Sri Lanka Institute of Information Technology

Assignment Report

IT23159730

IE2012 - Systems and Network Programming

B.Sc. (Hons) in Information Technology Specializing in

Cyber Security

Table of Contents

Basics of Linux Environments

Virtual Machine Setup:

Download the Oracle Virtual Box using the following link.

https://www.virtualbox.org/wiki/Downloads

Navigate through the following steps.

1. Double click on the file you downloaded to open Virtual box installation setup (exe file).
2. Click on ‘’**Next**” button to continue the setup.

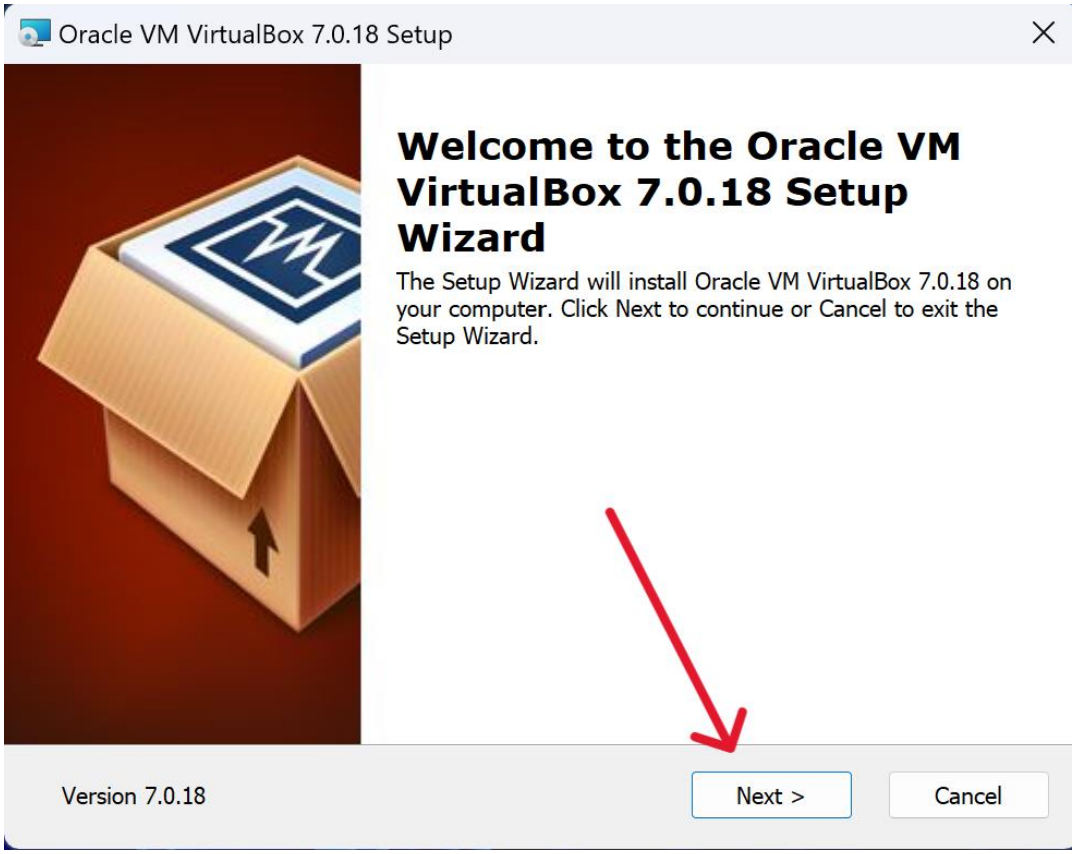

Figure 1

3. Select the location path you want to install the setup and then click on ‘’**Next**’’ button to continue the setup.

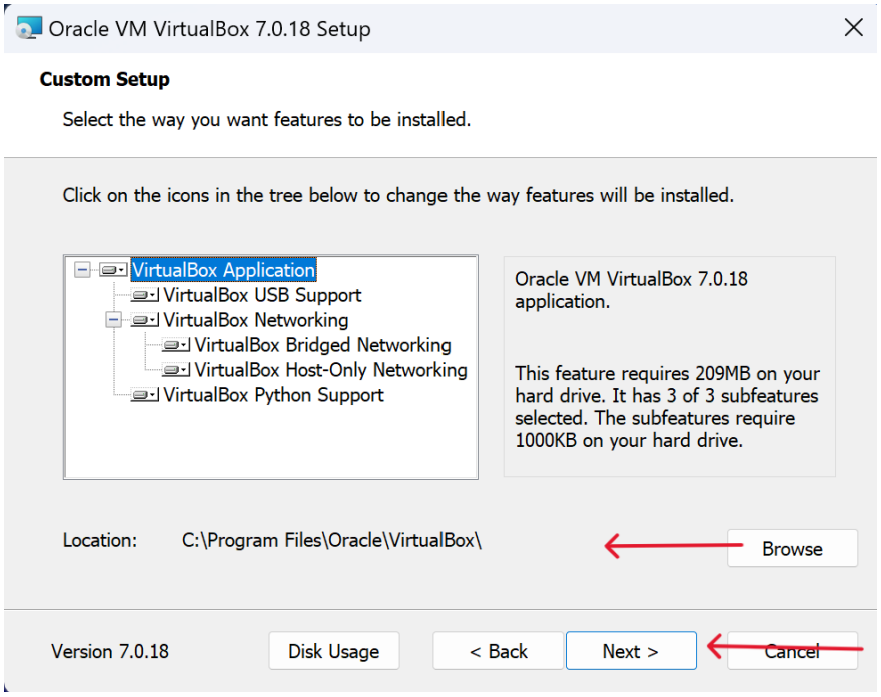

Figure 2

4. In this step there will be a warning message read it carefully and click on “**Yes**” button to continue the setup.

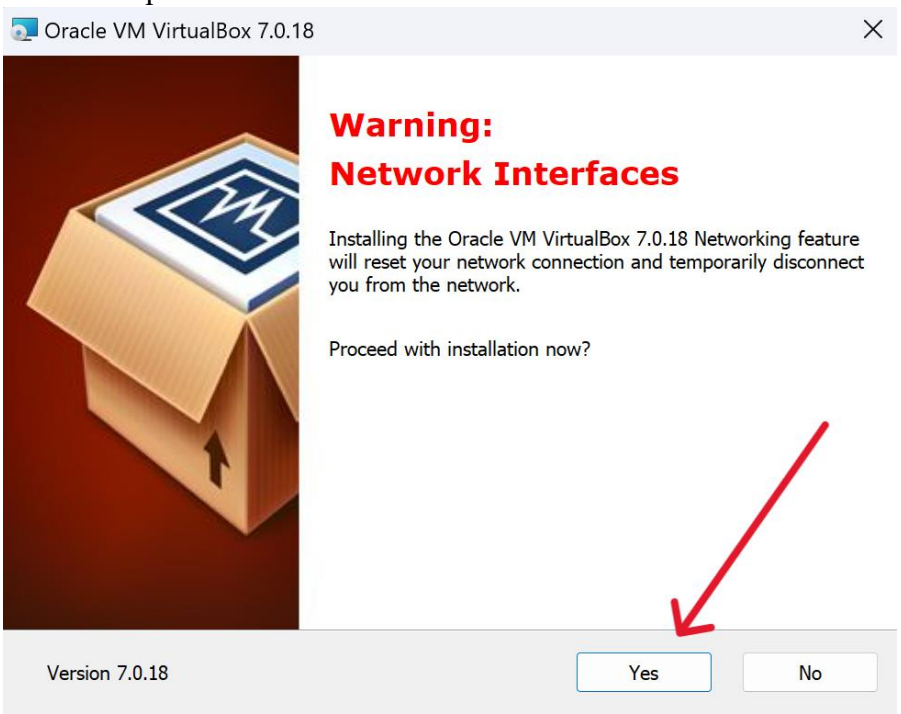

Figure 3

5. Click on ‘’**Install**” button to begin the installation and after the completion of installation then Click on ‘’**Finish**” button.

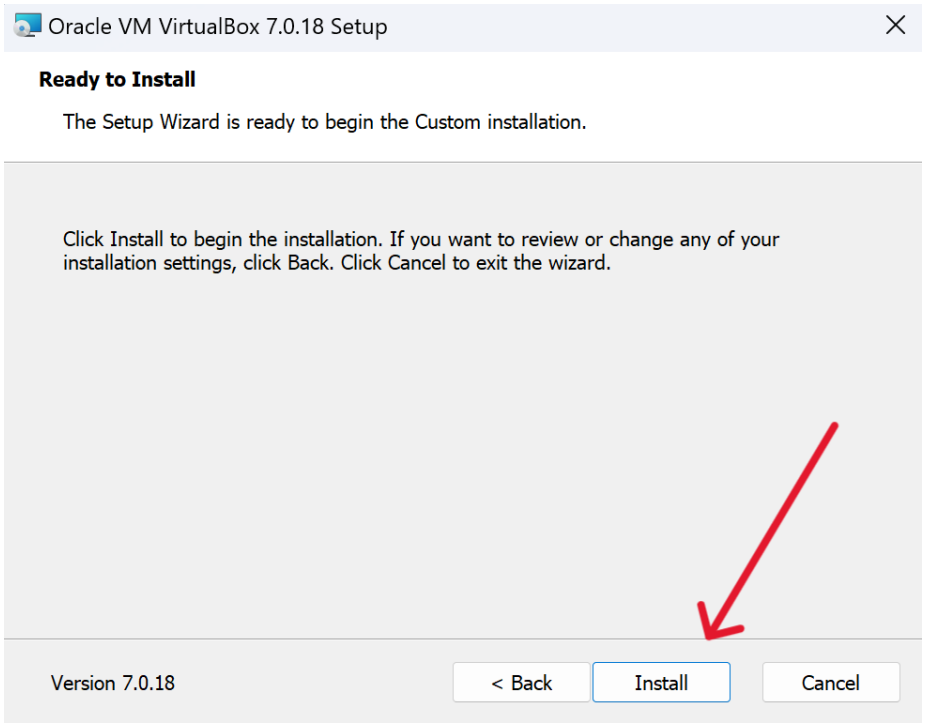

Figure 4

Figure 5

Setup the VirtualBox:

Download the Oracle Virtual Box using the following link.

https://ubuntu.com/download/desktop

Navigate through the following steps.

1. Open VirtualBox and Click on "**New**" button to create a new virtual machine.

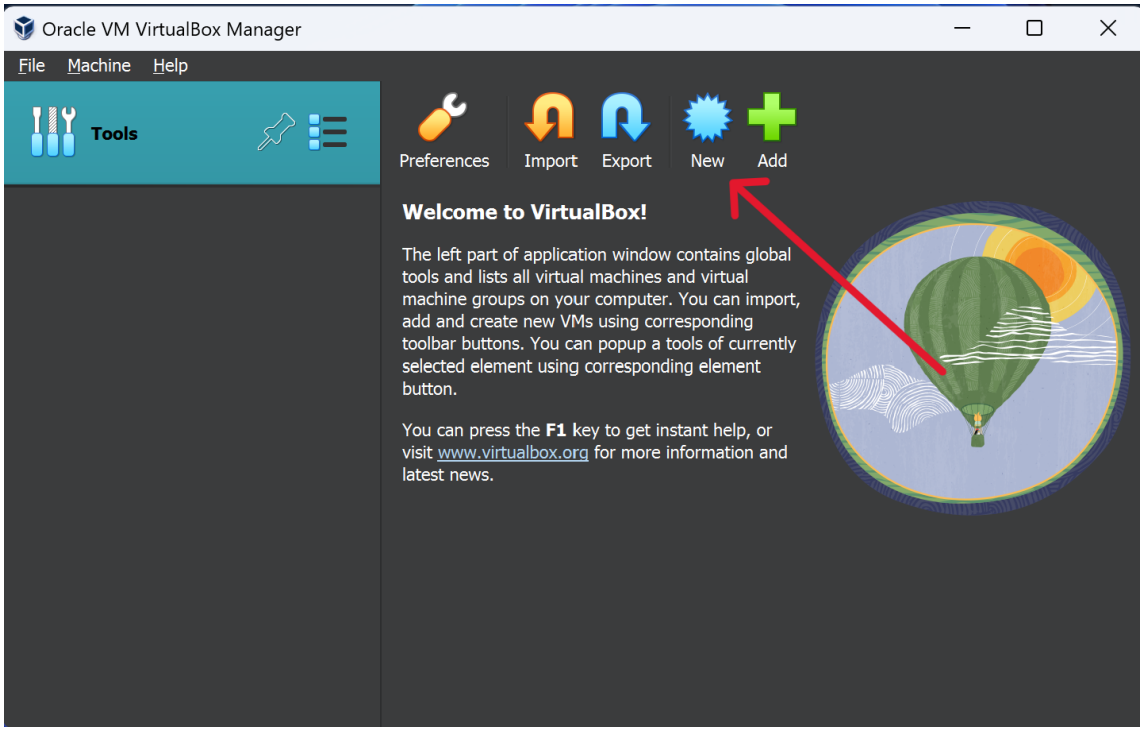

Figure 6

2. Type the Virtual Machine Name (Ubuntu).
3. Select the type as Linux.
4. Select the version Ubuntu(64-bit).

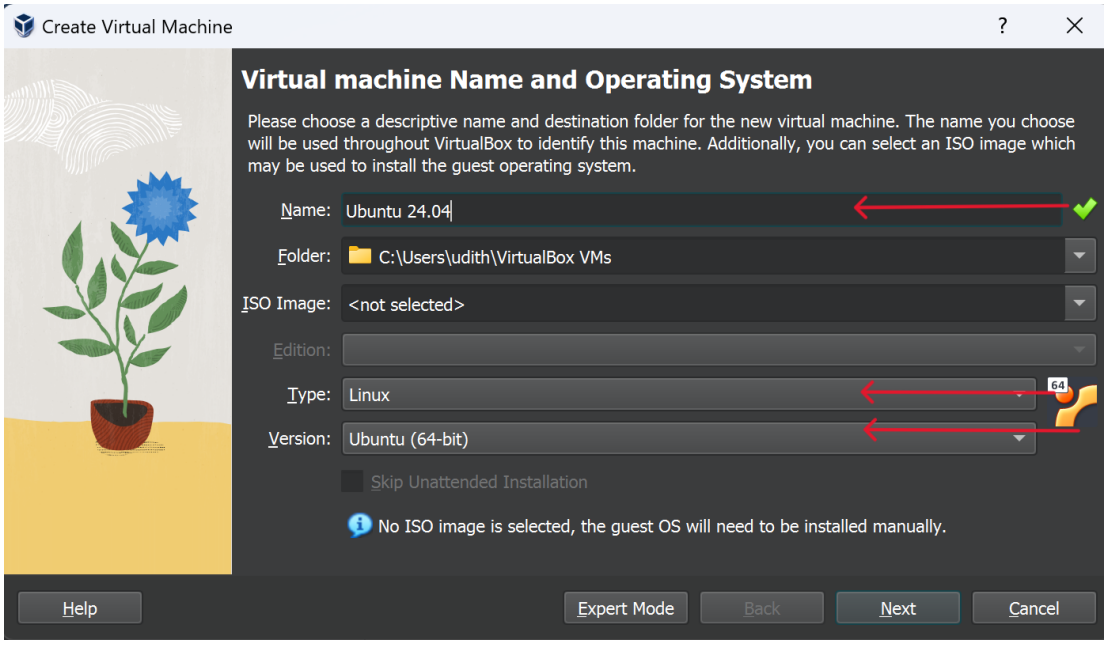

Figure 7

5. Select the the iso image you have downloaded.

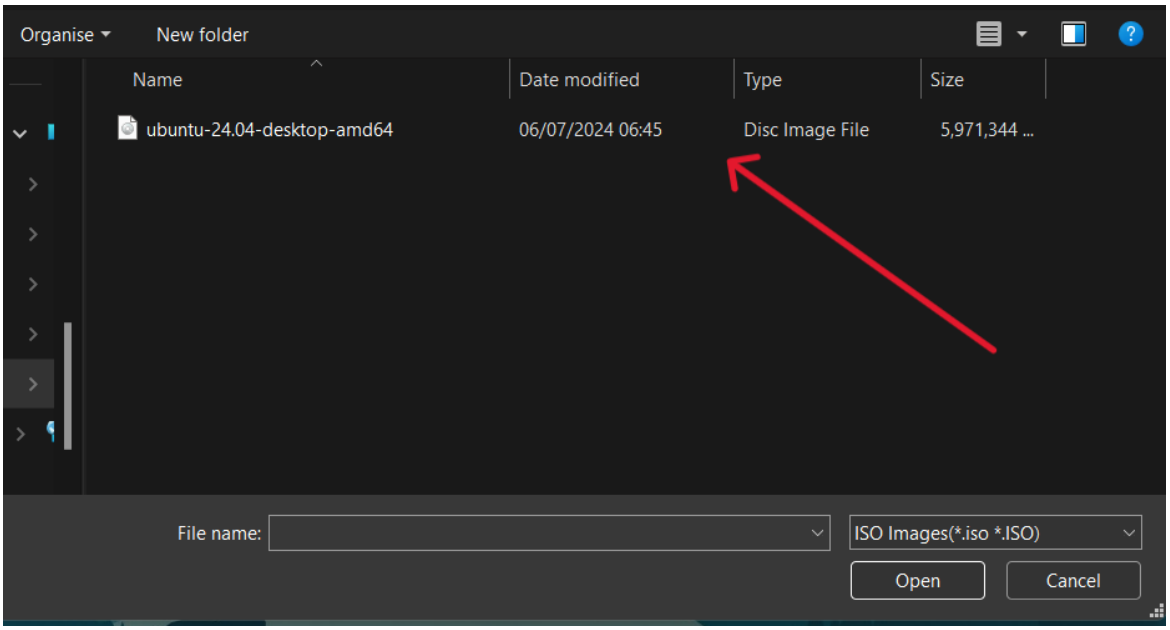

Figure 8

6. Create username and password as you preferred. you can also change Host name and Domain name. And then Click on "**Next**" button to continue.

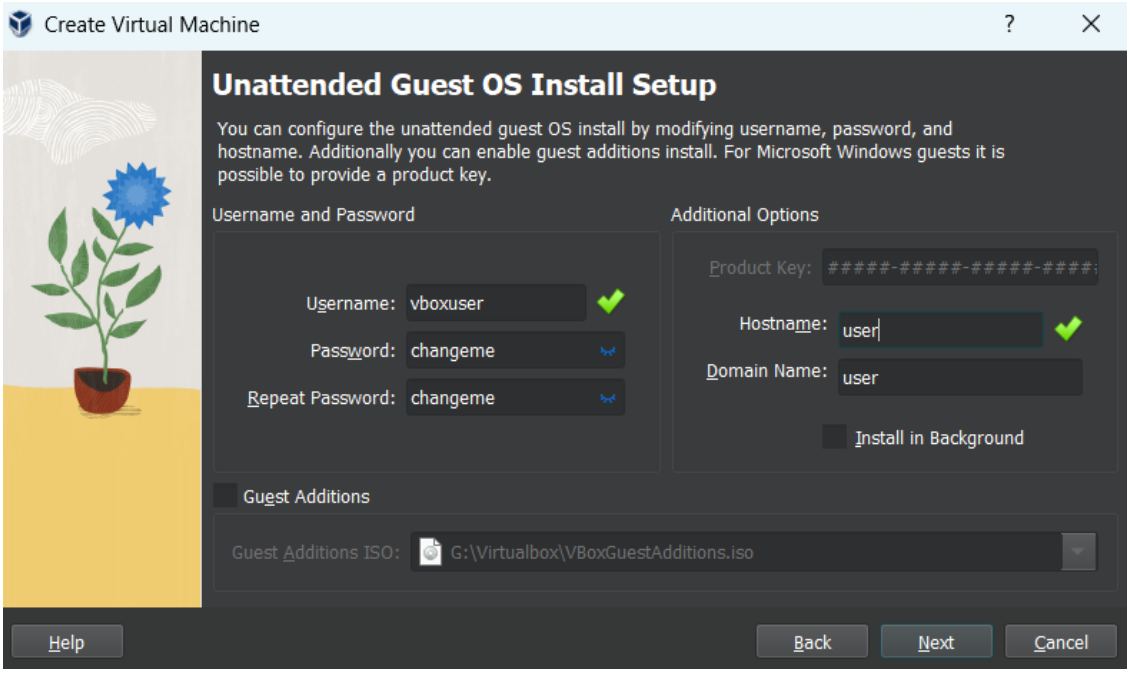

Figure 9

7. You need to select the amount of RAM and virtual CPU count as you preferred.

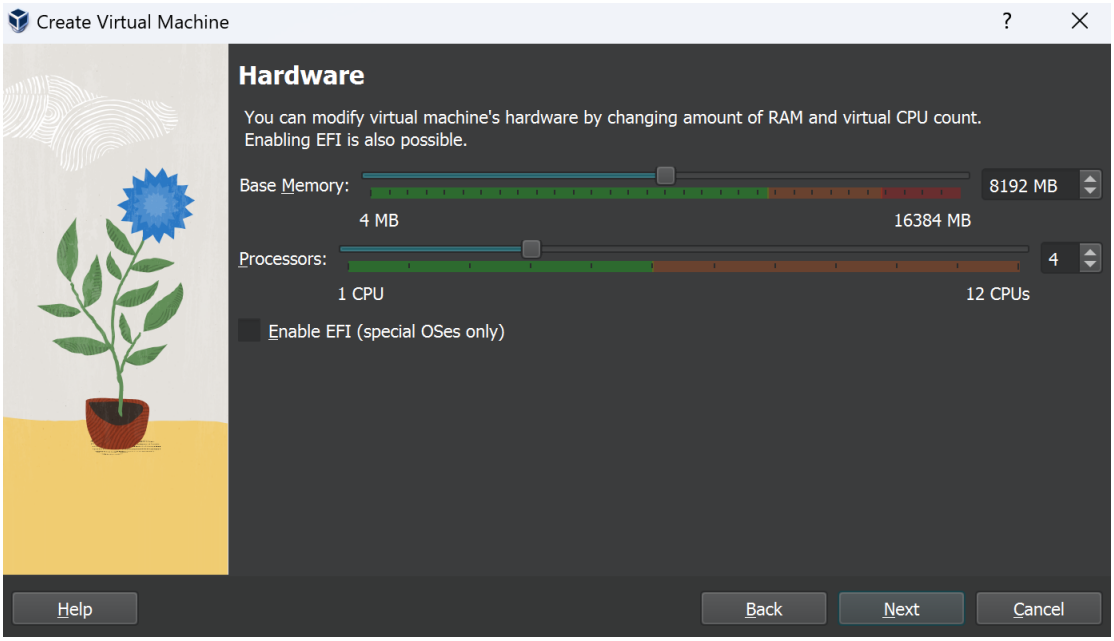

Figure 10

8. Then you need to select the virtual Hard Disk size and click on "**Next**" button to continue **.**

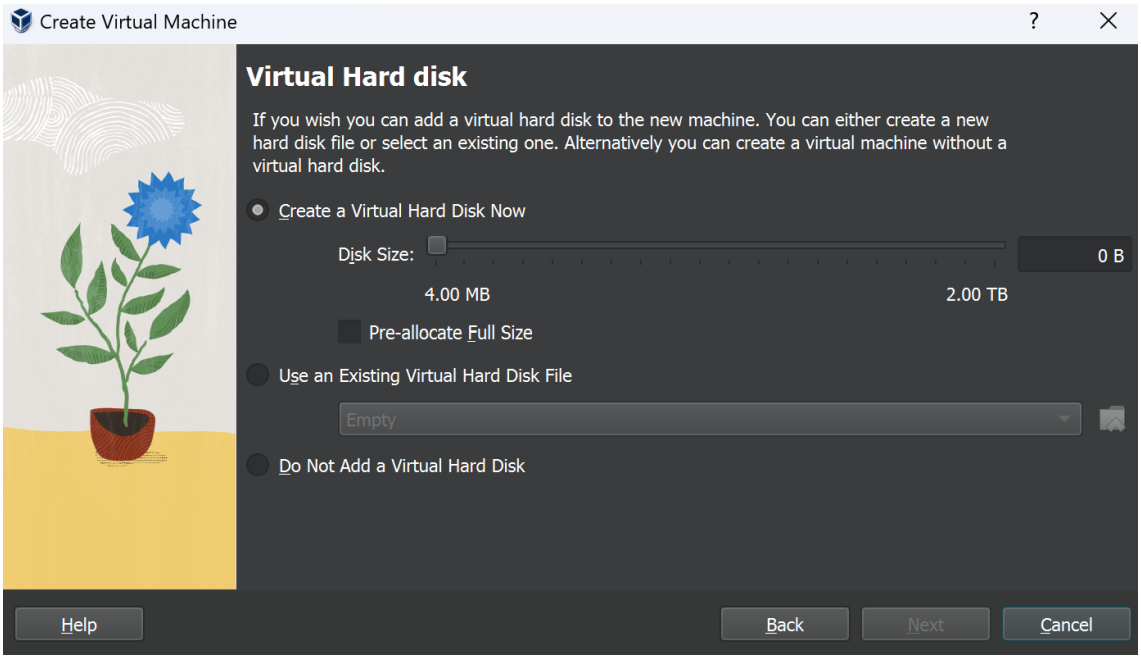

Figure 11

9. After the configuring you can click on "**Finish**" button to finish the configure part.

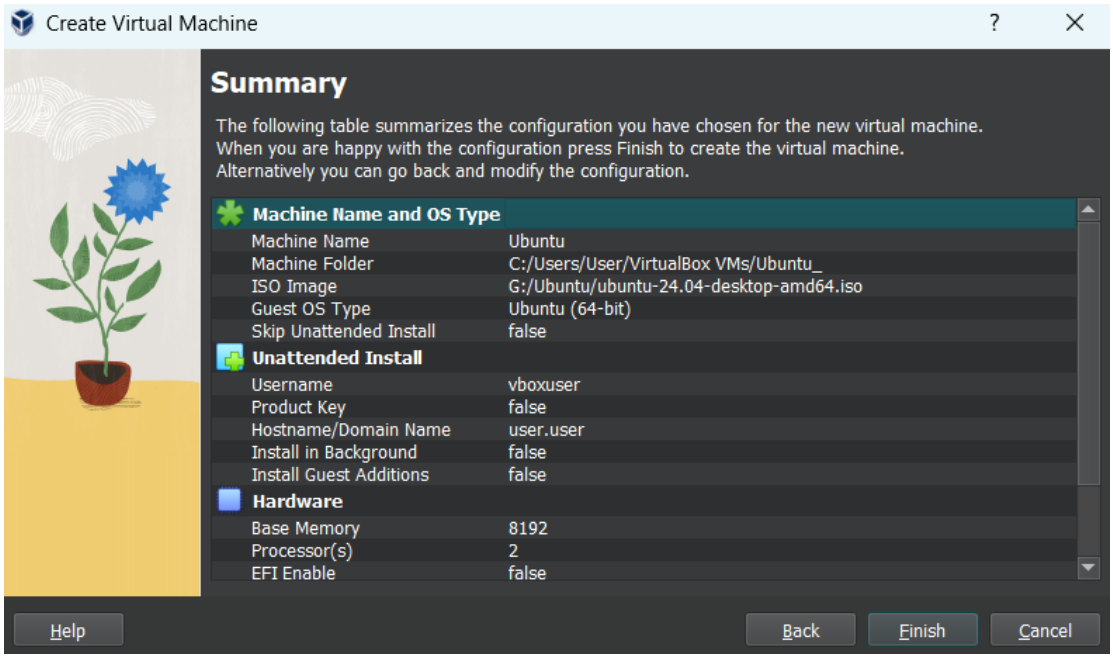

Figure 12

10. After the configuring part you need to redirect to VirtualBox home screen and click on "**Settings**" button to continue the next part.

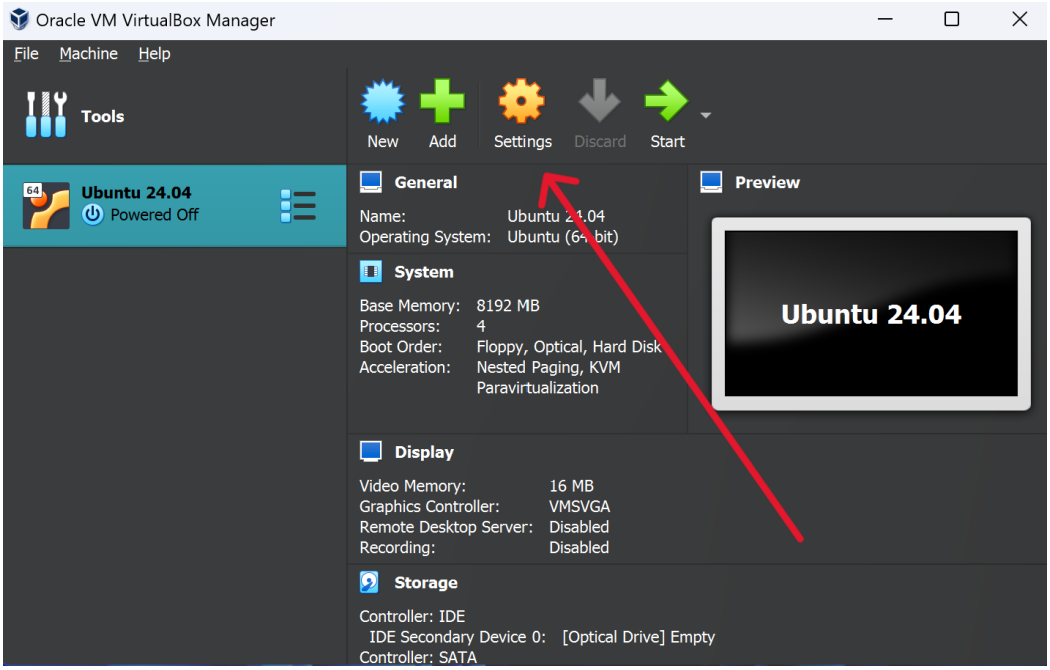

Figure 13

11. Then you need to change the Network settings like given below and click on "**Ok**" button to apply changes.

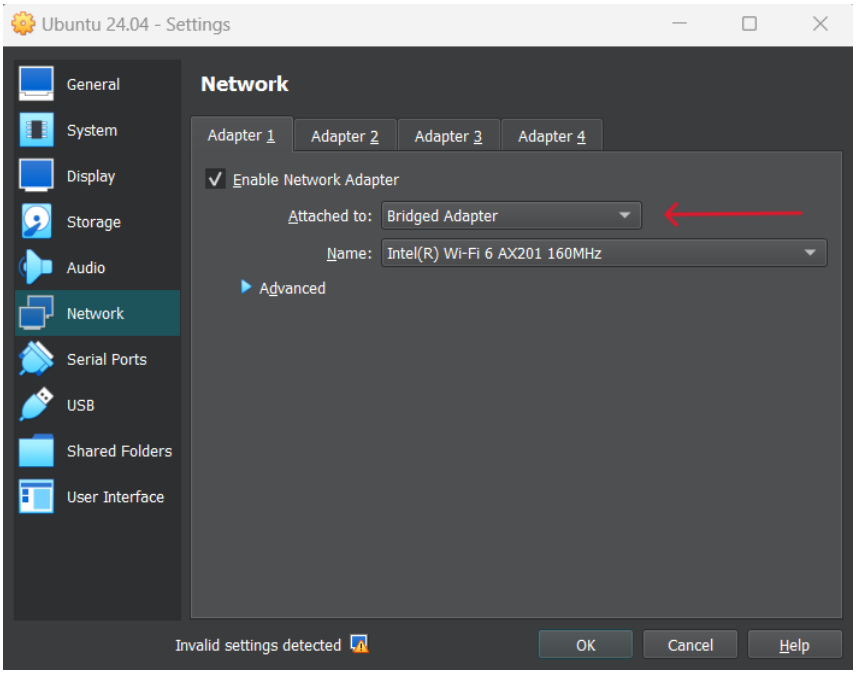

Figure 14

Install Ubuntu OS on VirtualBox

Navigate through the following steps.

1. First you need to select the virtual machine and click on "**Start**" button to Start the installation.

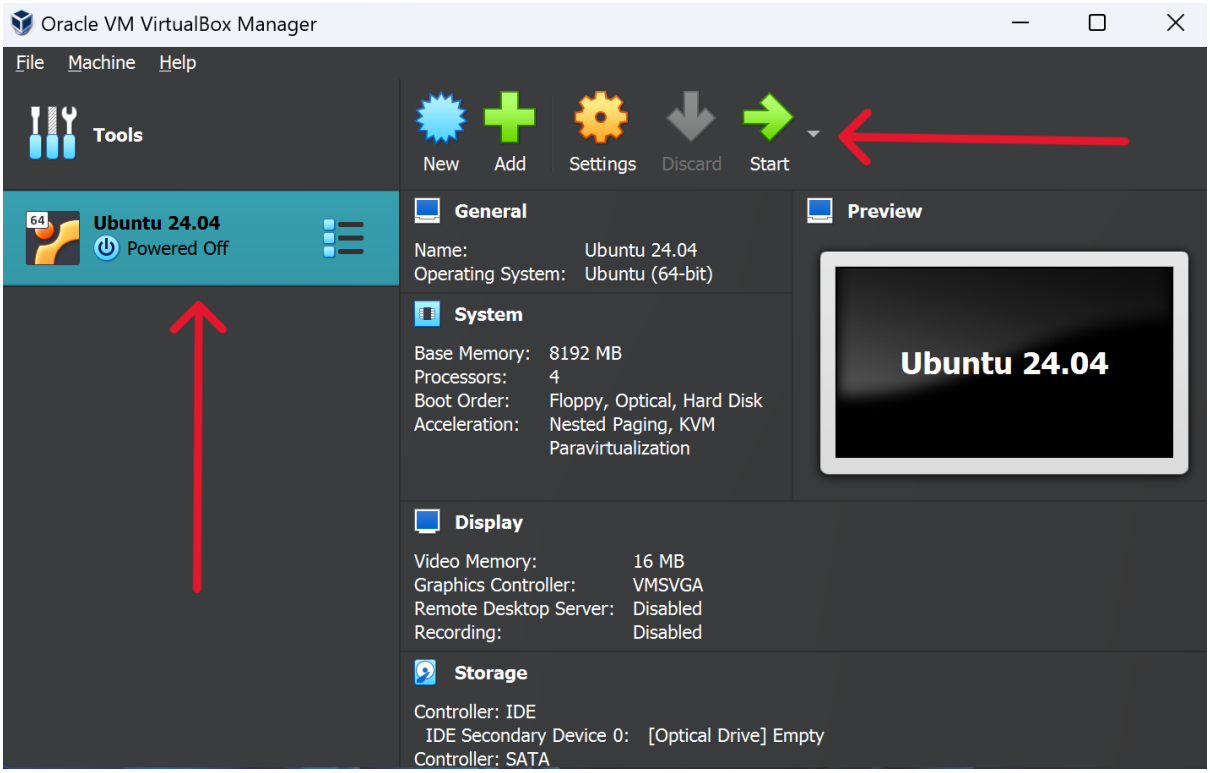

Figure 15

2. In the beginning of installation, you need to select the language you preferred and then click on "**Next**" button to continue the installation.

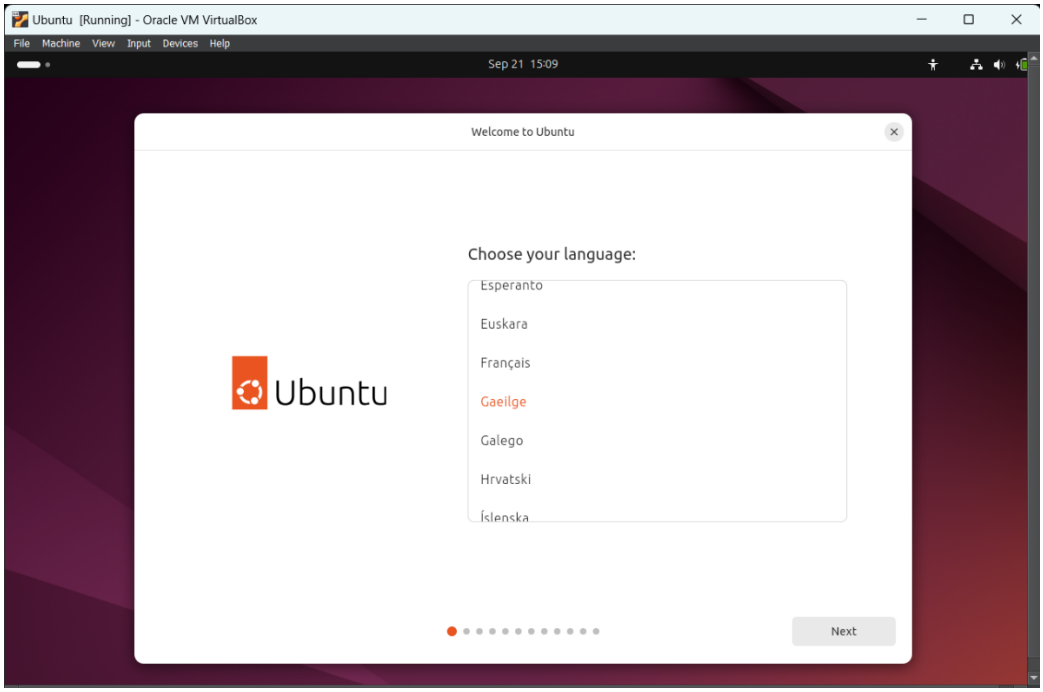

Figure 16

3. After the previous step you can see the accessibility in Ubuntu. You can just read it and click on "**Next**" button to continue the installation.
4. Then you need to select the keyboard layout language as you prefer. After the selection you can click on "**Next**" button to continue the installation.

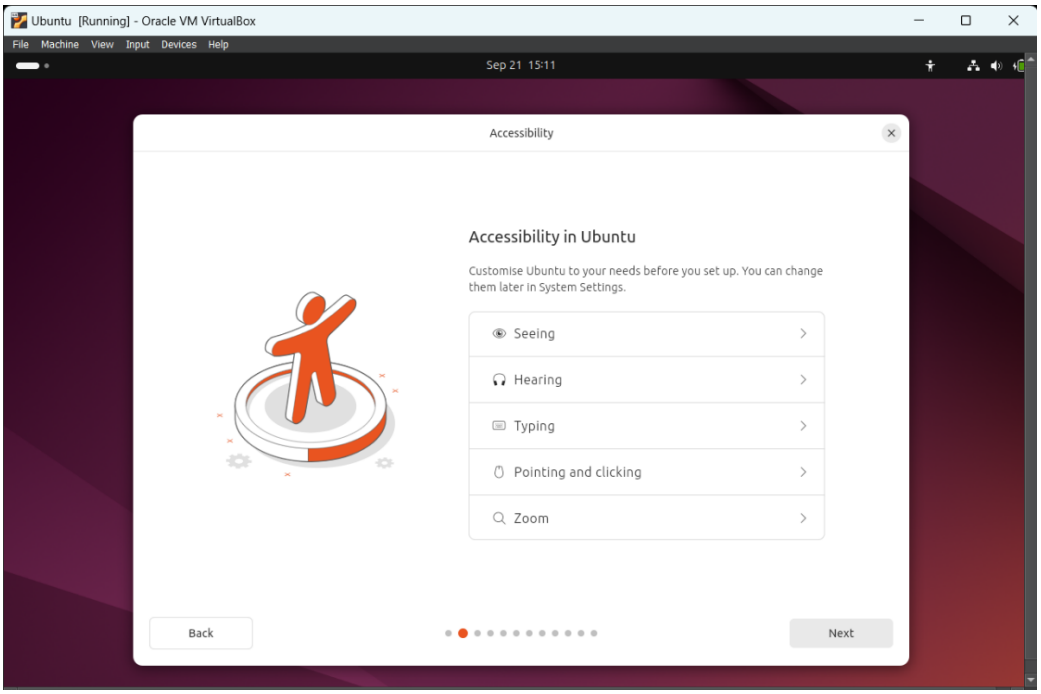

Figure 17

5. After that you need to select your internet connection type for your installation. You should select "**Use Wired Connection**" and then click on "**Next** "button to continue.

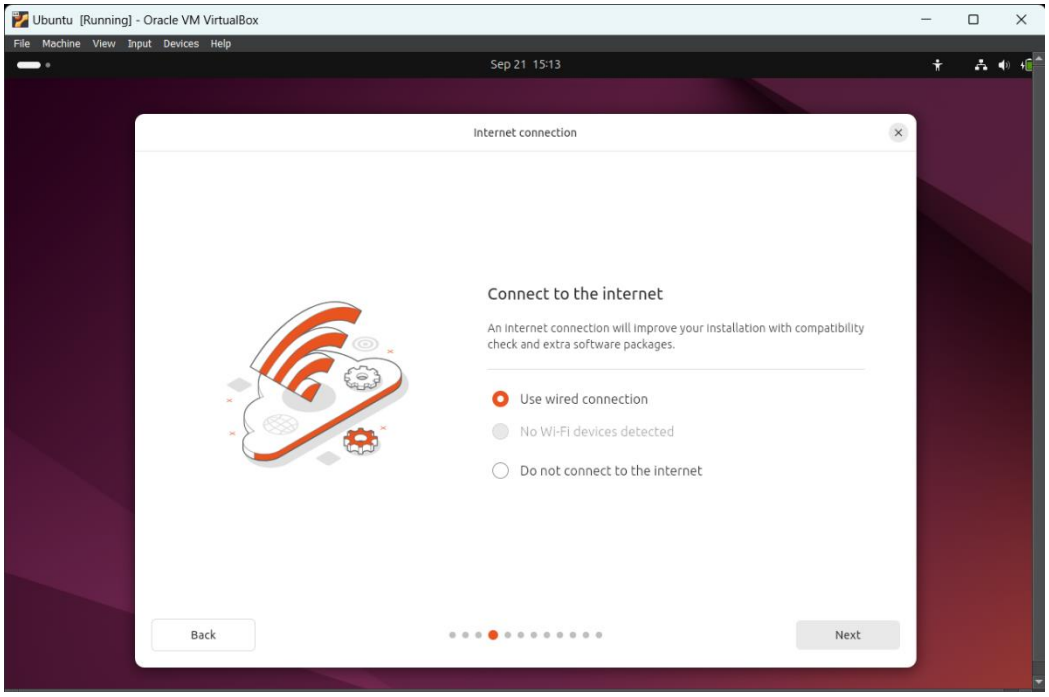

Figure 18

6. You can see "**What do you want to do with Ubuntu**" message with window. You need to select "**Install Ubuntu**" and click on next button to continue the installation.

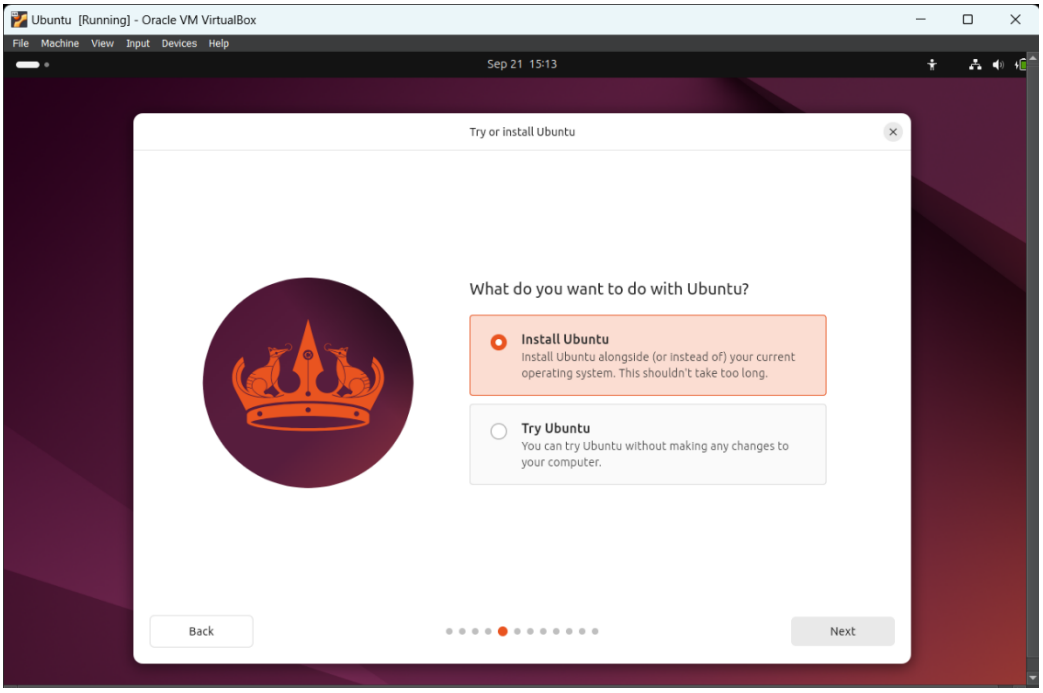

Figure 19

7. Then you need to select how you would like to install Ubuntu. You should select "**Interactive Installation**" it will be provide guided step by step through the installation and click on "**Next**" button to continue.

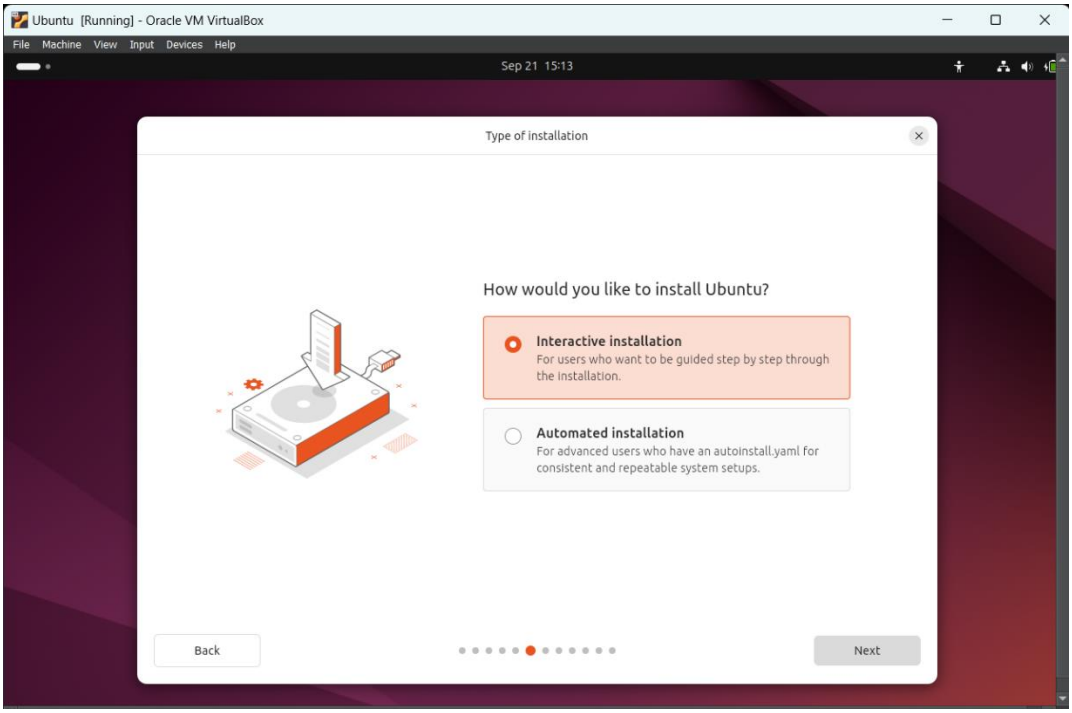

Figure 20

8. You can select what app would you like to start with Ubuntu and after the selection click on "**Nex**t" to continue the installation.

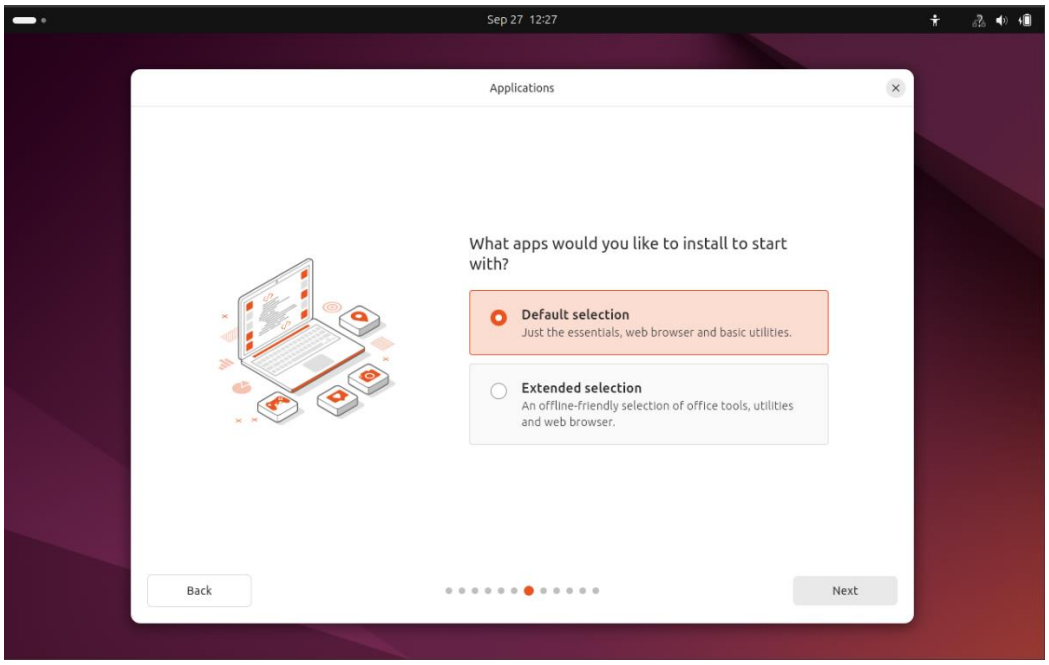

Figure 21

9. After the previous step you need to select disk setup for the installation.

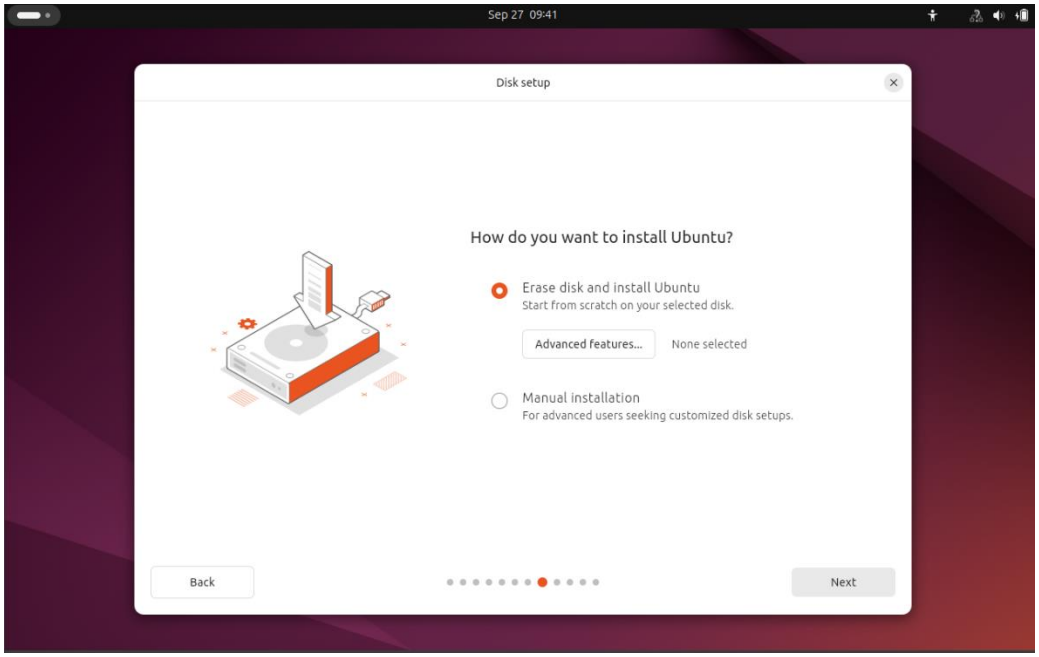

Figure 22

10. Then you need to select what types of recommended software you need to download. Select mention below type and click on "**Next**" button to continue.

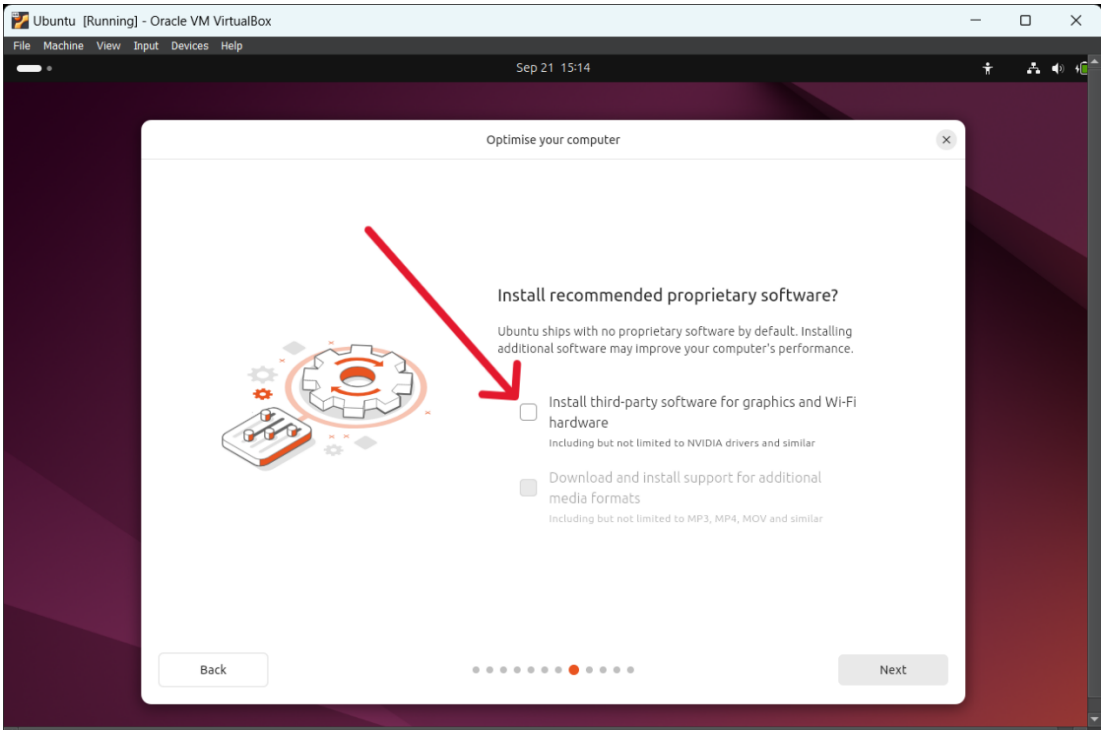

Figure 23

11. Then you need to create your Ubuntu Account. Fill in the blanks with your details and after that click on "**Next**" button to continue.

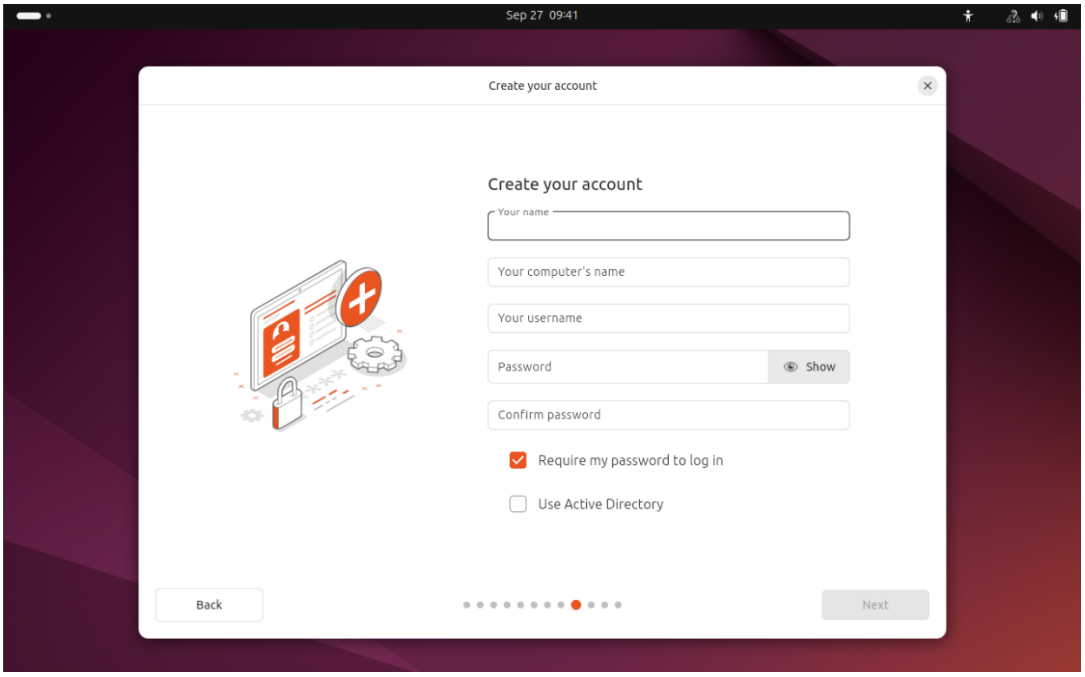

Figure 24

12. Now you need to select your time zone and click on "**Next**" button to continue.

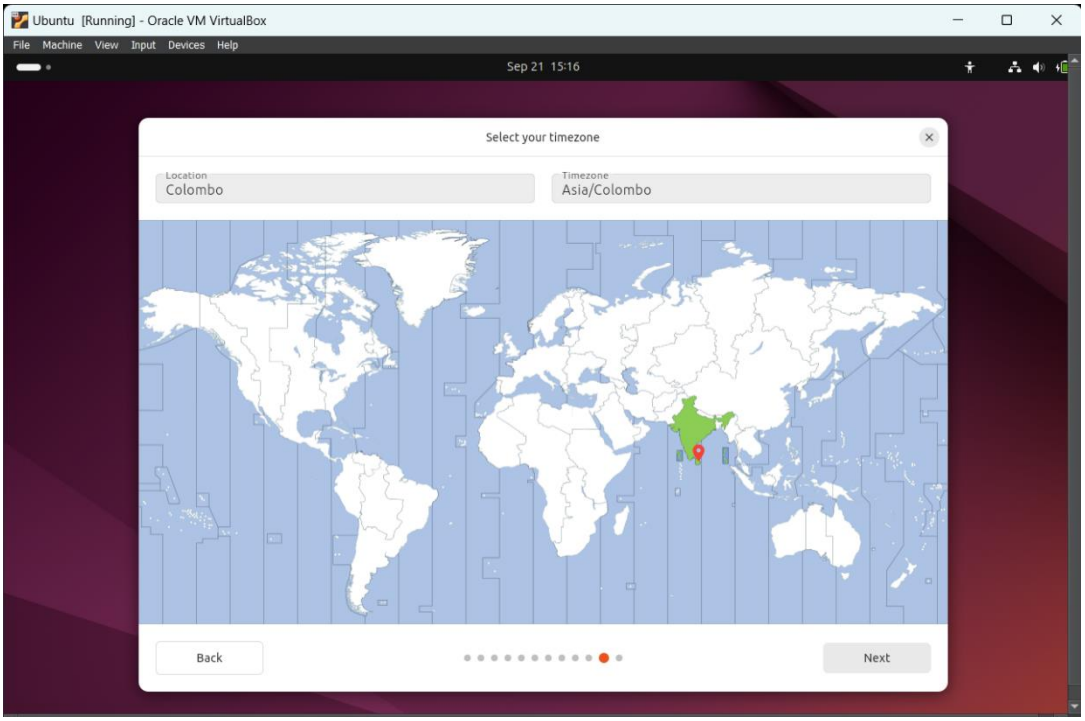

Figure 25

13. Now you can review your choices and click on "**Install**" button to start the installation. It will take some time to finish the installation.

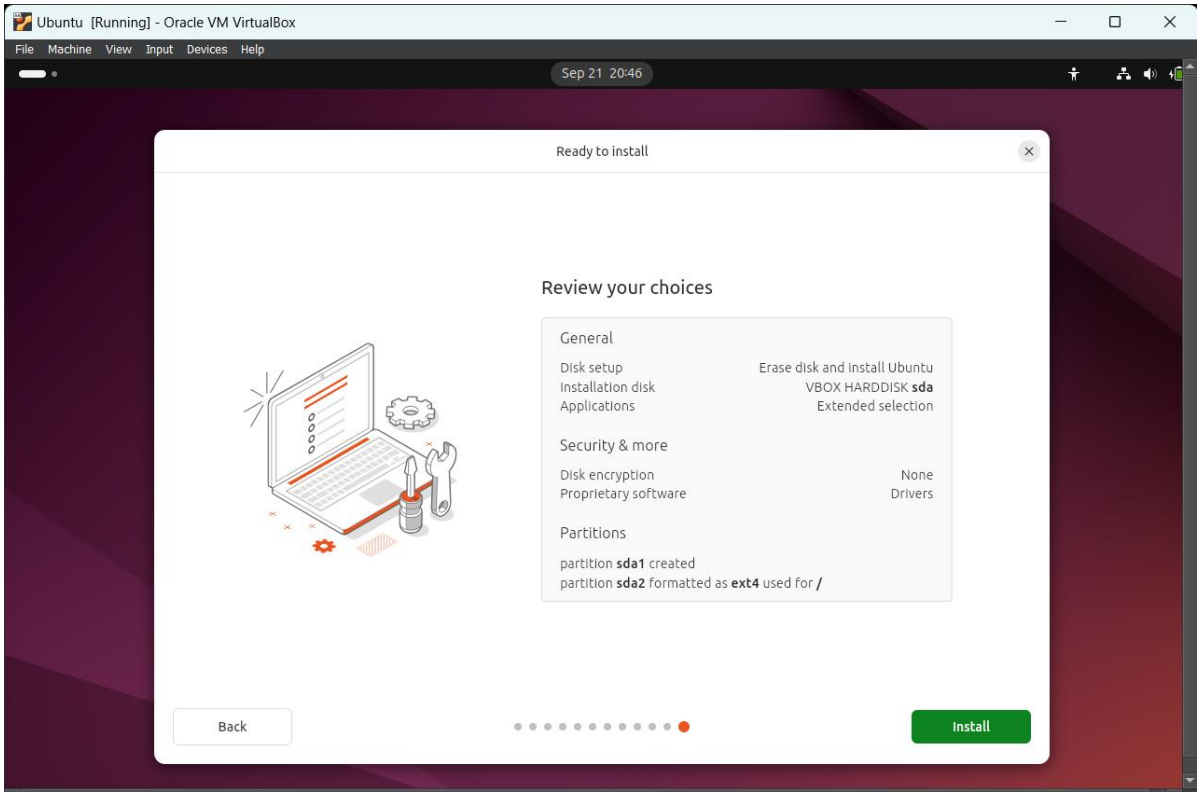

Figure 26

Basic Linux Commands

Open the Terminal

The terminal in Linux is a text-based interface that allows users to interact with the system through commands. It is used to perform tasks such as navigating directories, managing files, and executing programs, offering more control and efficiency compared to graphical interfaces.

First, we need to open the terminal in Linux. Navigate through the following steps to open it.

After the installation process is done, you can see the home screen of Ubuntu OS. Right click on mouse and click on "**Open in Terminal**" to open the Linux terminal.

Navigation Commands.

1. **pwd –** Print the current working directory.

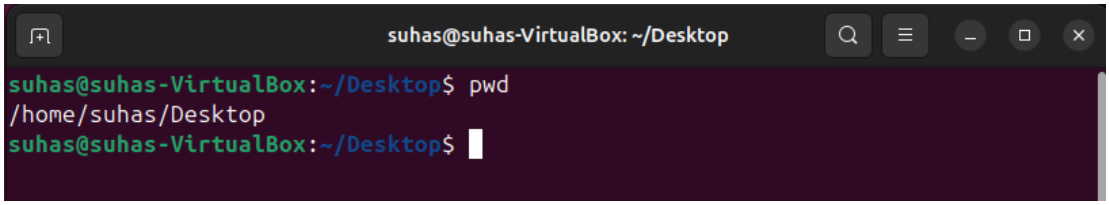

Figure 27

2. **cd-** Change the working directory.

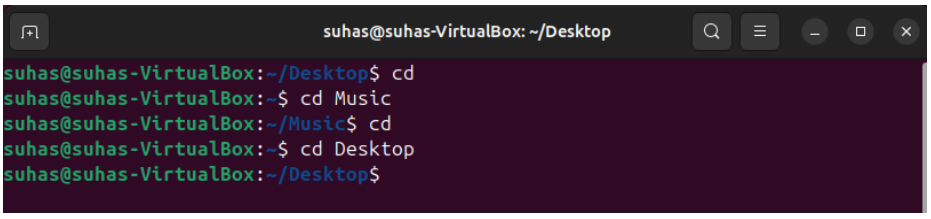

Figure 28

3. **ls –** List directory content.

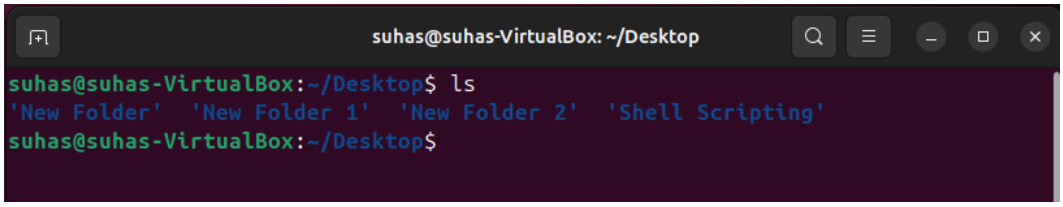

Figure 29

4. **mkdir –** Create a new directory (mkdir testfolder).

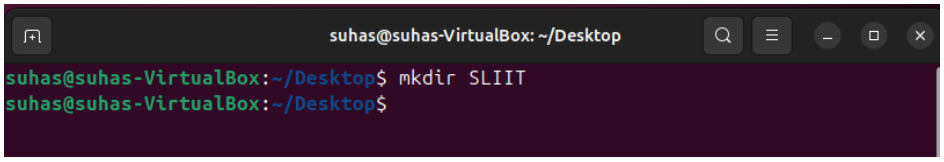

Figure 30

5. **rmdir –** Remove directory with all contents (rmdir testfolder).

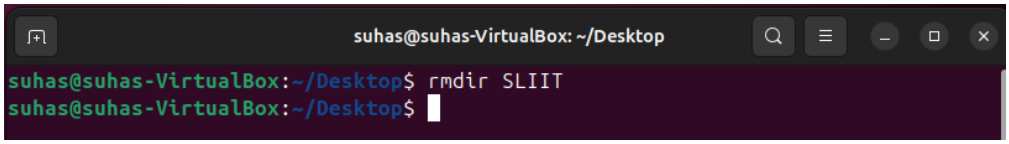

Figure 31

File Manipulation Commands

6. **touch –** Create an empty file.

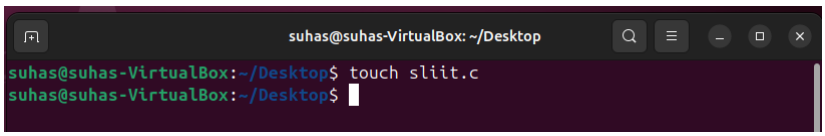

Figure 32

7. **cp –** Copy files or directories (cp [source] [destination]).

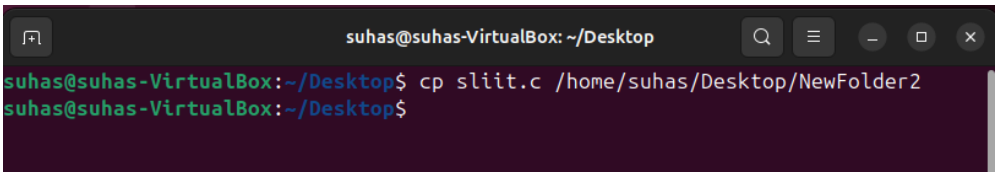

Figure 33

8. **mv –** Move or rename files or directories (mv [source] [destination]) .

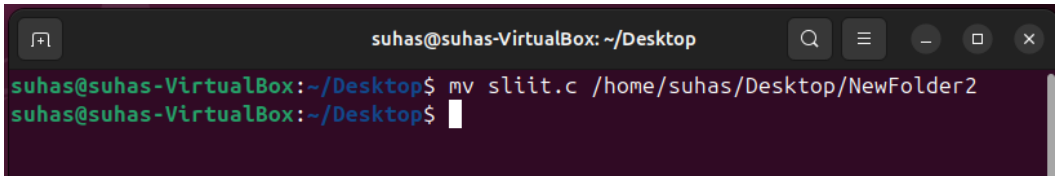

Figure 34

9. **rm –** Remove files or directories.

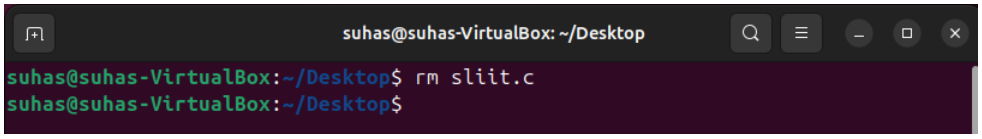

Figure 35

10.**cat –** Show contents of the file (cat testfile).

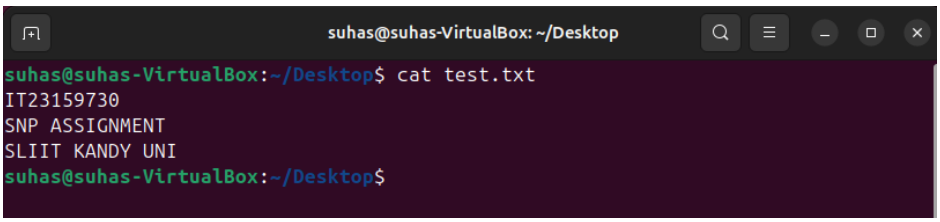

Figure 36

11.**nano-** Open nano text editor in terminal (nano testfile or nano testfile.txt**).**

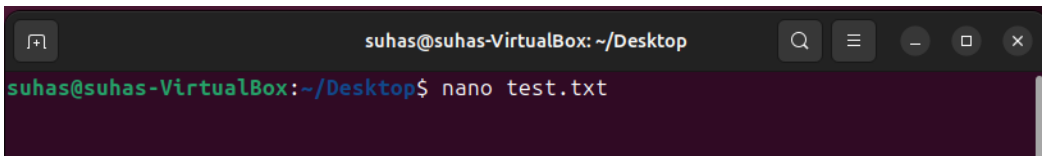

Figure 37

12.**vi** - Open vi text editor in terminal (vi testfile or vi testfile.txt**).**

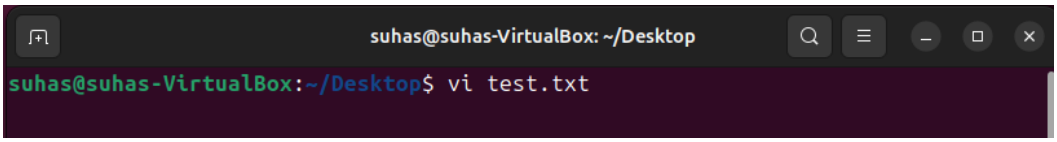

Figure 38

System Information and User Management Commands.

13. **uname -a -** Display system information.

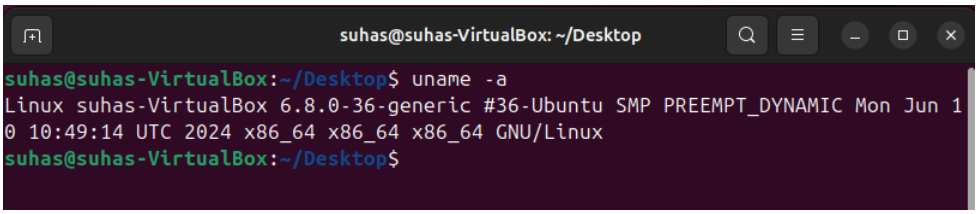

Figure 39

14. **df -h -** Display disk usage in a human-readable format.

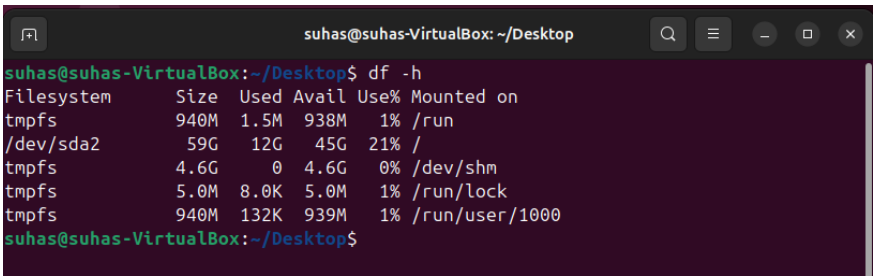

Figure 40

15. **free -m -** Display memory usage in megabytes**.**

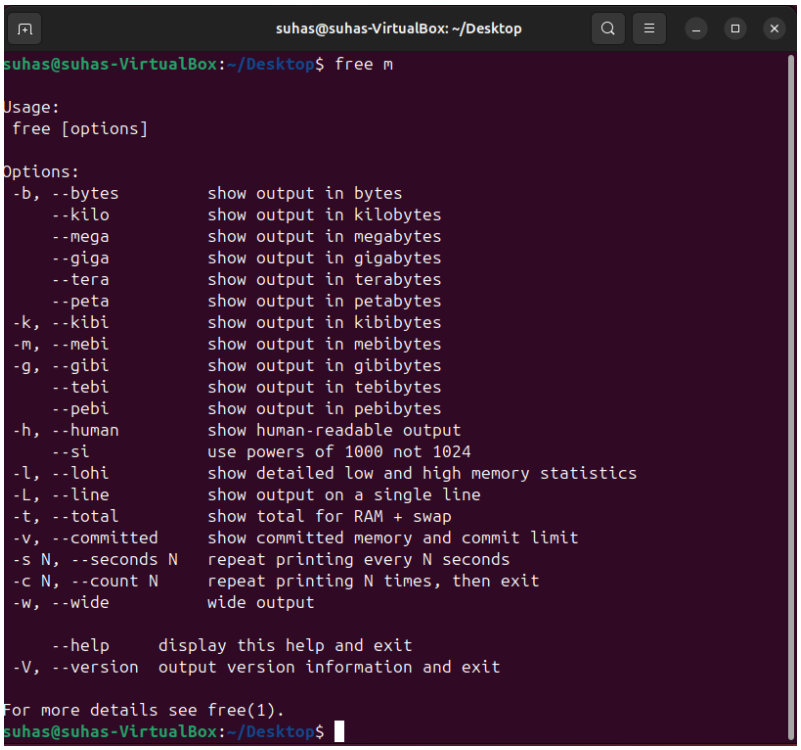

Figure 41

16.**whoami –** Shows the current logged-in user.

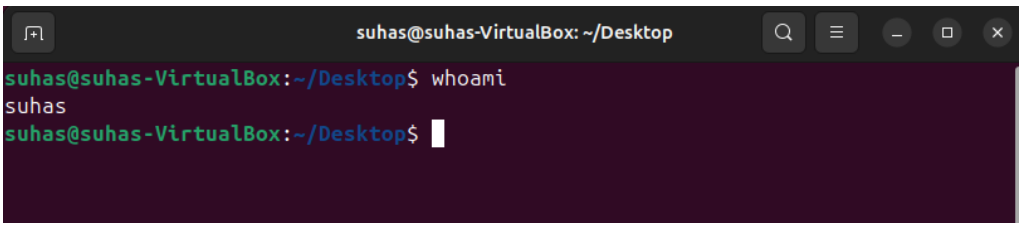

Figure 42

17.**id [username]-** Display user identity and group information.

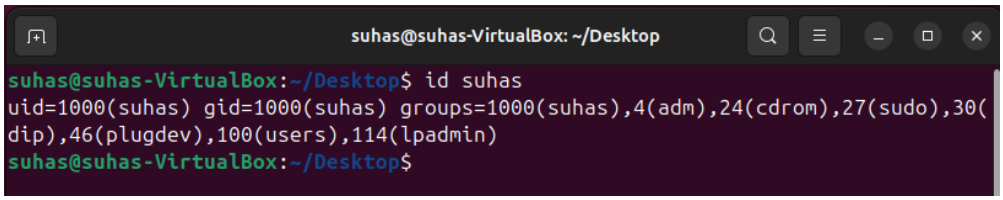

Figure 43

18.**sudo [command] -** Run a command with superuser privileges.

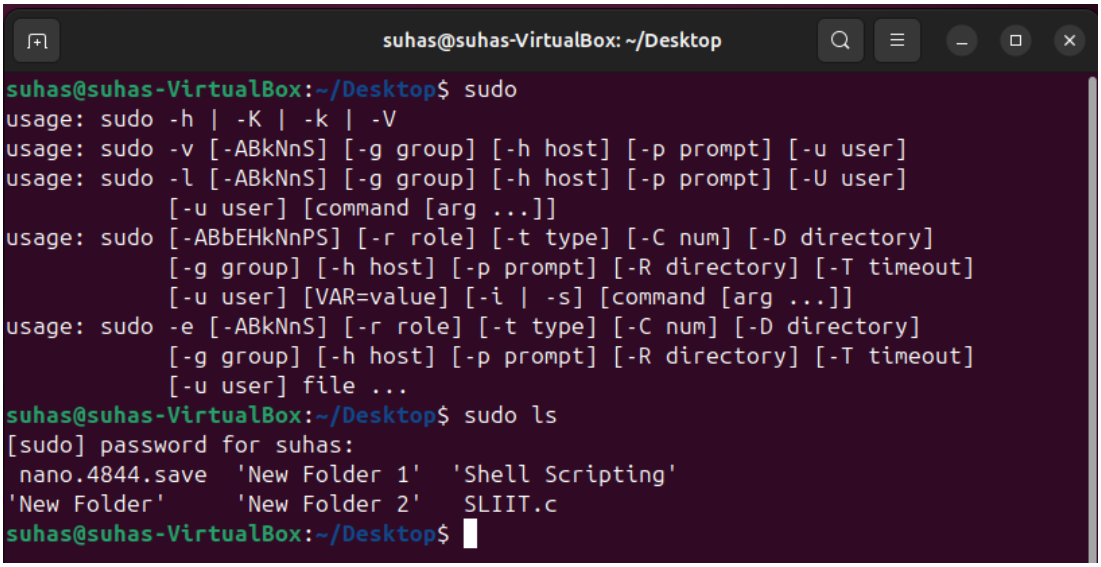

Figure 44

19. **useradd –** Create a new user (sudo useradd [username]).

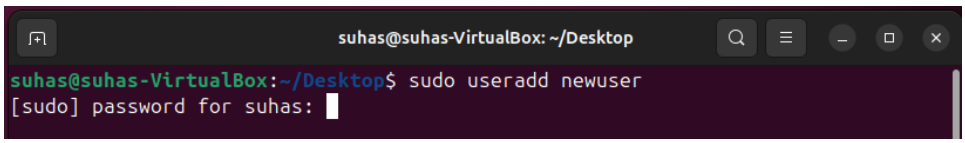

Figure 45

20. **passwd –** Change user password.

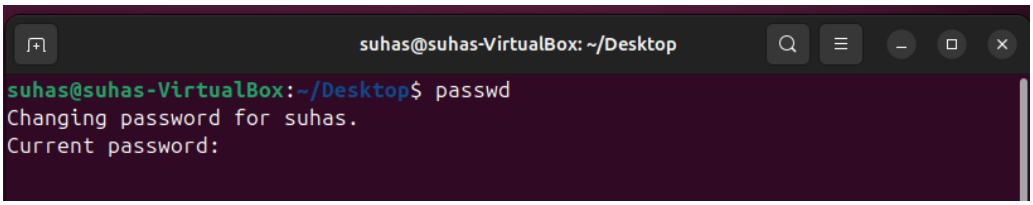

Figure 46

21. **history –** Display the history of commands.

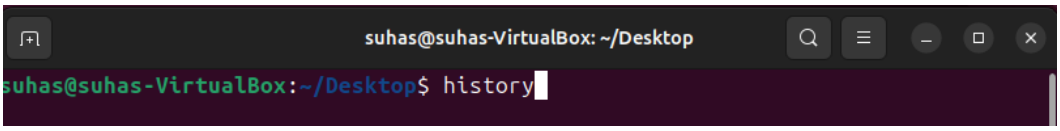

Figure 47

22. **clear -** Clear the terminal window.

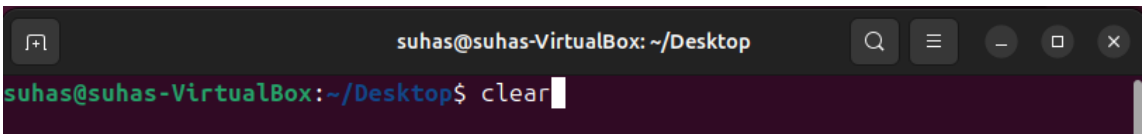

Figure 48

DHCP, DNS, and NTP Services Configuration.

DHCP Service Configuration.

1. First, Open the terminal and install the DHCP server package.
   sudo apt update
   sudo apt install isc-dhcp-server

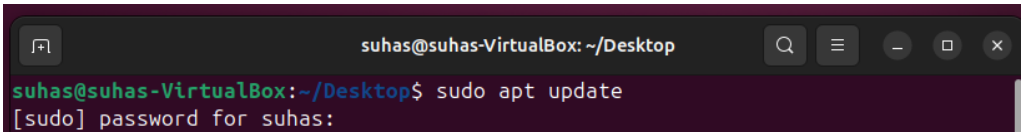

Figure 49

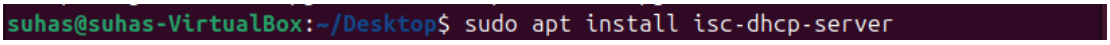

Figure 50

2. Then check the available network interfaces and get current ip address.
   ip a

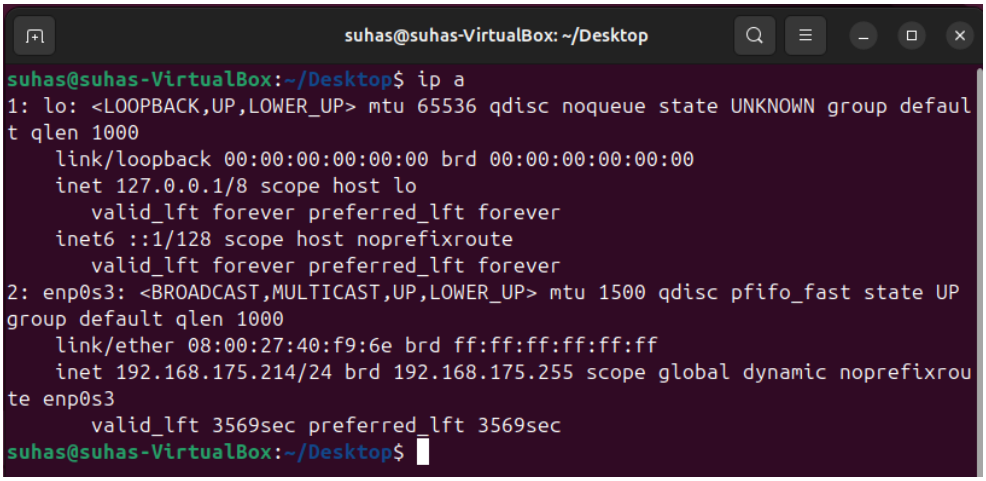

Figure 51

So, now you can get,
Name of the ip address = “enp0s3”
Your (current) ip address = “192.168.175.214/24”

3. Edit the main configuration file (/etc/dhcp/dhcpd.conf) to set network parameters.

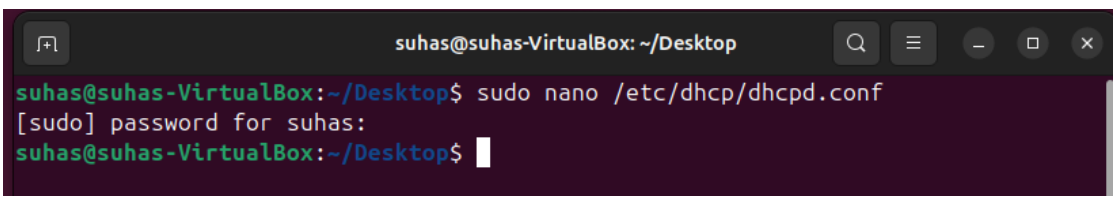

Figure 52

Configure the subnet and range of IP addresses to be assigned.

First, you need to uncomment the following comments and edit the configuration.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.175.20 192.168.175.254;
option domain-name-servers ns1.internal.example.org;
option domain-name “example.org”;
option subnet-mask 255.255.255.0
option routers 192.168.175.1;
option broadcast-address 192.168.175.255;
default-lease-time 600;
max-lease-time 7200;
}
```

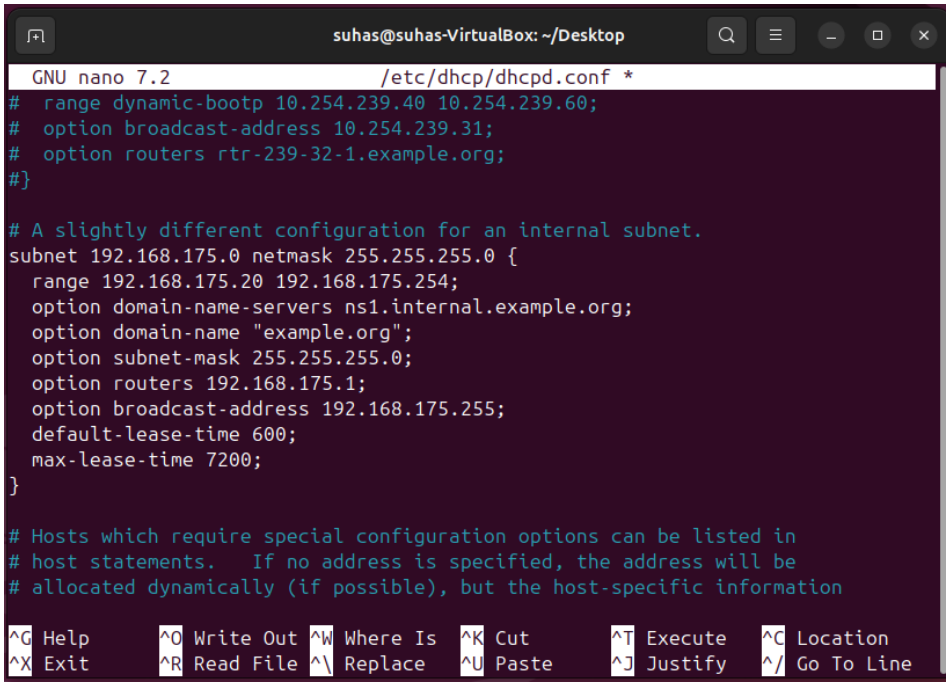

Figure 53

After that you can press “**Ctrl+o**” “**Enter**” and “**Ctrl+x**” to save and exit from the editor.

4. Assign Network Interfaces
   Edit the interface configuration file.
   sudo nano /etc/default/isc-dhcp-server

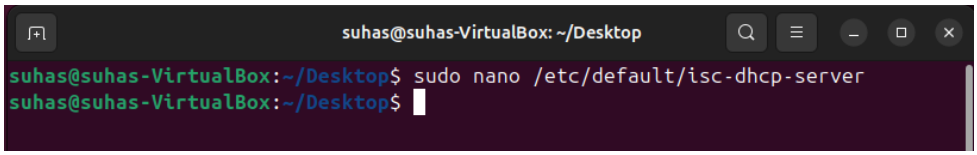

Figure 54

Find the line for INTERFACESv4 and Replace it with your network interface .

INTERFACESv4="enp0s3"

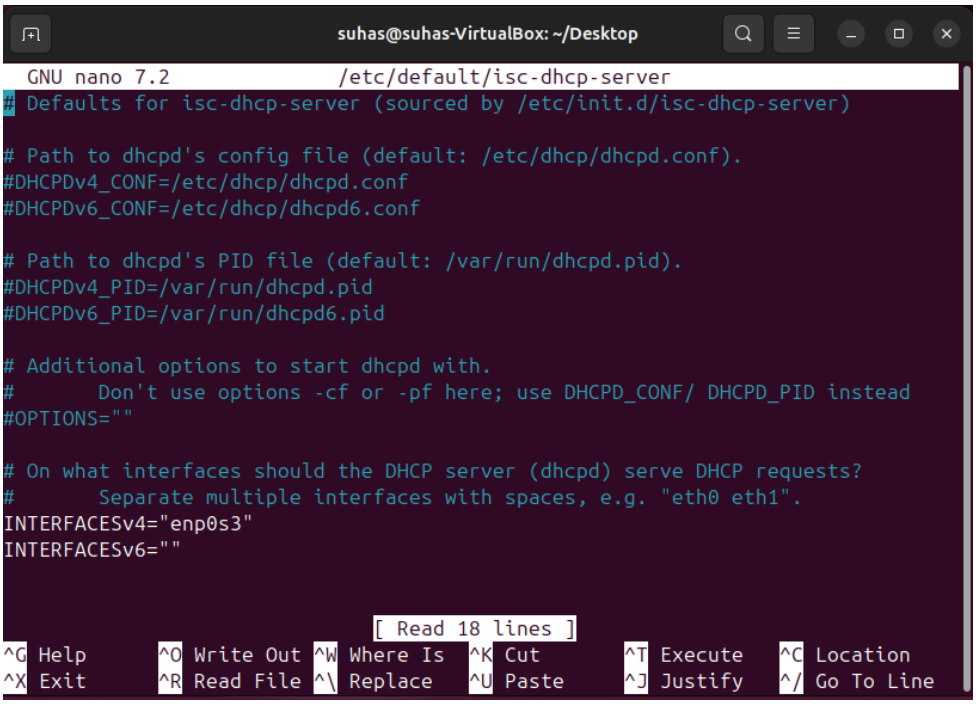

Figure 55

After that you can press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

5. Restart the DHCP Service
   After configuration, restart the DHCP service
   sudo systemctl restart isc-dhcp-server

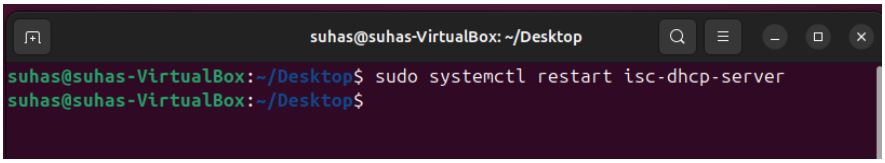

Figure 56

6. Enable the Service on Boot.
   sudo systemctl enable isc-dhcp-server

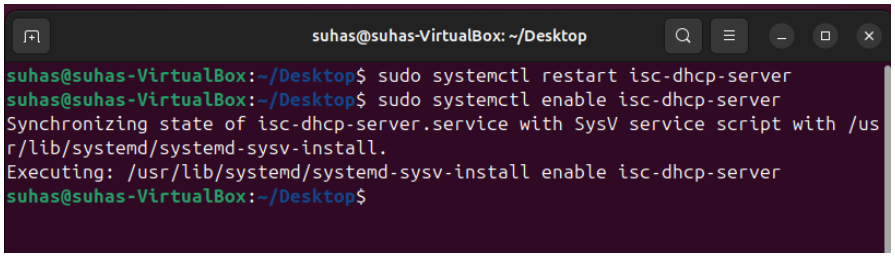

Figure 57

7. Verify the Status
You can check if the DHCP server is running properly.
sudo systemctl status isc-dhcp-server

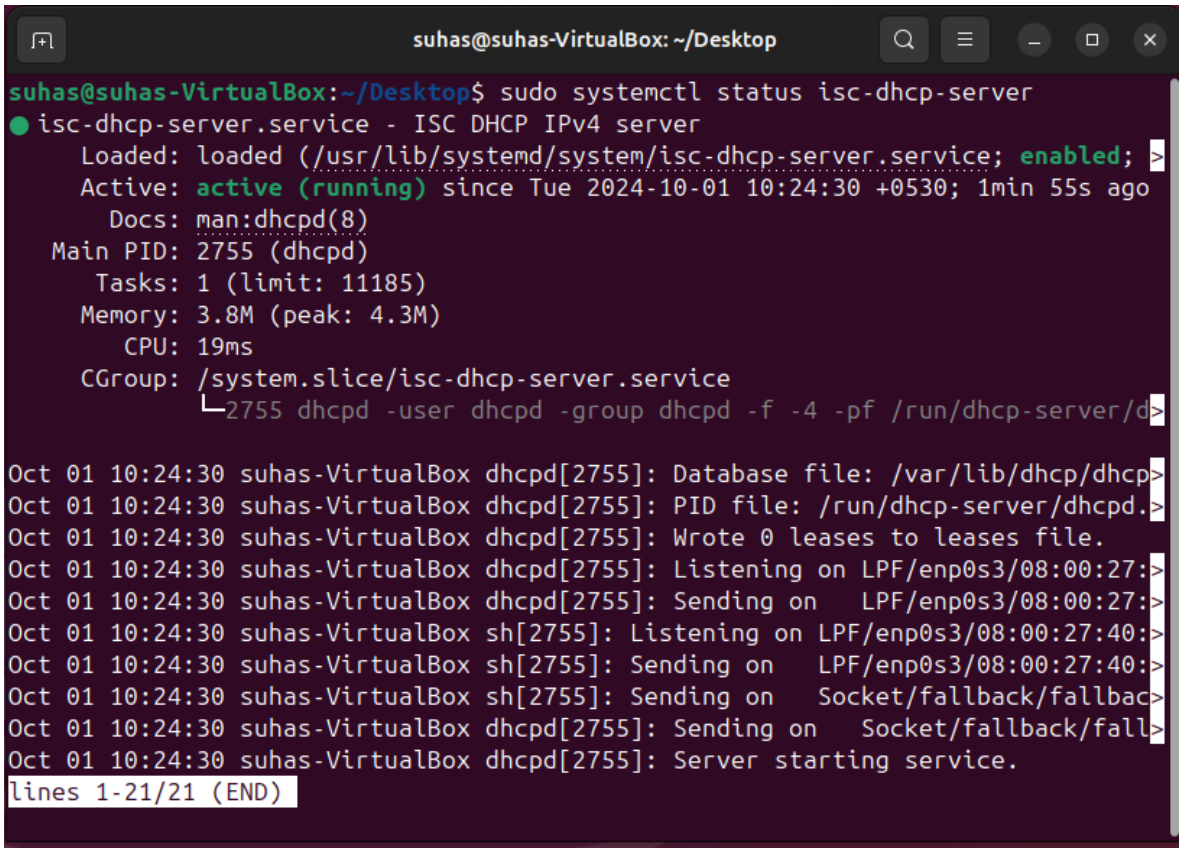

Figure 58

DNS Services Configuration.

1. First, Open the terminal and install bind9
   sudo apt update
   sudo apt install bind9

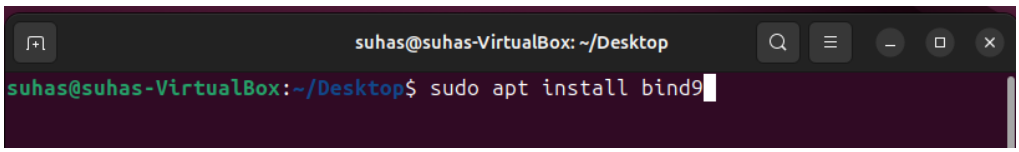

Figure 59

2. Edit the main configuration file.
   sudo nano /etc/bind/named.conf.options

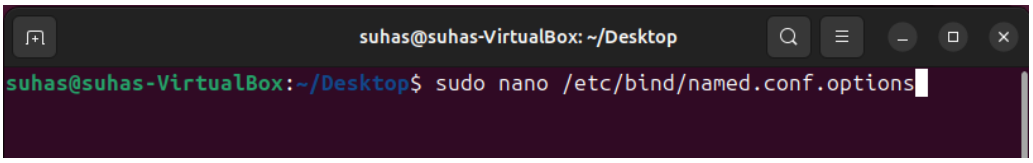

Figure 60

Configure DNS server options such as forwarders, directory, and listen-on settings.

First, you need to uncomment the following comments and edit the configuration.
8.8.8.8 - Google DNS server

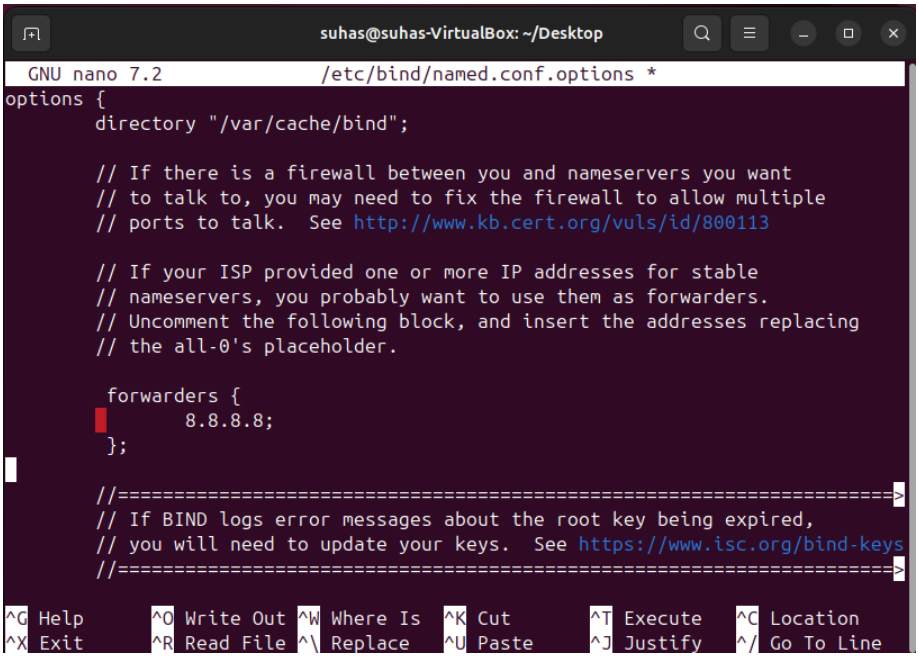

Figure 61

After that you can press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

3. Restart and Enable bind9.
   sudo systemctl restart bind9
   sudo systemctl enable bind9

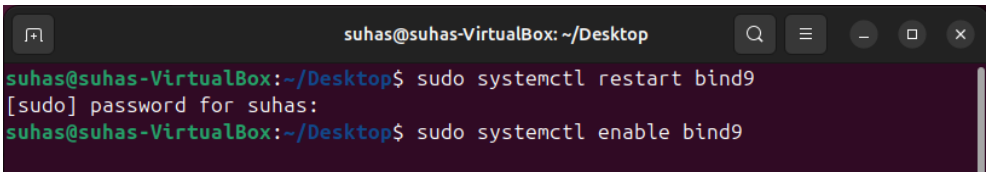

Figure 62

4. Verify the Status.
   You can check if the DNS server is running properly.
   sudo systemctl status bind9.

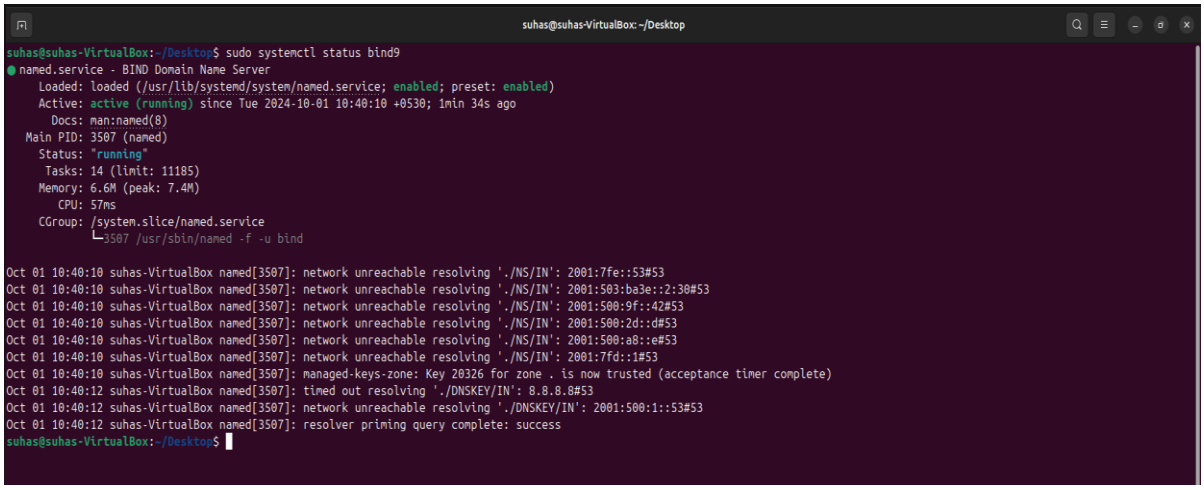

Figure 63

5. Test the DNS server.
   For this step we need **nslookup** command.
   nslookup [example.com].

NTP Services Configuration.

1. First, Open the terminal and install ntp
   sudo apt update
   sudo apt install ntp

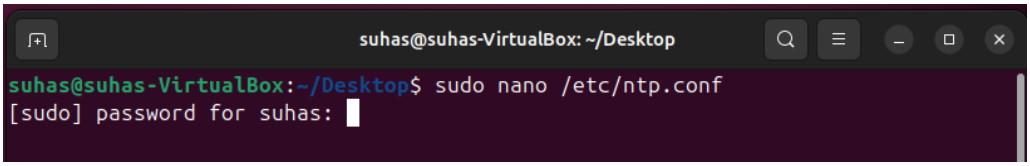

Figure 64

2. Edit the ntp configuring file.
   sudo nano /etc/ntp.conf

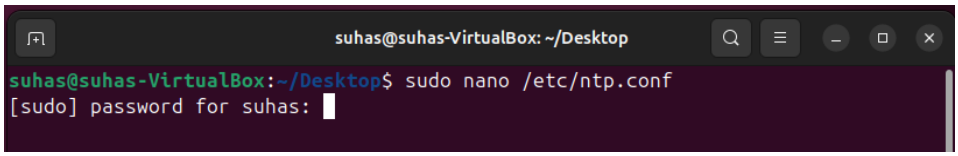

Figure 65

You can add or edit the external time servers that NTP uses to synchronise your system clock in the configuration file.
Type the default ntp pool servers mentioned below.
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org

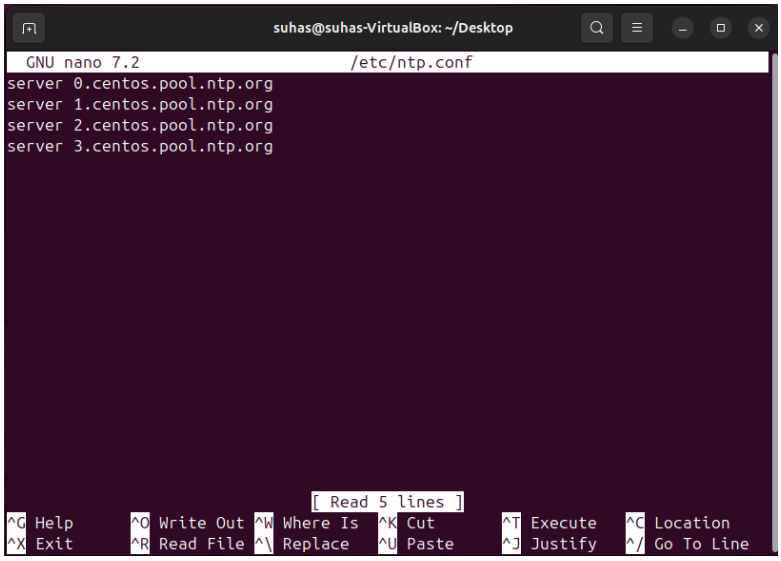

Figure 66

After that you can press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

3. Restart and enable ntp.
   sudo systemctl restart ntp.
   sudo systemctl restart ntp.

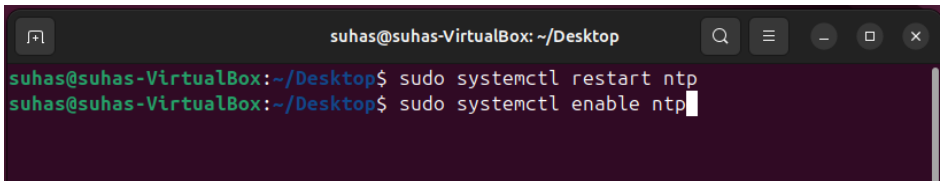

Figure 67

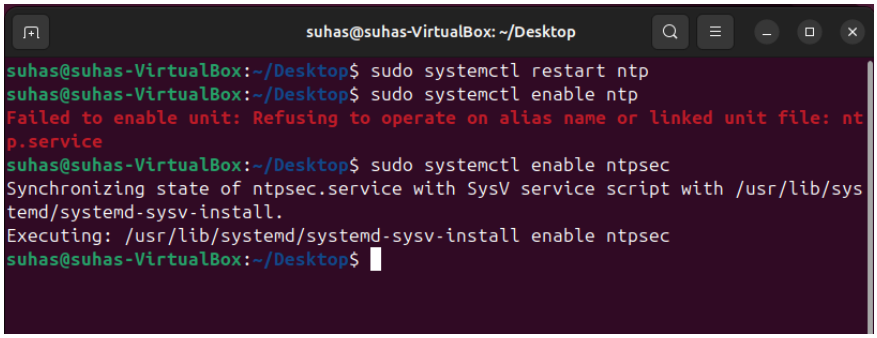

Figure 68

If you see above kind of error. Your enable commands

change like this "**sudo systemctl enable ntpsec**"

4. Check the status of the ntp service.
   sudo systemctl status ntp.

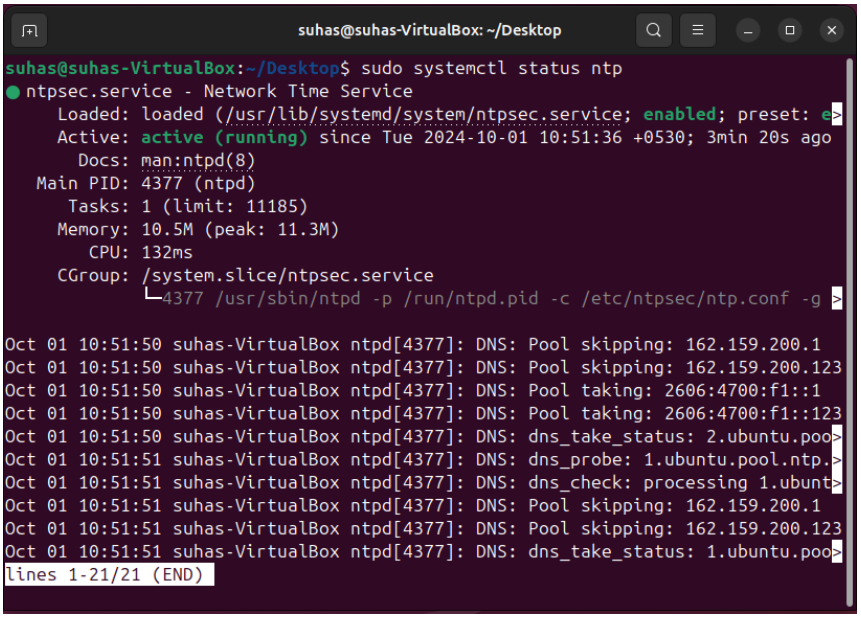

Figure 69

5. Verify that ntp working properly.
   ntpq -p

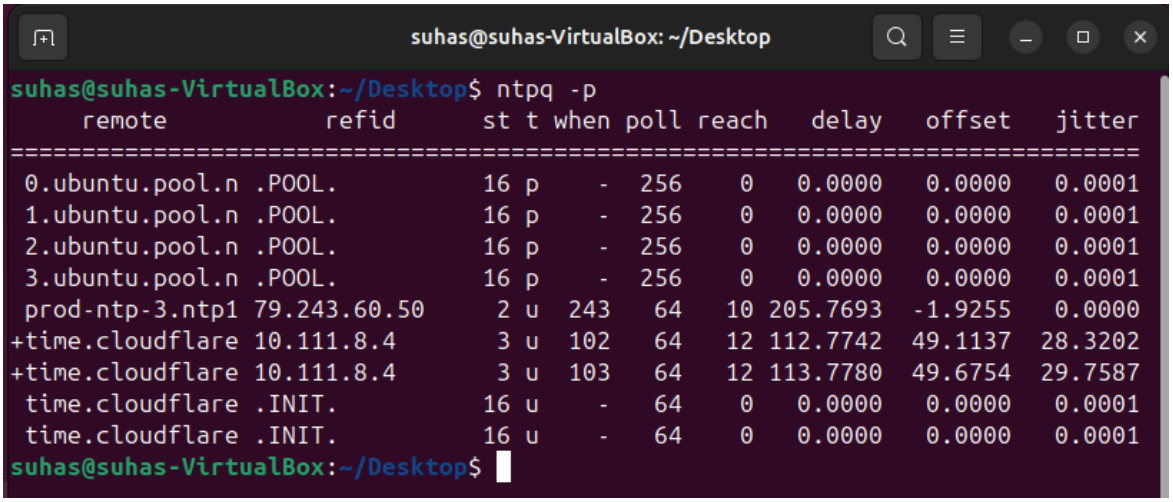

Figure 70

Shell Scripting and Security.

System Details Report Scipt

1. Open the terminal and create a new script file using any text editor.
   nano system_report.sh

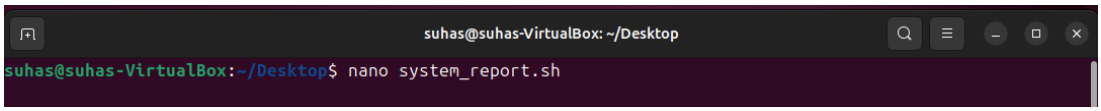

Figure 71

2. Then type in the file like below mentioned.

Figure 72

After that you can press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

3. Make the file executable and run.
   chmod +x system_report.sh
   ./system_report.sh

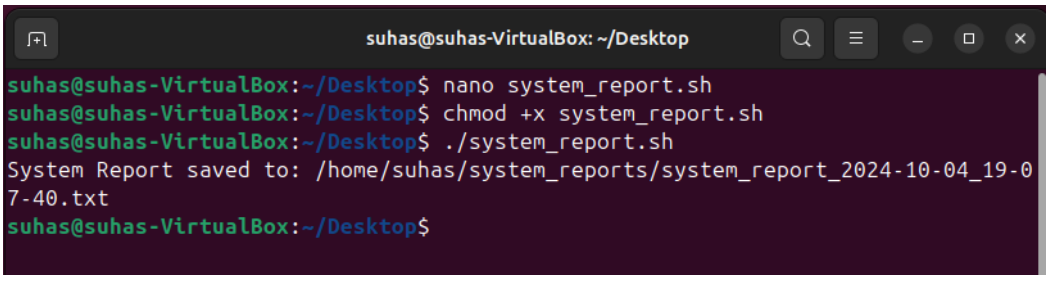

Figure 73

4. View the output file
   cd /home/suhas/system_reports
   cat system_report_[report file name after created]

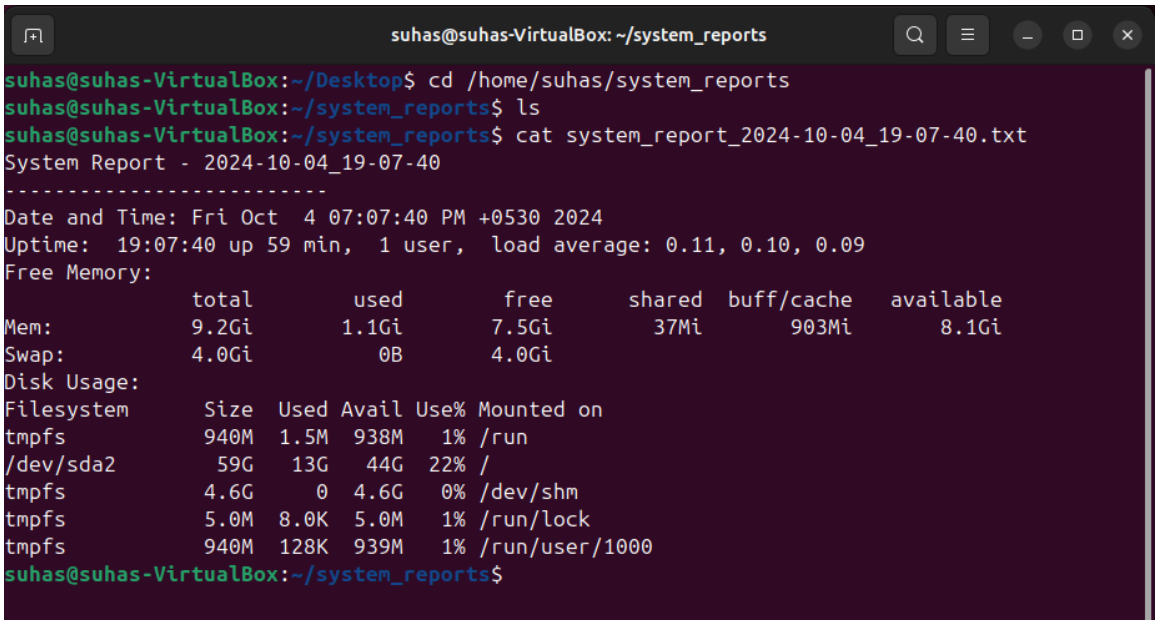

Figure 74

Backup Script

1. Open the terminal and create a new script file using any text editor.
   nano backup_documents.sh

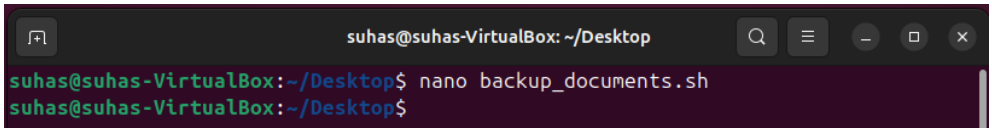

Figure 75

2. Then type in the file like below mentioned.

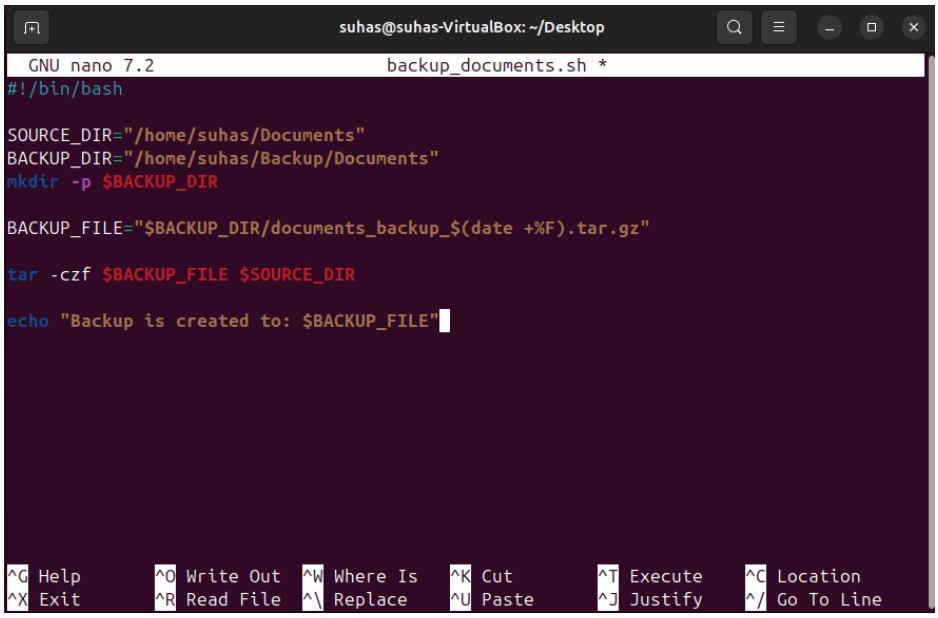

Figure 76

After that you can press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

3. Make the file executable and run.
   chmod +x system_report.sh
   ./system_report.sh

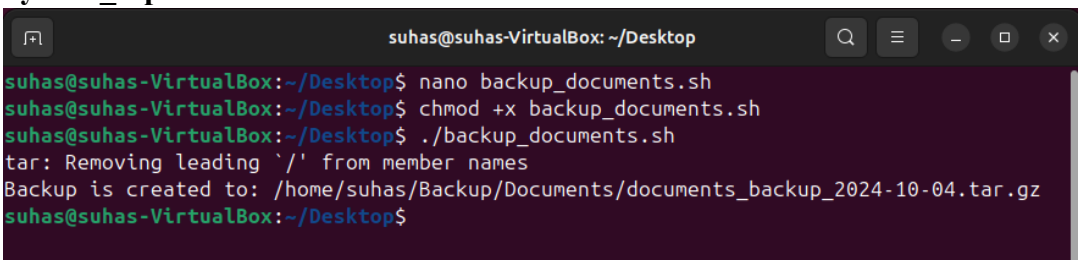

Figure 77

4. View the output file.
   cd /home/suhas/Backup/Documents
   cat documents_backup_[backup file name after created]

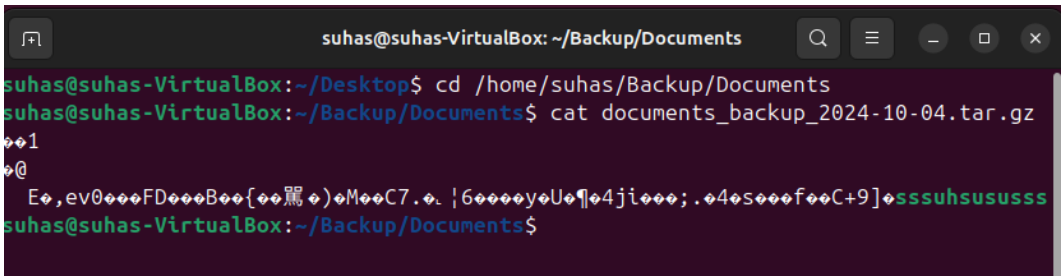

Figure 78

Shell Scripting Scheduling with Cron job

1. Open and select the crontab editor as you preferred.
   crontab -e

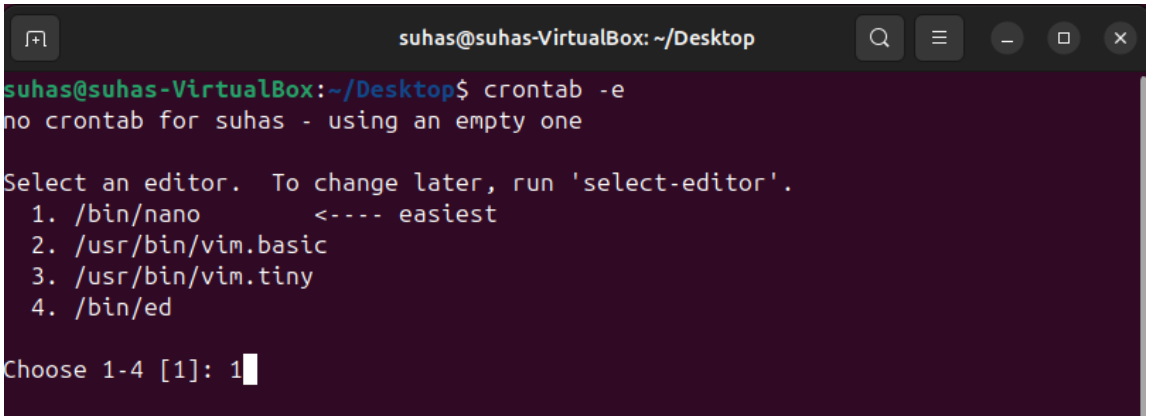

Figure 79

2. Add both cron jobs to the file and press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.
   0 9 * * * /home/suhas/system_reports/system_report.sh
   0 9 * * * /home/suhas/Backup/Documents/documents_backup_2024-10-04.tar.gz

   To run system_report.sh and documents_backup_2024-10-04.tar.gz scripts everyday at 9.00 A.M.

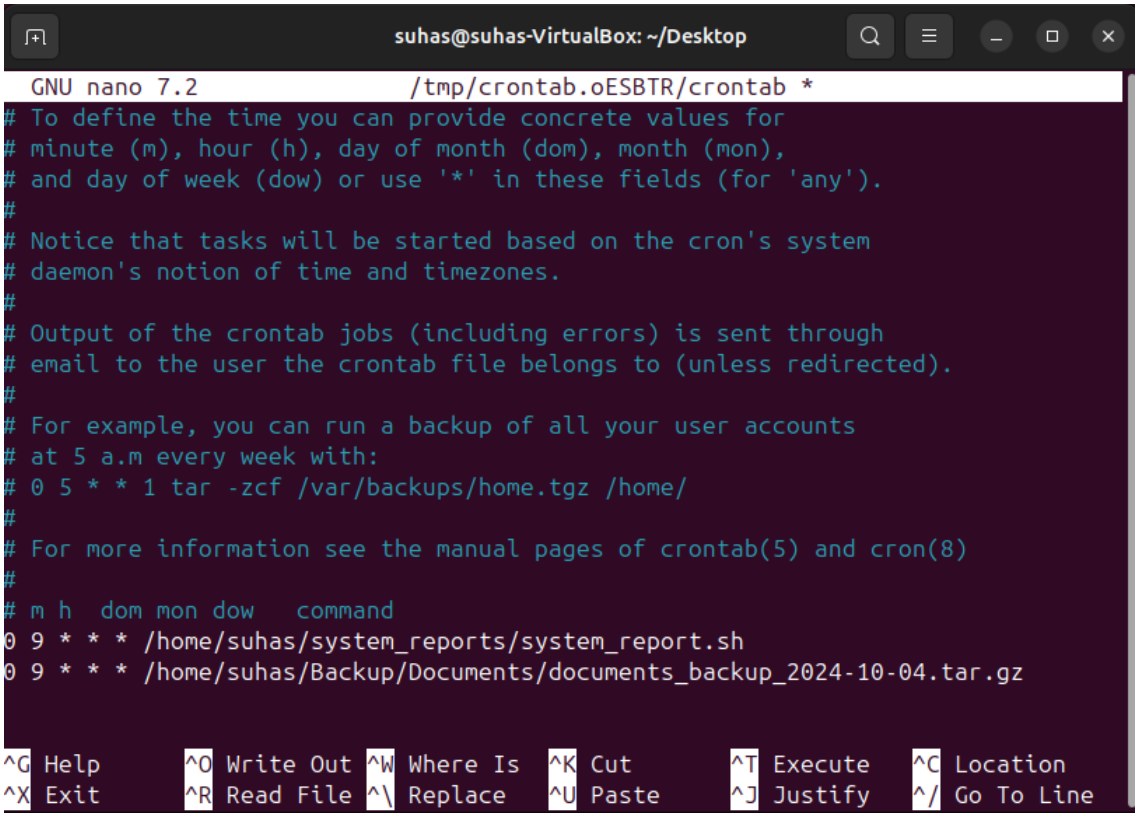

Figure 80

3. Check the cronjobs.
   crontab l

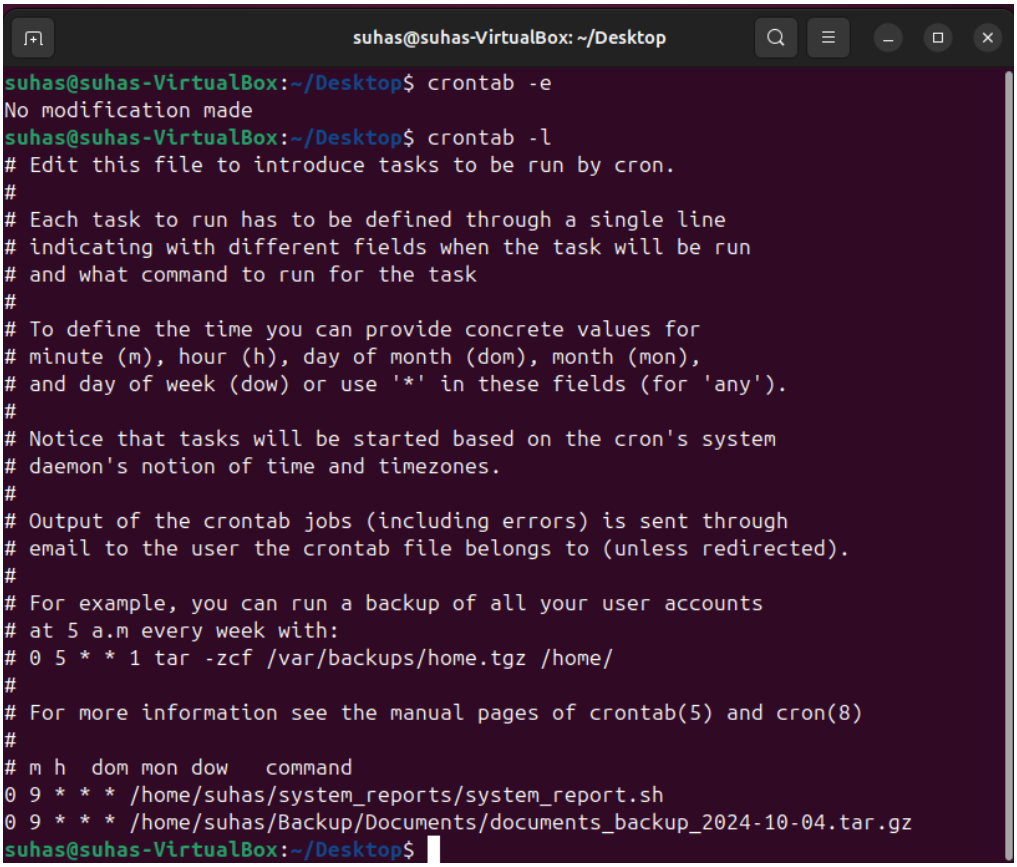

Figure 81

Configuring steps for SSH server, iptables and ACLs

SSH server

1. First you need to install the package list and install openssh-server.
   sudo apt update
   sudo apt install openssh-server

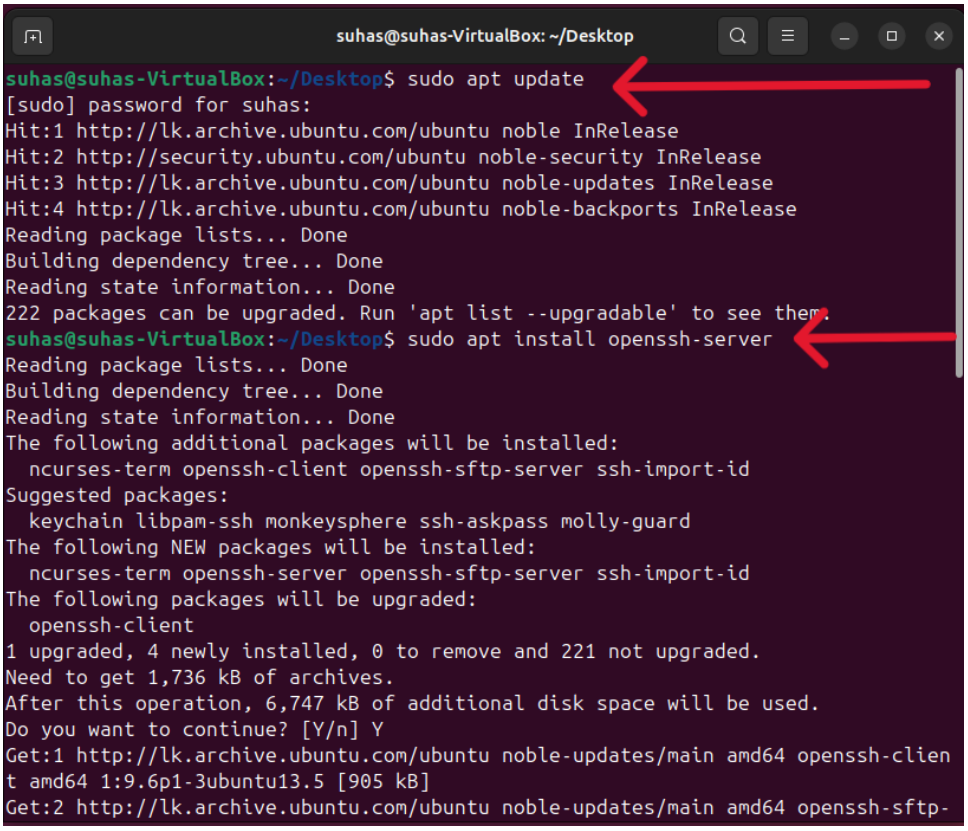

Figure 82

2. Start and enable ssh.
   sudo systemctl start ssh
   sudo systemctl enable ssh

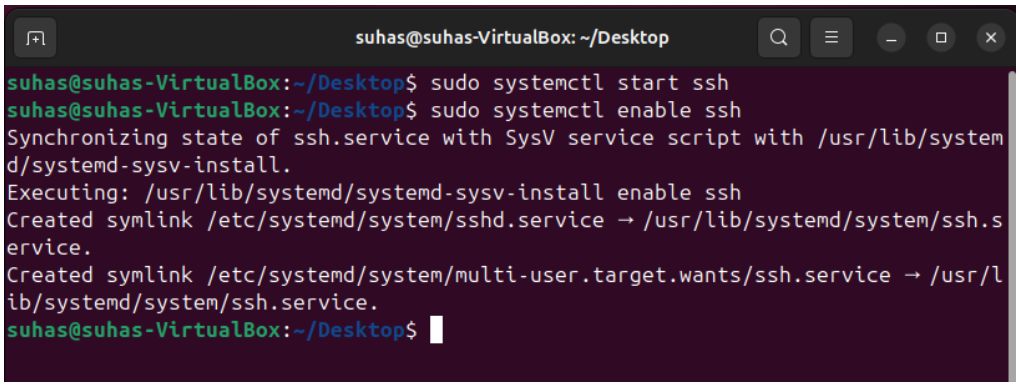

Figure 83

3. Check the status of the ssh server.
   sudo systemctl status ssh.

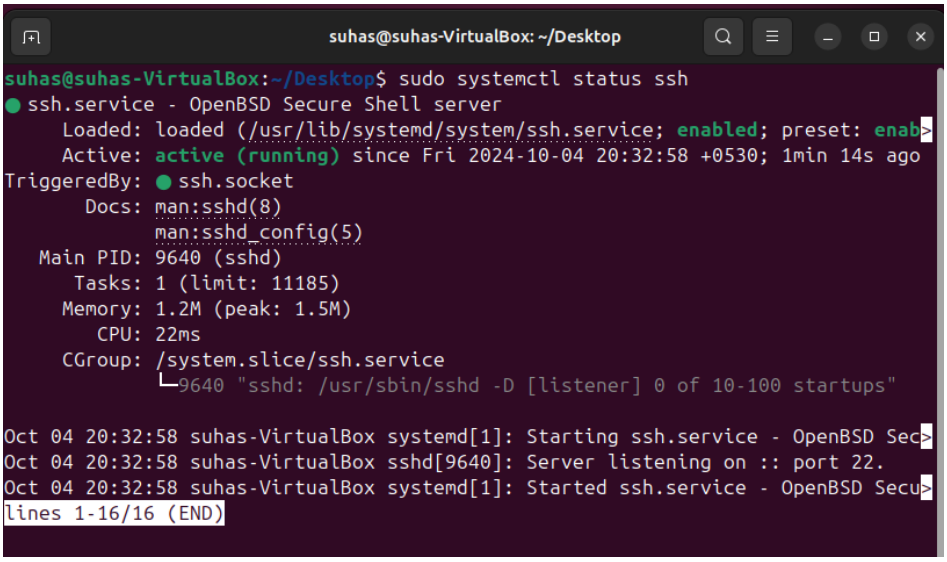

Figure 84

Connecting VM machines using SSH.

1. Configures the firewall to allow ssh connections
   If you have a firewall running, make sure to allow the SSH port (default 22) through the firewall.
   sudo ufw allow ssh
   sudo ufw enable ssh

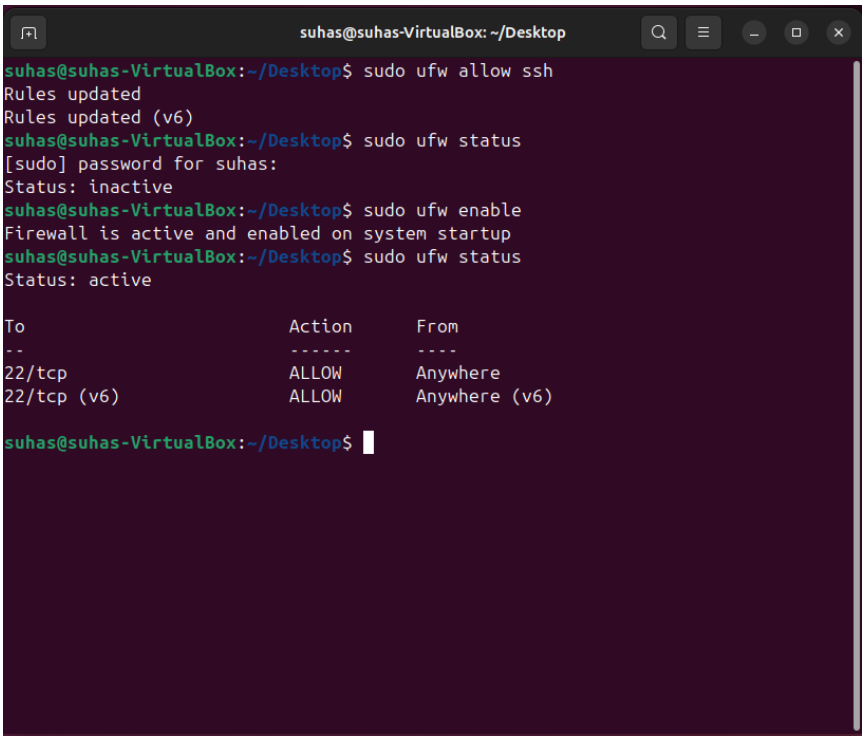

Figure 85

2. Find the VMs IP Address.
   ip a

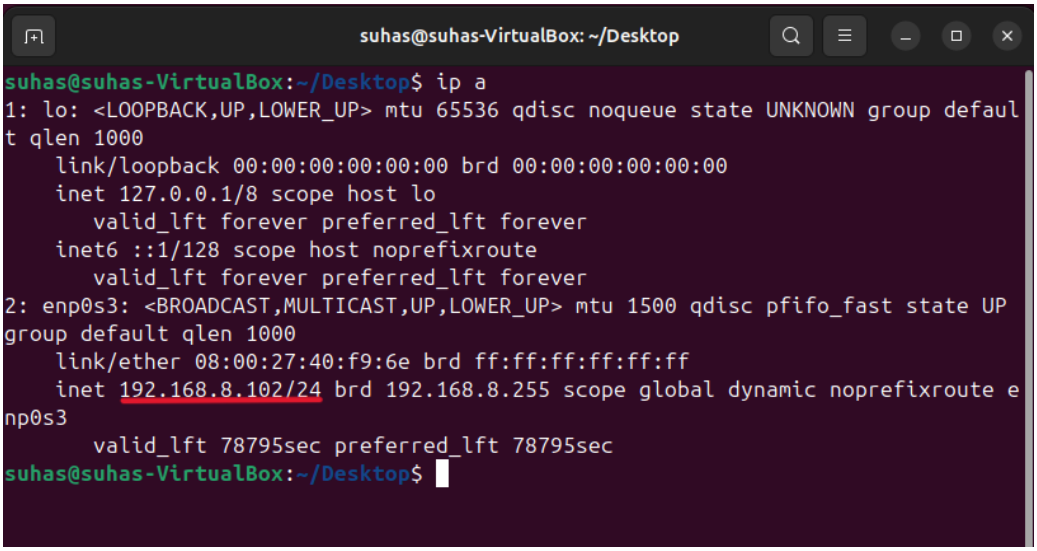

Figure 86

3. SSH into VM from another computer.
   Open terminal on other computer and run following command.
   ssh username@VMs_ipaddress
   ssh suhas@192.168.8.102

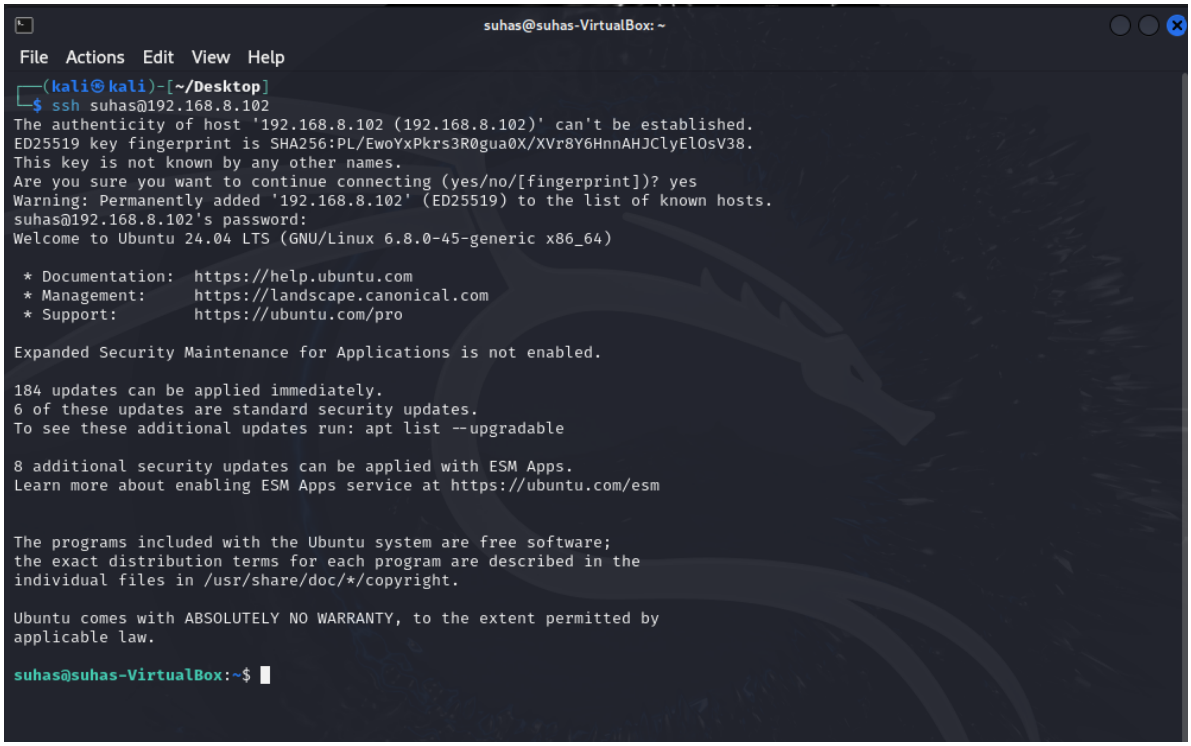

Figure 87

Iptables and ACLs

Web server security.

1. Allow HTTP traffic on port 80.
   sudo iptables -A INPUT -p tcp –dport 80 -j ACCEPT

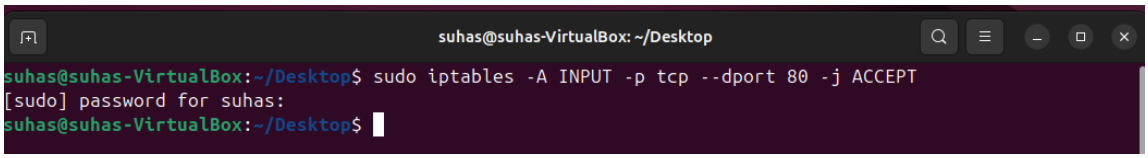

Figure 88

2. Allow HTTPS traffic on port 443.
   sudo iptables -A INPUT -p tcp –dport 443 -j ACCEPT

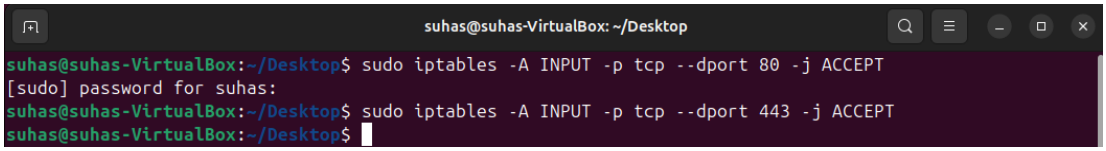

Figure 89

3. Block all other incoming traffic by default.
   sudo iptables -P INPUT DROP

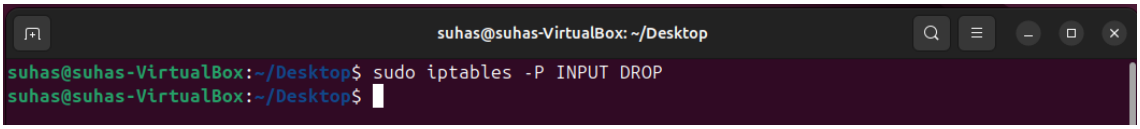

Figure 90

Remote Administration Access.

1. Allow SSH access from the trusted IP address.
   Get your current IP Address
   ip a
   sudo iptables -A INPUT -p tcp –dport22 -s 192.168.8.102 -j ACCEPT

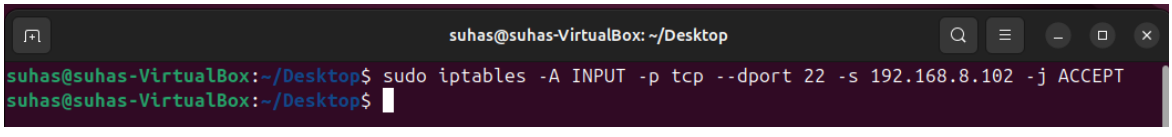

Figure 91

2. Block SSH access from all other IP addresses.
   sudo iptables -A INPUT -p tcp –dport 22 -j DROP

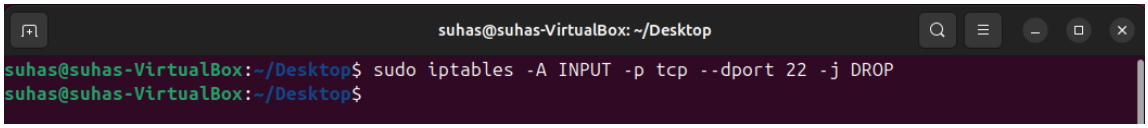

Figure 92

Allow Specific Applications

1. Allow traffic for the application on port 443(video conferencing).
   sudo iptables -A INPUT -p tcp –dport 443 -j ACCEPT

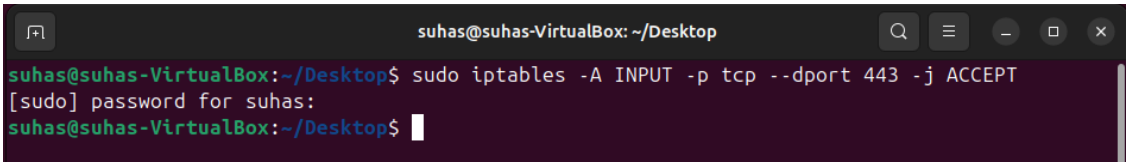

Figure 93

Allow Pings (ICMP Echo Request)

1. Allow ICMP (ping) request.
   sudo iptables -A INPUT -p icmp –icmp-type echo-request -j ACCEPT

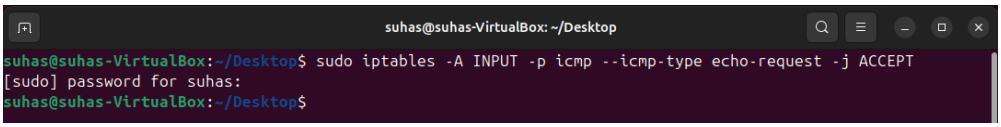

Figure 94

Printer Server Access

1. Allow traffic to the printer server on port 9100 from local network.
   sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 –dport 9100 -j ACCEPT

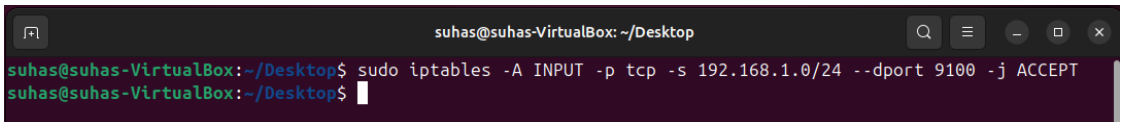

Figure 95

2. Block external access to the printer server.
   sudo iptables -A INPUT -p tcp –dport 9100 -j DROP

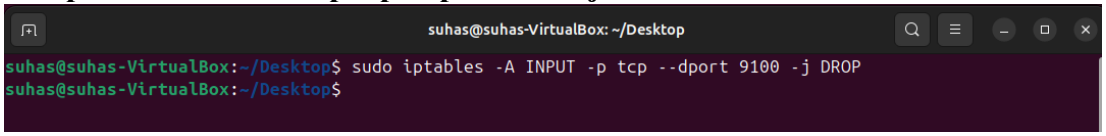

Figure 96

Implementing Best Practices in a Linux Based Environment.

1. Configuring Firewall Rules with iptables.
   By configuring a firewall, we can minimise the attack area by controlling both incoming and outgoing traffic.

   - Allow HTTP and HTTPS traffic.
     sudo iptables -A INPUT -p tcp –dport 80 -j ACCEPT
     sudo iptables -A INPUT -p tcp –dport 443 -j ACCEPT

   - Allow SSH only from a trusted ip(with your current IP).
     sudo iptables -A INPUT -p tcp -s 127.0.0.1/8 –dport 22 -j ACCEPT

   - Allow ICMP (ping) requests.
     sudo iptables -A INPUT -p icmp –icmp-type echo-request -j ACCEPT

   - Drop all other traffic by default.
     sudo iptables -P INPUT DROP

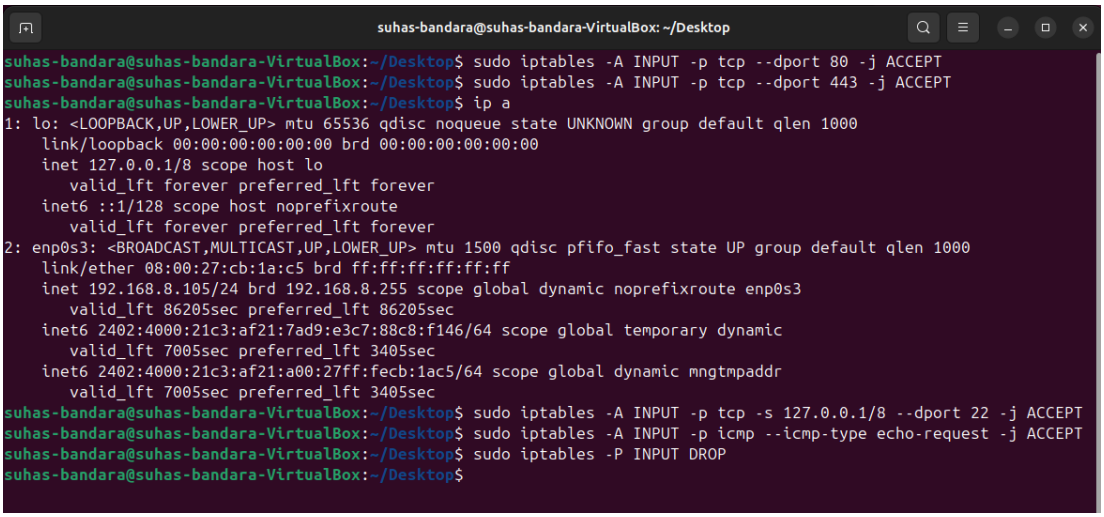

Figure 97

2. Disable Unnecessary Services.

- You can list all active services and determine which ones are unnecessary.
  sudo systemctl list-units --type=service --state=running

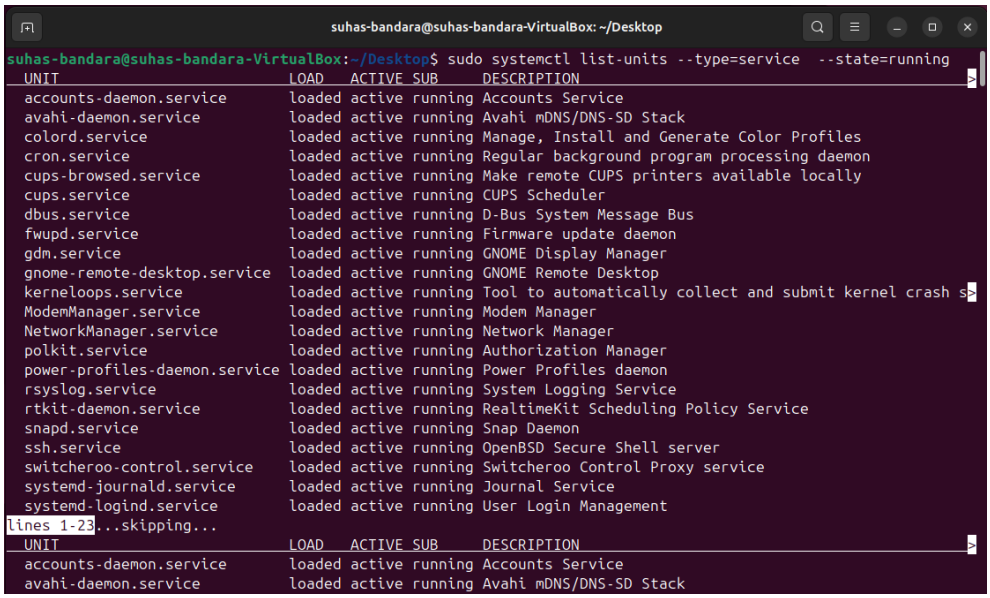

Figure 98

Then select and disable services that aren't necessary.
sudo systemctl disable systemd-journald.service

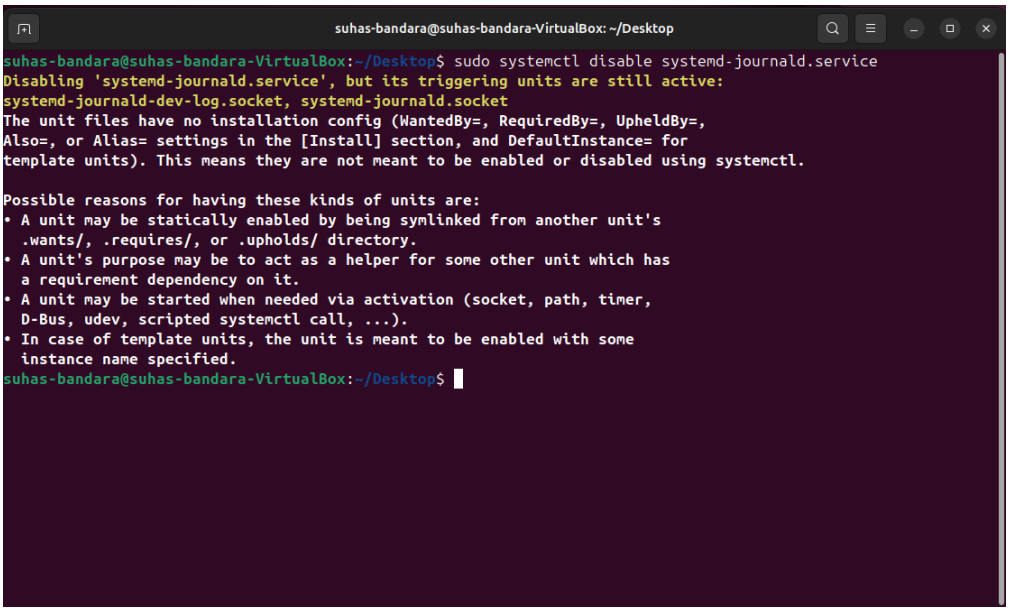

Figure 99

3. Keeping Software Updated.
    - Update the package lists
      sudo apt update

    - Upgrade all install packages.
      sudo apt upgrade -y

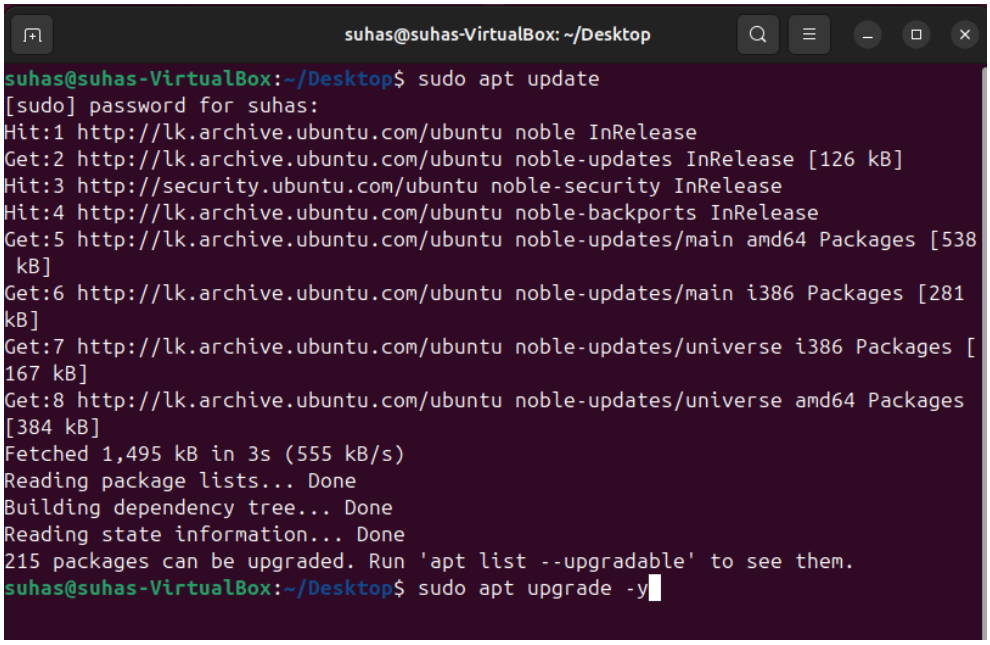

Figure 100

4. Enforcing Strong Password Policies.

    - Edit the PAM configuring file to enforced password complexity.
      sudo nano /etc/pam.d/common-password

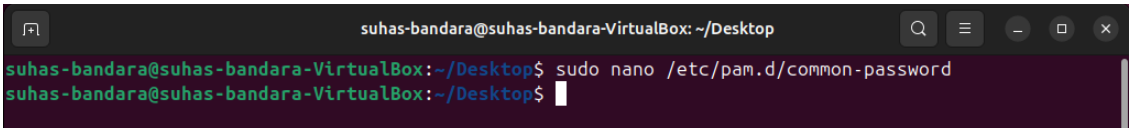

Figure 101

And then modify the following line.

password requisite pam_pwquality.so retry=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1

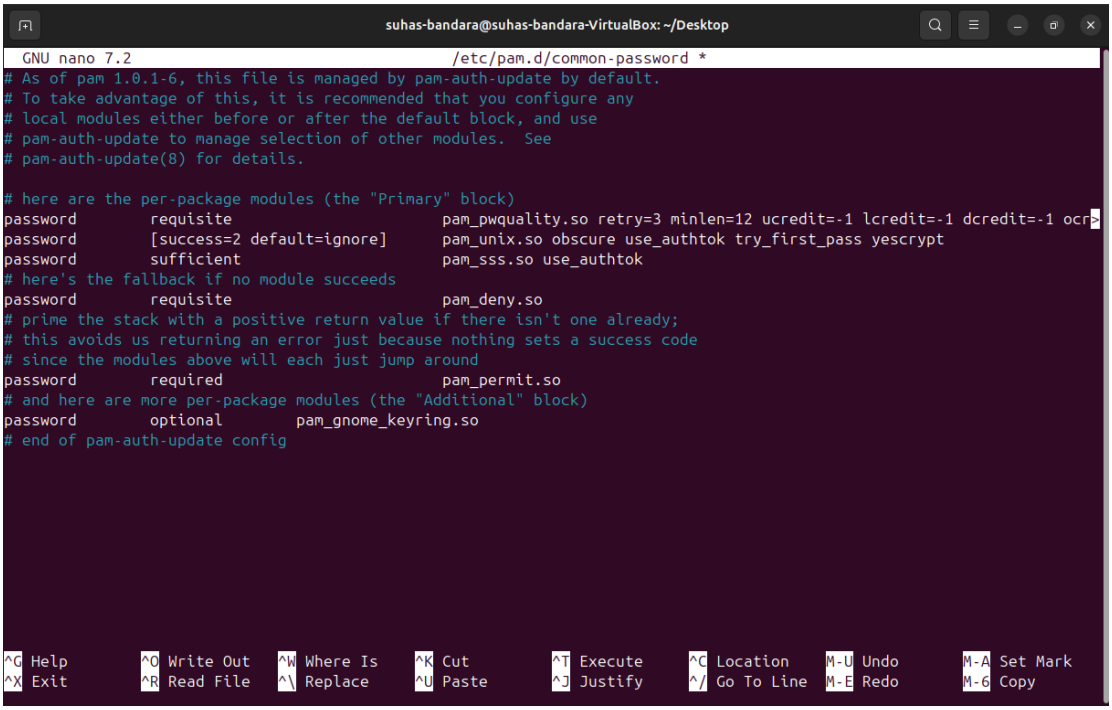

Figure 102

After that press "**Ctrl+o**" "**Enter**" and "**Ctrl+x**" to save and exit from the editor.

5. Network Port Scanning and Monitoring.

- Install Nmap.
  sudo apt install nmap

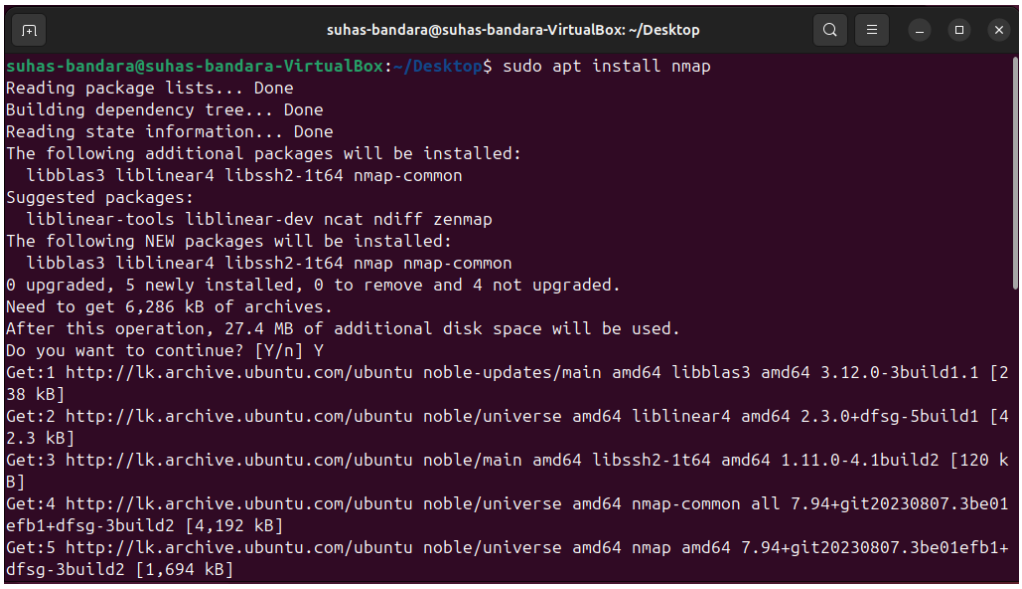

Figure 103

- Scan open ports on the local machine.
  sudo nmap -sT localhost

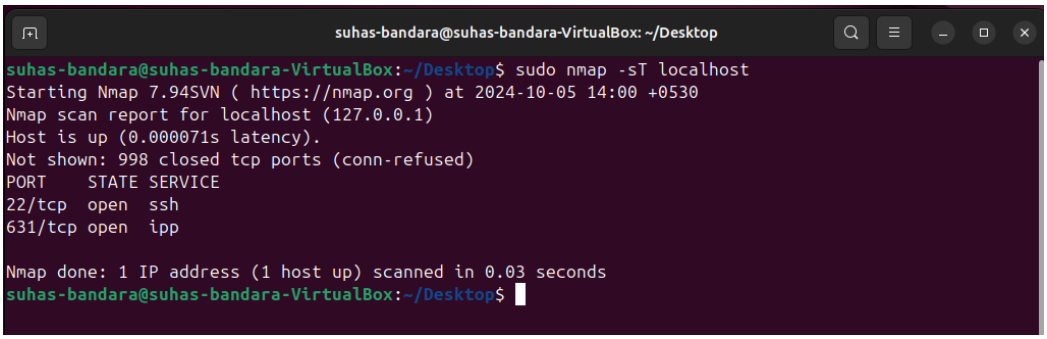

Figure 104