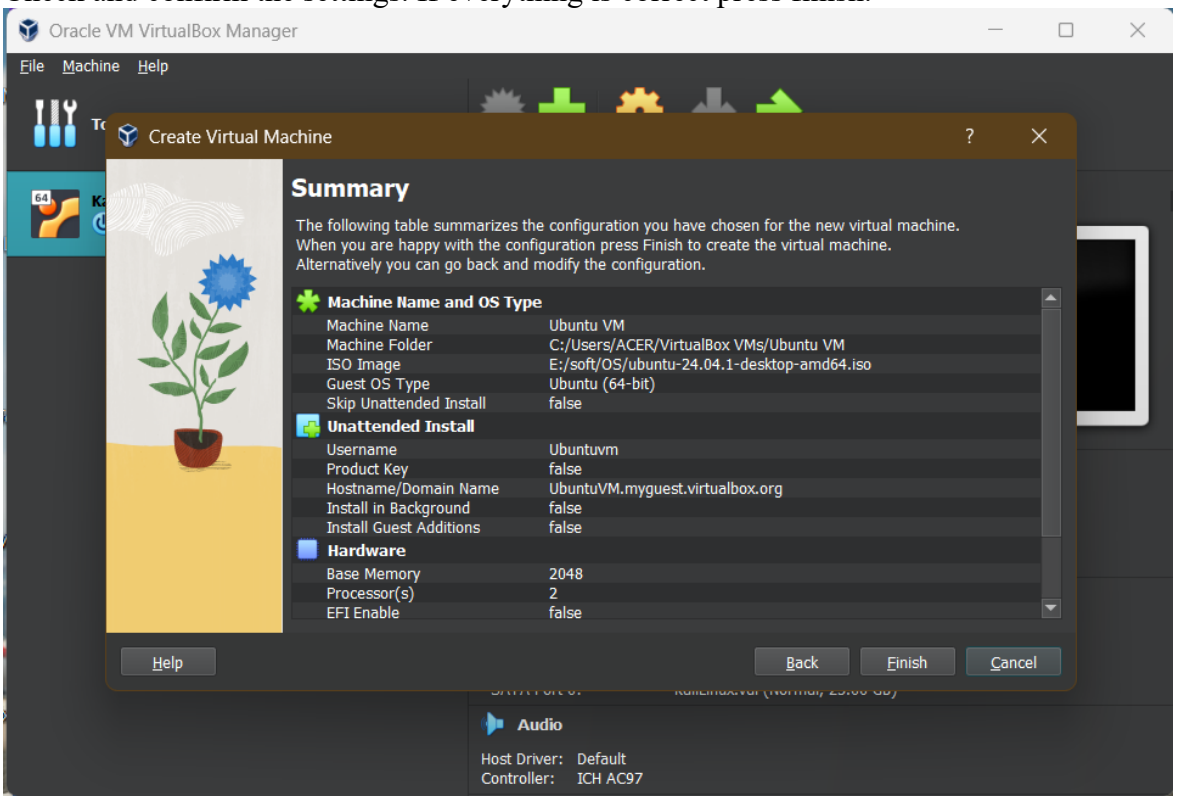
Select enough Base Memory space and Processors.



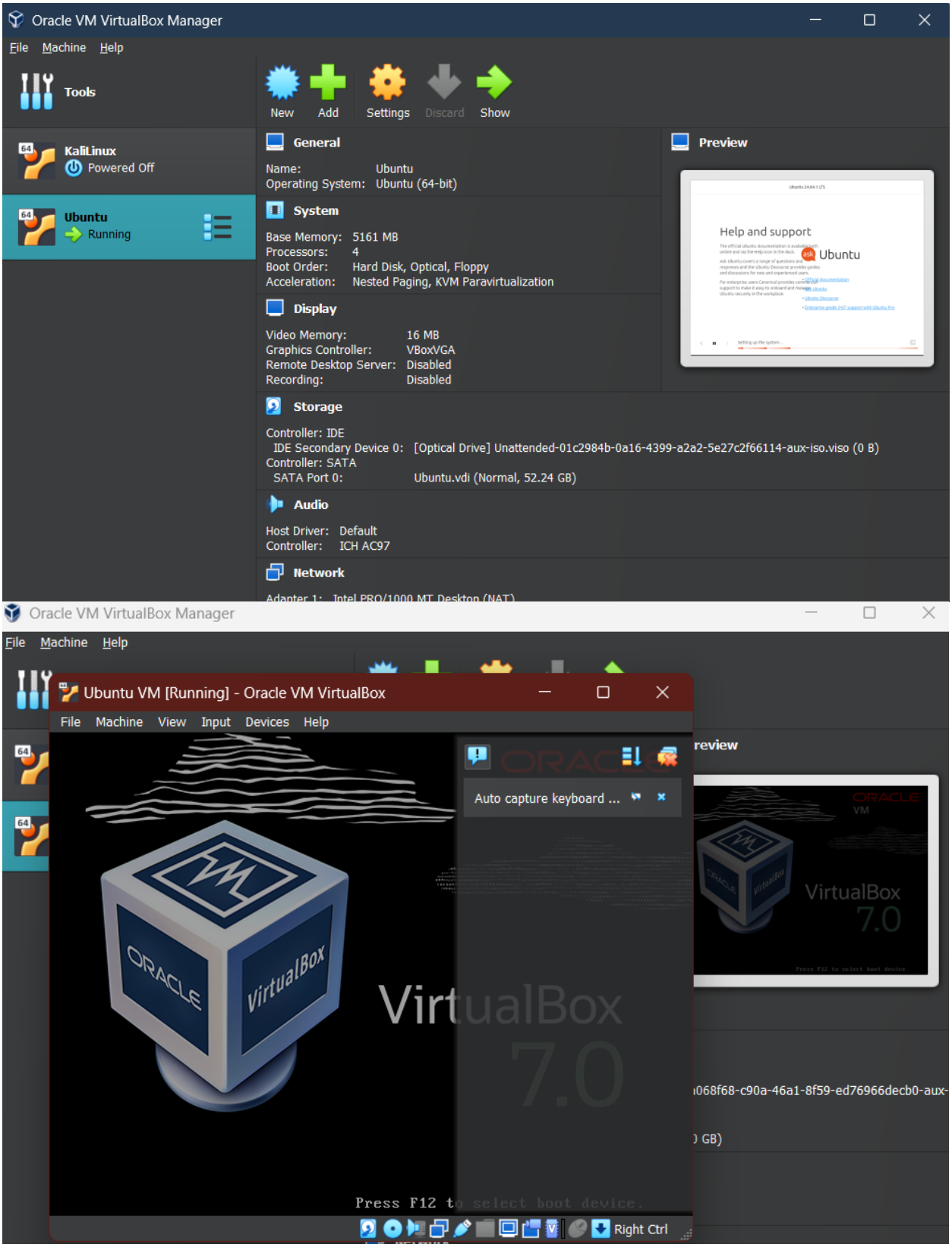
Select enough disk space for the virtual machine.



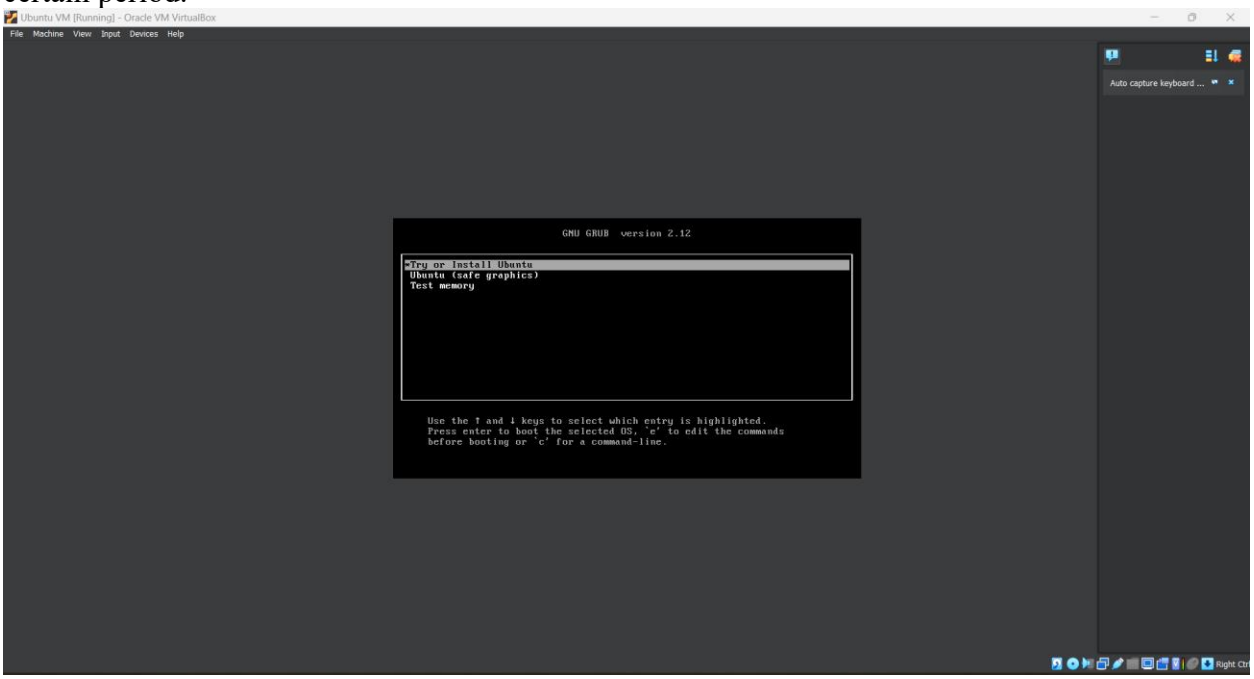
Check and confirm the settings. If everything is correct press finish.



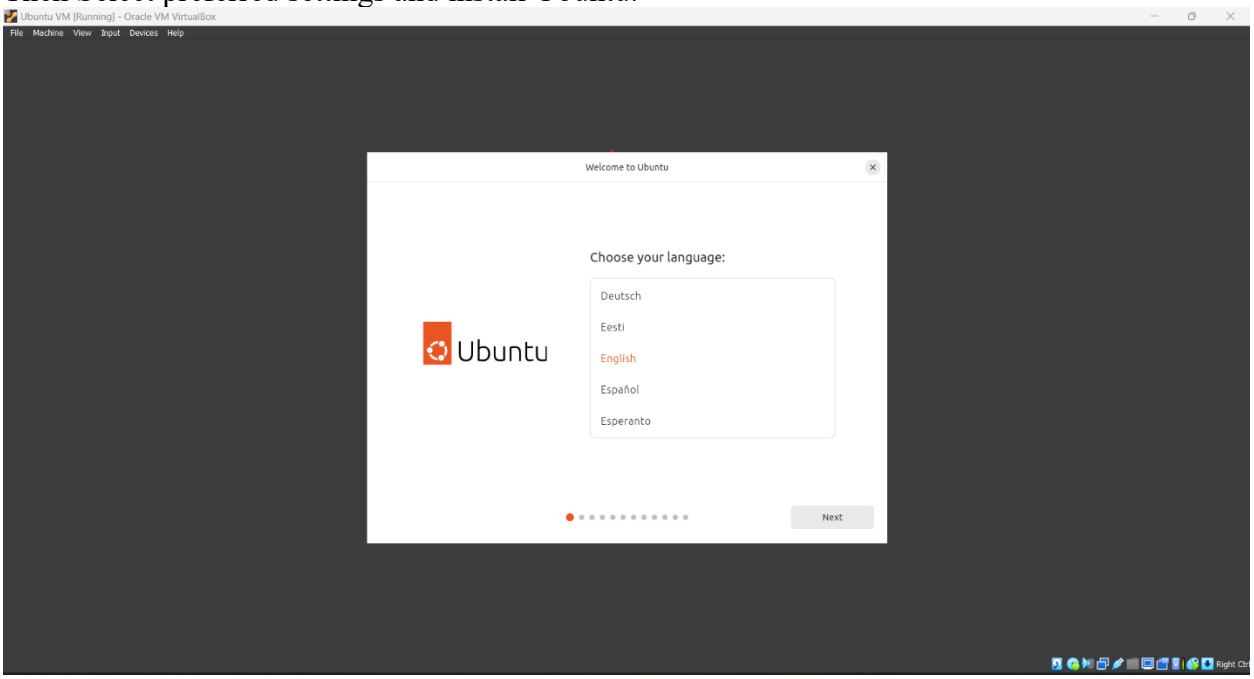
Now select the newly created virtual machine and click on start.

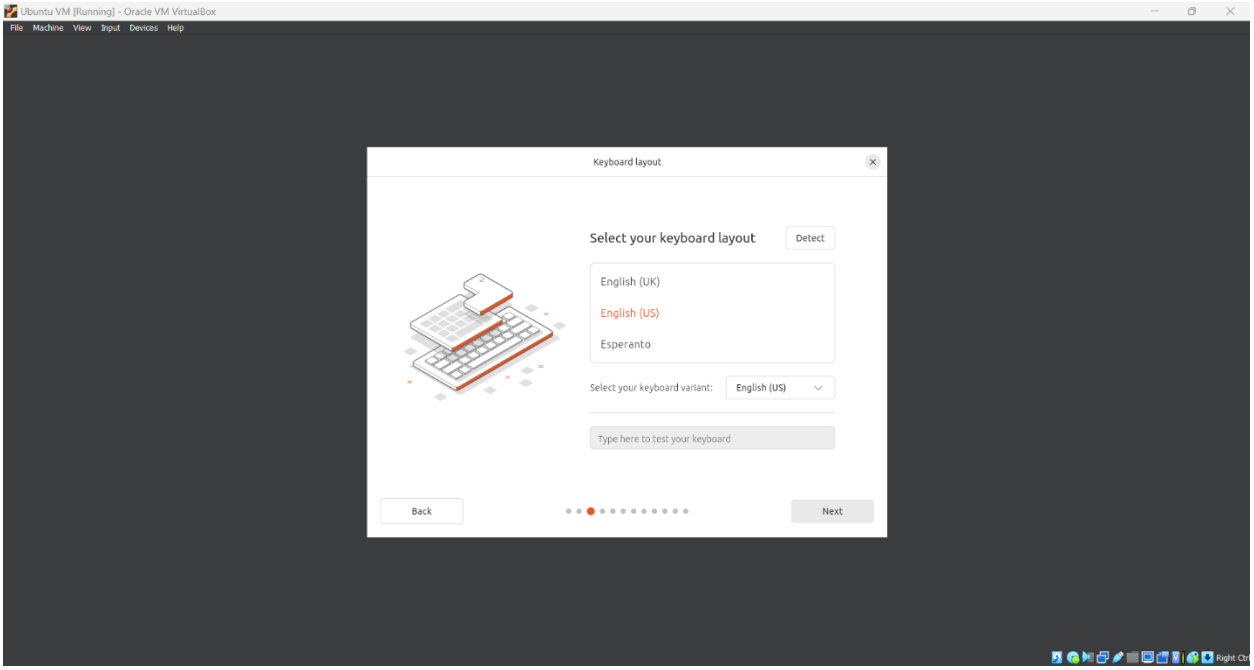


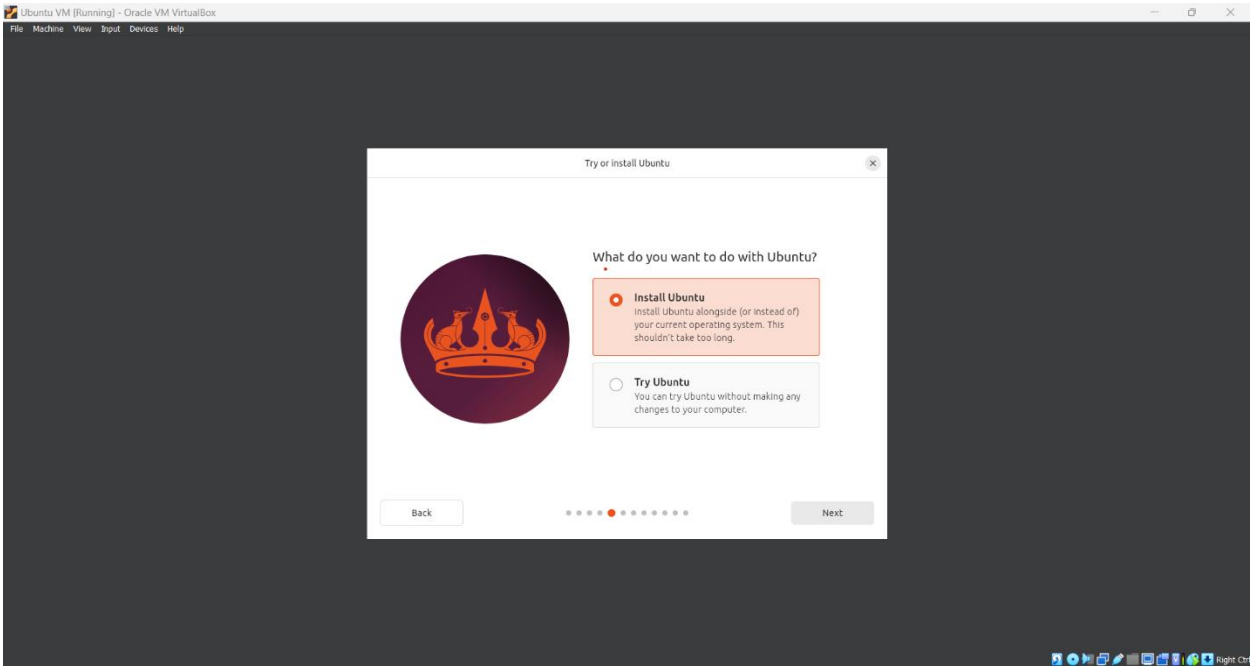
Select Try or install Ubuntu options (Highlighted option will be selected automatically after certain period.

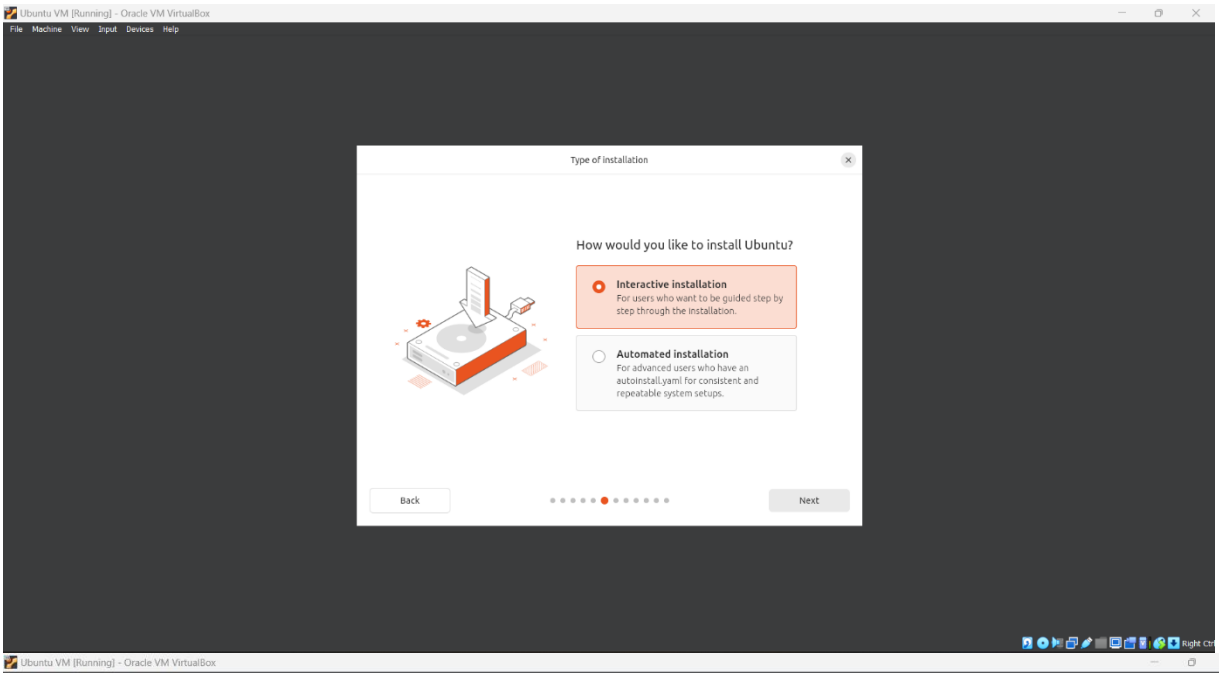


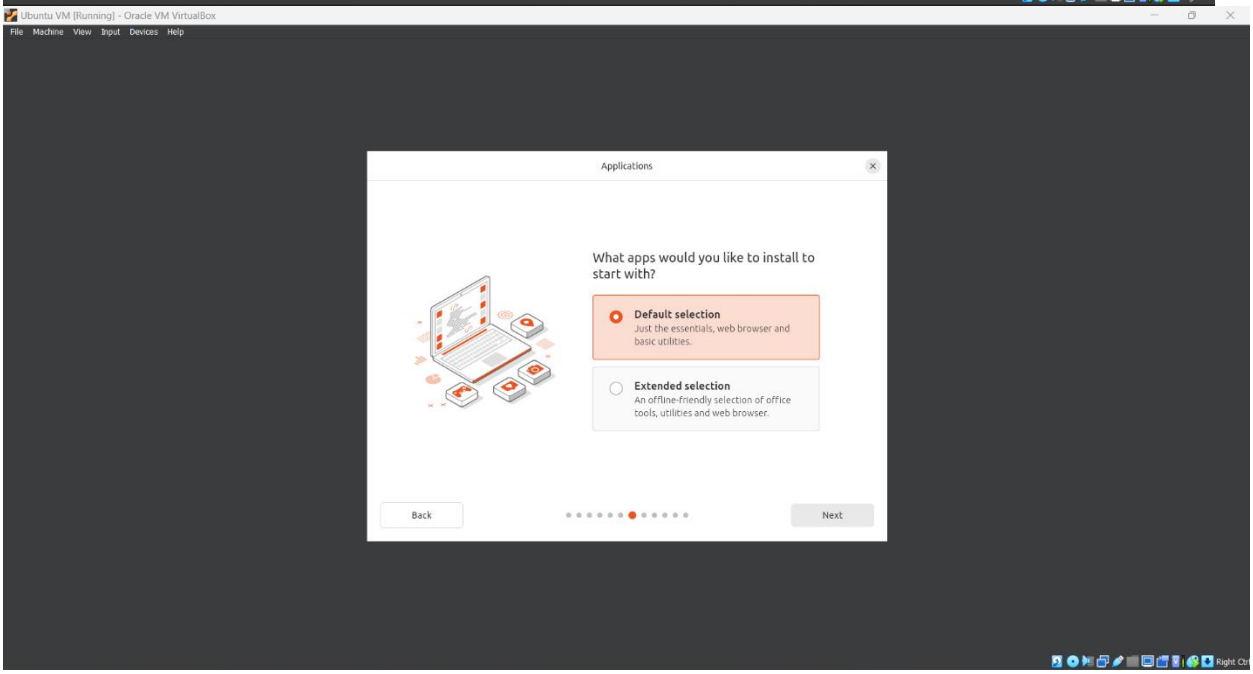
Then Select preferred settings and install Ubuntu.

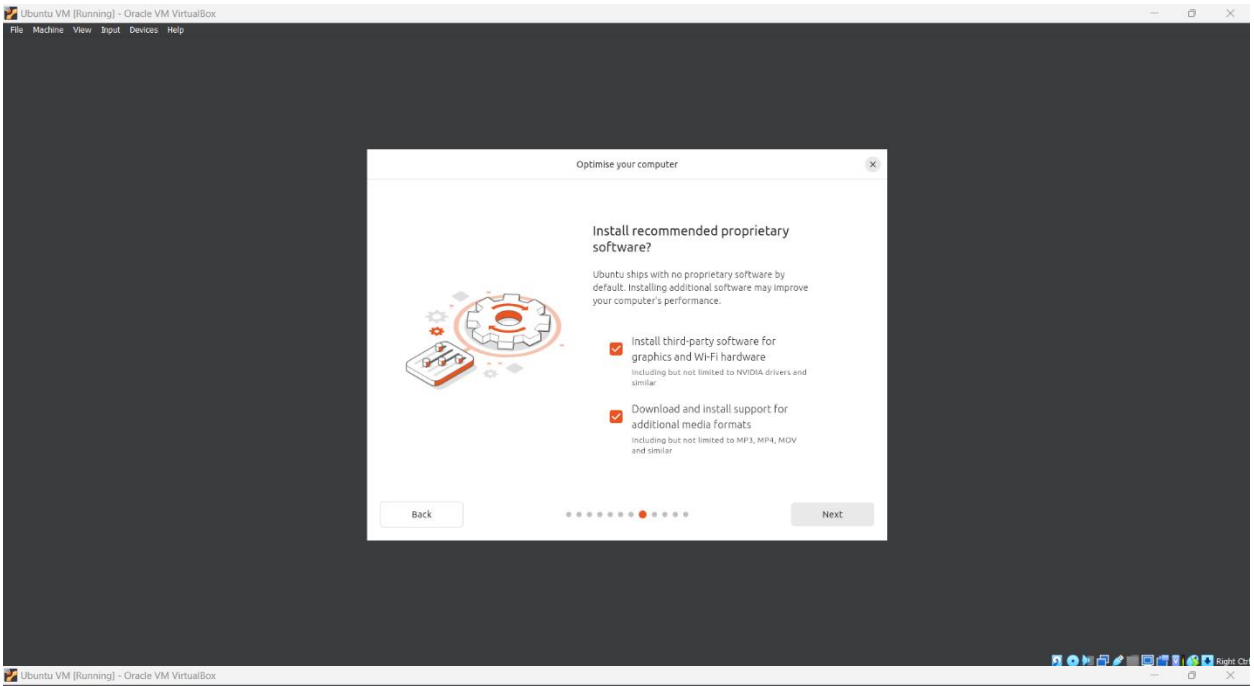


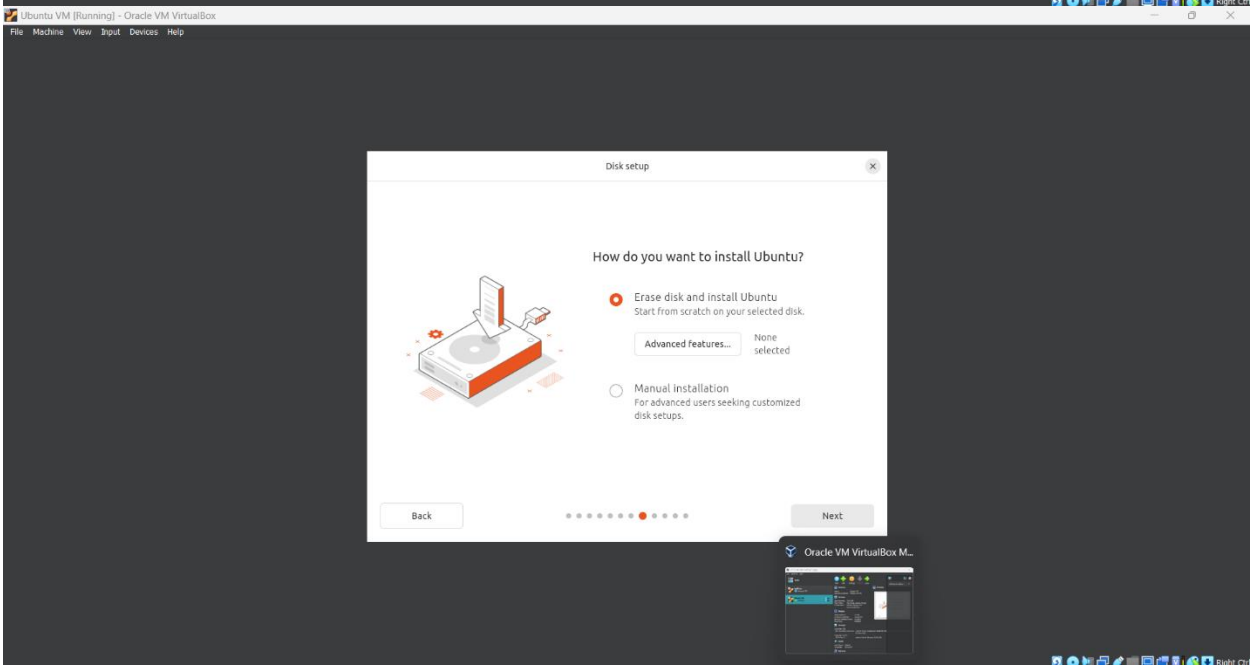

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Keyboard layout
Select your keyboard layout
Detect
English (UK)
English (US)
Esperanto
Select your keyboard variant:
English (US)
Type here to test your keyboard
Back
Next

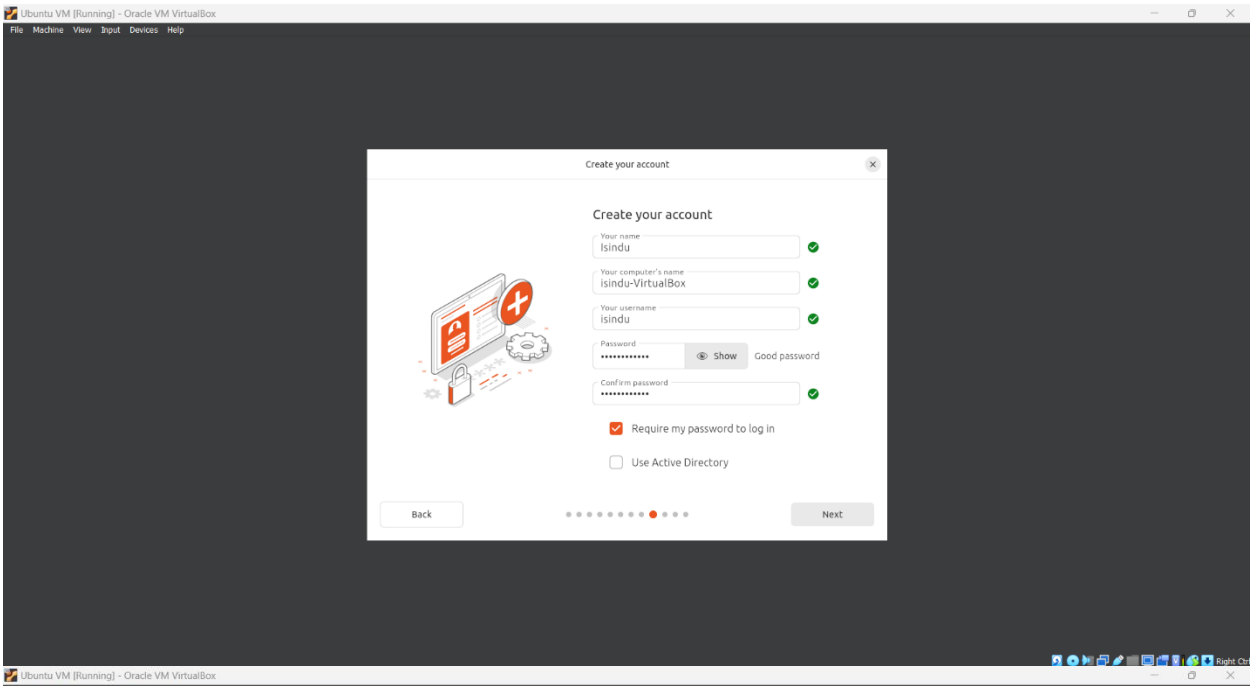

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Try or install Ubuntu
What do you want to do with Ubuntu?
Install Ubuntu
Install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.
Try Ubuntu
You can try Ubuntu without making any changes to your computer.
Back
Next

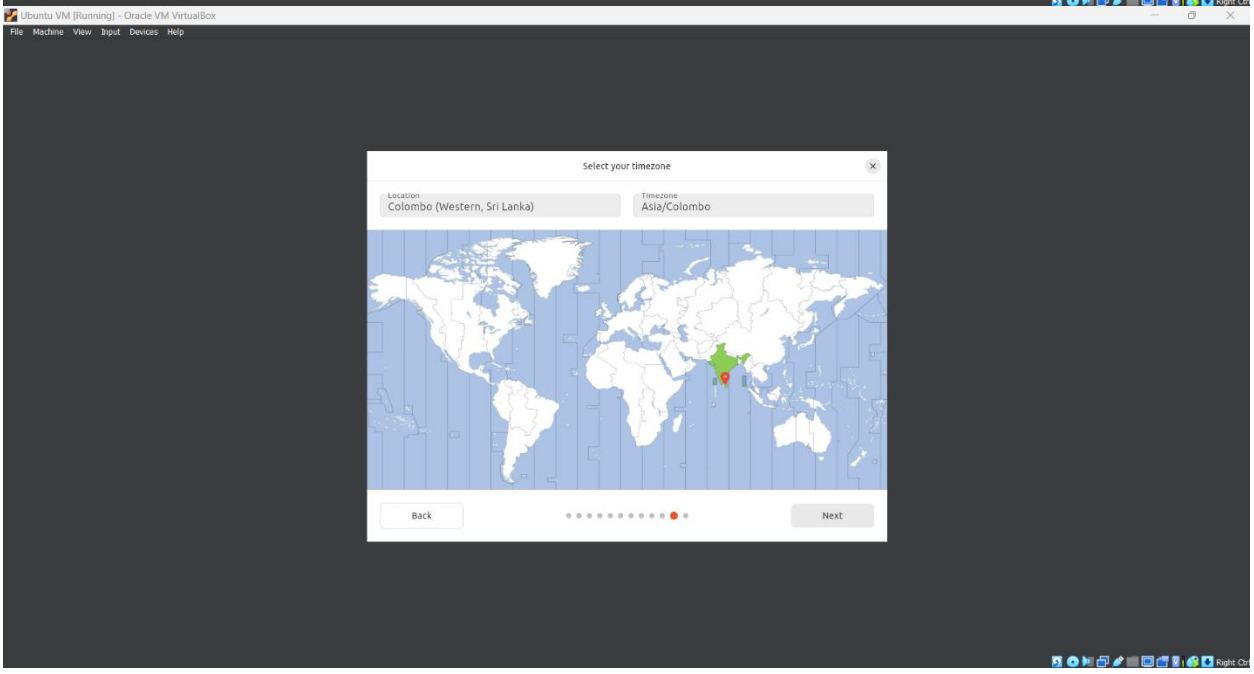

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type of installation
How would you like to install Ubuntu?
Interactive installation
For users who want to be guided step by step through the installation.
Automated installation
For advanced users who have an autoinstall.yaml for consistent and repeatable system setups.
Back
Next

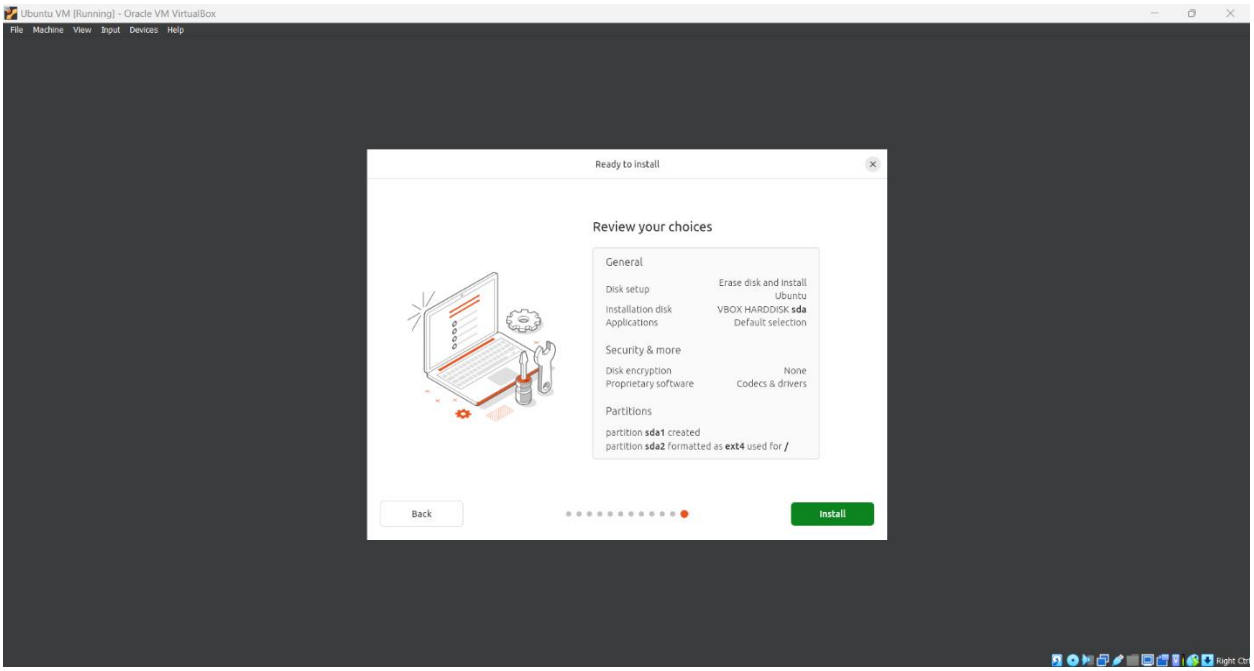

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
What apps would you like to install to start with?
Default selection
Just the essentials, web browser and basic utilities.
Extended selection
An offline-friendly selection of office tools, utilities and web browser.
Back
Next

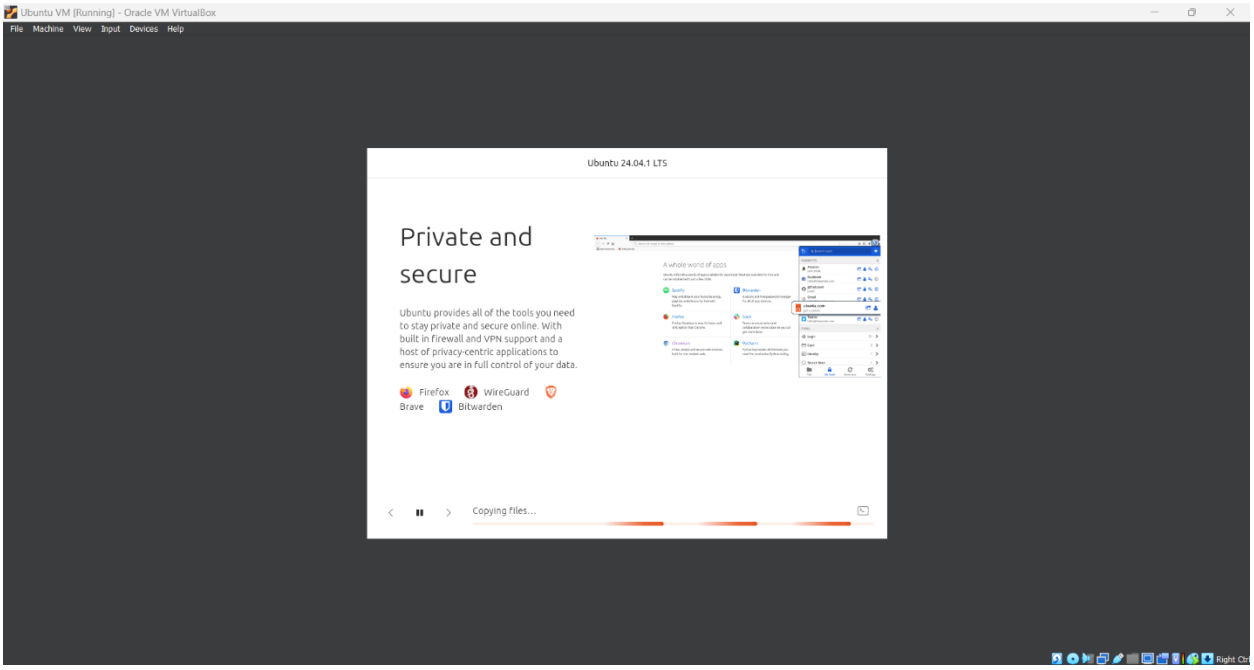

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Optimise your computer
Install recommended proprietary software?
Ubuntu ships with no proprietary software by default. Installing additional software may improve your computer's performance.
Install third-party software for graphics and Wi-Fi hardware
Including but not limited to NVIDIA drivers and similar
Download and install support for additional media formats
Including but not limited to MP3, MP4, MOV and similar
Back
Next


Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Disk setup
How do you want to install Ubuntu?
Erase disk and install Ubuntu
Start from scratch on your selected disk.
Advanced features...
None selected
Manual installation
For advanced users seeking customized disk setups.
Back
Next
Oracle VM VirtualBox M...

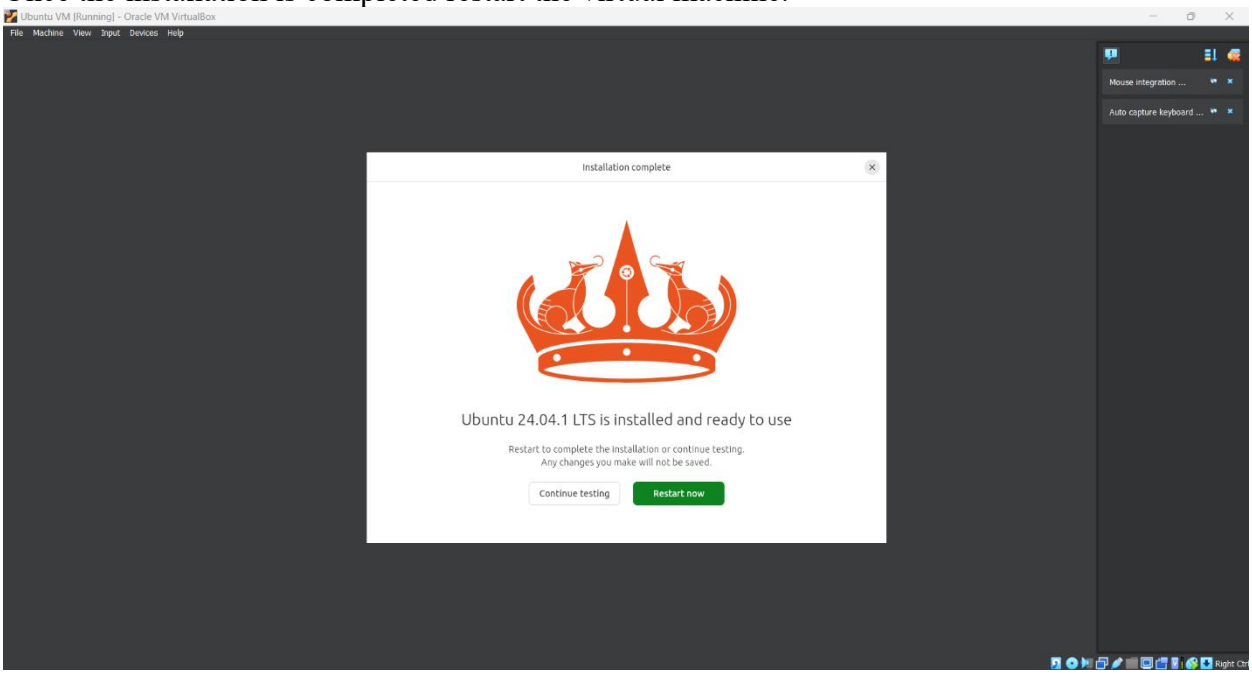

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Create your account
Create your account
Your name
isindu
Your computer's name
isindu-VirtualBox
Your username
isindu
Password
Show
Good password
Confirm password
Require my password to log in
Use Active Directory
Back
Next


Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select your timezone
Location
Colombo (Western, Sri Lanka)
Timezone
Asia/Colombo
Back
Next


Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ready to install
Review your choices
General
Disk setup
Erase disk and install Ubuntu
Installation disk
VBOX HARDDISK sda
Applications
Default selection
Security & more
Disk encryption
None
Proprietary software
Codecs & drivers
Partitions
partition sda1 created
partition sda2 formatted as ext4 used for /
Back
Install

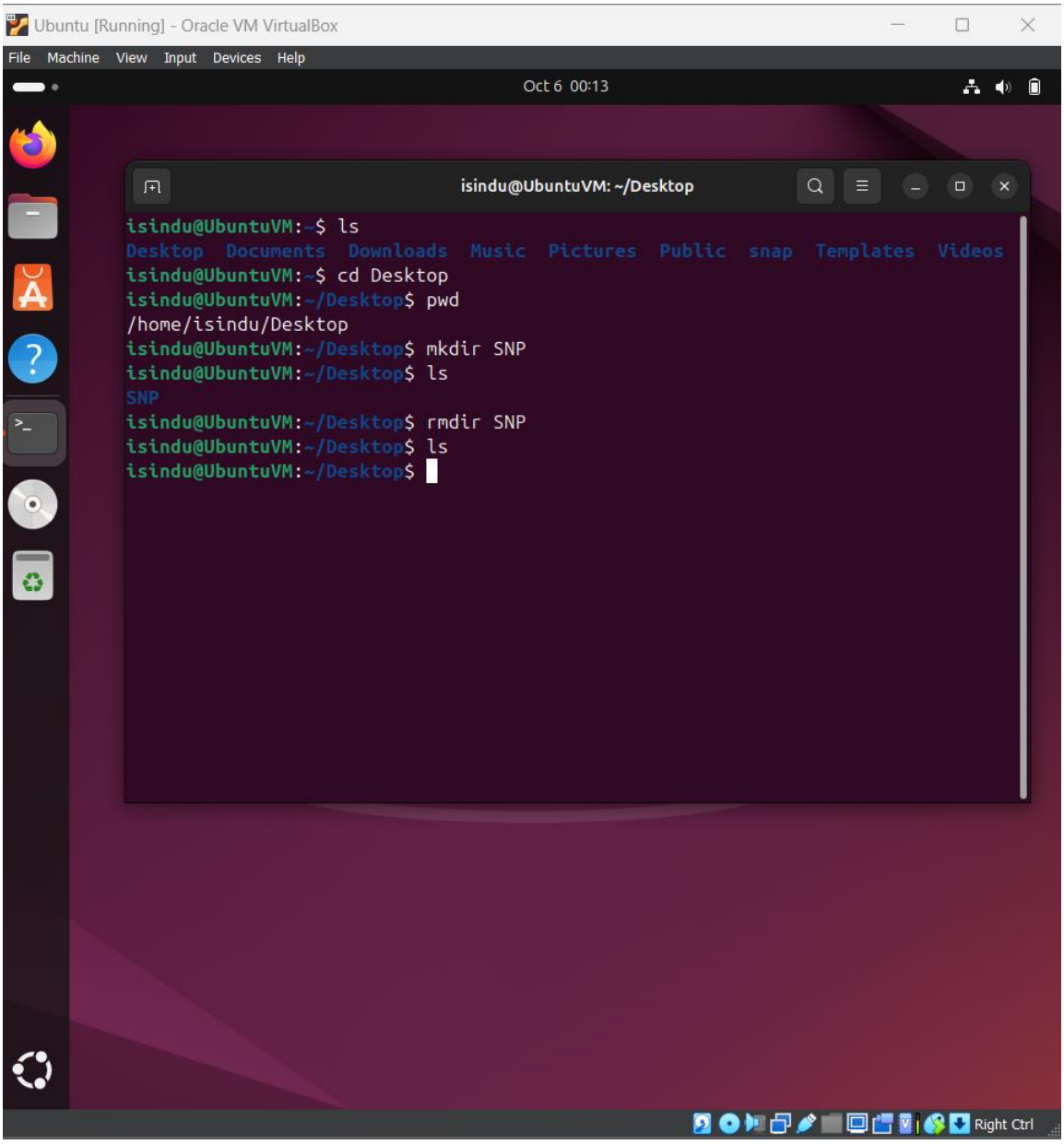

Ubuntu VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 24.04.1 LTS
Private and secure
Ubuntu provides all of the tools you need to stay private and secure online. With built in firewall and VPN support and a host of privacy-centric applications to ensure you are in full control of your data.
Firefox
WireGuard
Brave
Bitwarden
Copying files...

Once the installation is completed restart the virtual machine.



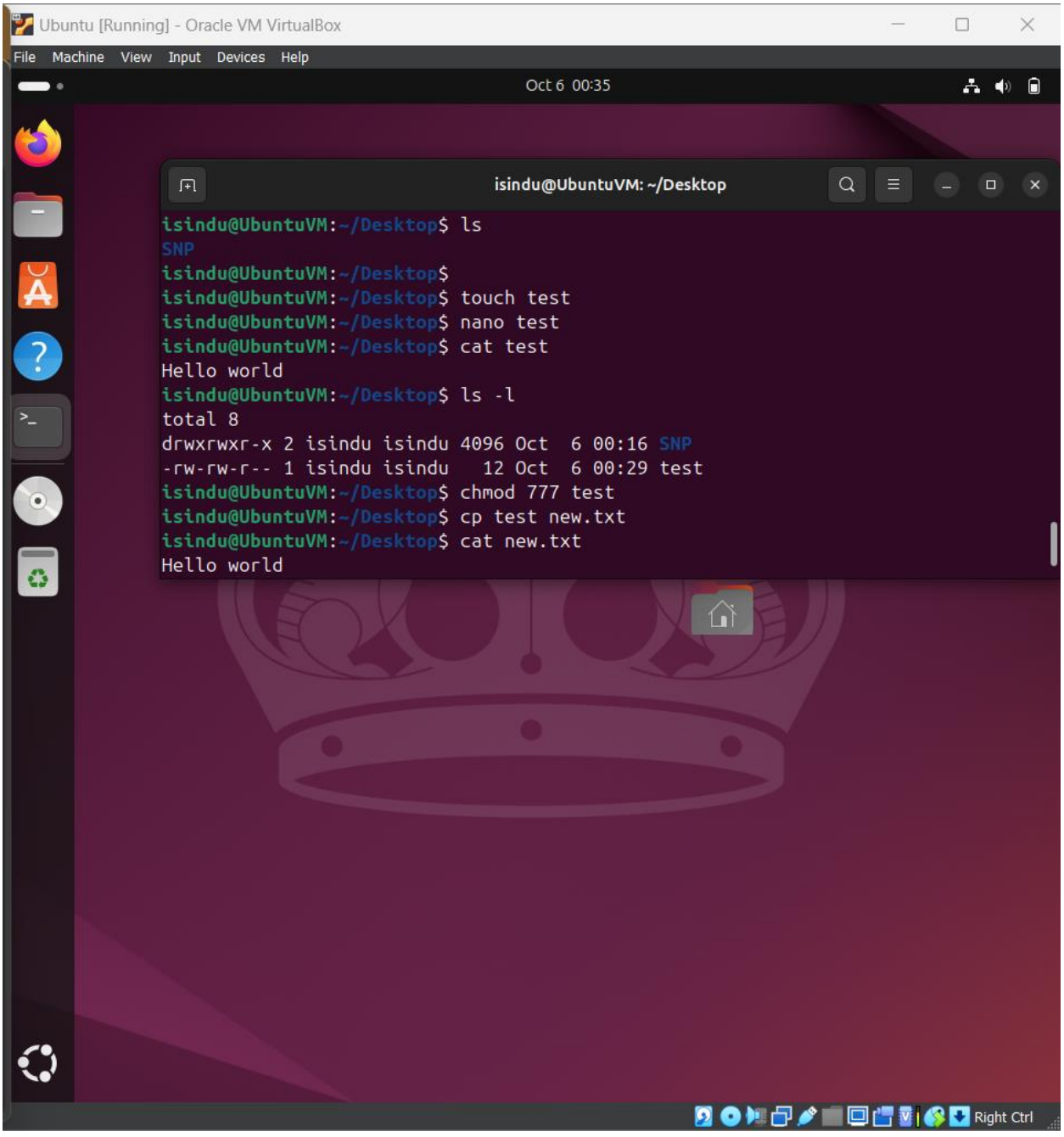
1.2) Basic Navigation Commands and functionalities.

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



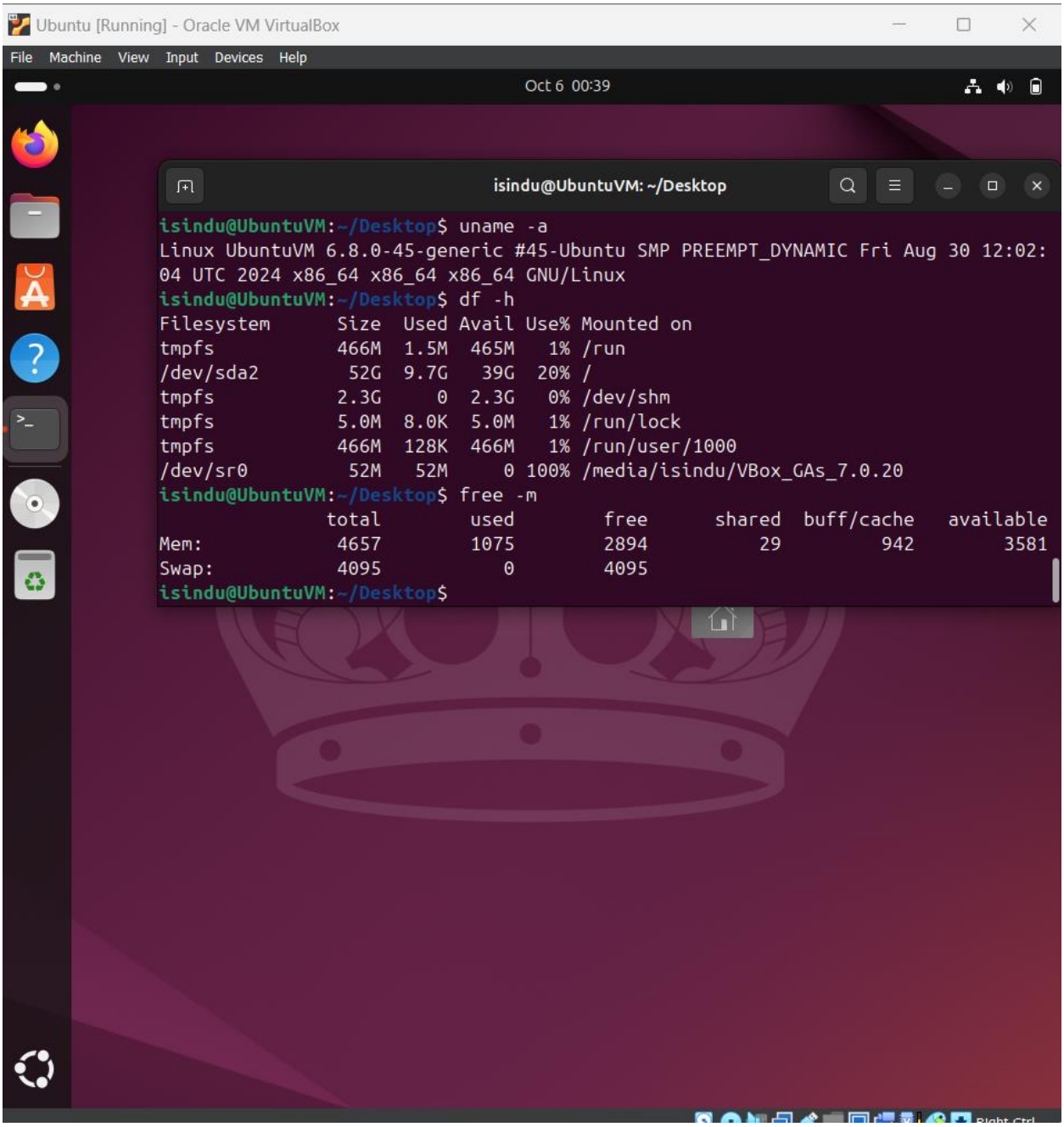
1.3) File manipulation commands

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



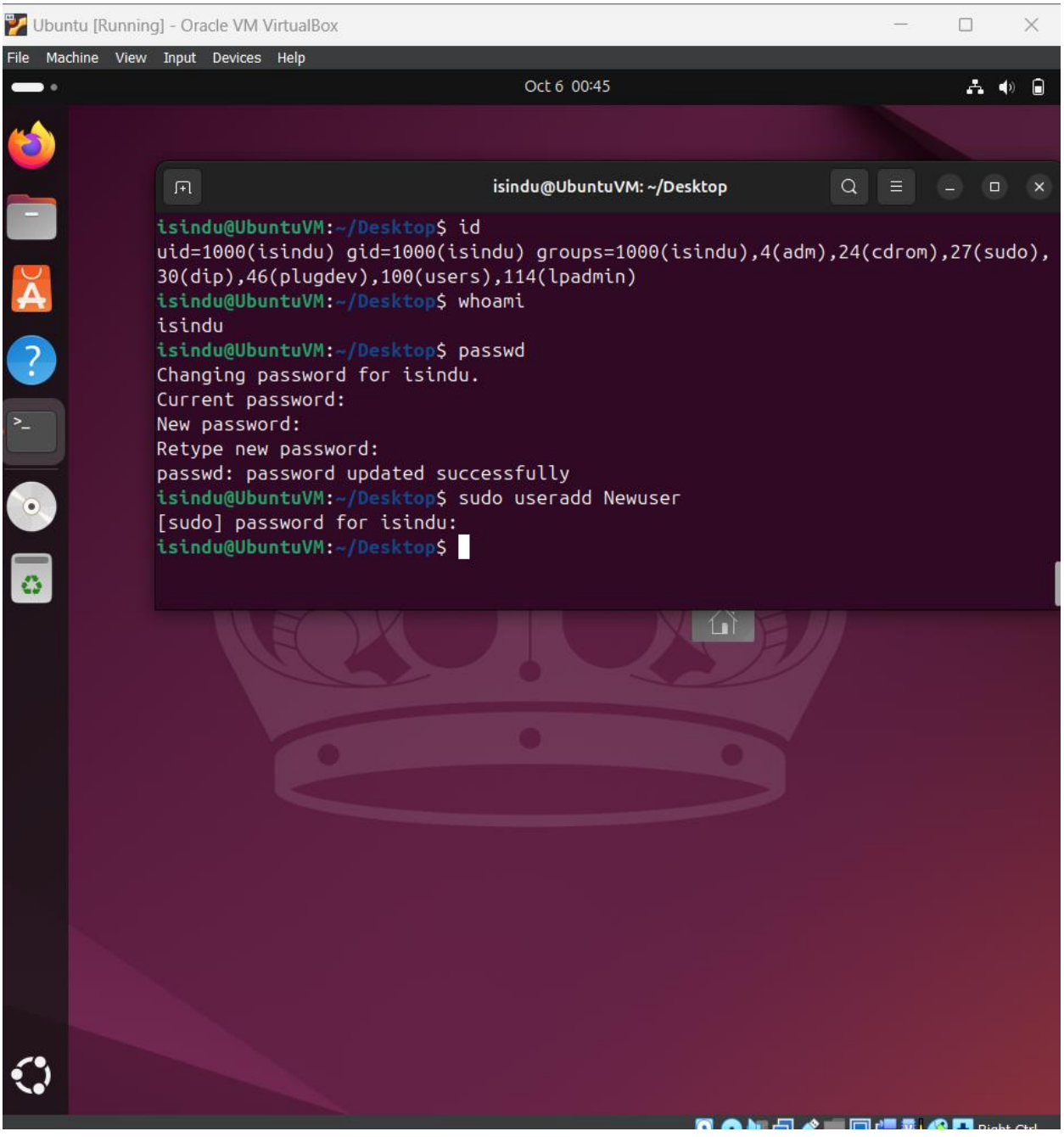
1.4) System Information Commands

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



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



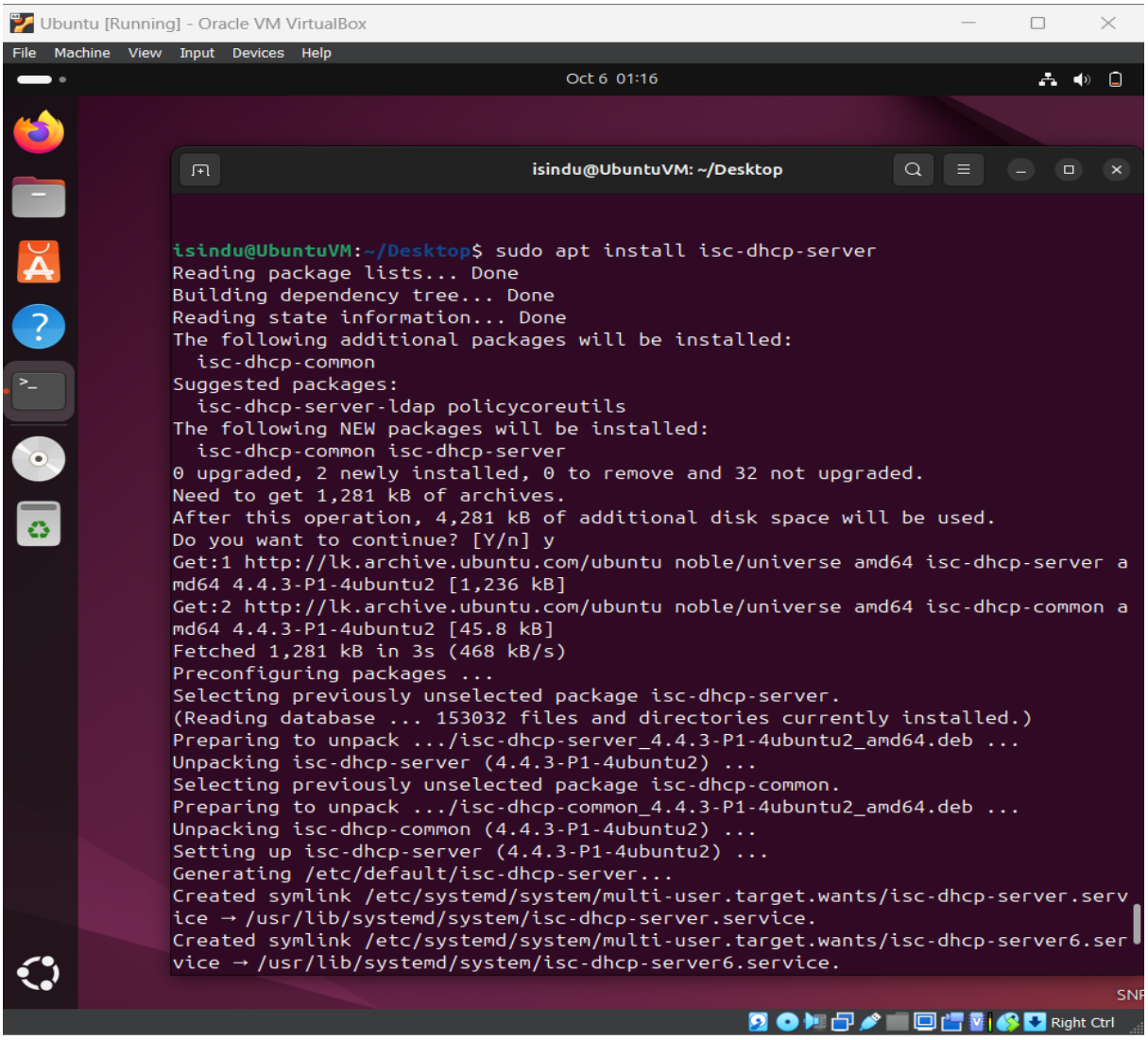
2. DHCP, DNS and NTP Services

2.1) DHCP (Dynamic Host Configuration Protocol)

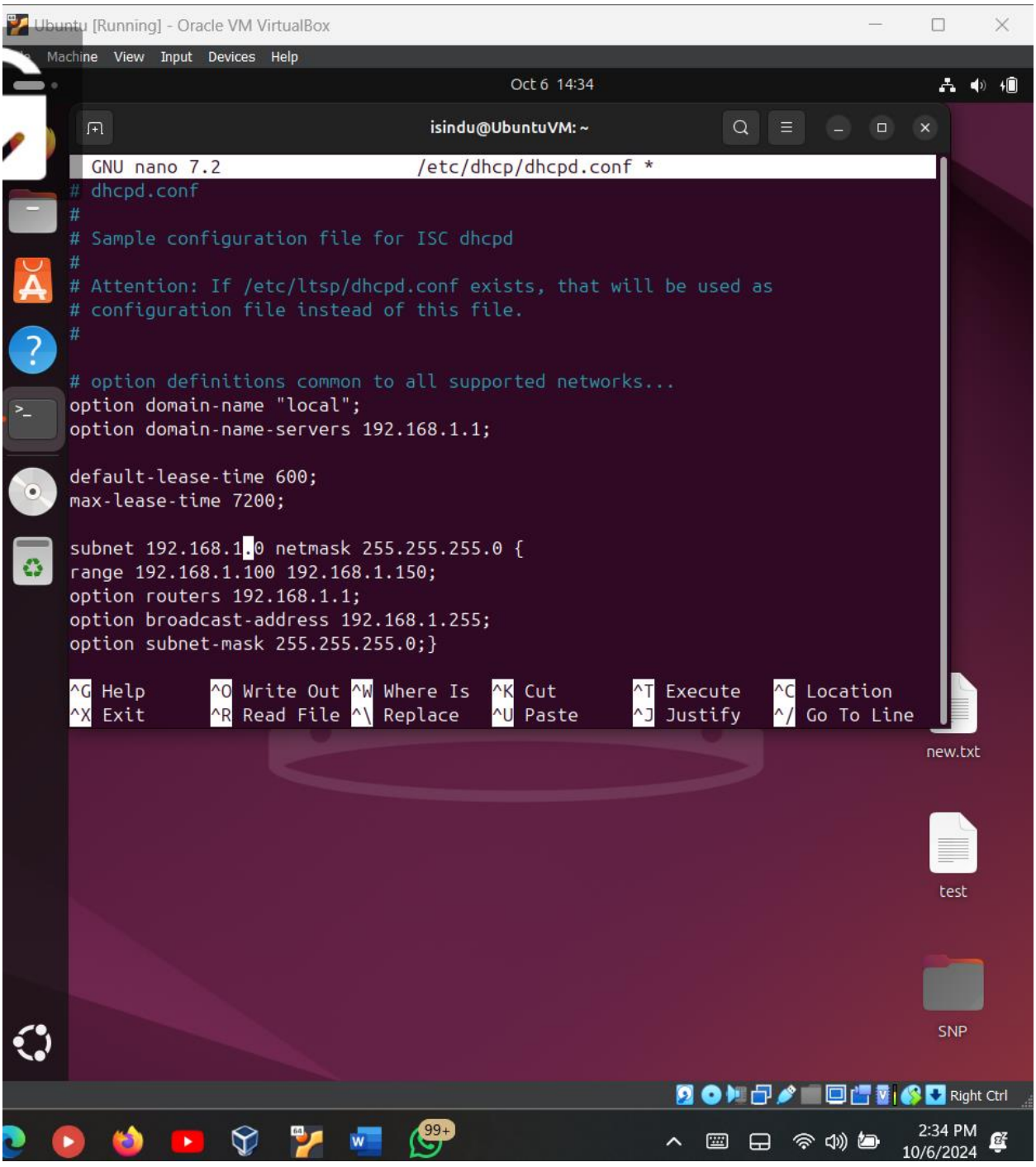
DHCP (Dynamic Host Configuration Protocol) is a protocol used to automatically assign IP addresses to devices on a network.

2.2) Installation and configuration

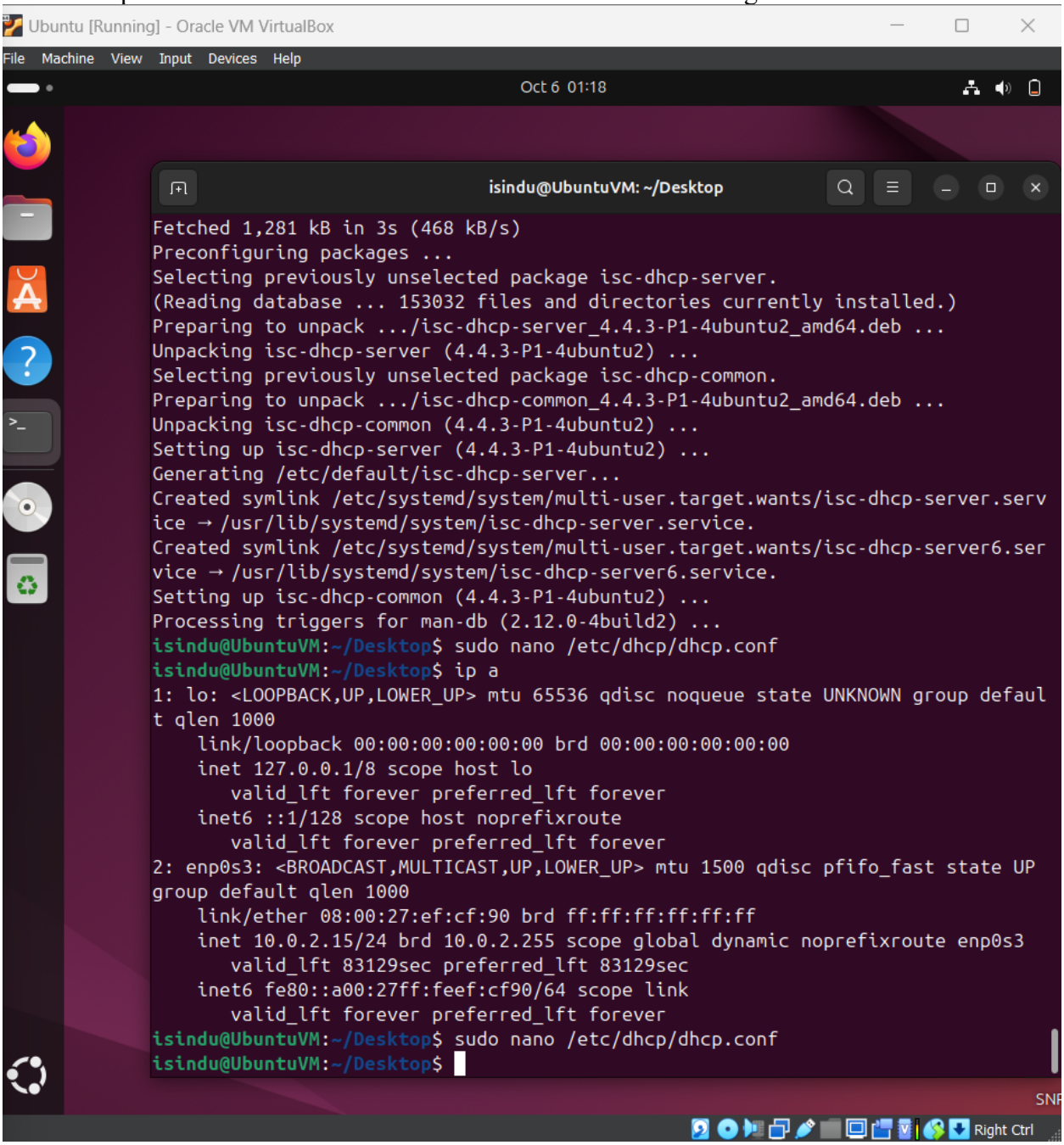
Open Terminal and install DHCP server package with “sudo apt install isc-dhcp-server” command.

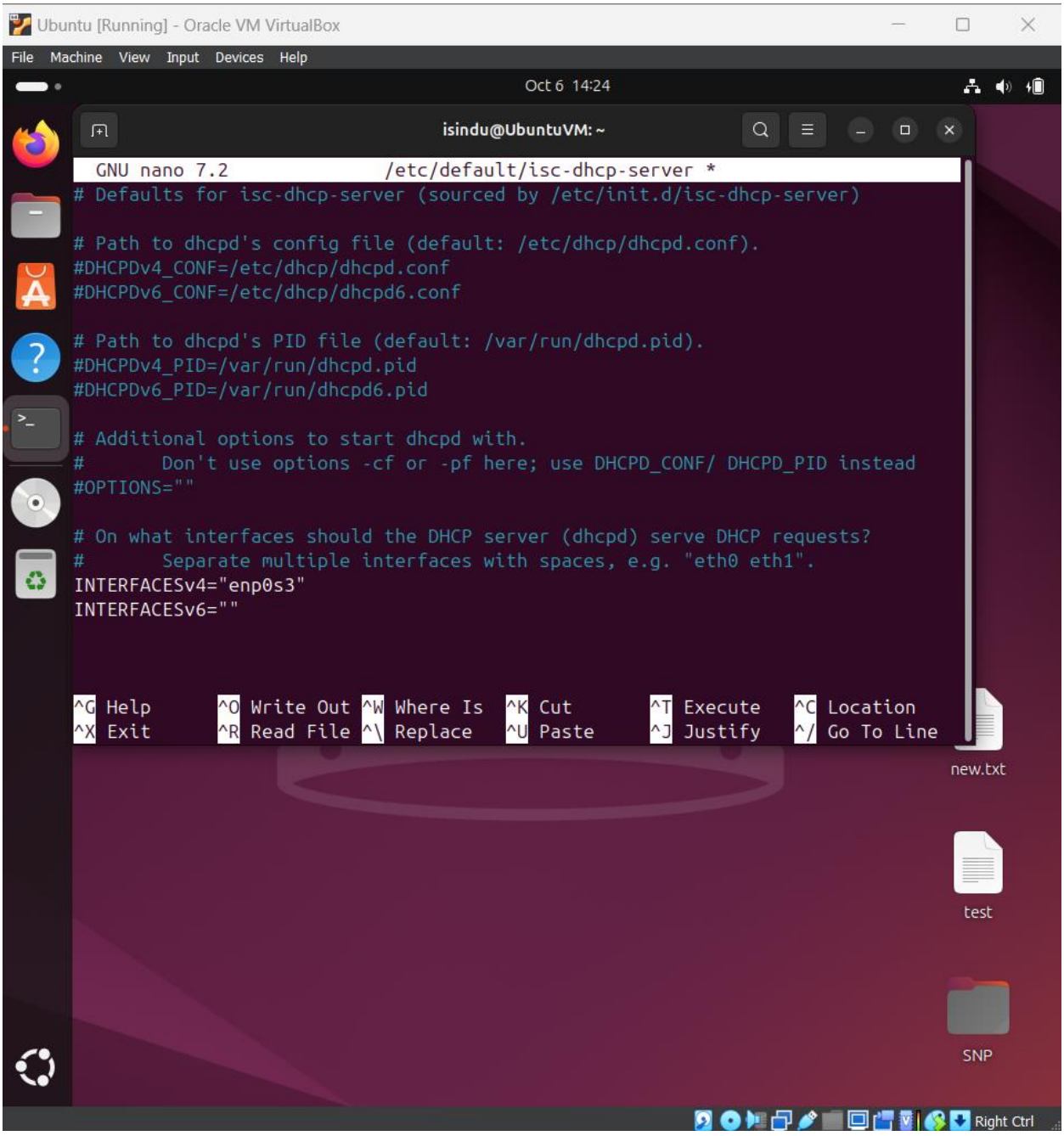


Use “sudo nano /etc/dhcp/dhcpd.conf ” to open and edit DHCP configuration file and modify it do define the network settings for the DHCP server and save it.



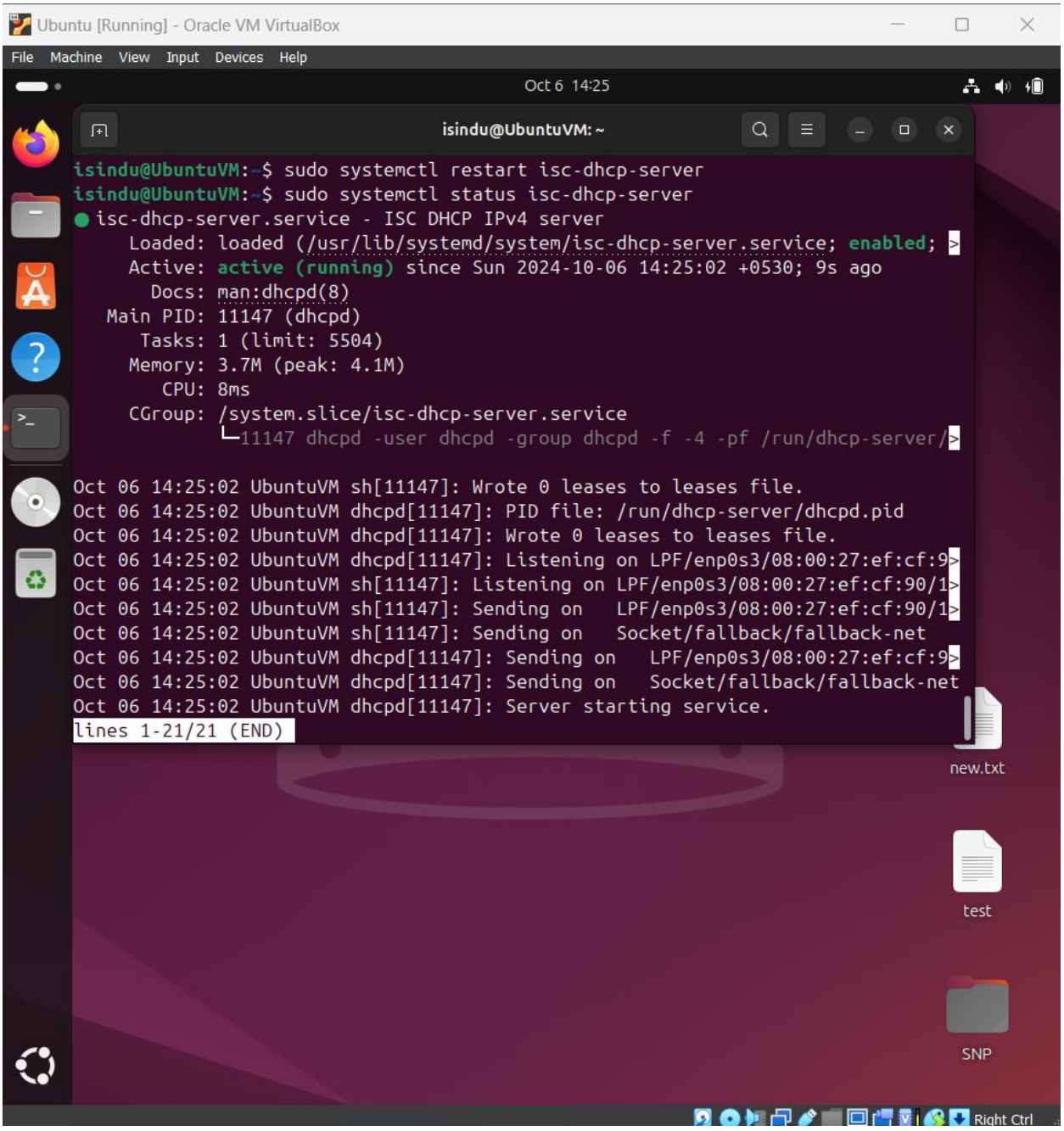
Use “sudo nano /etc/default/isc-dhcp-server” command to open and edit the DHCP server default file. Use “ip a” command to check network interface and make changes to the relevant interface.

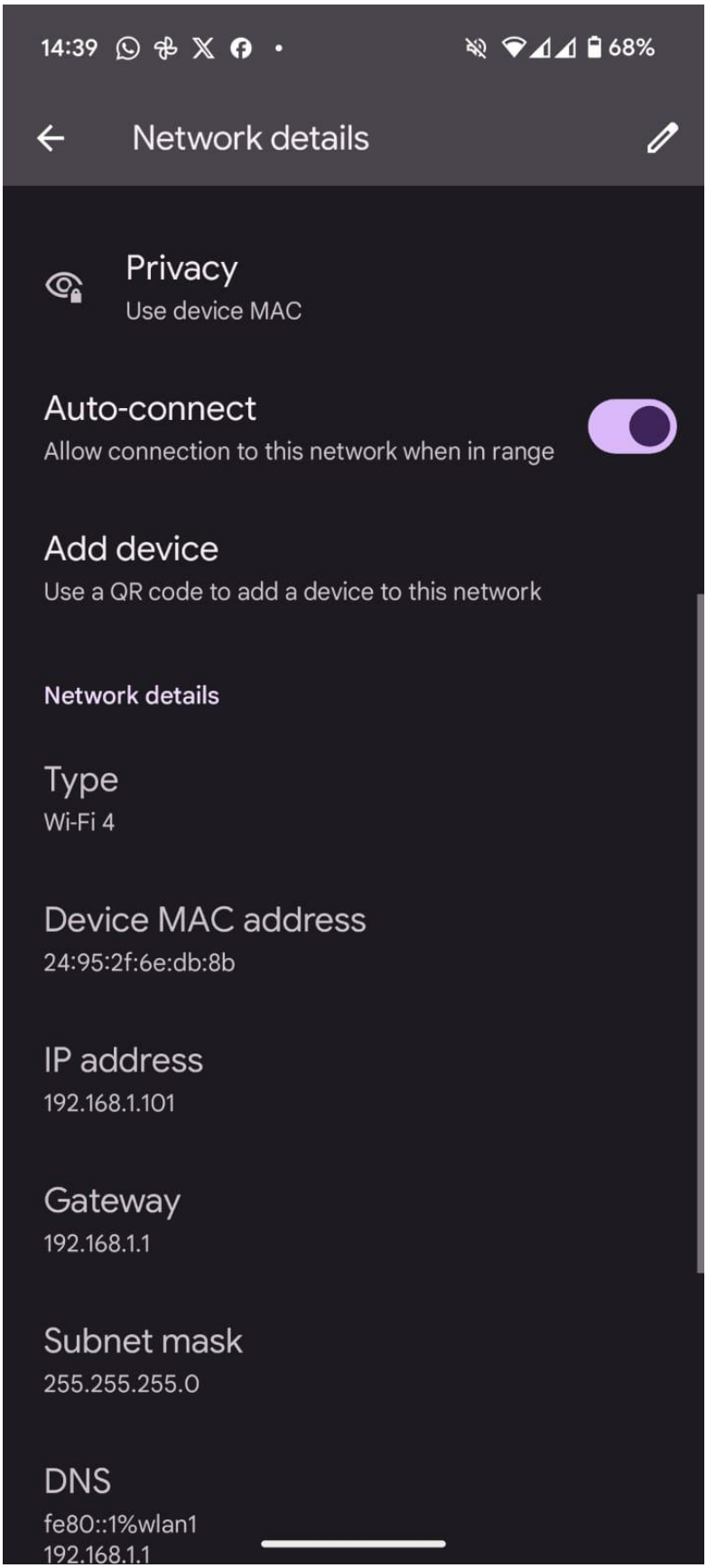




Start the service with the command “sudo systemctl start isc-dhcp-server”. We can enable it to run on boot with the command “sudo sytemctl enable isc-dhcp-server”.

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.



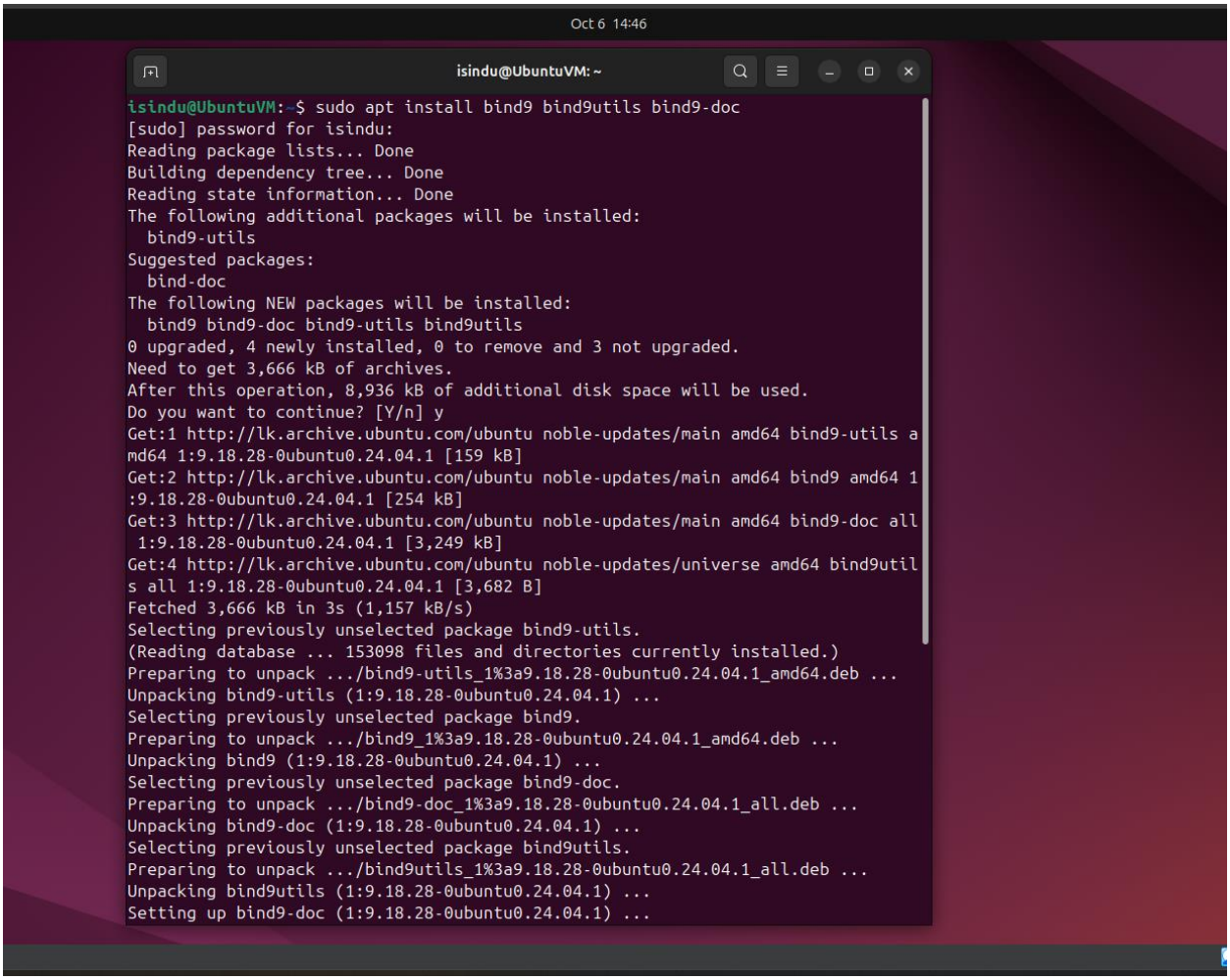

14:39
68%
Network details
Privacy
Use device MAC
Auto-connect
Allow connection to this network when in range
Add device
Use a QR code to add a device to this network
Network details
Type
Wi-Fi 4
Device MAC address
24:95:2f:6e:db:8b
IP address
192.168.1.101
Gateway
192.168.1.1
Subnet mask
255.255.255.0
DNS
fe80::1%wlan1
192.168.1.1

2.3) DNS (Domain Name System)

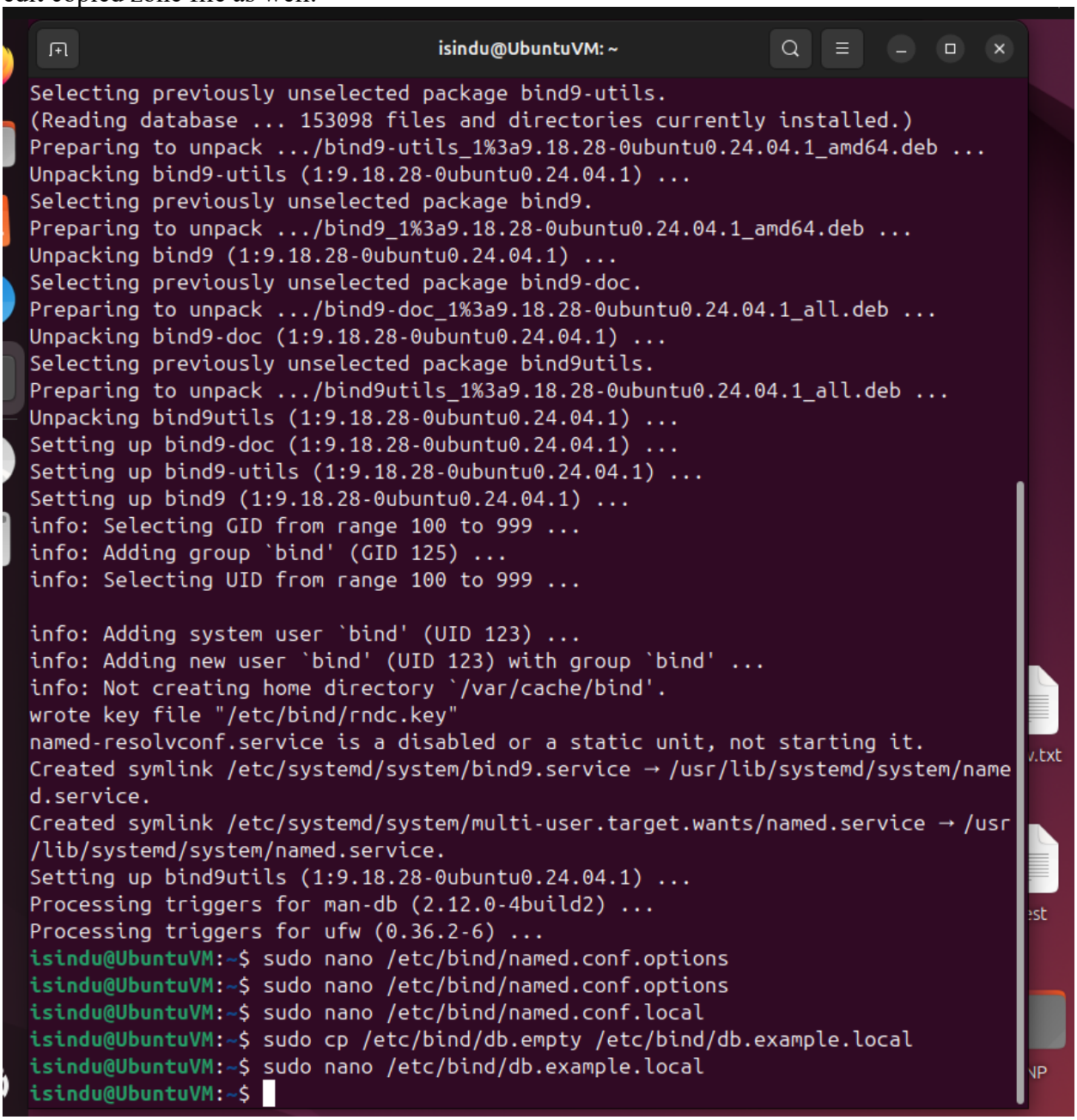
DNS (Domain Name System) plays a crucial role in translating human domains names to machine readable IP addresses which allows users to access websites with ease.

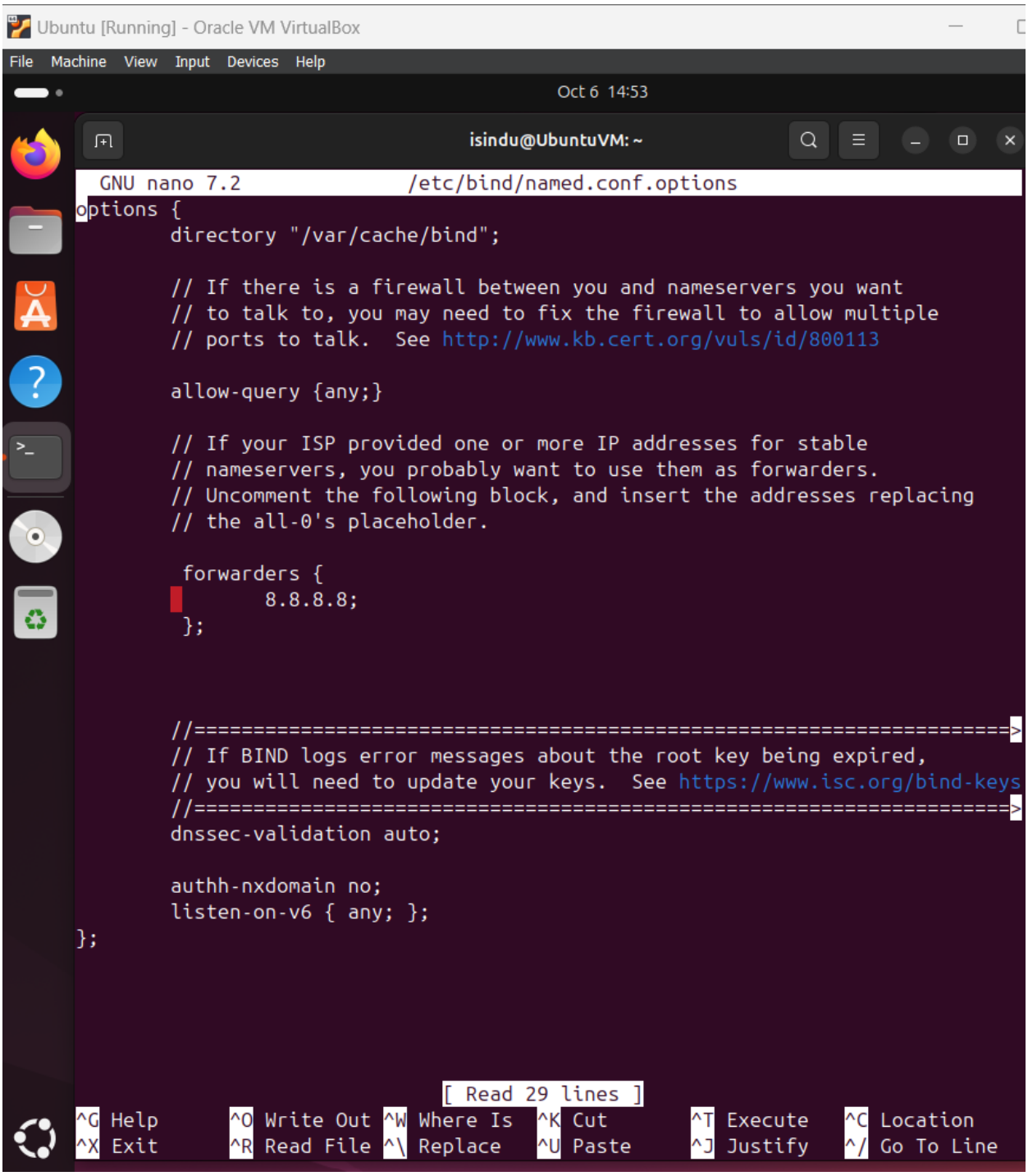
2.4) Installation and Configuration

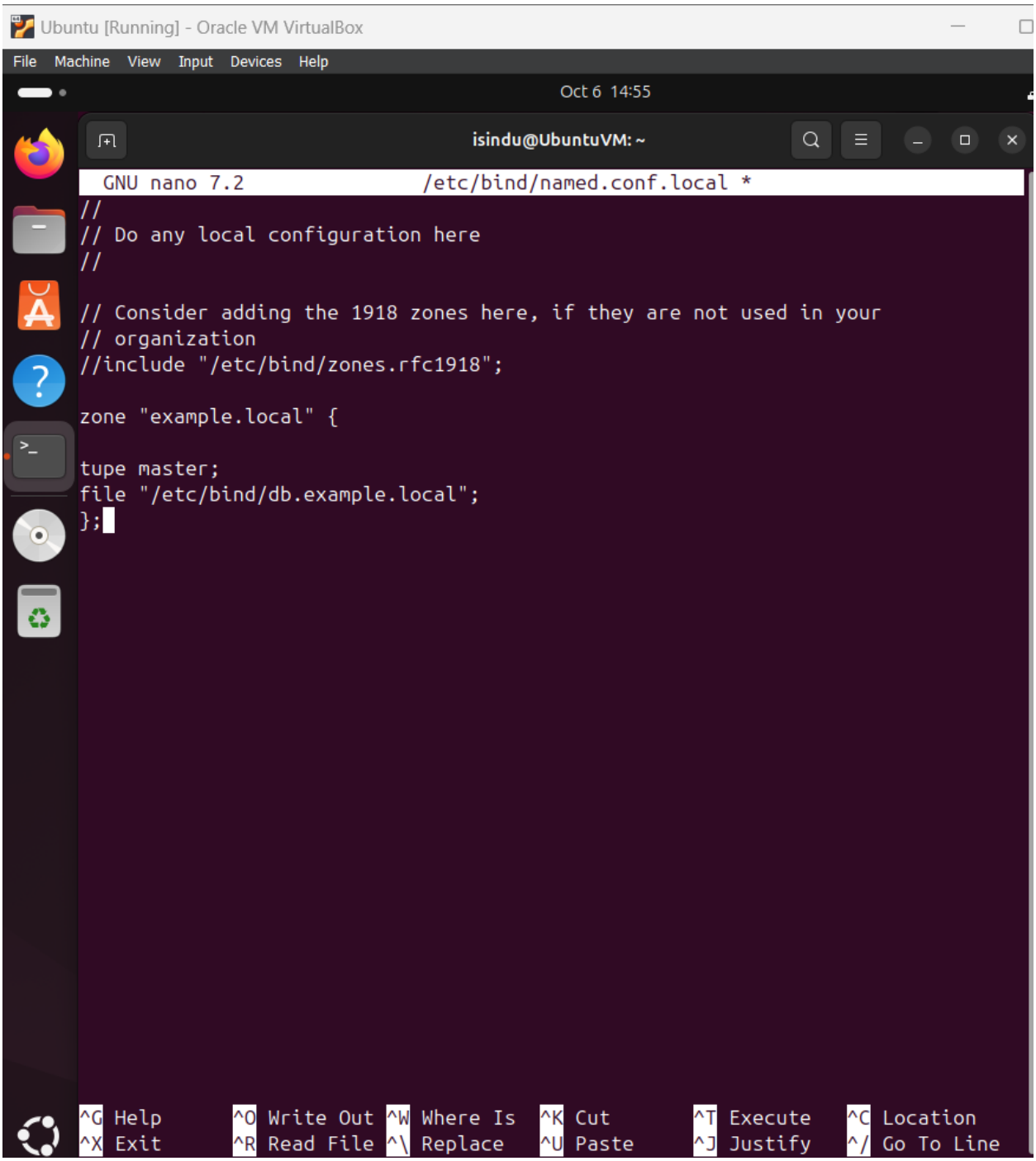
Install a DNS Server like BIND (Berkeley Internet Name Domain) and packages with “sudo apt install bind9 bind9utils bind9-doc” command.

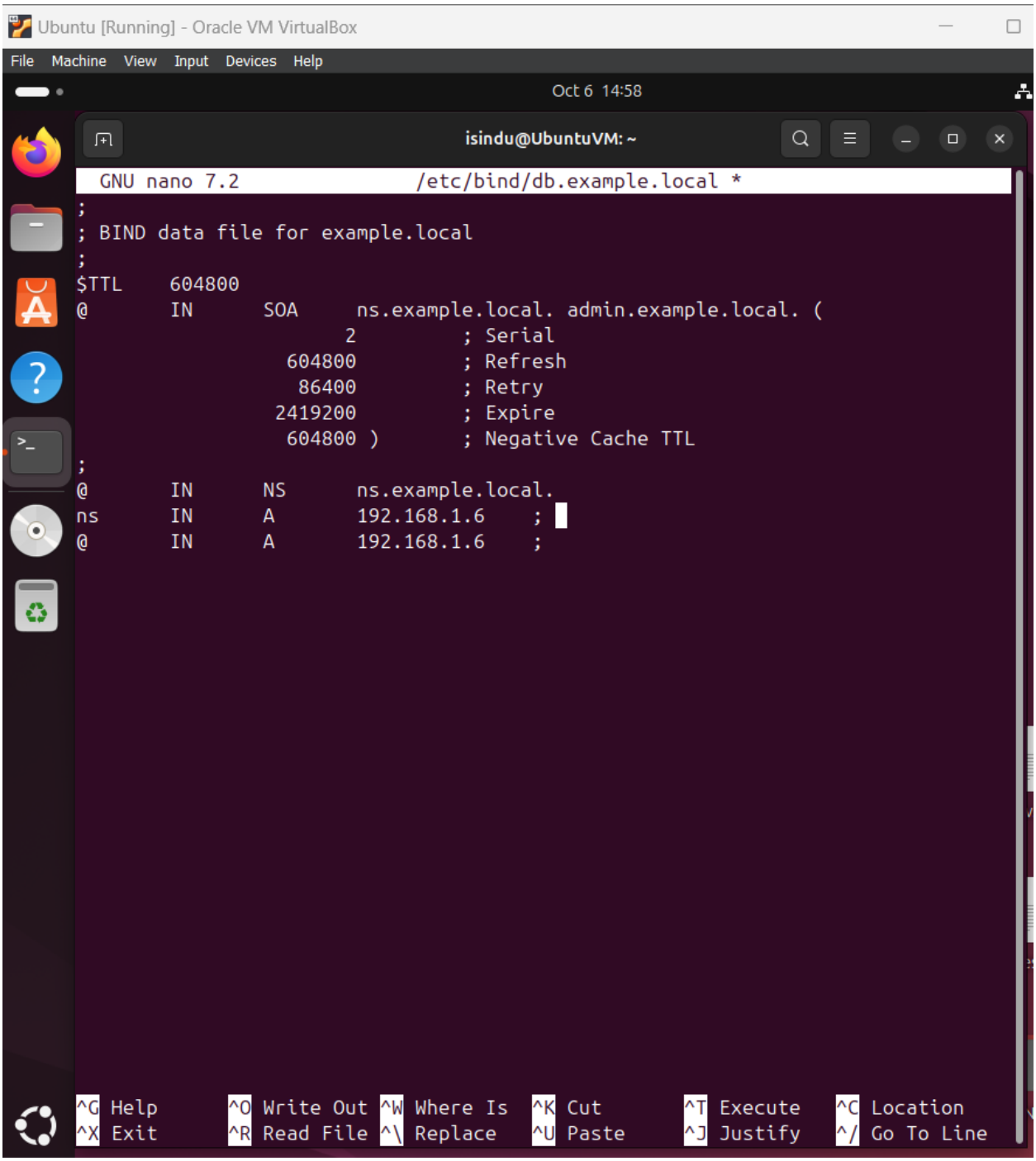


Open and edit BIND configuration file, zone configuration and copy the default zone file and edit copied zone file as well.

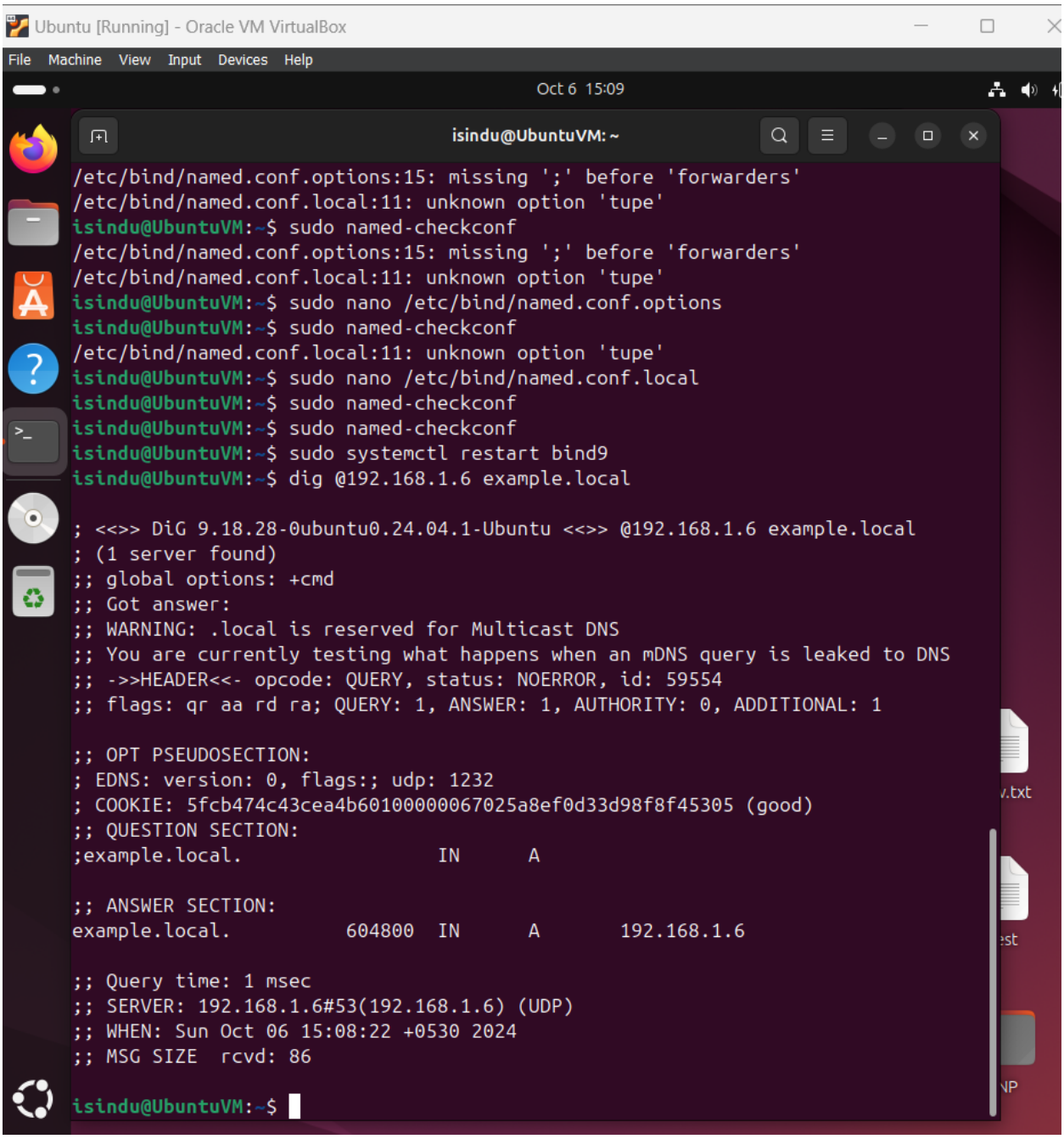



Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Oct 6 14:53
isindu@UbuntuVM: ~
GNU nano 7.2 /etc/bind/named.conf.options
options {
directory "/var/cache/bind";
// If there is a firewall between you and nameservers you want
// to talk to, you may need to fix the firewall to 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;
authh-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" {
tupe master;
file "/etc/bind/db.example.local";
};
^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 14:58
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.

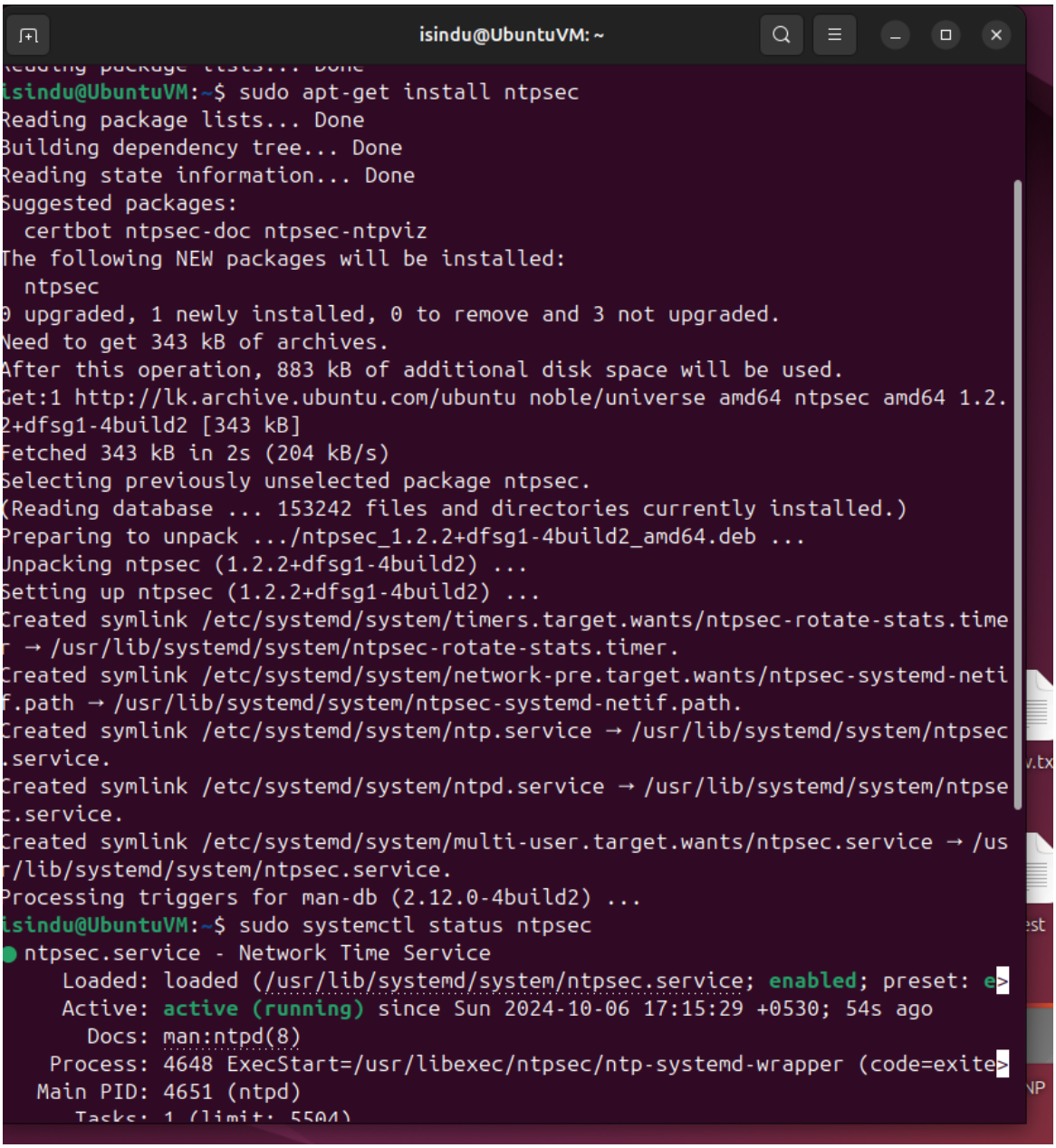


2.5) NTP (Network Time Protocol)

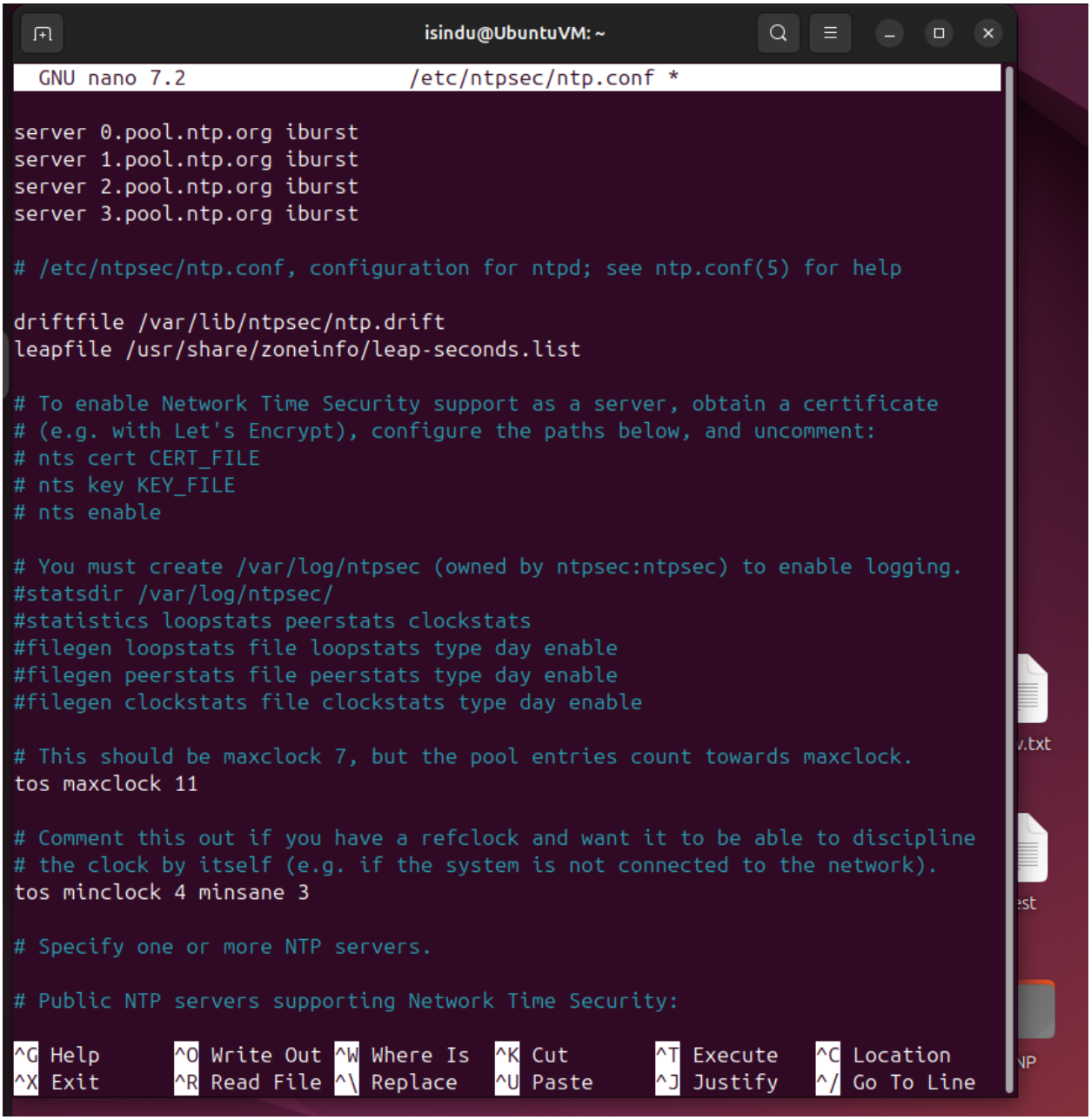
NTP (Network Time Protocol) is a protocol designed to synchronize the clocks of computers in a network. IT ensures that all the computers on the network maintain the accurate time.

2.6) Installation and Configuration

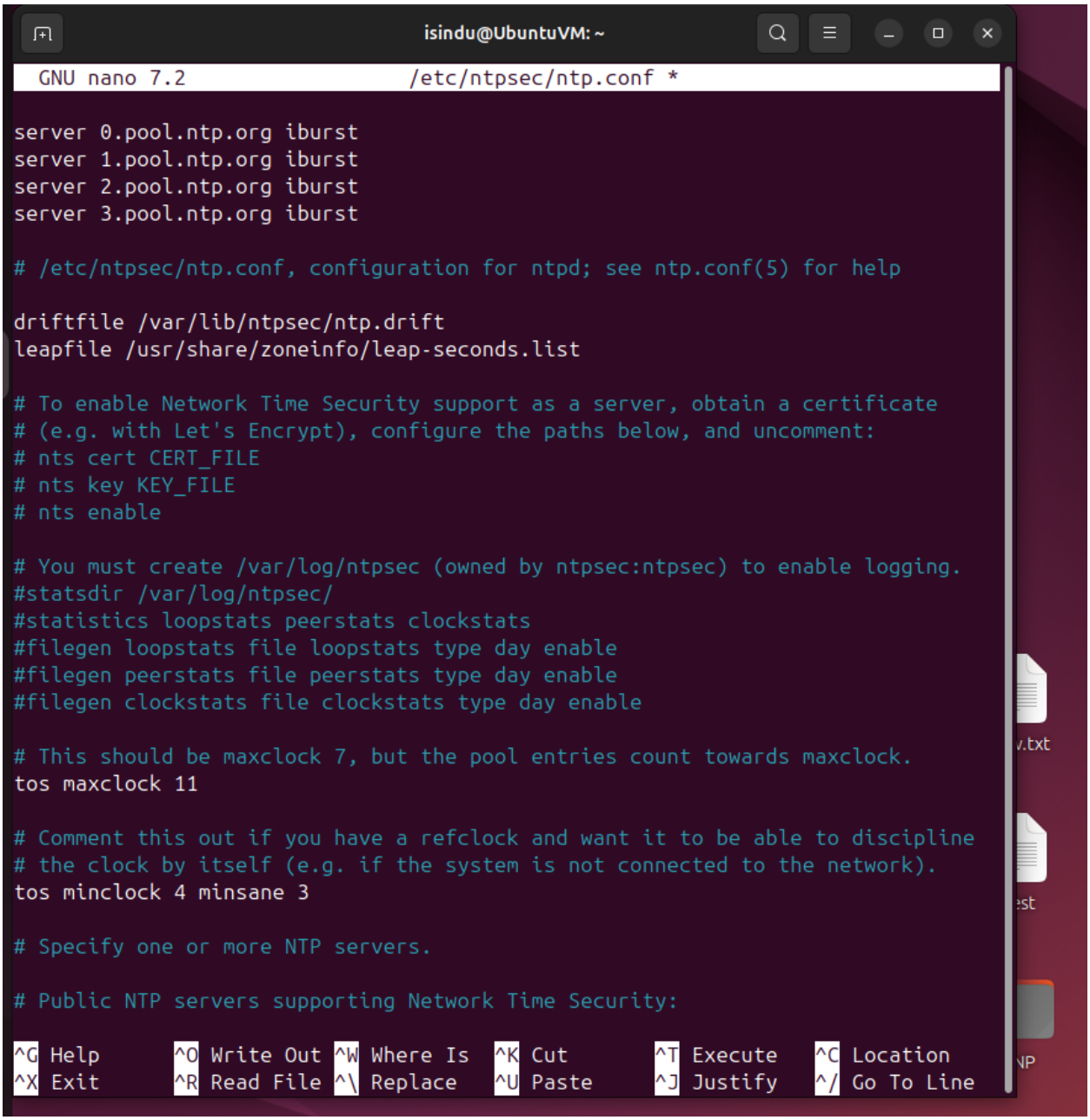
Install the ntpsec package “sudo apt-get ins ntpsec” then verify the ins with “sudo systemctl status ntpsec”.



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



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.



3. Shell Scripting and Security

3.1) Shell Scripting

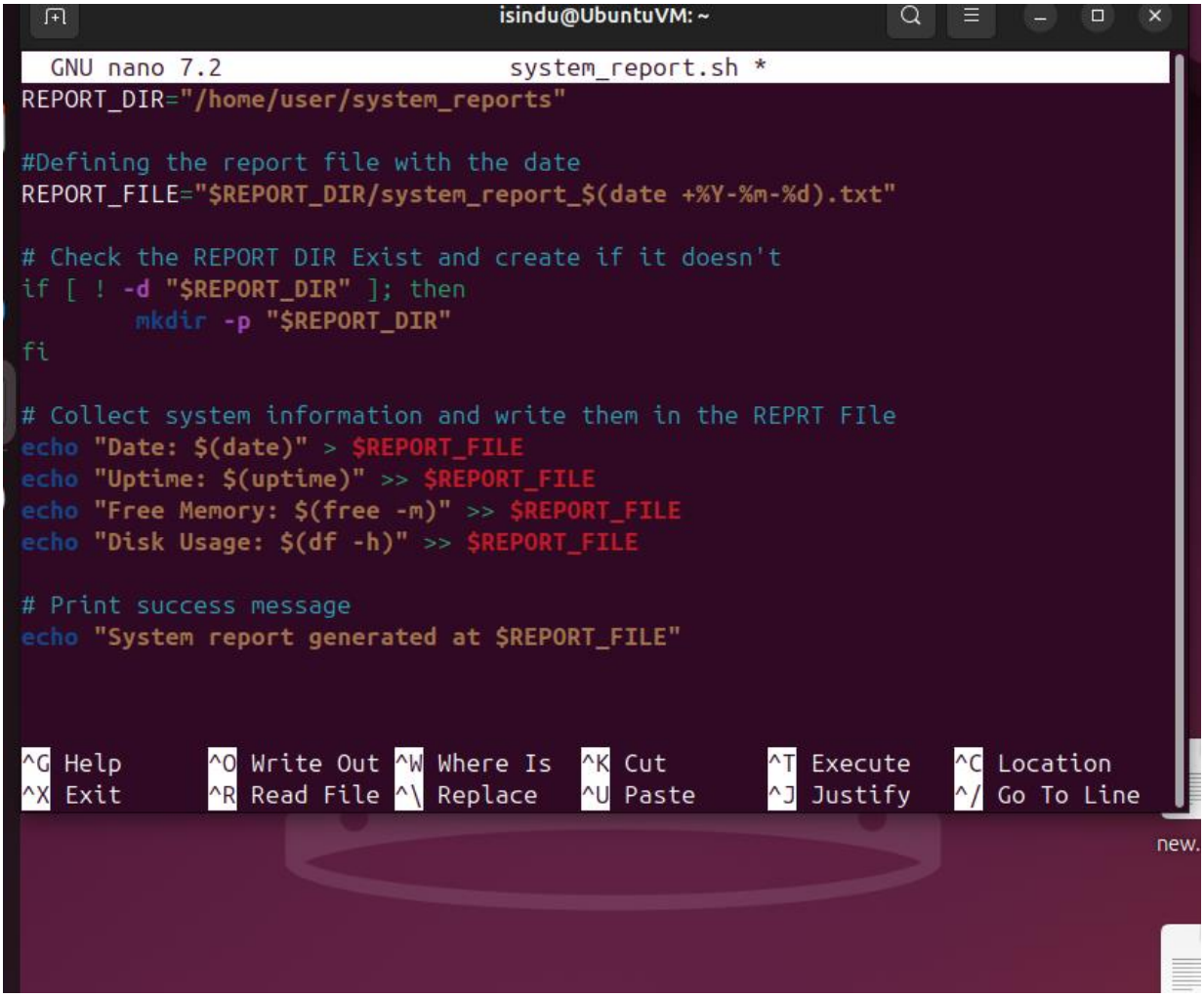
i. Script to automate a report that captures system details every day.

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

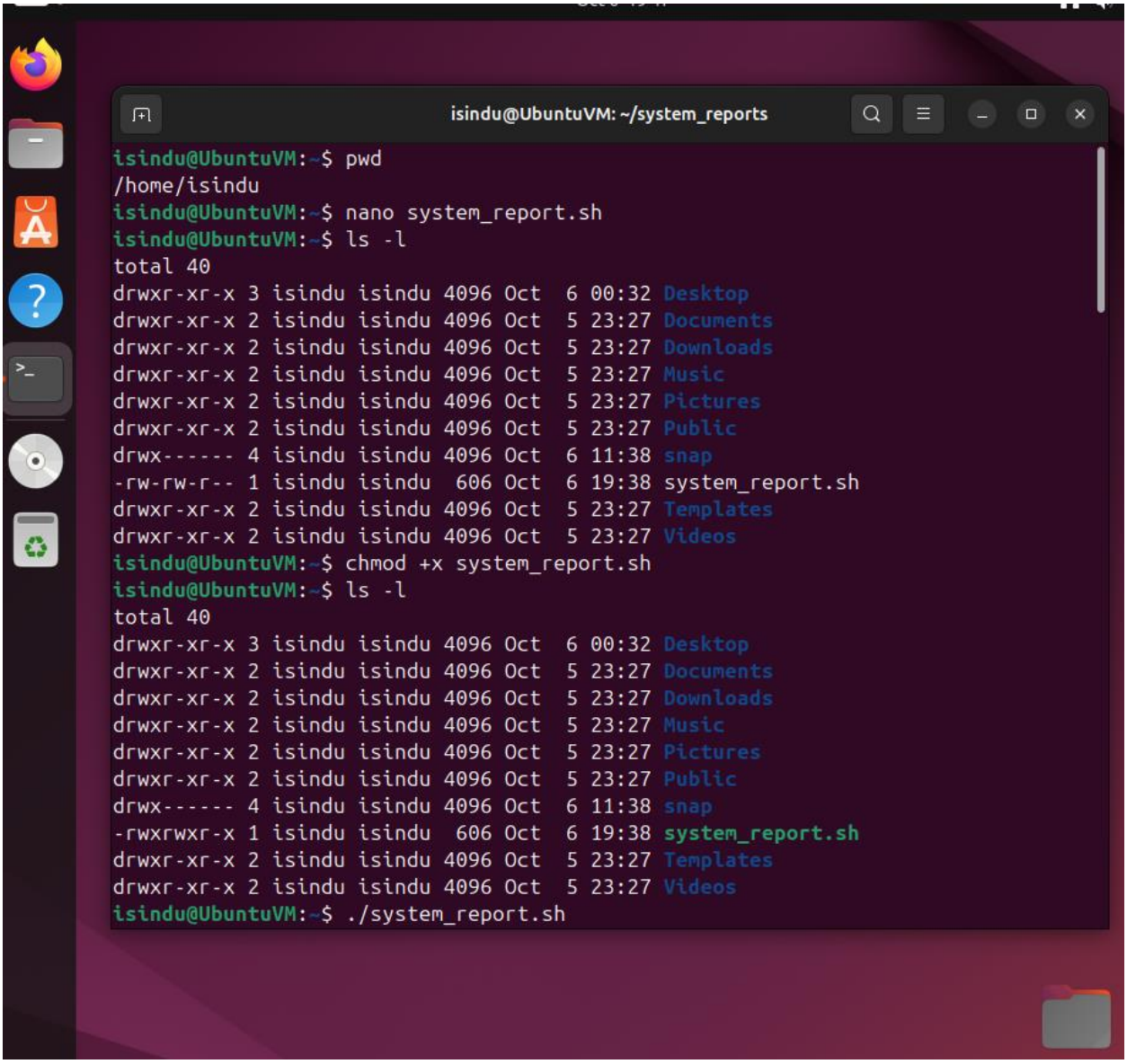
“nano system_report.sh”

Then Write the following script

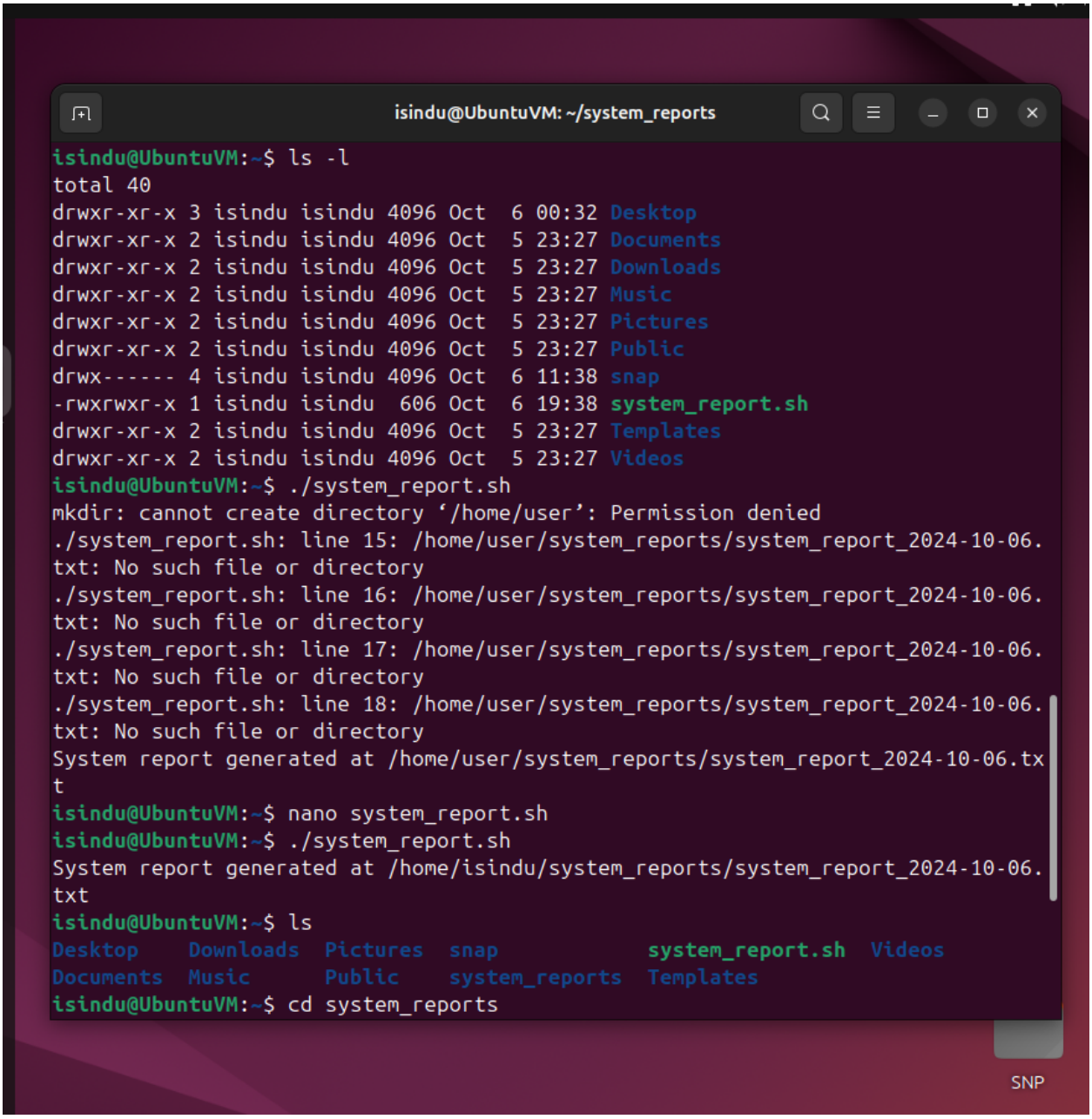
```
REPORT_DIR="/home/isindu/system_reports"

#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"
```



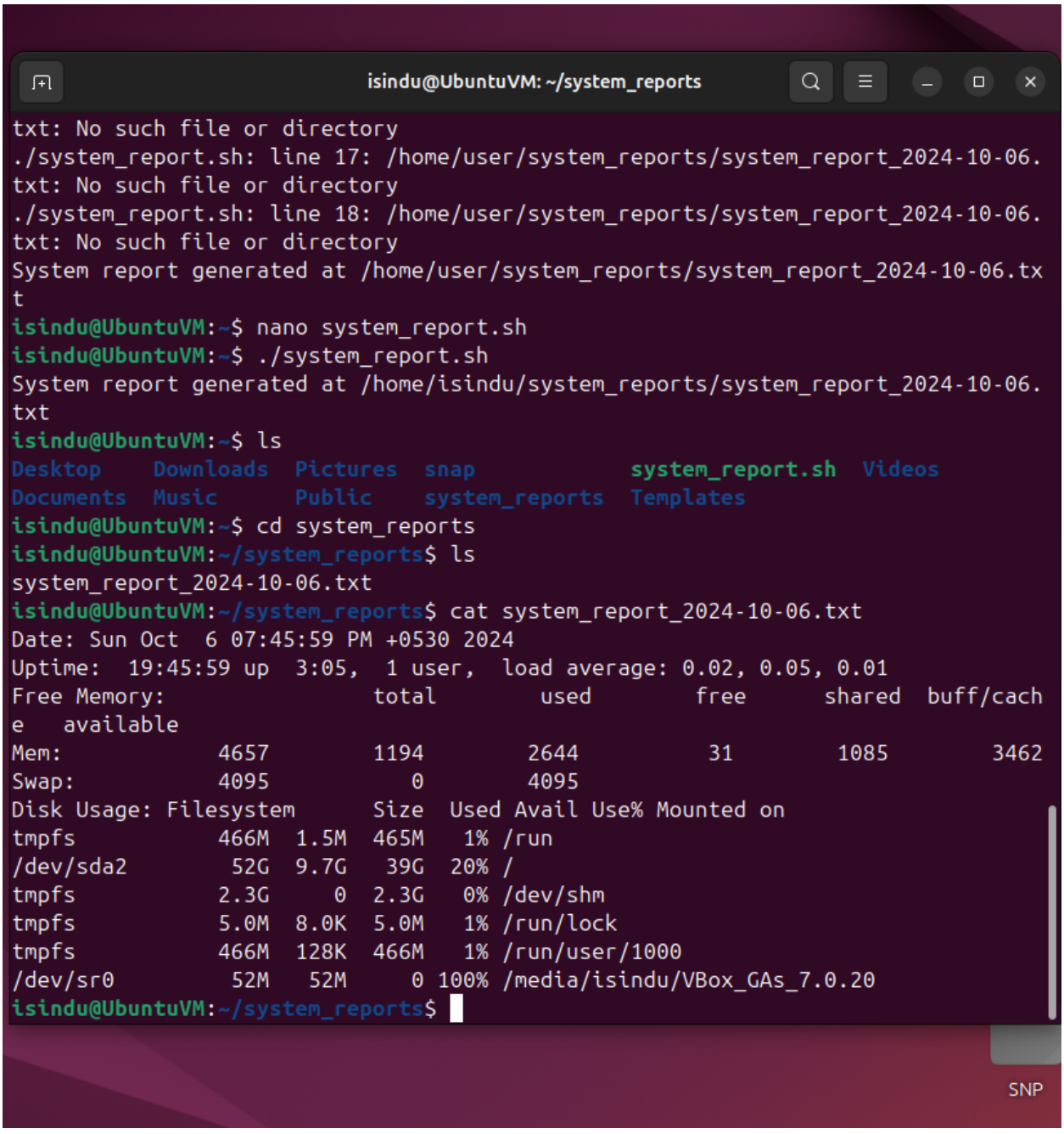
Make the script executable with “chmod +x system_report.sh”



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


isindu@UbuntuVM: ~/system_reports
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
SNP

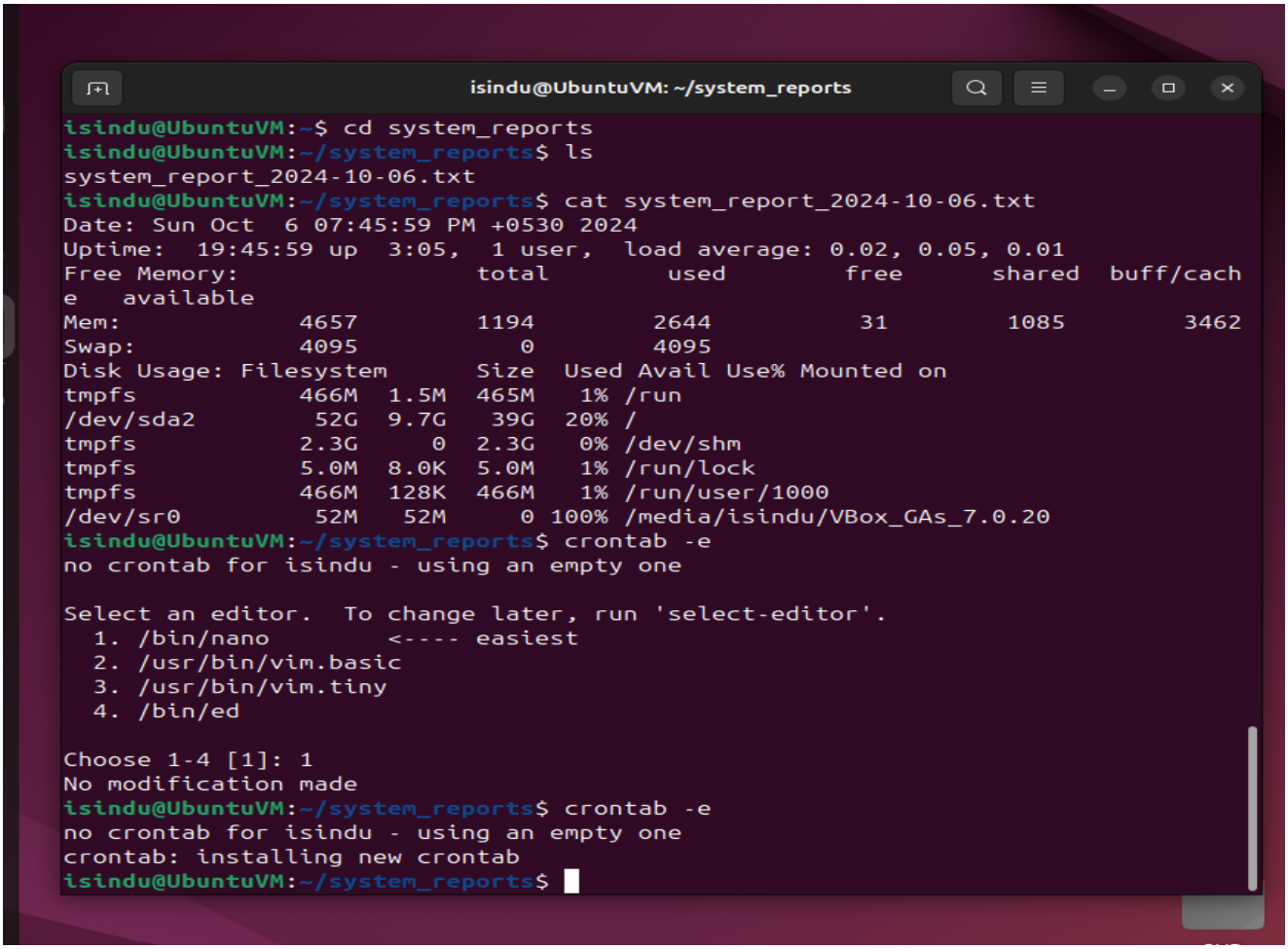
Read and check the contents of the file with “cat /system_reports/ system_report_2024-10-06.txt”

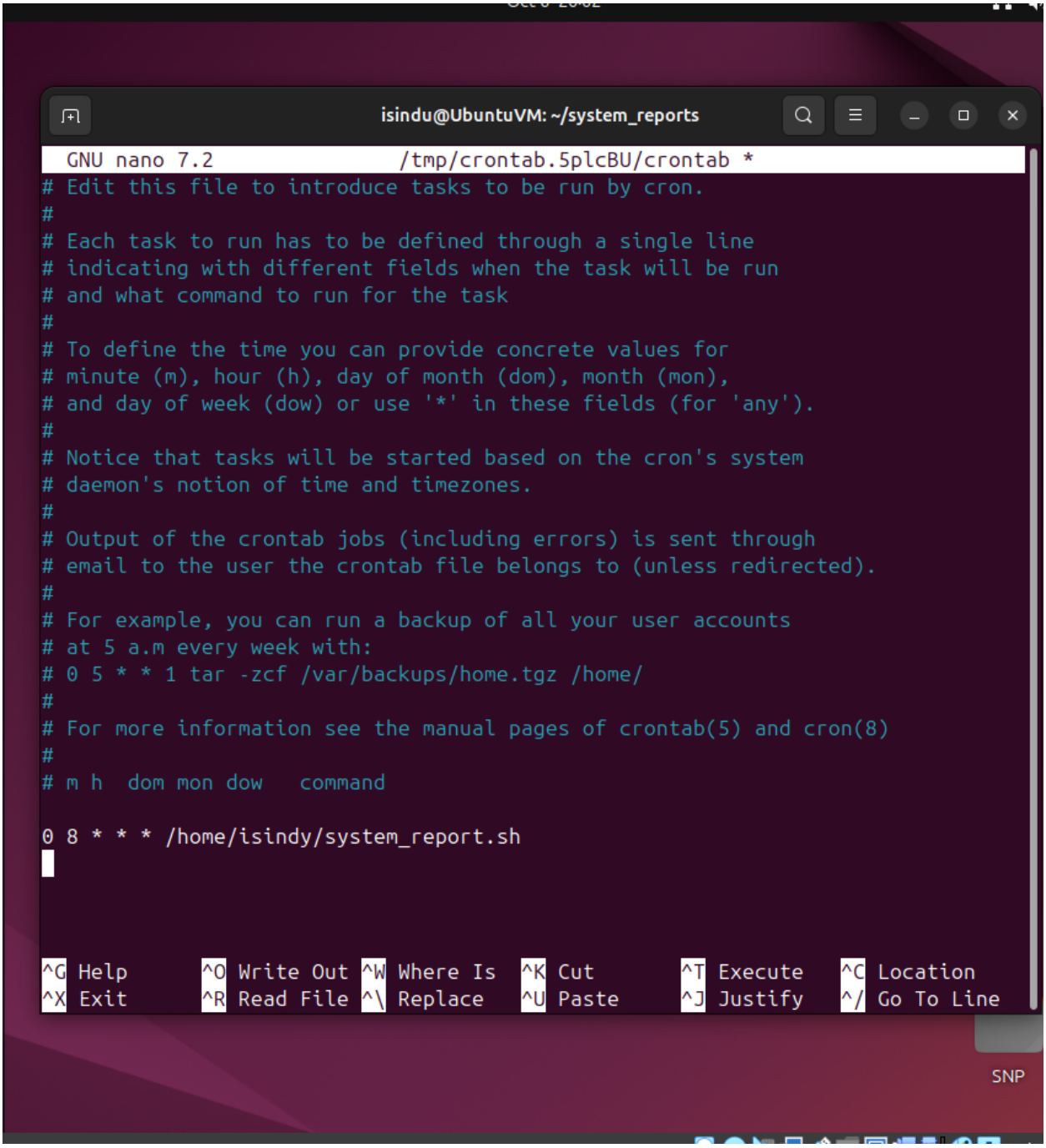


This report contains current date, system uptime, number of users, Memory details, disk usage etc.

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




isindu@UbuntuVM: ~/system_reports
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

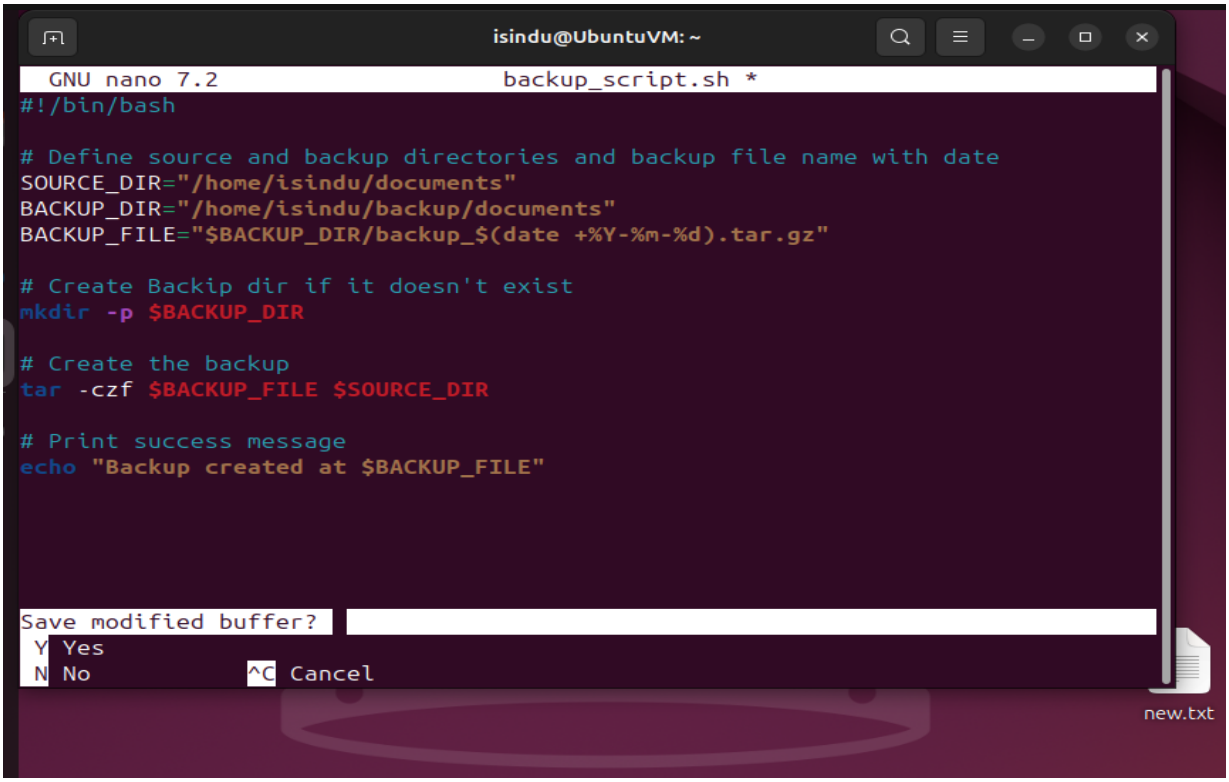
ii. Script to automate the backup of the Documents directory

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

“nano backup_script.sh”

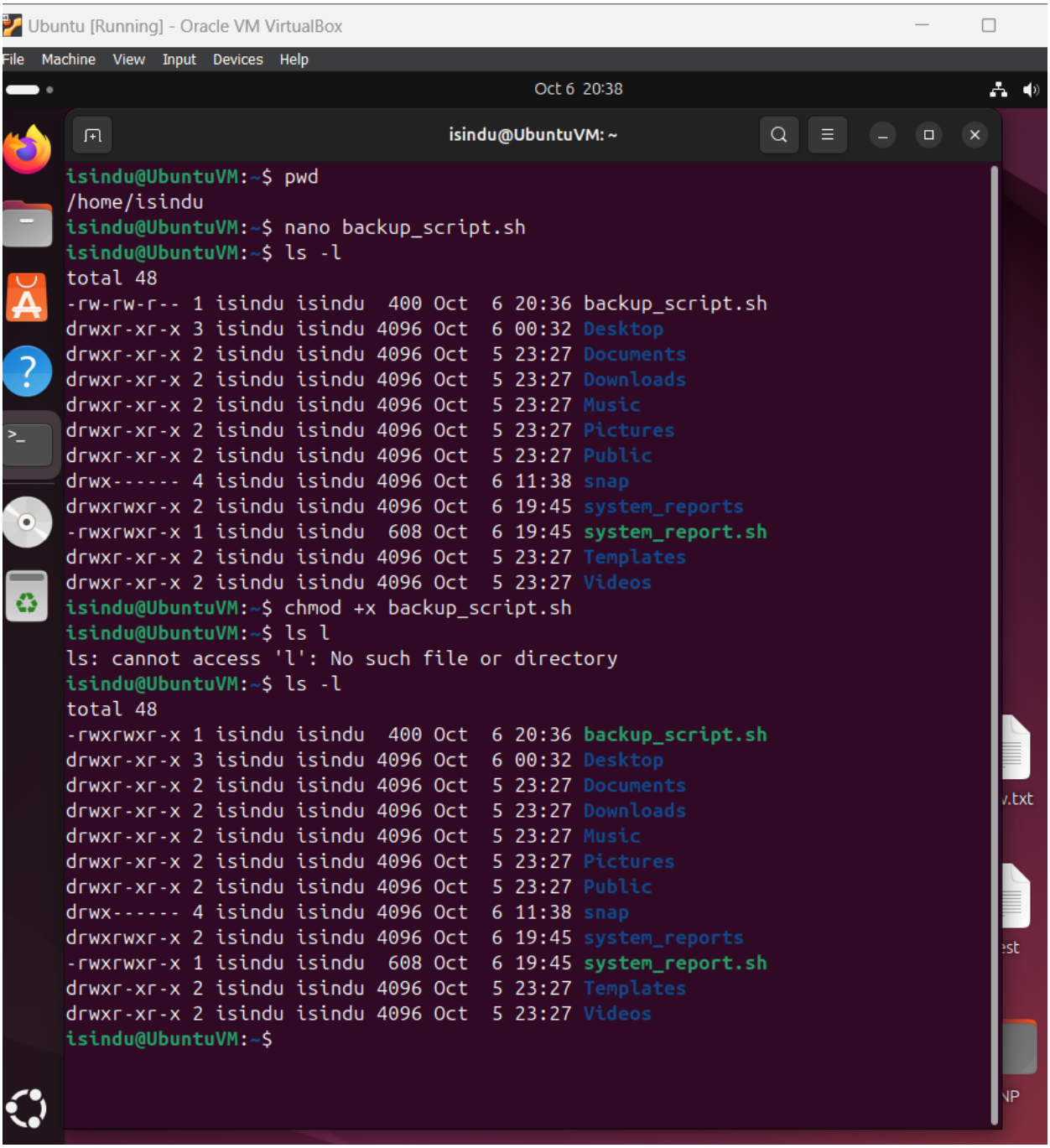
Insert the following script and save the file.

```
#!/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 Backip 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"
```

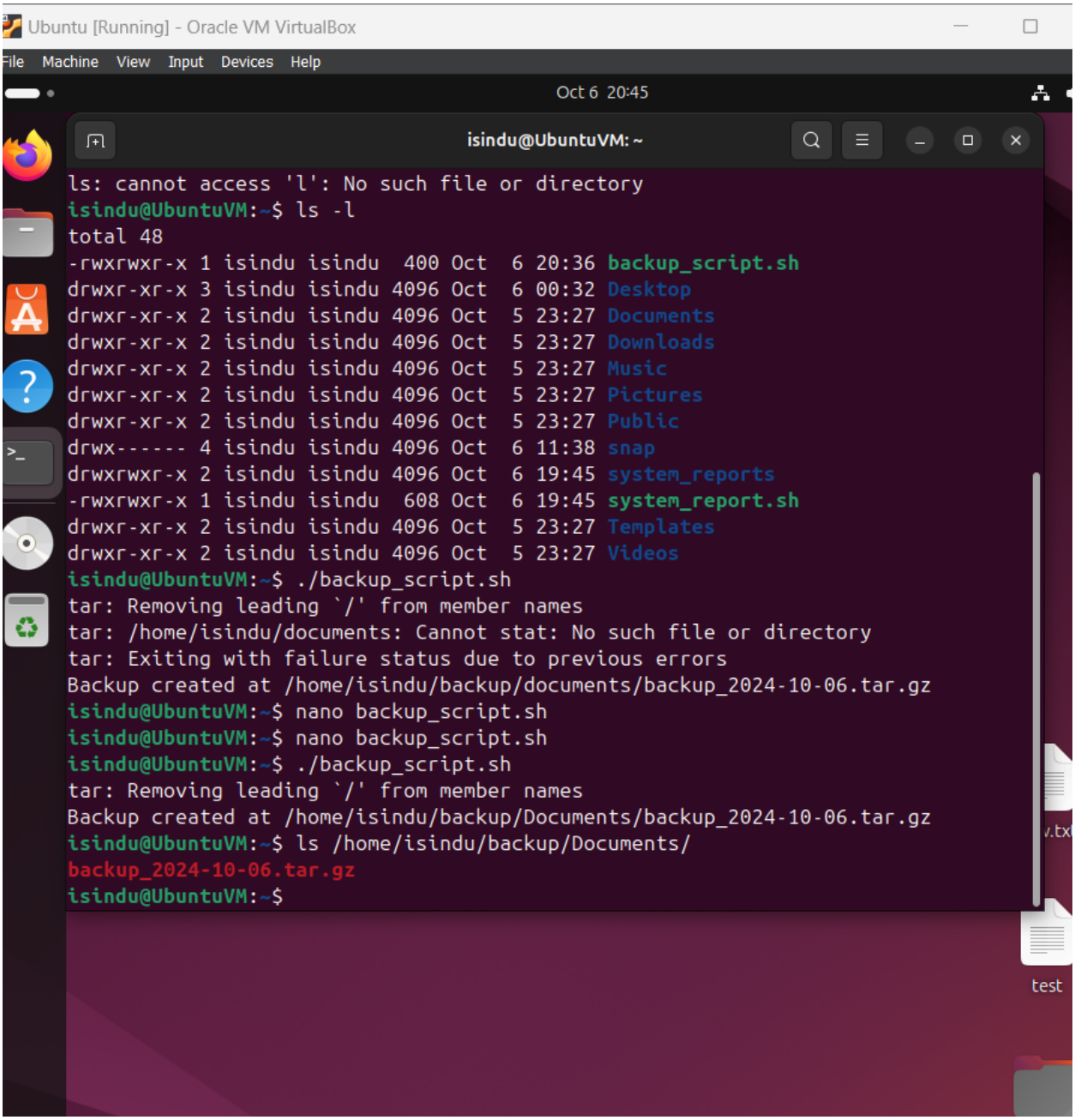


Make the script executable.

“Chmod +x backup_script.sh”



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



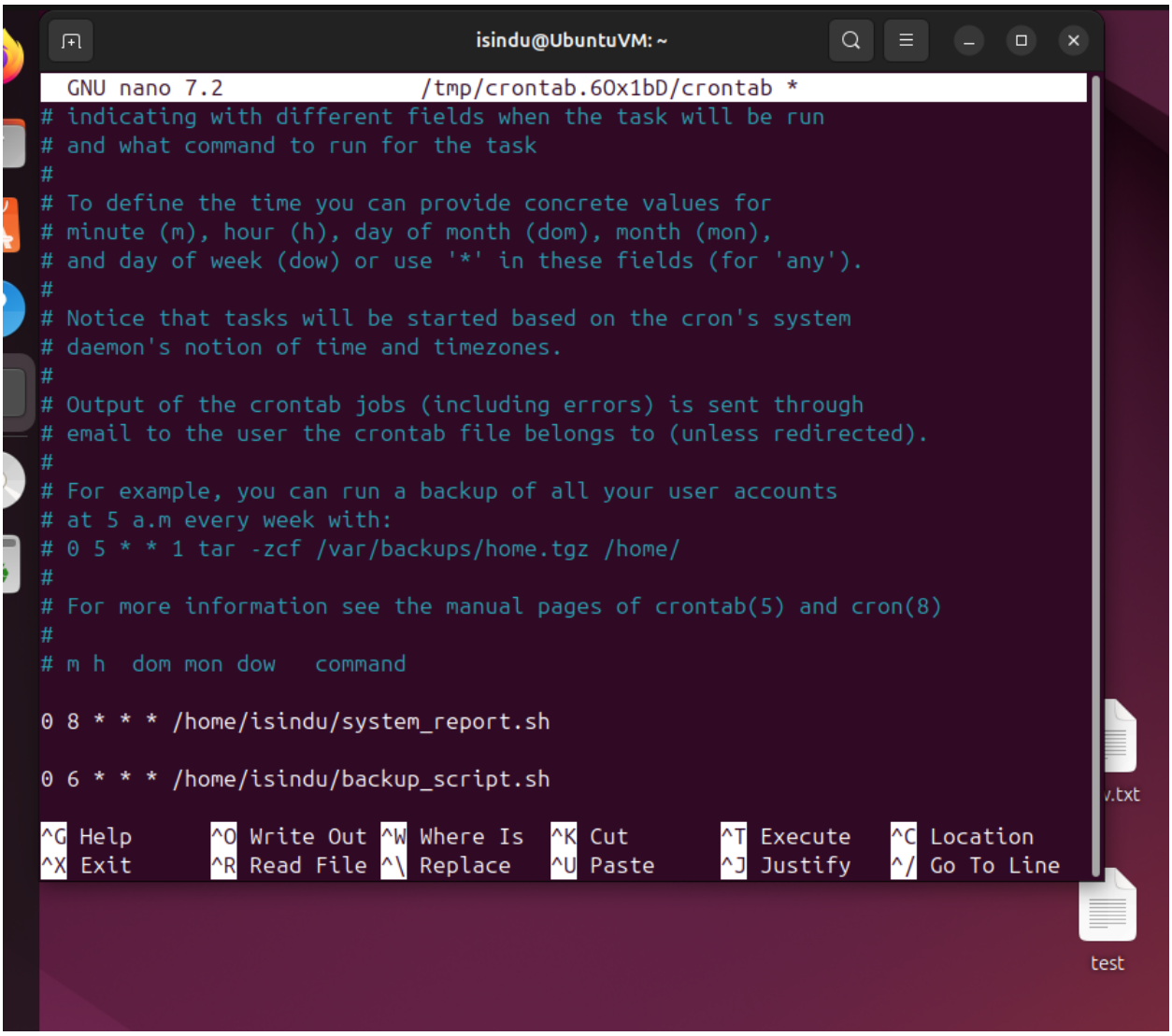
If you got the successful message check the Documents directory for the backup file.

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

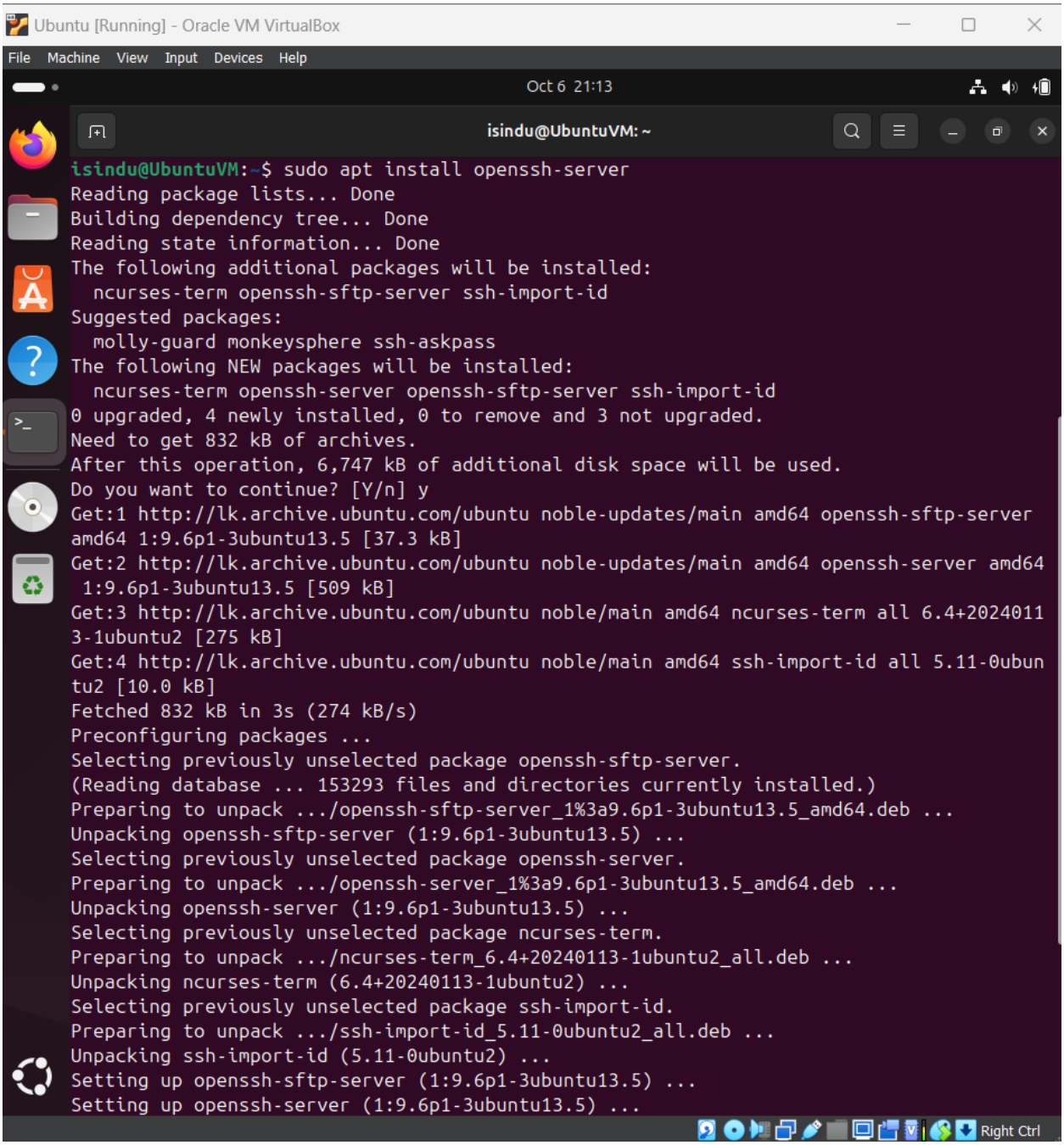


This tells Cron to run the script every day at 6.00 am

3.2) SSH (Secure Shell)

Install the ssh server.

“sudo apt install openssh-server”



After installation start the SSH service with following command.

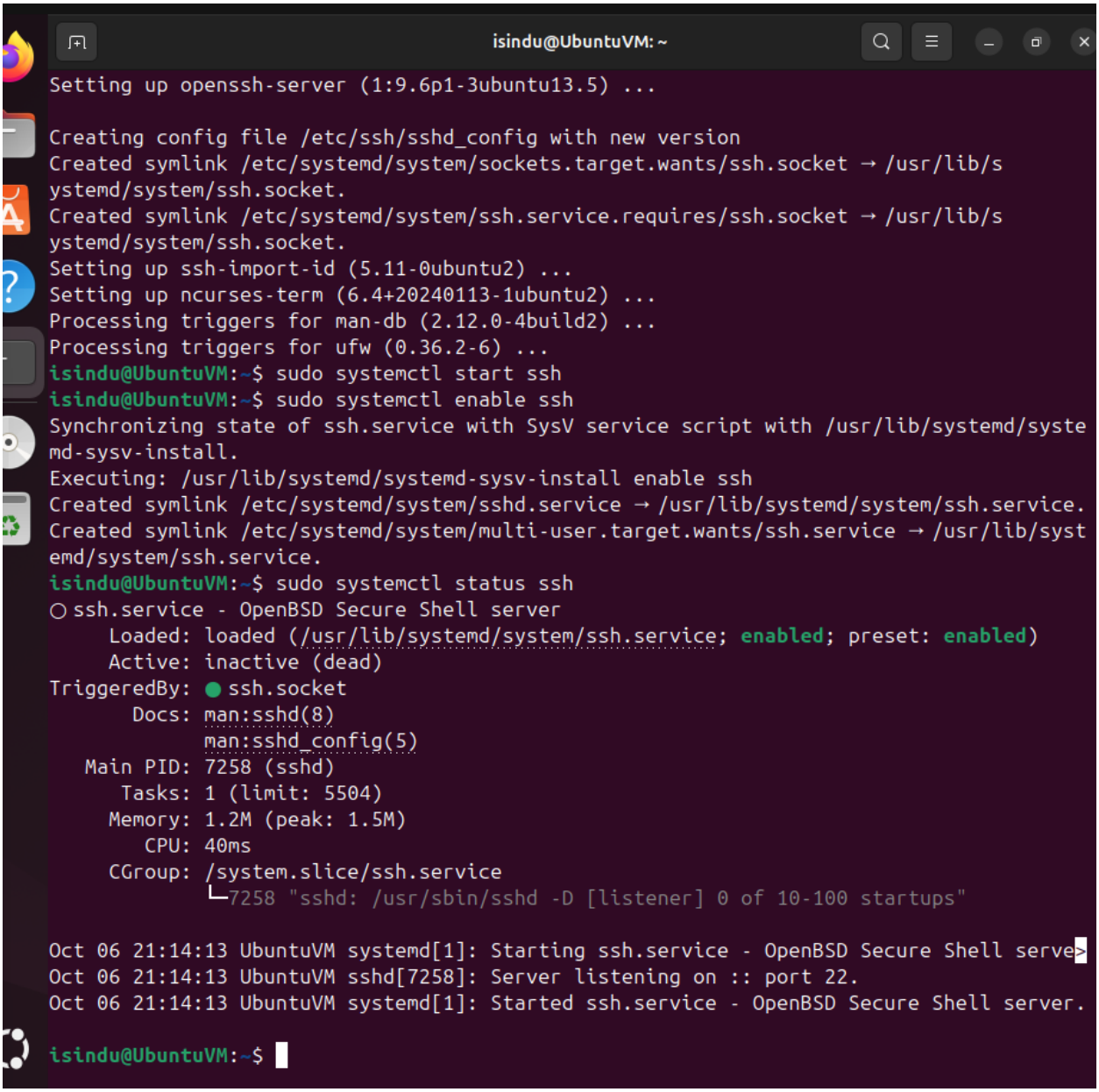
“suto systemctl start ssh”

Make the service auto start at boot.

“sudo systemctl enable ssh”

Check the status of the system.

“sudo systemctl status ssh”

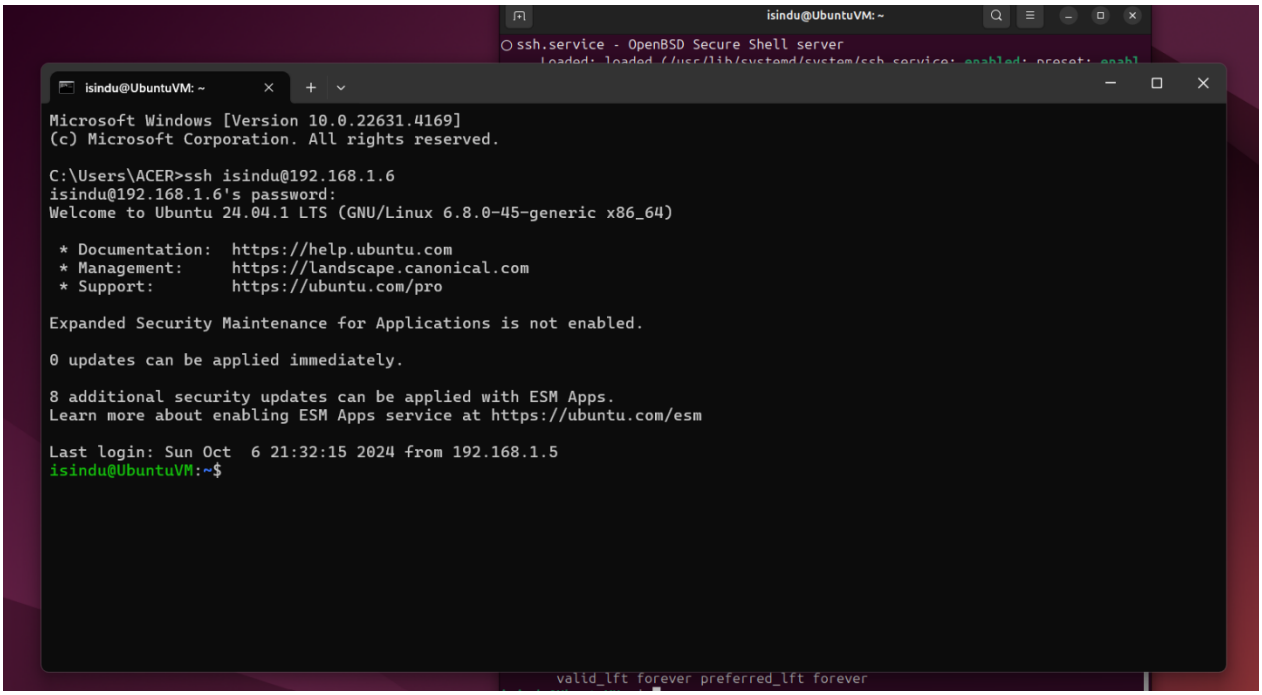


Find the ip address of the virtual machine.

“ip a”

```
isindu@UbuntuVM:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 gr
oup 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 enp
0s3
       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”

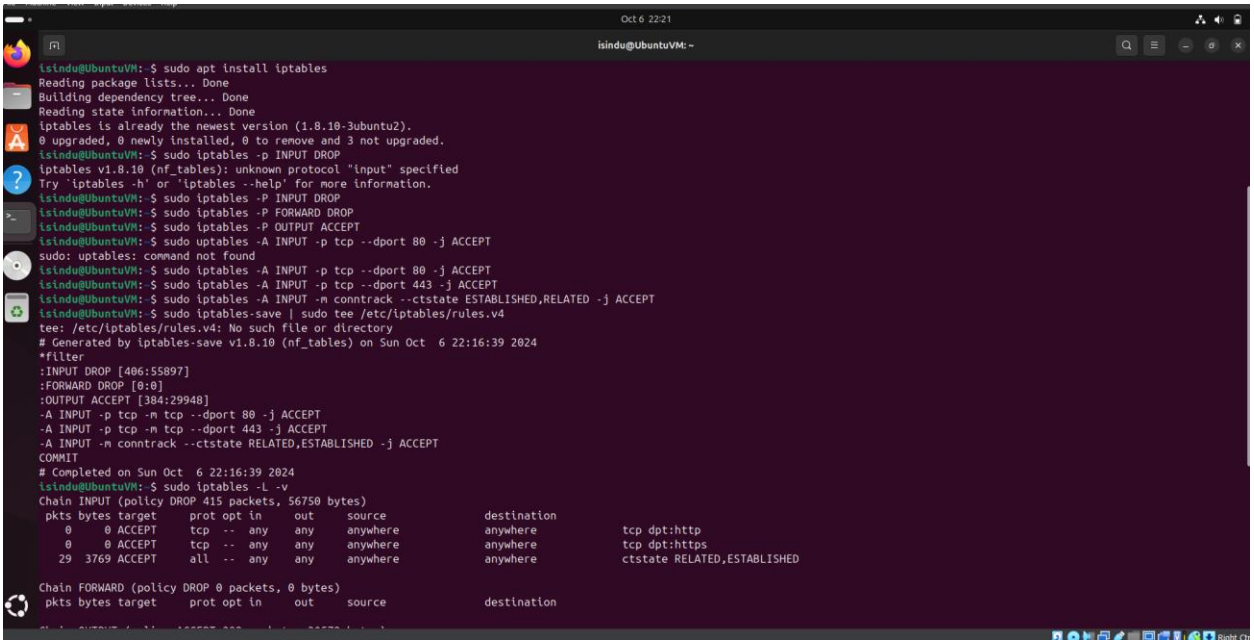
Set default policies
“sudo iptables -P INPUT DROP”
“sudo iptables -P FORWARD DROP”
“sudo iptables -P OUTPUT ACCEPT”

Allow incoming traffic on port 80 (HTTP)
“sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT”

Allow incoming traffic onn 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”

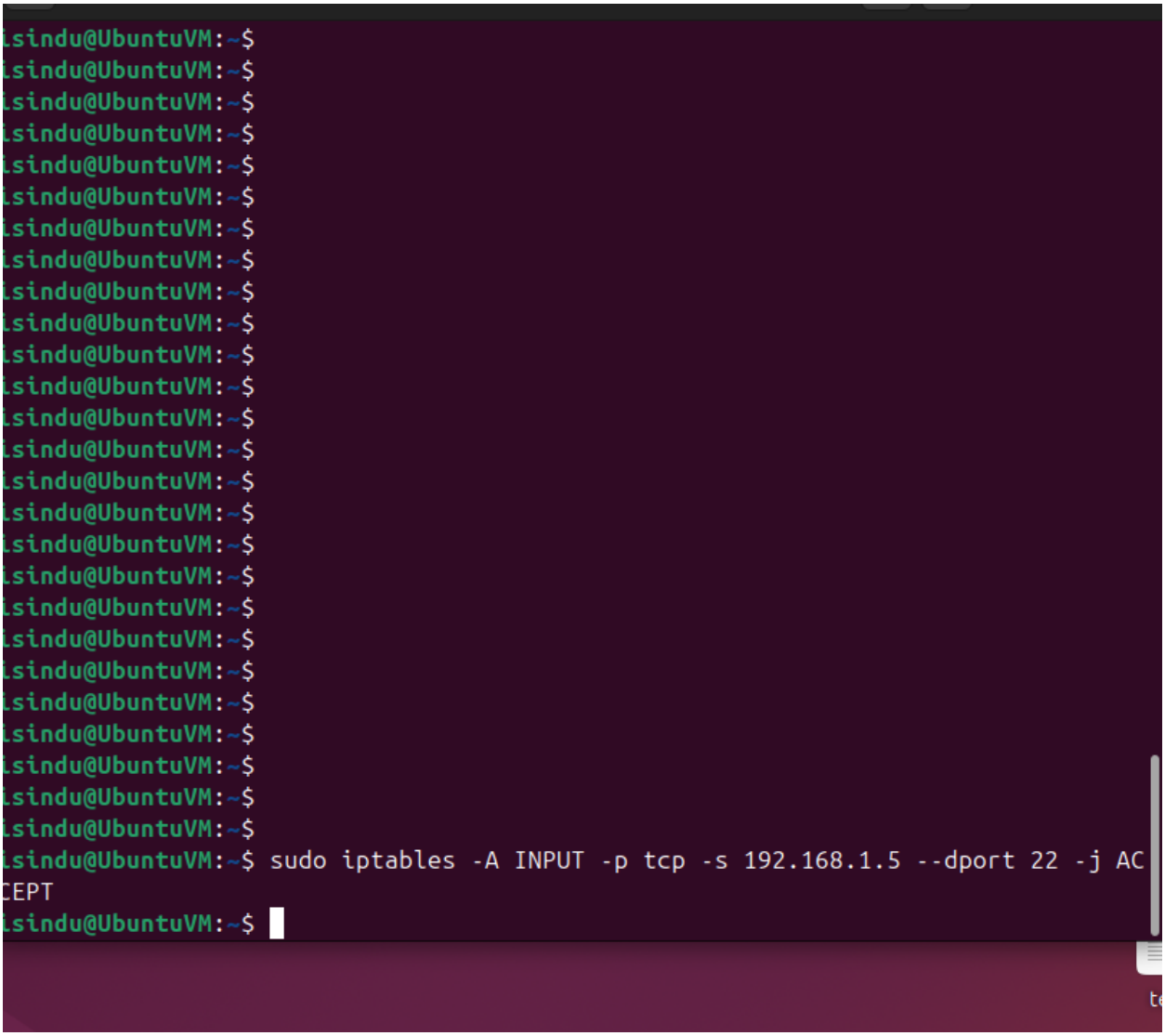
Save set rules.
“sudo iptables-save | sudo tee /etc/iptables/rules.v4”



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”



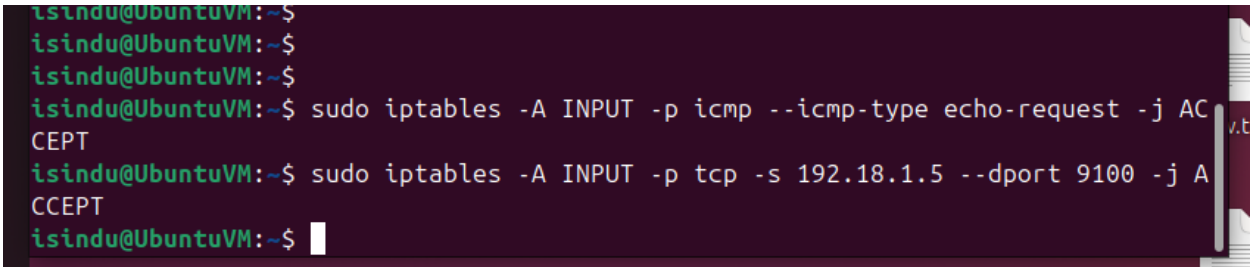
iii. Allow Specific Application

Use the following command to allow specific application.

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

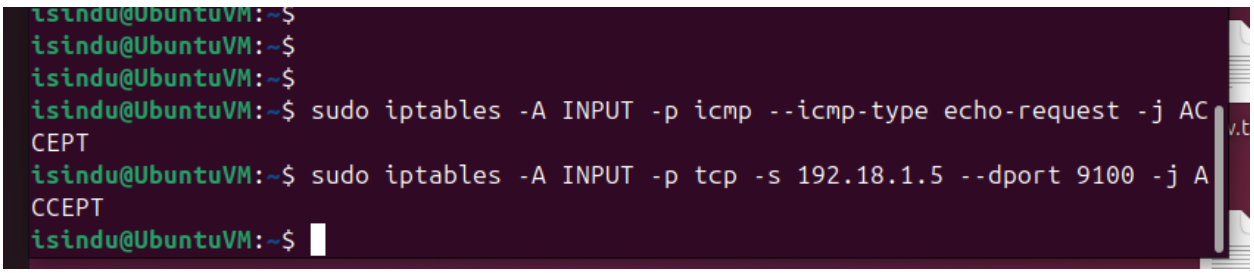
iv. Allow Pings (ICMP Echo Reques)

Use the following commands to allow ping request (ICMP Echo Request)
“sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT”



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 192.18.1.5 --dport 9100 -j ACCEPT”



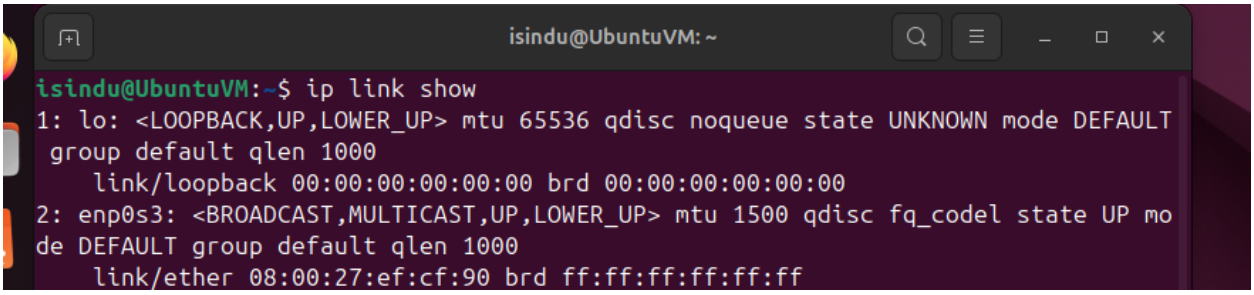
```
isindu@UbuntuVM:~$ sudo iptables -L
[sudo] password for isindu:
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     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.

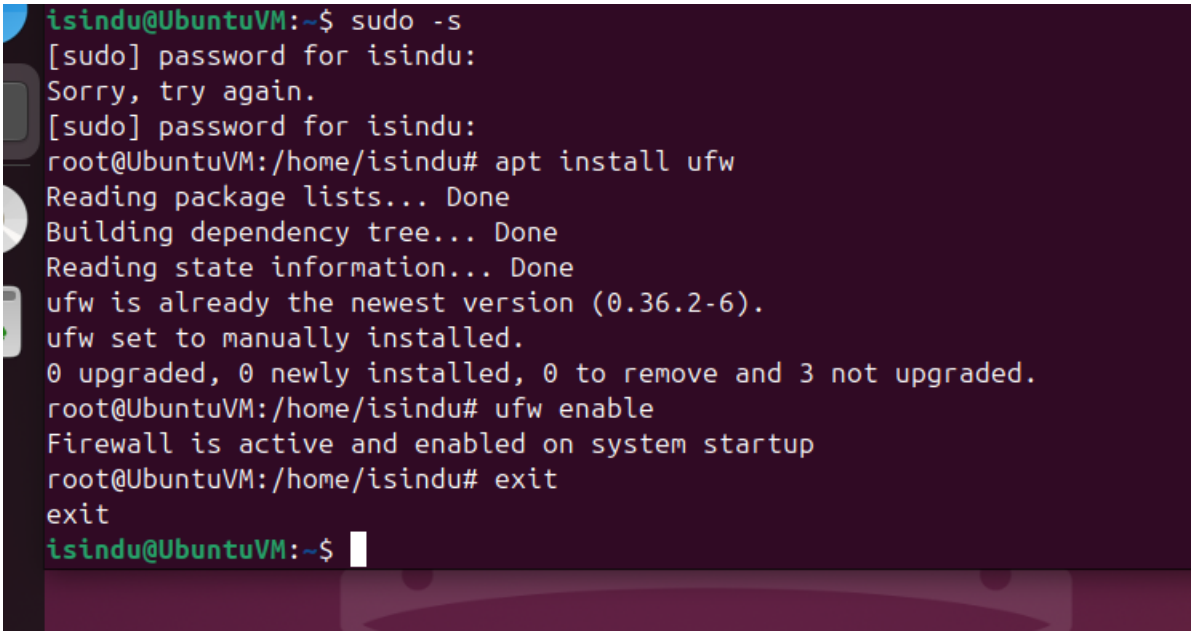
“ip link show” command lists out the interfaces in the system.



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



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”

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 at 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.