

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

1.	Basics of Linux Environments.....	3
	Virtual Machine Setup:	3
	Setup the VirtualBox:	6
	Install Ubuntu OS on VirtualBox	11
2.	Basic Linux Commands.....	18
	Navigation Commands.	18
	File Manipulation Commands.....	20
	System Information and User Management Commands.	22
3.	DHCP, DNS, and NTP Services Configuration.	25
	DHCP Service Configuration.....	25
	DNS Services Configuration.	29
	NTP Services Configuration.....	31
4.	Shell Scripting and Security.....	34
	System Details Report Script.....	34
	Backup Script.....	36
	Shell Scripting Scheduling with Cron job.....	37
5.	Configuring steps for SSH server, iptables and ACLs	40
	SSH server.....	40
	Connecting VM machines using SSH.....	41
	Iptables and ACLs.....	43
	Web server security.....	43
	Remote Administration Access.....	43
	Allow Specific Applications	44
	Allow Pings (ICMP Echo Request).....	44
	Printer Server Access	44
6.	Implementing Best Practices in a Linux Based Environment.	45

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.

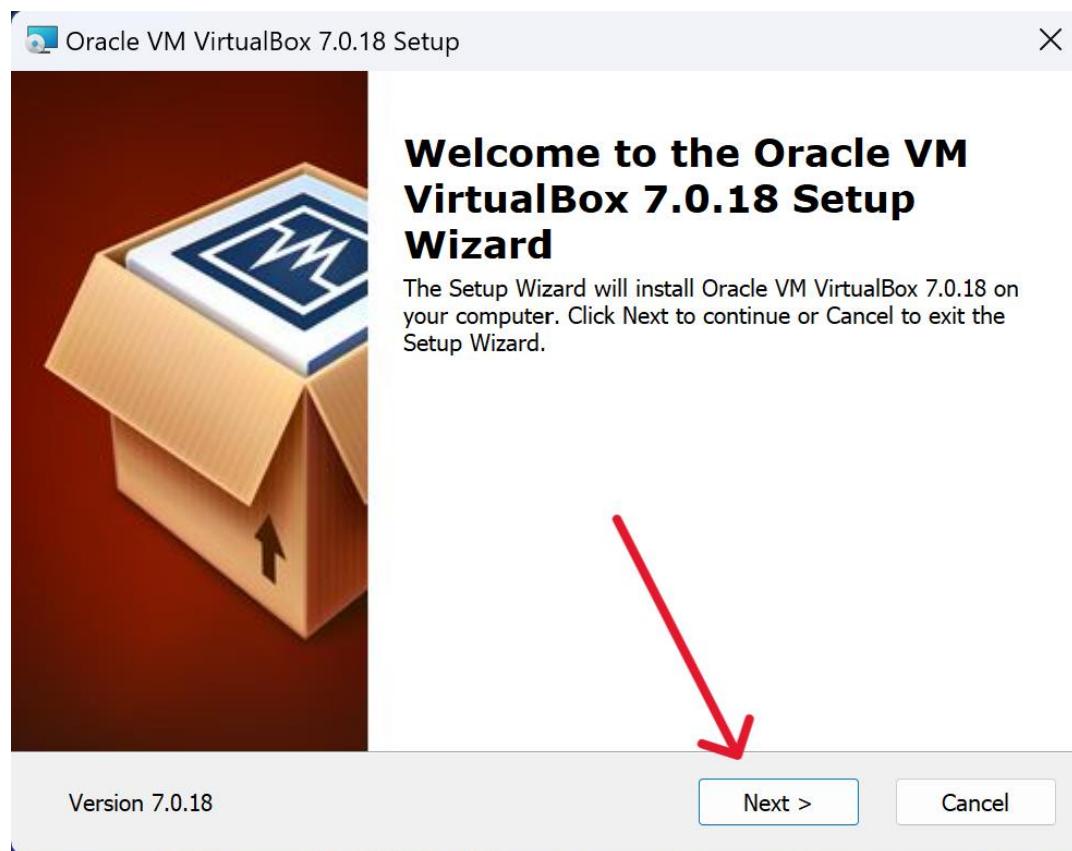


Figure 1

3. Select the location path you want to install the setup and then click on “Next” button to continue the setup.

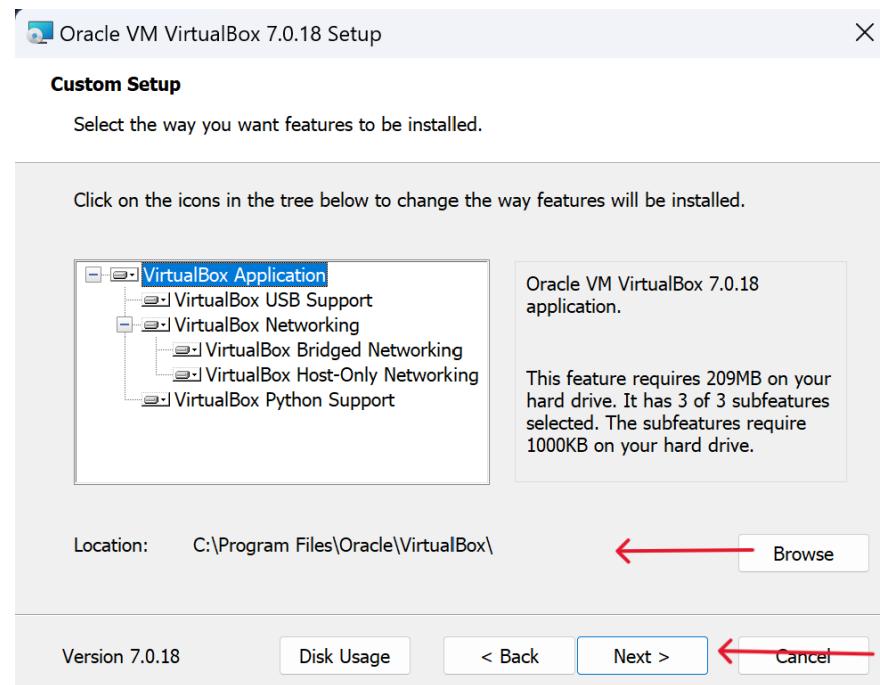


Figure 2

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

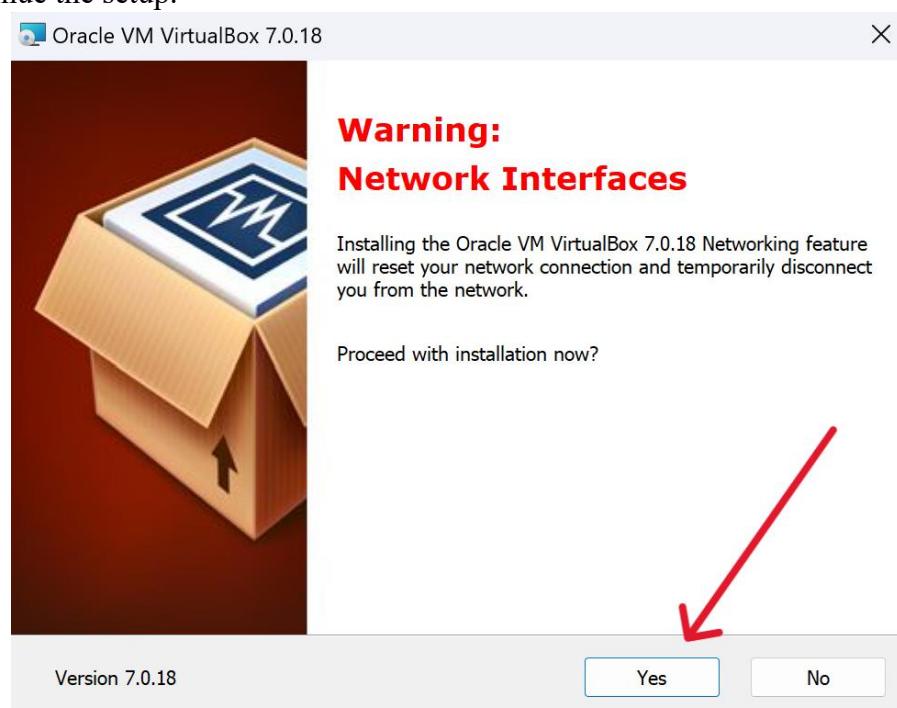


Figure 3

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

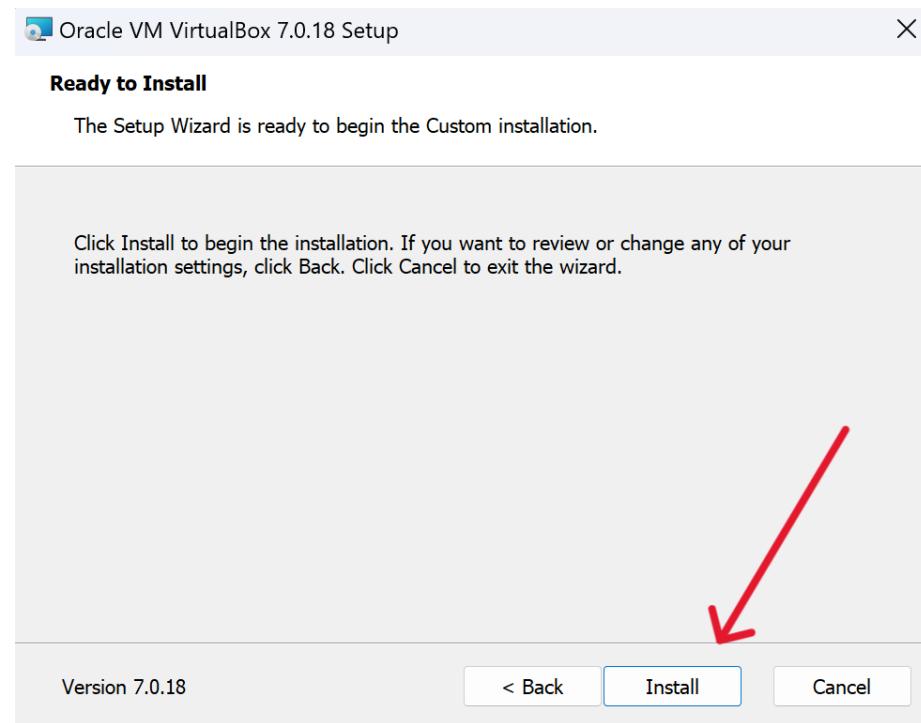


Figure 4



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.

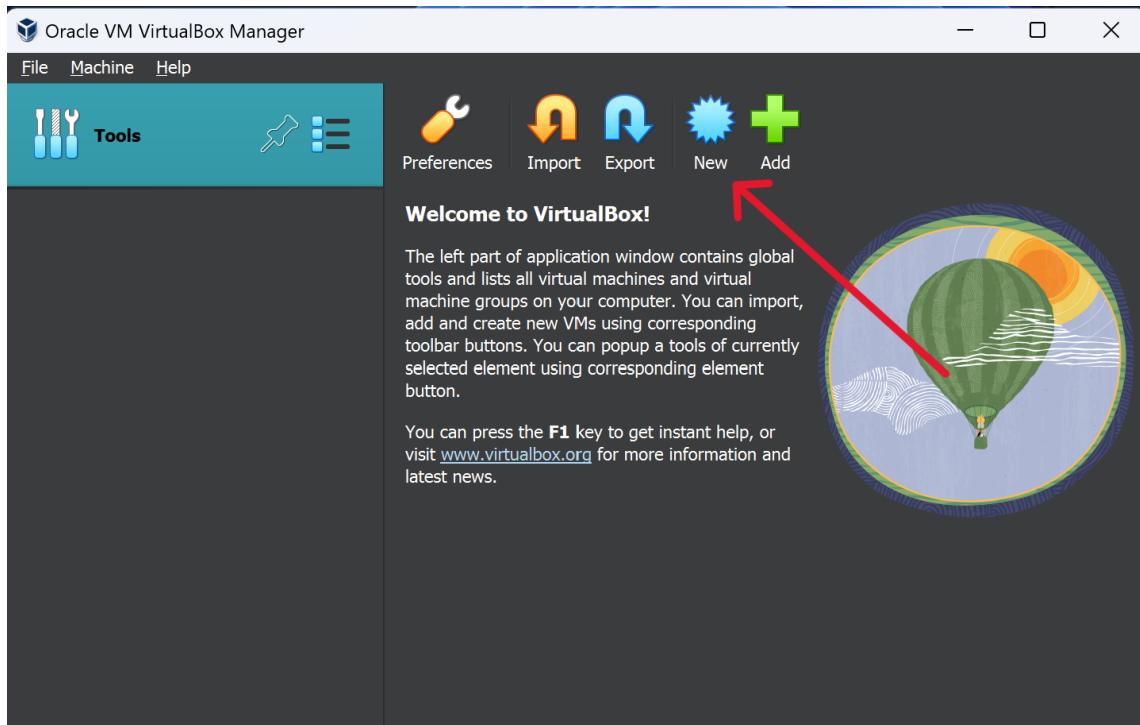


Figure 6

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

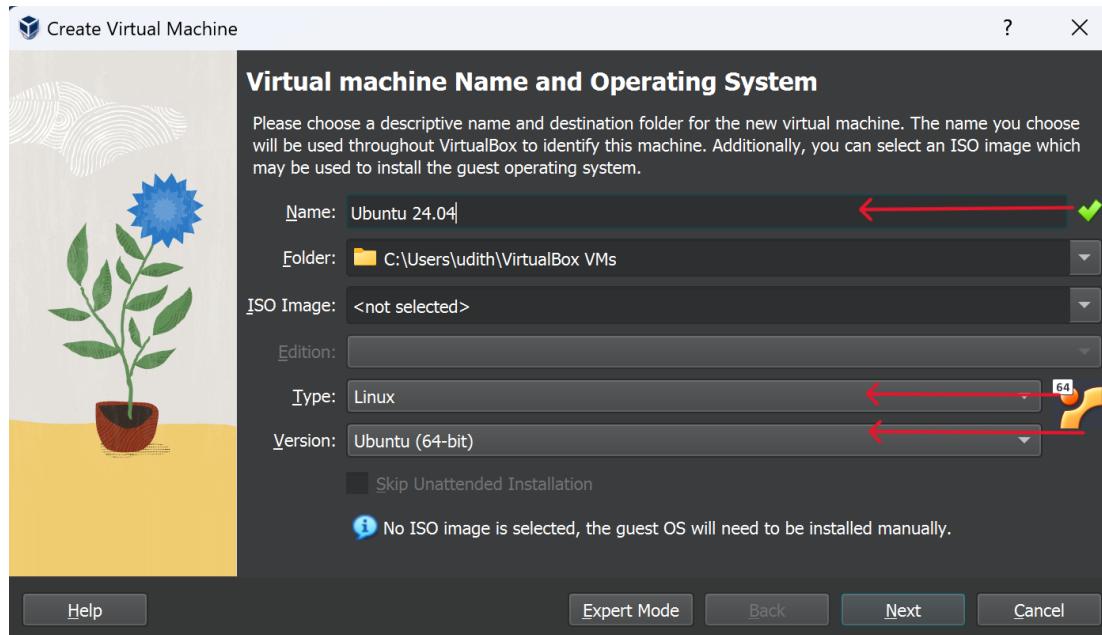


Figure 7

5. Select the iso image you have downloaded.

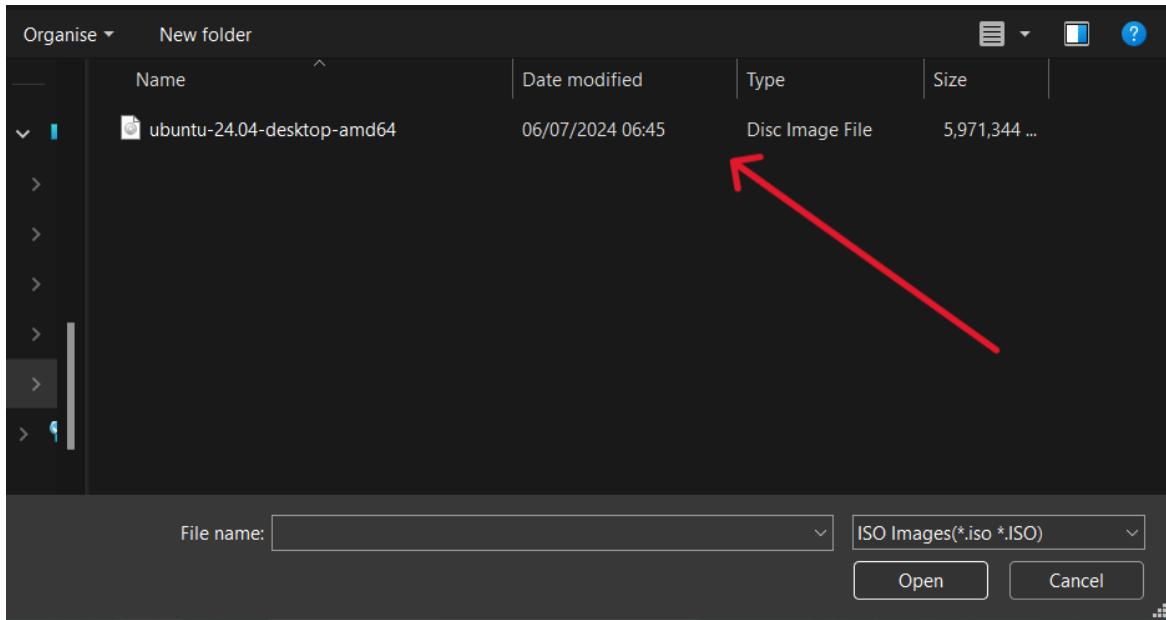


Figure 8

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.

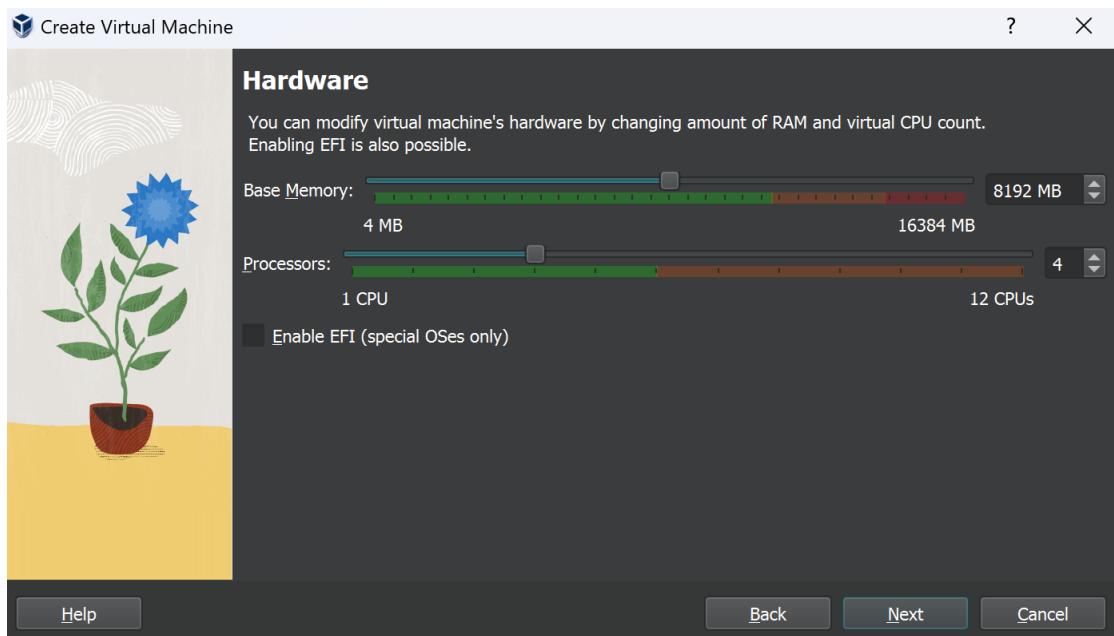


Figure 10

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.

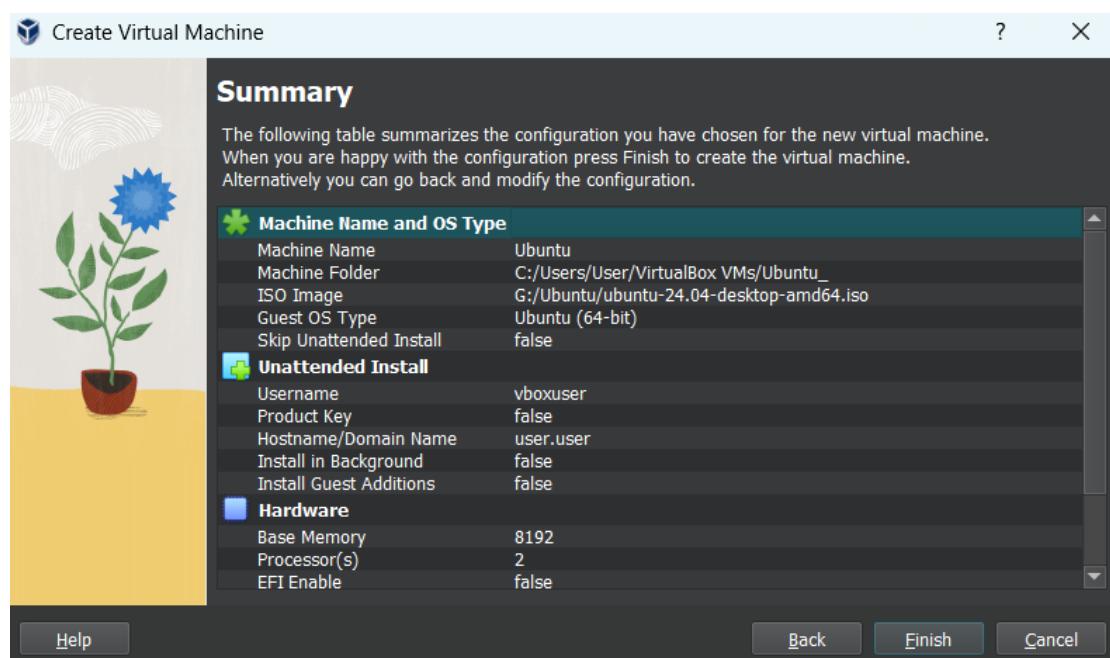


Figure 12

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

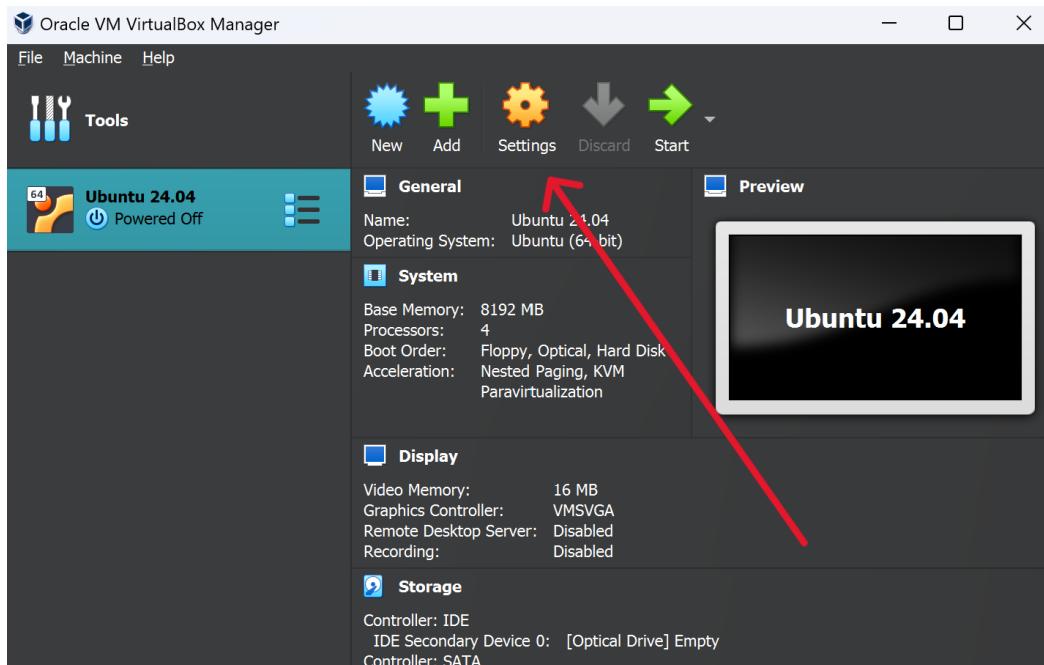


Figure 13

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

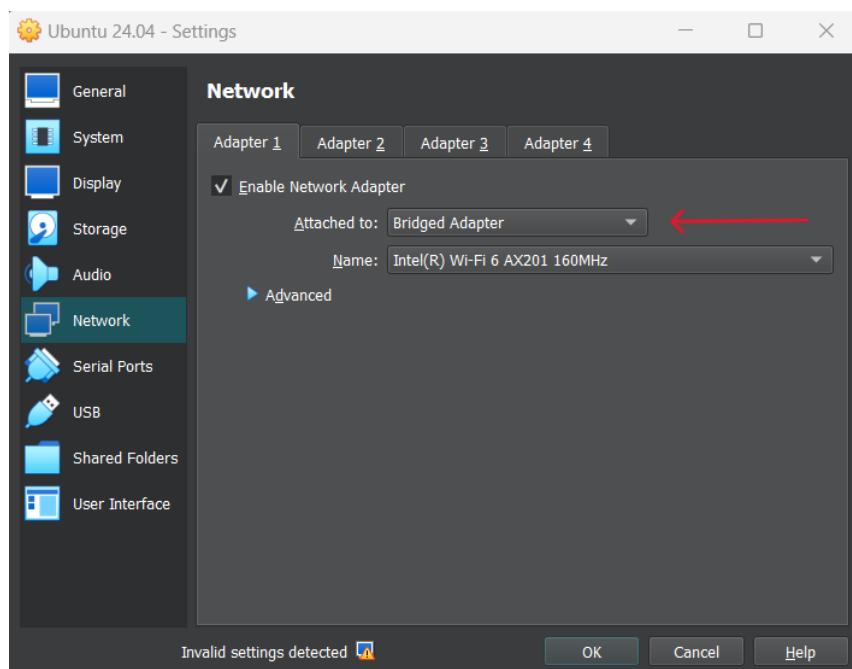


Figure 14

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.

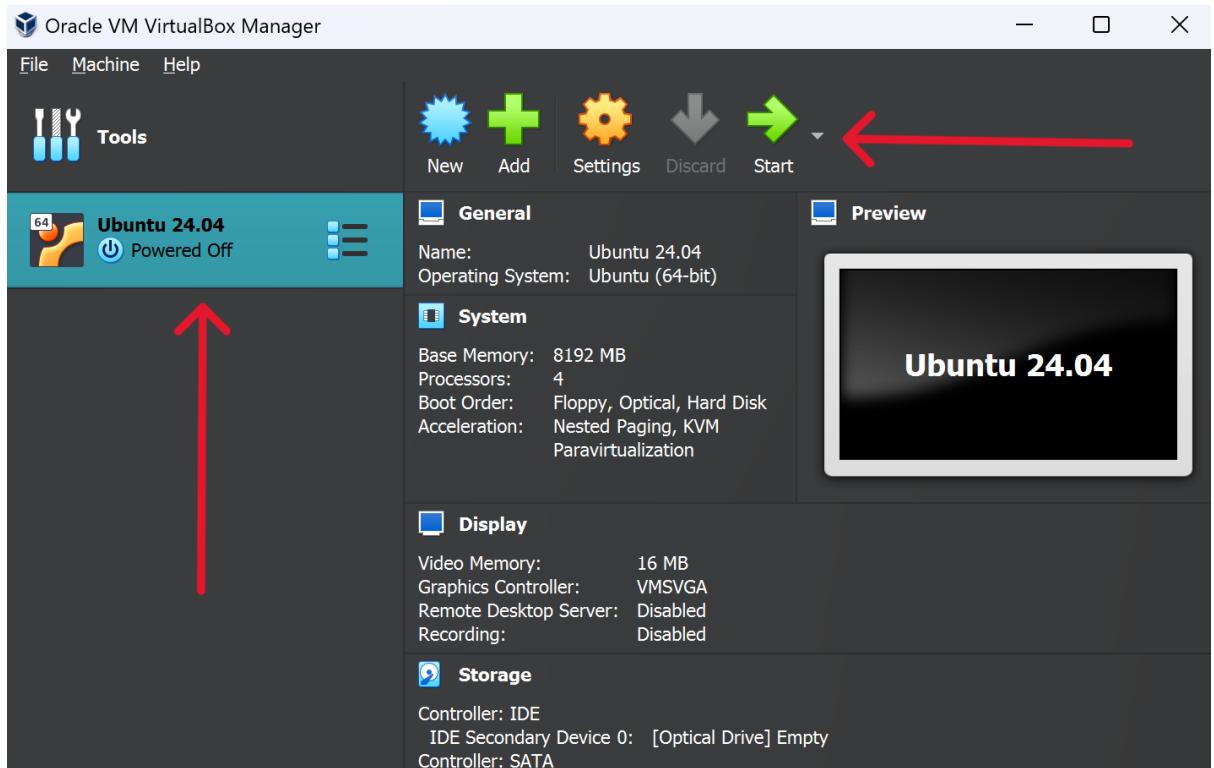


Figure 15

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

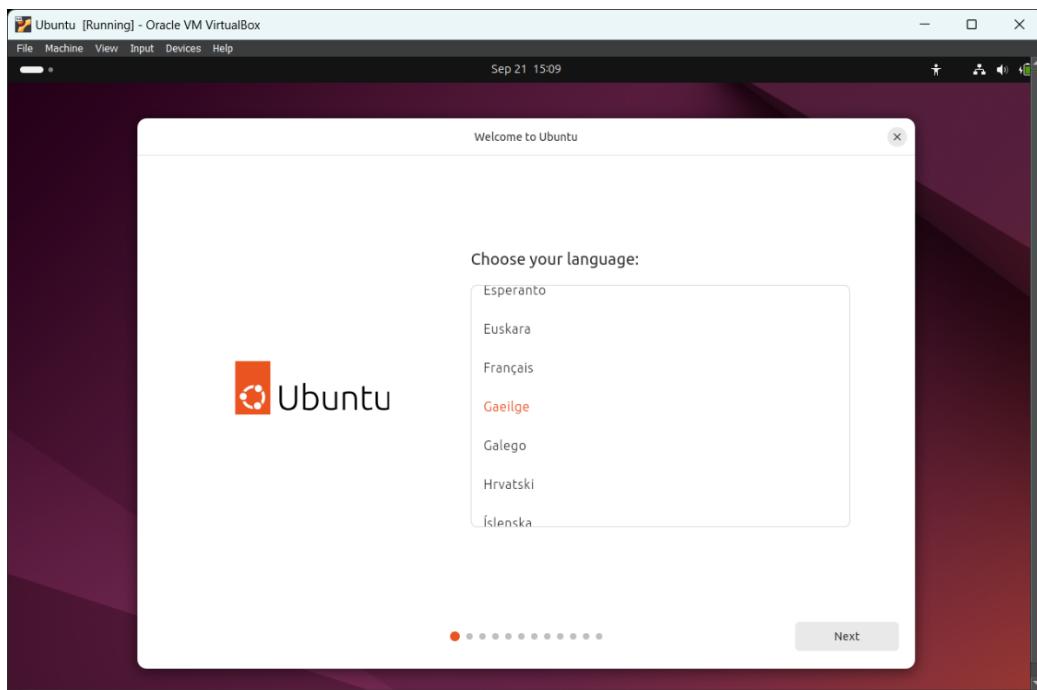


Figure 16

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.

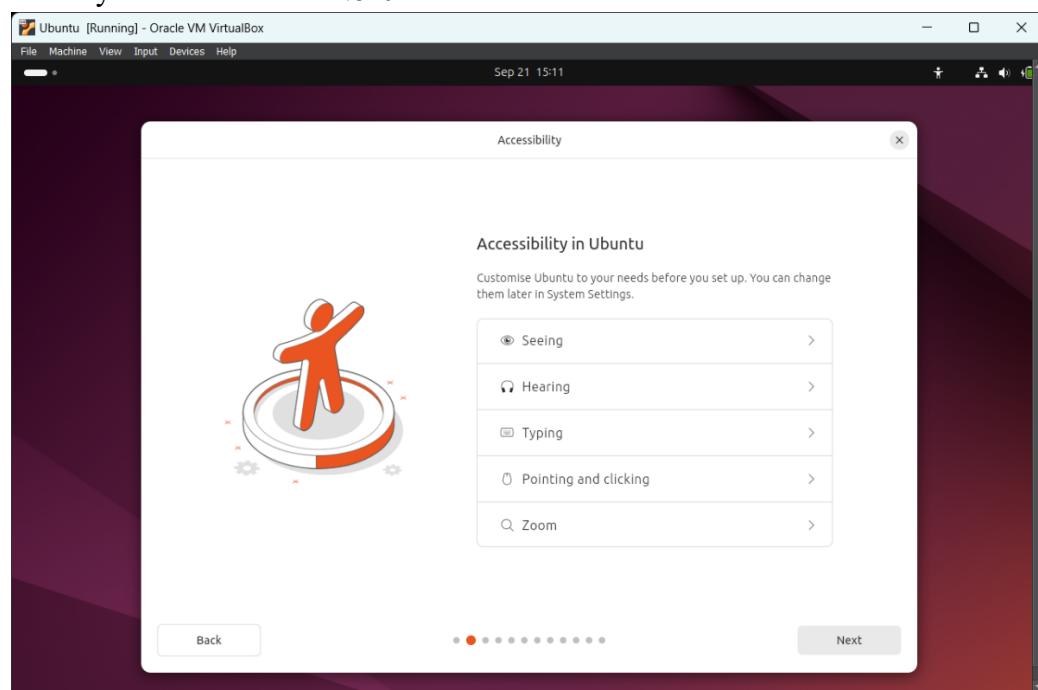


Figure 17

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.

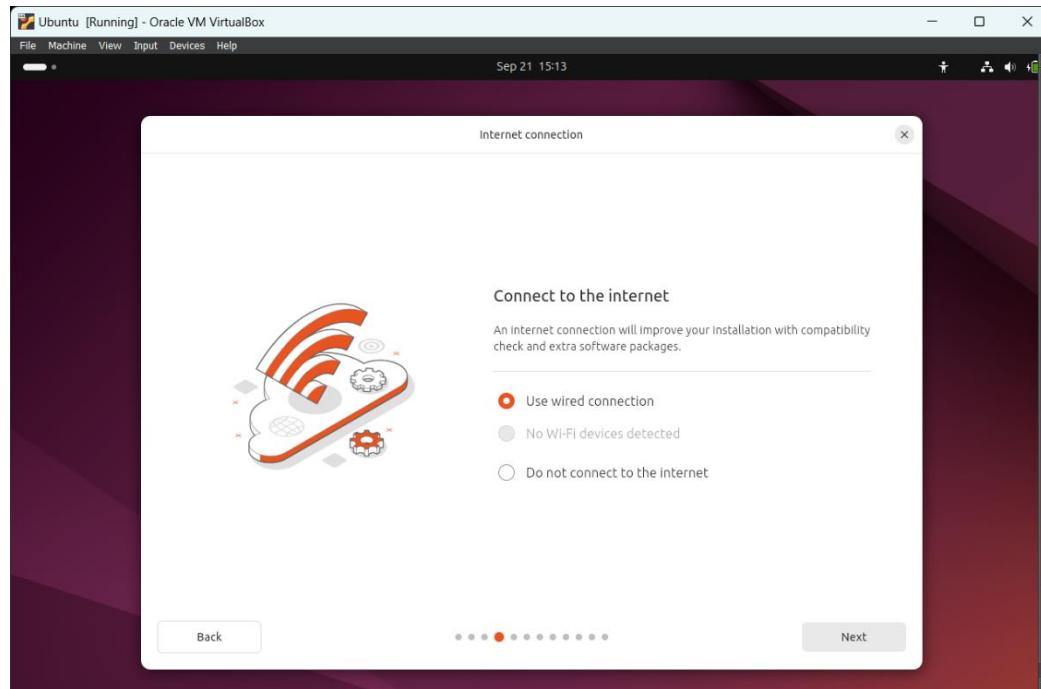


Figure 18

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.

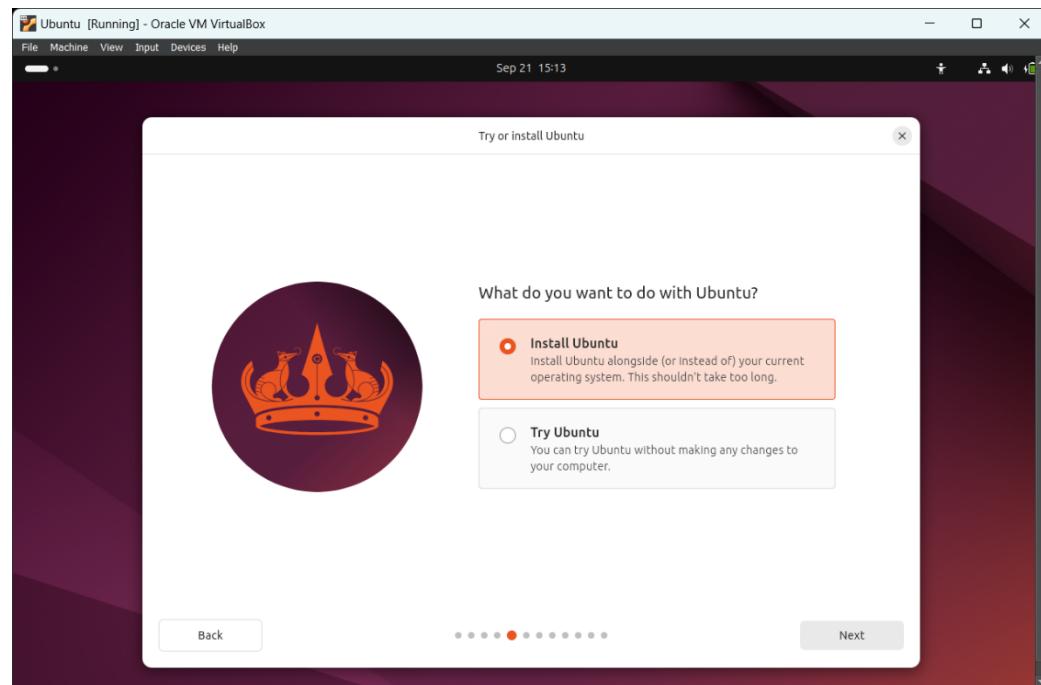


Figure 19

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

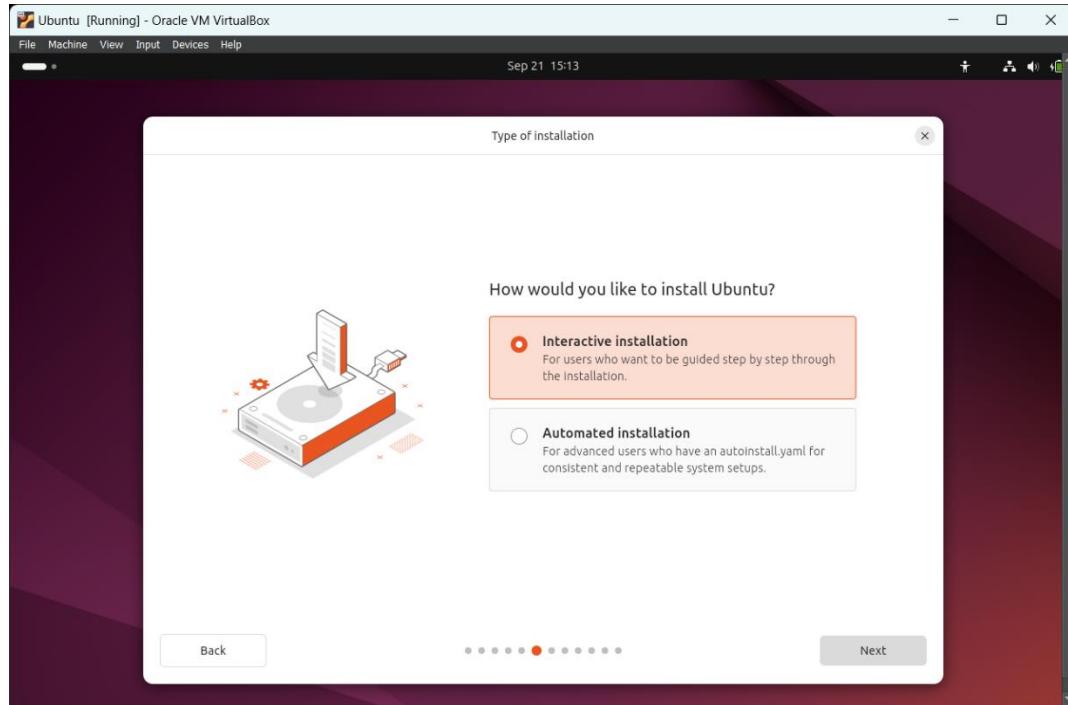


Figure 20

8. You can select what app would you like to start with Ubuntu and after the selection click on “**Next**” to continue the installation.

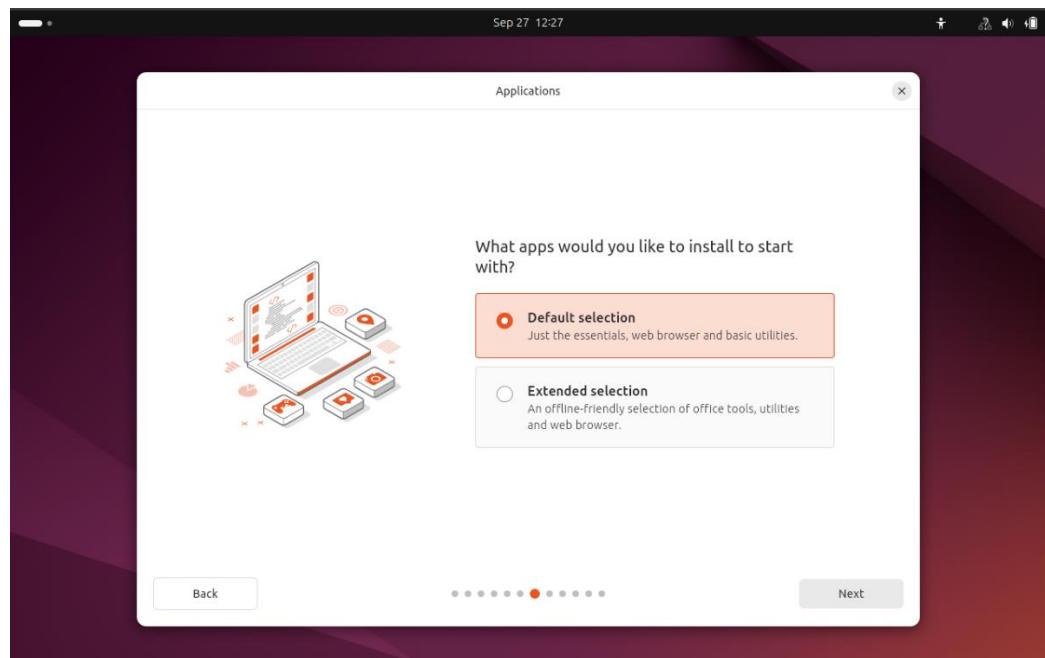


Figure 21

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

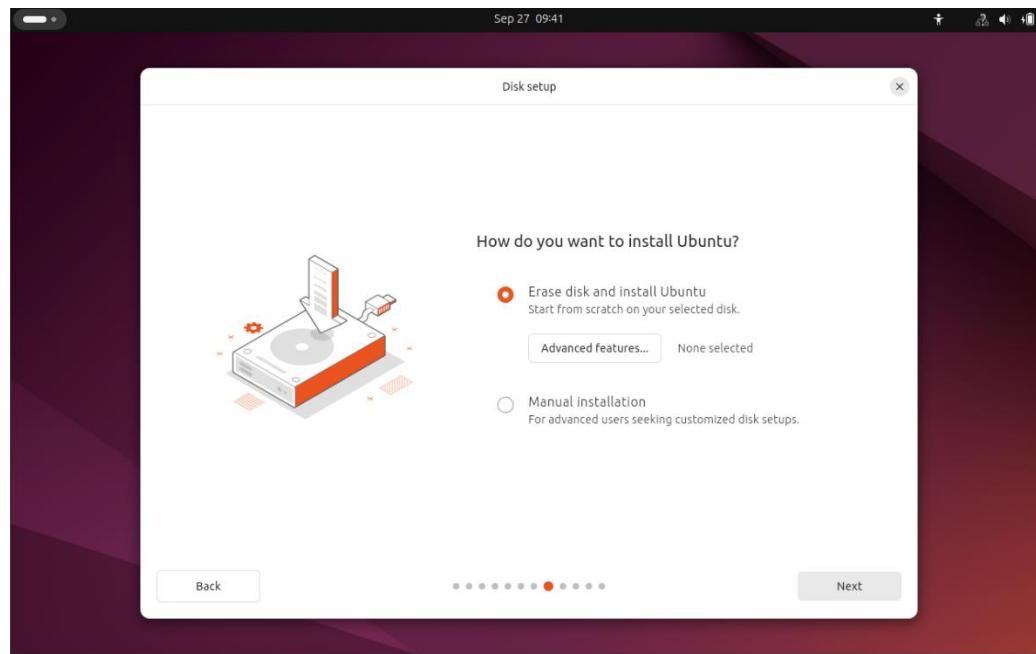


Figure 22

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.

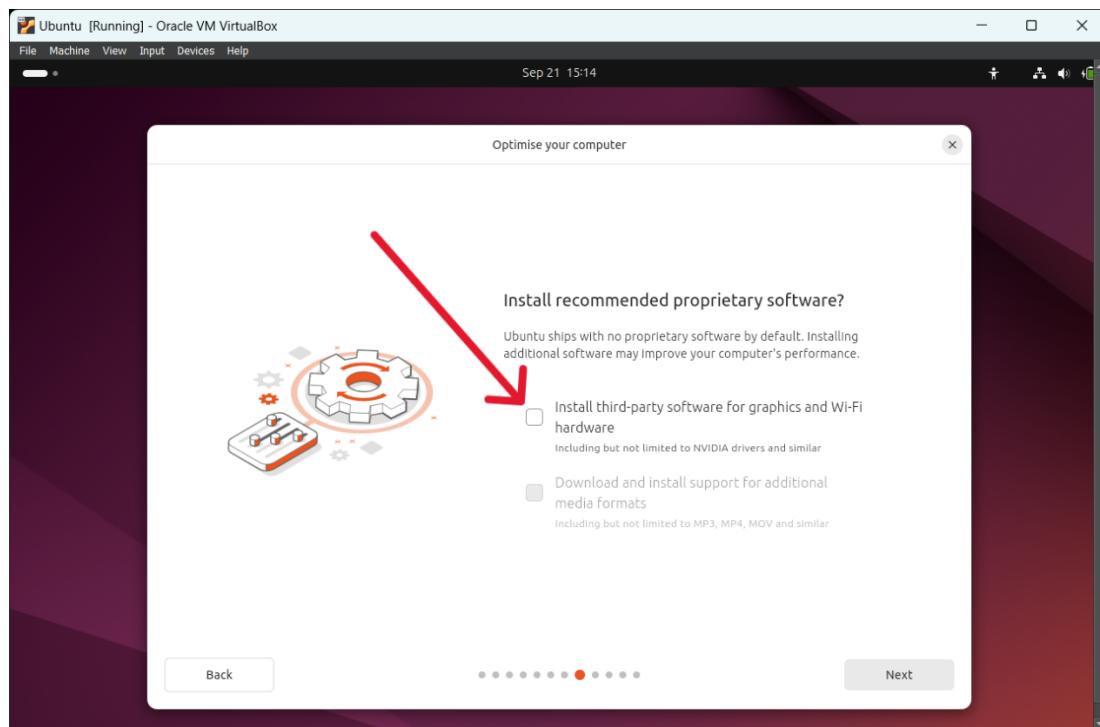


Figure 23

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.

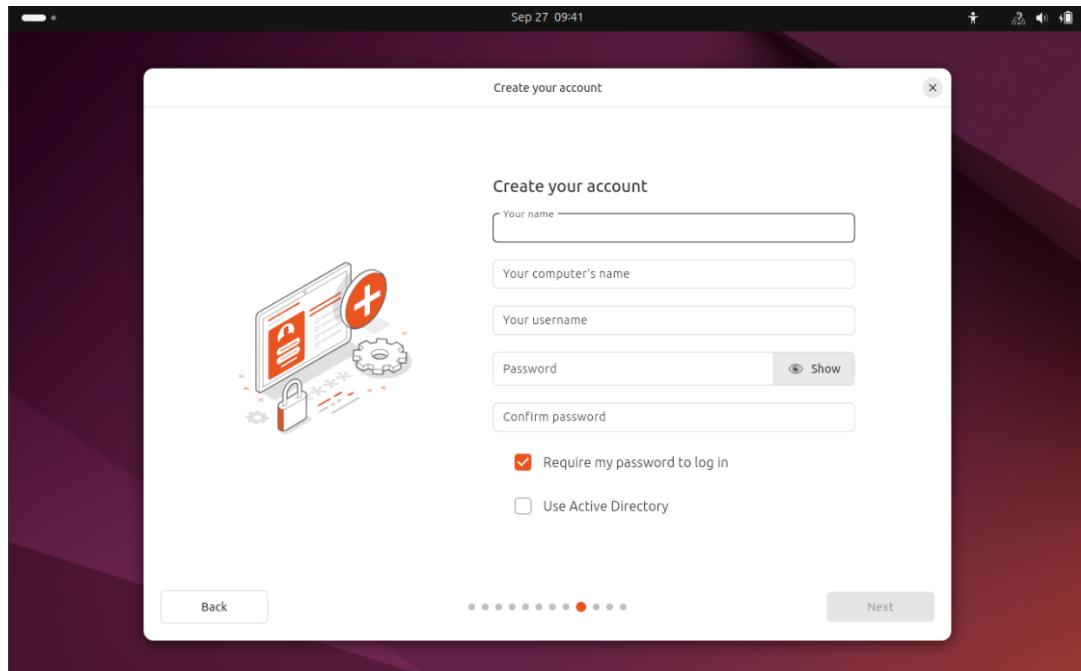


Figure 24

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

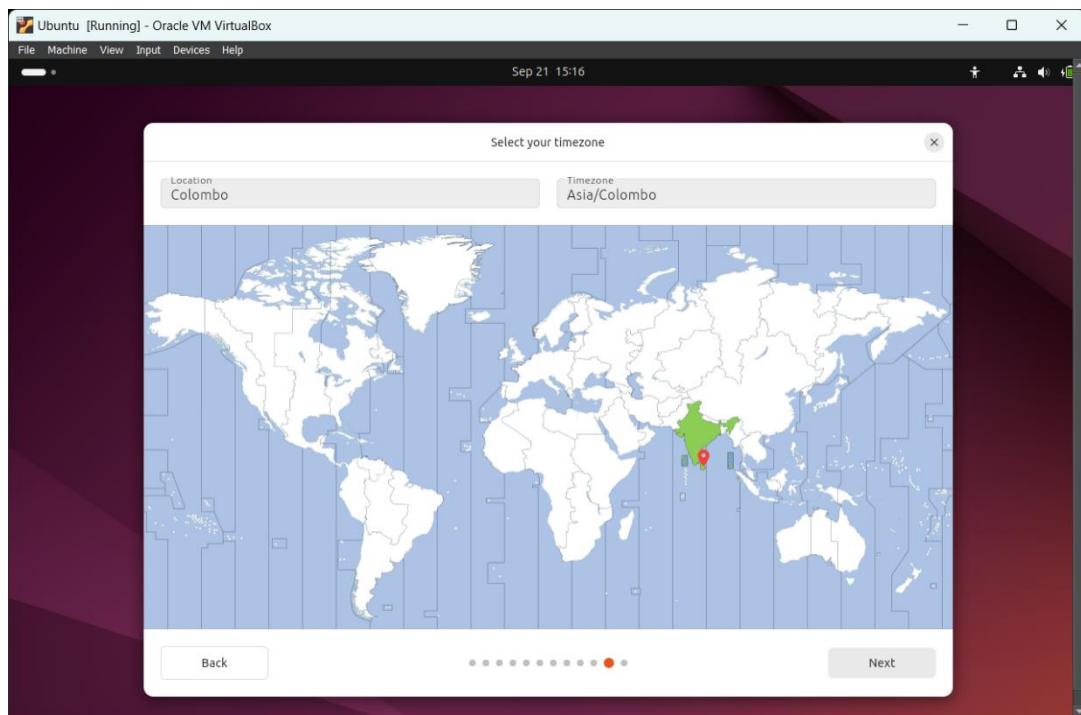


Figure 25

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.

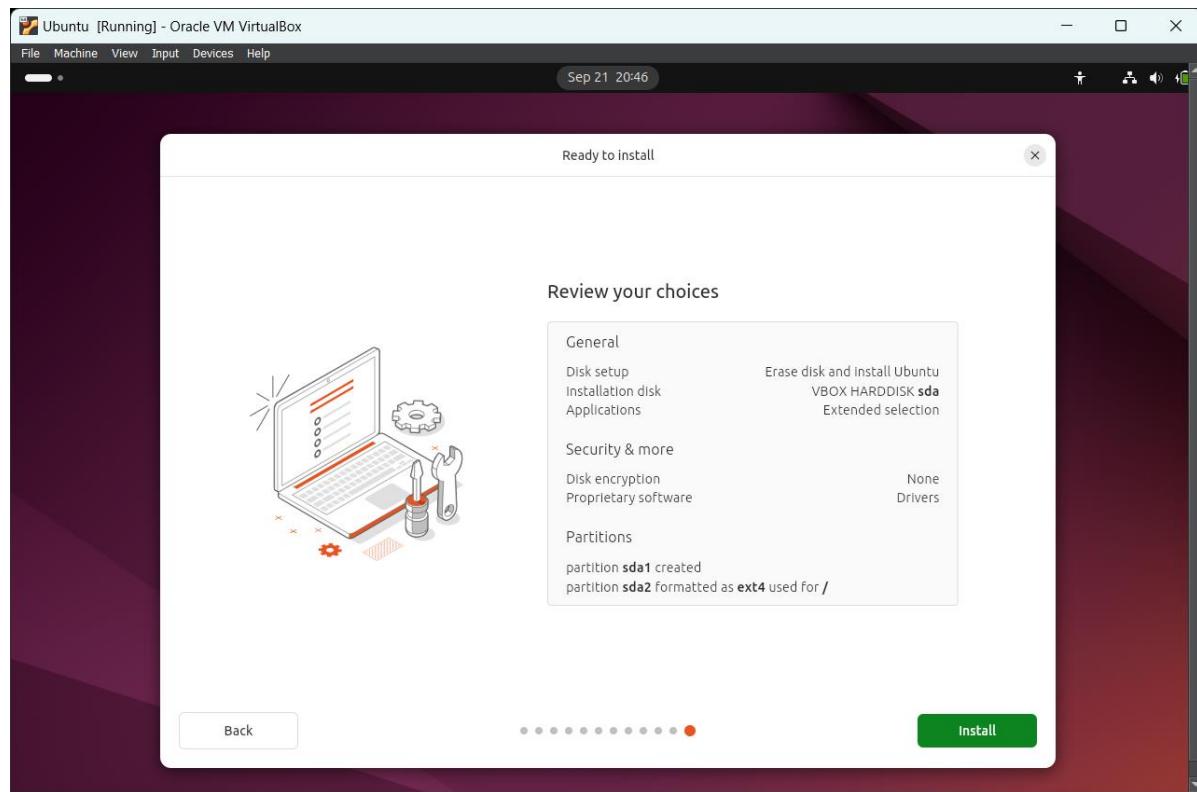


Figure 26

Basic Linux Commands

Open the Terminal

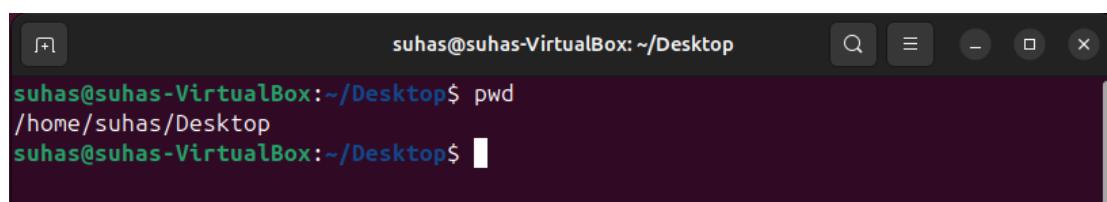
The terminal in Linux is a text-based interface that allows users to interact with the system through commands. It is used to perform tasks such as navigating directories, managing files, and executing programs, offering more control and efficiency compared to graphical interfaces.

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.

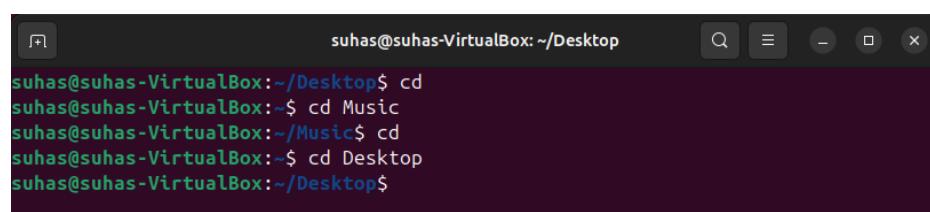
1. **pwd** – Print the current working directory.



```
suhas@suhas-VirtualBox:~/Desktop$ pwd
/home/suhas/Desktop
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 27

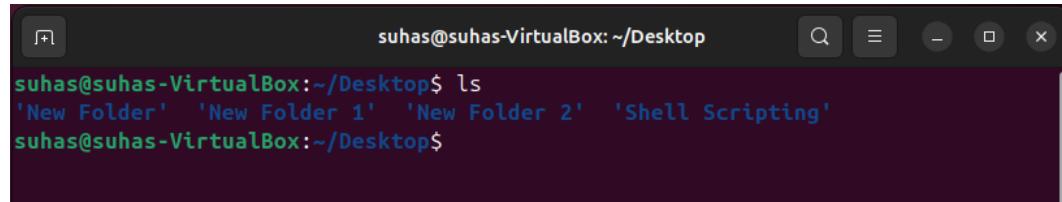
2. **cd**- Change the working directory.



```
suhas@suhas-VirtualBox:~/Desktop$ cd
suhas@suhas-VirtualBox:~$ cd Music
suhas@suhas-VirtualBox:~/Music$ cd
suhas@suhas-VirtualBox:~$ cd Desktop
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 28

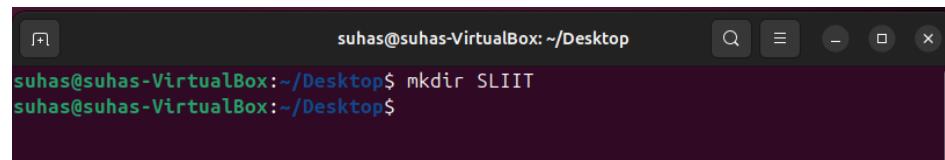
3. **ls** – List directory content.



```
suhas@suhas-VirtualBox:~/Desktop$ ls
'New Folder'  'New Folder 1'  'New Folder 2'  'Shell Scripting'
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 29

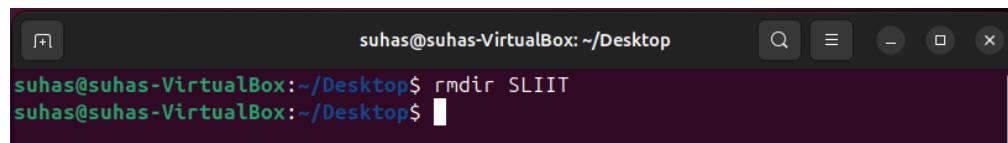
4. **mkdir** – Create a new directory (mkdir testfolder).



```
suhas@suhas-VirtualBox:~/Desktop$ mkdir SLIIT
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 30

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

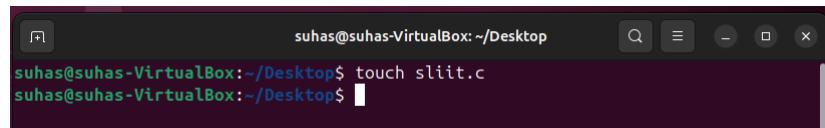


```
suhas@suhas-VirtualBox:~/Desktop$ rmdir SLIIT
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 31

File Manipulation Commands

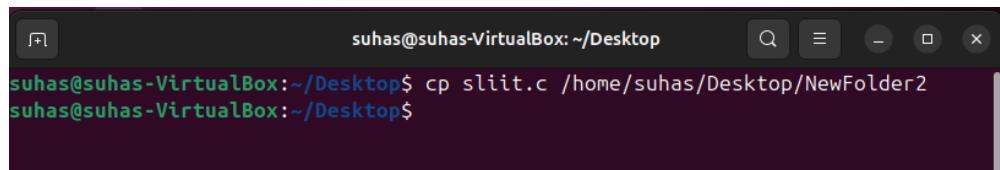
6. **touch** – Create an empty file.



```
suhas@suhas-VirtualBox:~/Desktop$ touch sliit.c
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 32

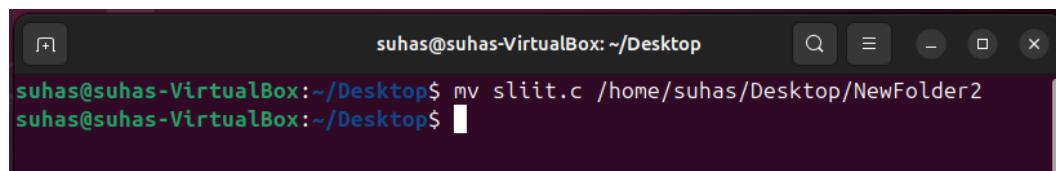
7. **cp** – Copy files or directories (cp [source] [destination]).



```
suhas@suhas-VirtualBox:~/Desktop$ cp sliit.c /home/suhas/Desktop/NewFolder2
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 33

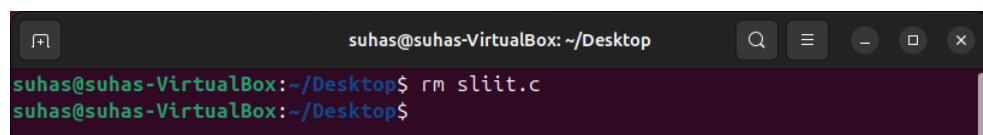
8. **mv** – Move or rename files or directories (mv [source] [destination]) .



```
suhas@suhas-VirtualBox:~/Desktop$ mv sliit.c /home/suhas/Desktop/NewFolder2
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 34

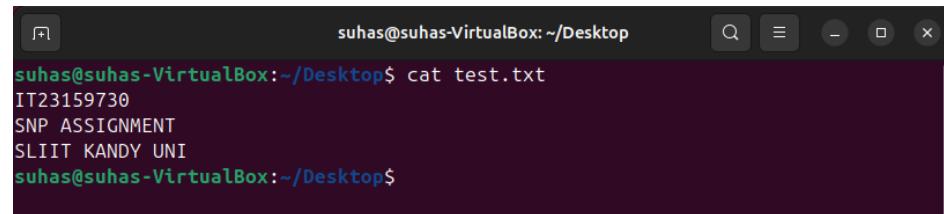
9. **rm** – Remove files or directories.



```
suhas@suhas-VirtualBox:~/Desktop$ rm sliit.c
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 35

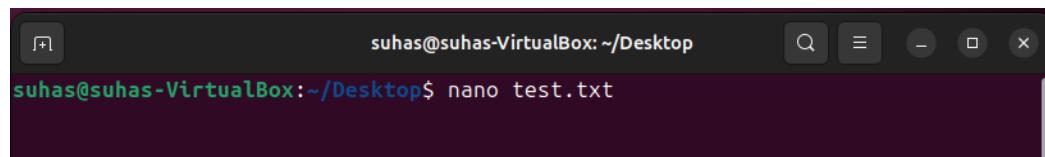
10.cat – Show contents of the file (cat testfile).



```
suhas@suhas-VirtualBox:~/Desktop$ cat test.txt
IT23159730
SNP ASSIGNMENT
SLIIT KANDY UNI
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 36

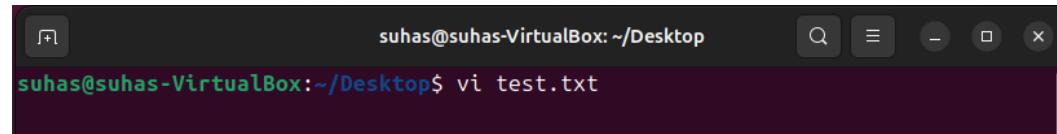
11.nano- Open nano text editor in terminal (nano testfile or nano testfile.txt).



```
suhas@suhas-VirtualBox:~/Desktop$ nano test.txt
```

Figure 37

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

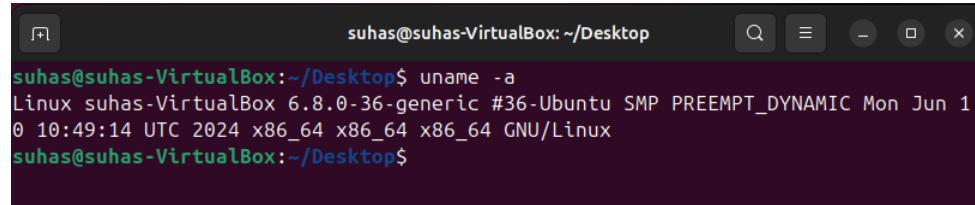


```
suhas@suhas-VirtualBox:~/Desktop$ vi test.txt
```

Figure 38

System Information and User Management Commands.

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

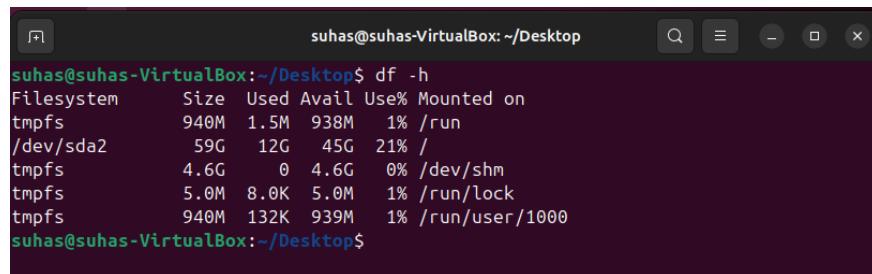


```
suhas@suhas-VirtualBox:~/Desktop$ uname -a
Linux suhas-VirtualBox 6.8.0-36-generic #36-Ubuntu SMP PREEMPT_DYNAMIC Mon Jun 1
0 10:49:14 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
suhas@suhas-VirtualBox:~/Desktop$
```

A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The window shows the command "uname -a" being run, which outputs the system's kernel version, architecture, and other details. The terminal has a dark background with light-colored text and standard window controls at the top.

Figure 39

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

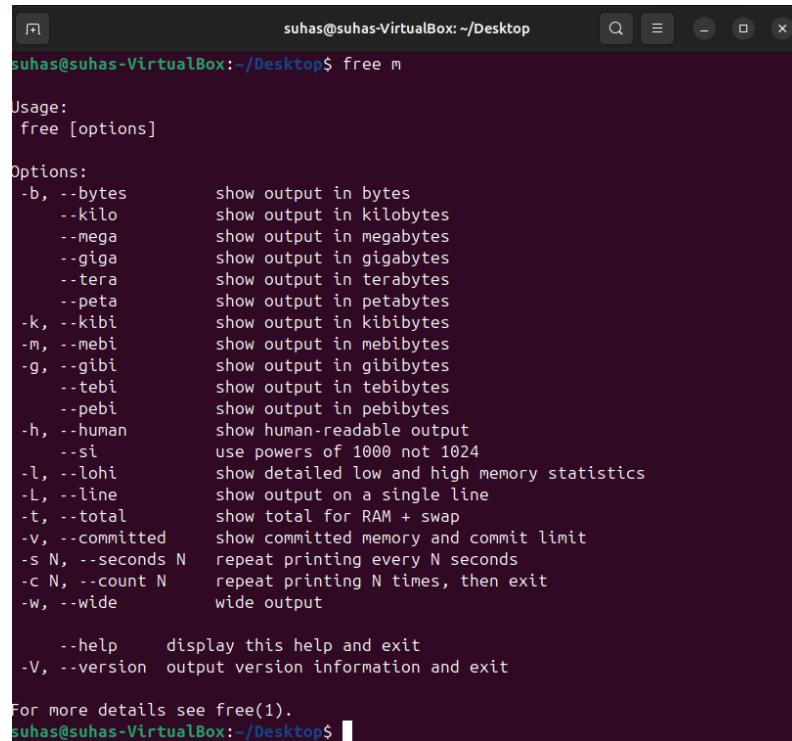


```
suhas@suhas-VirtualBox:~/Desktop$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs          940M   1.5M  938M   1% /run
/dev/sda2        59G   12G   45G  21% /
tmpfs          4.6G     0  4.6G   0% /dev/shm
tmpfs          5.0M  8.0K  5.0M   1% /run/lock
tmpfs          940M 132K  939M   1% /run/user/1000
suhas@suhas-VirtualBox:~/Desktop$
```

A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The window shows the command "df -h" being run, which displays disk usage across various file systems. The output includes the size, used space, available space, percentage usage, and mount point for each file system. The terminal has a dark background with light-colored text and standard window controls at the top.

Figure 40

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



```
suhas@suhas-VirtualBox:~/Desktop$ free -m
Usage:
  free [options]

Options:
  -b, --bytes      show output in bytes
  -kilo            show output in kilobytes
  --mega           show output in megabytes
  --giga           show output in gigabytes
  --tera           show output in terabytes
  --peta           show output in petabytes
  -k, --kibi       show output in kibibytes
  -m, --mebi       show output in mebibytes
  -g, --gibi       show output in gibibytes
  --tebi           show output in tebibytes
  --pebi           show output in pebibytes
  -h, --human      show human-readable output
  --si              use powers of 1000 not 1024
  -l, --lohi       show detailed low and high memory statistics
  -L, --line        show output on a single line
  -t, --total      show total for RAM + swap
  -v, --committed  show committed memory and commit limit
  -s N, --seconds N repeat printing every N seconds
  -c N, --count N  repeat printing N times, then exit
  -w, --wide        wide output

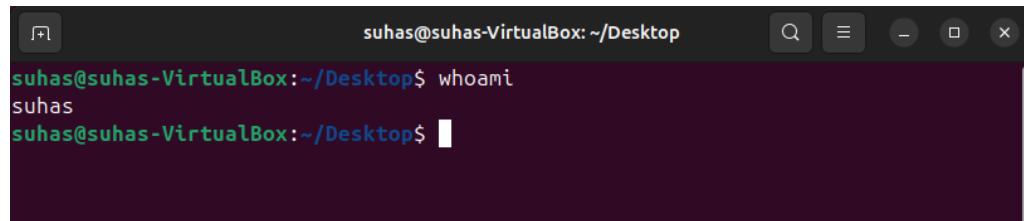
  --help      display this help and exit
  -V, --version  output version information and exit

For more details see free(1).
suhas@suhas-VirtualBox:~/Desktop$
```

A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The window shows the command "free -m" being run, which displays memory usage in megabytes. The output includes the total, used, and free memory for both RAM and swap space. The terminal has a dark background with light-colored text and standard window controls at the top.

Figure 41

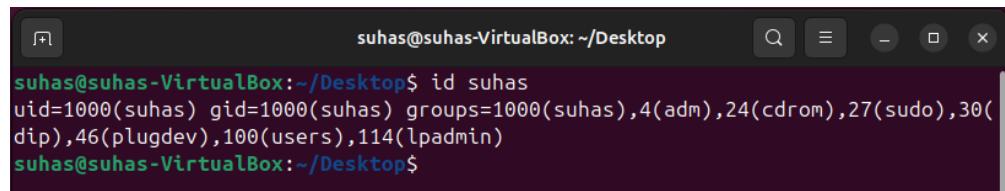
16.whoami – Shows the current logged-in user.



```
suhas@suhas-VirtualBox:~/Desktop$ whoami
suhas
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 42

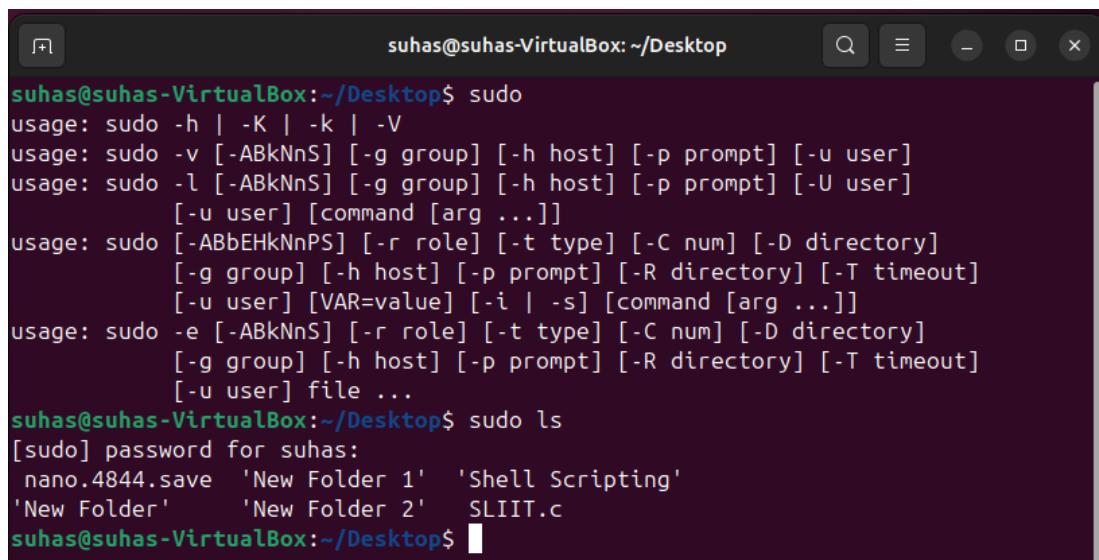
17.id [username]- Display user identity and group information.



```
suhas@suhas-VirtualBox:~/Desktop$ id suhas
uid=1000(suhas) gid=1000(suhas) groups=1000(suhas),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114(lpadmin)
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 43

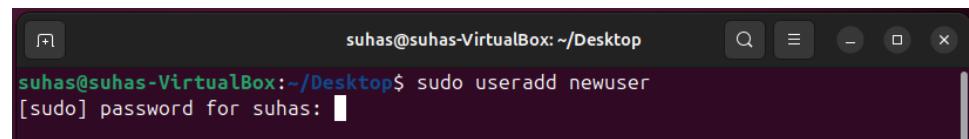
18.sudo [command] - Run a command with superuser privileges.



```
suhas@suhas-VirtualBox:~/Desktop$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user]
      [-u user] [command [arg ...]]
usage: sudo [-ABbEHkNnPS] [-r role] [-t type] [-C num] [-D directory]
          [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
          [-u user] [VAR=value] [-i | -s] [command [arg ...]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory]
          [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
          [-u user] file ...
suhas@suhas-VirtualBox:~/Desktop$ sudo ls
[sudo] password for suhas:
nano.4844.save  'New Folder 1'  'Shell Scripting'
'New Folder'     'New Folder 2'   SLIIT.c
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 44

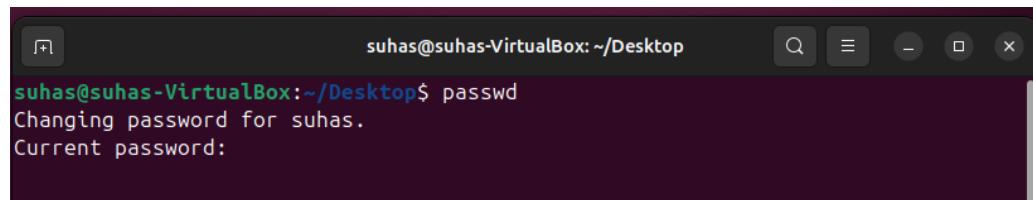
19.useradd – Create a new user (sudo useradd [username]).



```
suhas@suhas-VirtualBox: ~/Desktop$ sudo useradd newuser
[sudo] password for suhas:
```

Figure 45

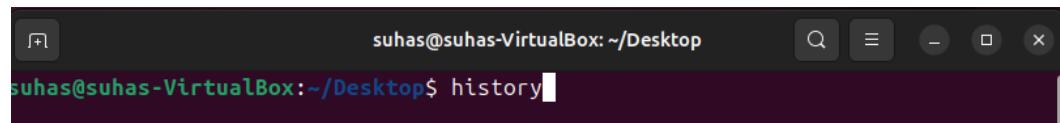
20.passwd – Change user password.



```
suhas@suhas-VirtualBox: ~/Desktop$ passwd
Changing password for suhas.
Current password:
```

Figure 46

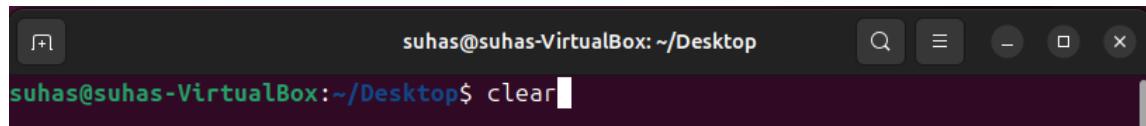
21.history – Display the history of commands.



```
suhas@suhas-VirtualBox: ~/Desktop$ history
```

Figure 47

22.clear - Clear the terminal window.



```
suhas@suhas-VirtualBox: ~/Desktop$ clear
```

Figure 48

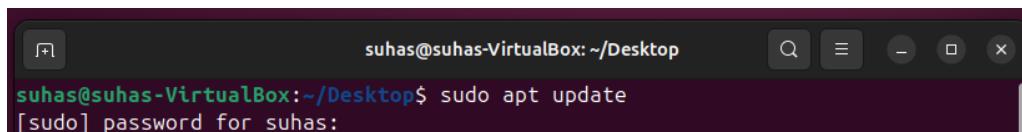
DHCP, DNS, and NTP Services Configuration.

DHCP Service Configuration.

1. First, Open the terminal and install the DHCP server package.

```
sudo apt update
```

```
sudo apt install isc-dhcp-server
```



```
suhas@suhas-VirtualBox:~/Desktop$ sudo apt update  
[sudo] password for suhas:
```

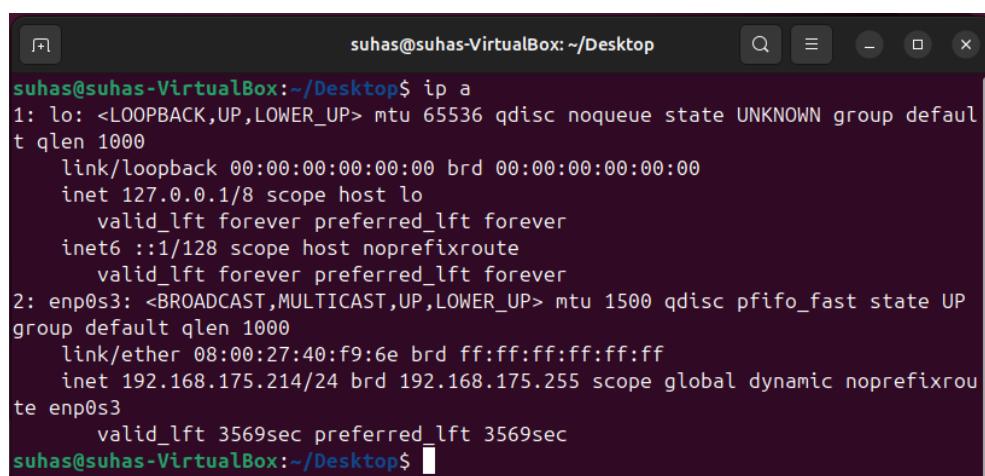
Figure 49

```
suhas@suhas-VirtualBox:~/Desktop$ sudo apt install isc-dhcp-server
```

Figure 50

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

```
ip a
```



```
suhas@suhas-VirtualBox:~/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 08:00:27:40:f9:6e brd ff:ff:ff:ff:ff:ff  
    inet 192.168.175.214/24 brd 192.168.175.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 3569sec preferred_lft 3569sec  
suhas@suhas-VirtualBox:~/Desktop$
```

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.

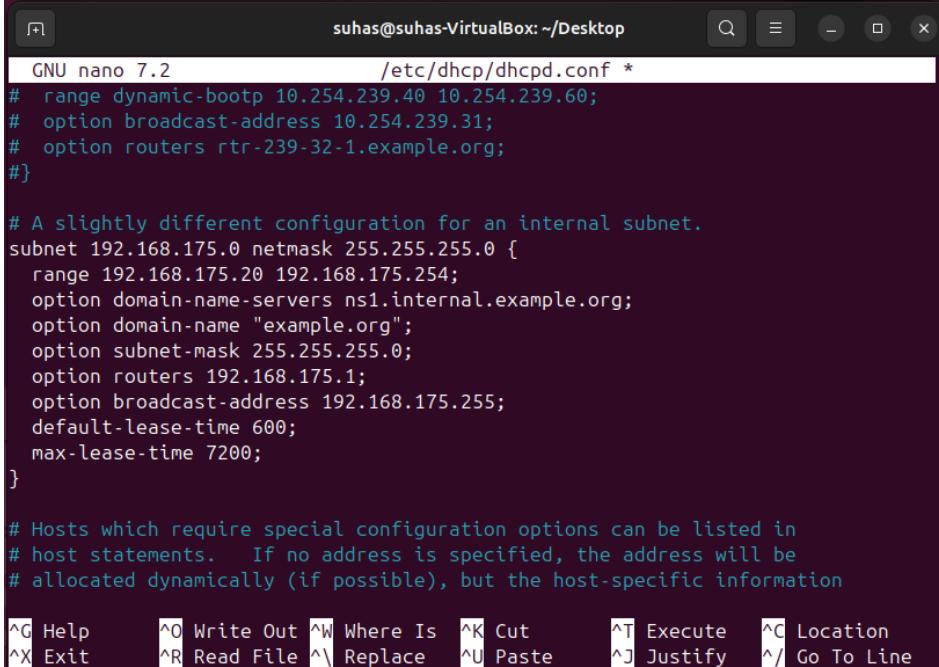
```
suhas@suhas-VirtualBox:~/Desktop$ sudo nano /etc/dhcp/dhcpd.conf  
[sudo] password for suhas:  
suhas@suhas-VirtualBox:~/Desktop$
```

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;  
}
```



```
GNU nano 7.2          /etc/dhcp/dhcpd.conf *  
# range dynamic-bootp 10.254.239.40 10.254.239.60;  
# option broadcast-address 10.254.239.31;  
# option routers rtr-239-32-1.example.org;  
#}  
  
# A slightly different configuration for an internal subnet.  
subnet 192.168.175.0 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;  
}  
  
# Hosts which require special configuration options can be listed in  
# host statements. If no address is specified, the address will be  
# allocated dynamically (if possible), but the host-specific information  
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File  ^L Replace    ^U Paste     ^J Justify   ^/ Go To Line
```

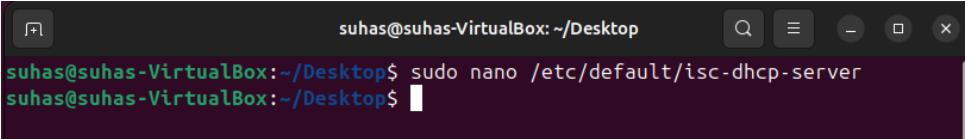
Figure 53

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

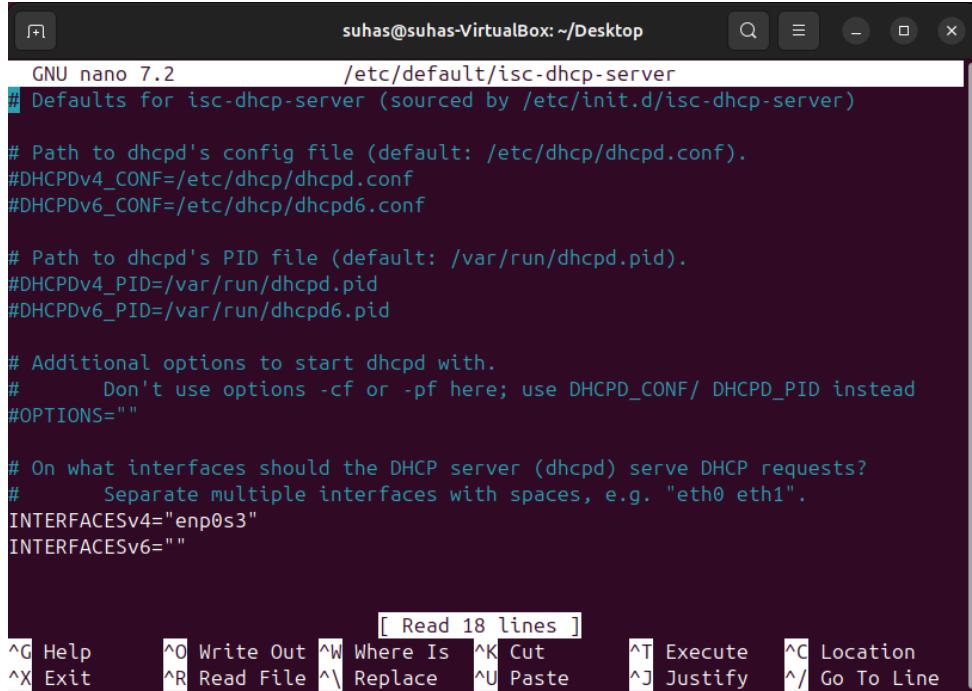


```
suhas@suhas-VirtualBox:~/Desktop$ sudo nano /etc/default/isc-dhcp-server  
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 54

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

INTERFACESv4="enp0s3"



```
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/dhcpcd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpcd6.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=""

[ Read 18 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
```

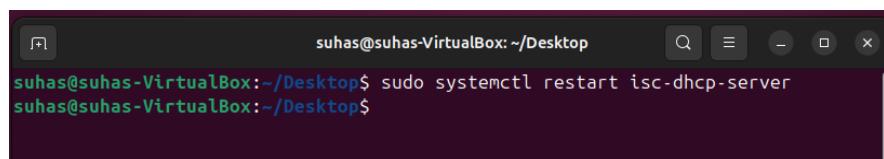
Figure 55

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

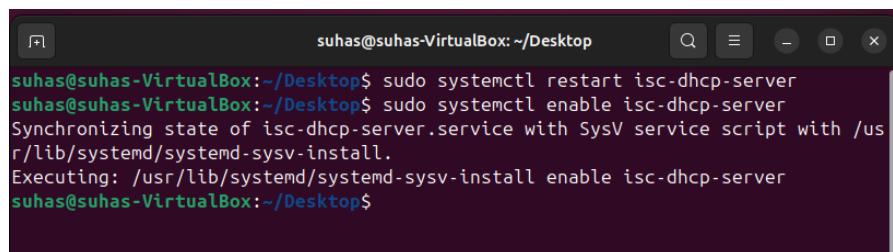


```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl restart isc-dhcp-server
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 56

6. Enable the Service on Boot.

sudo systemctl enable isc-dhcp-server



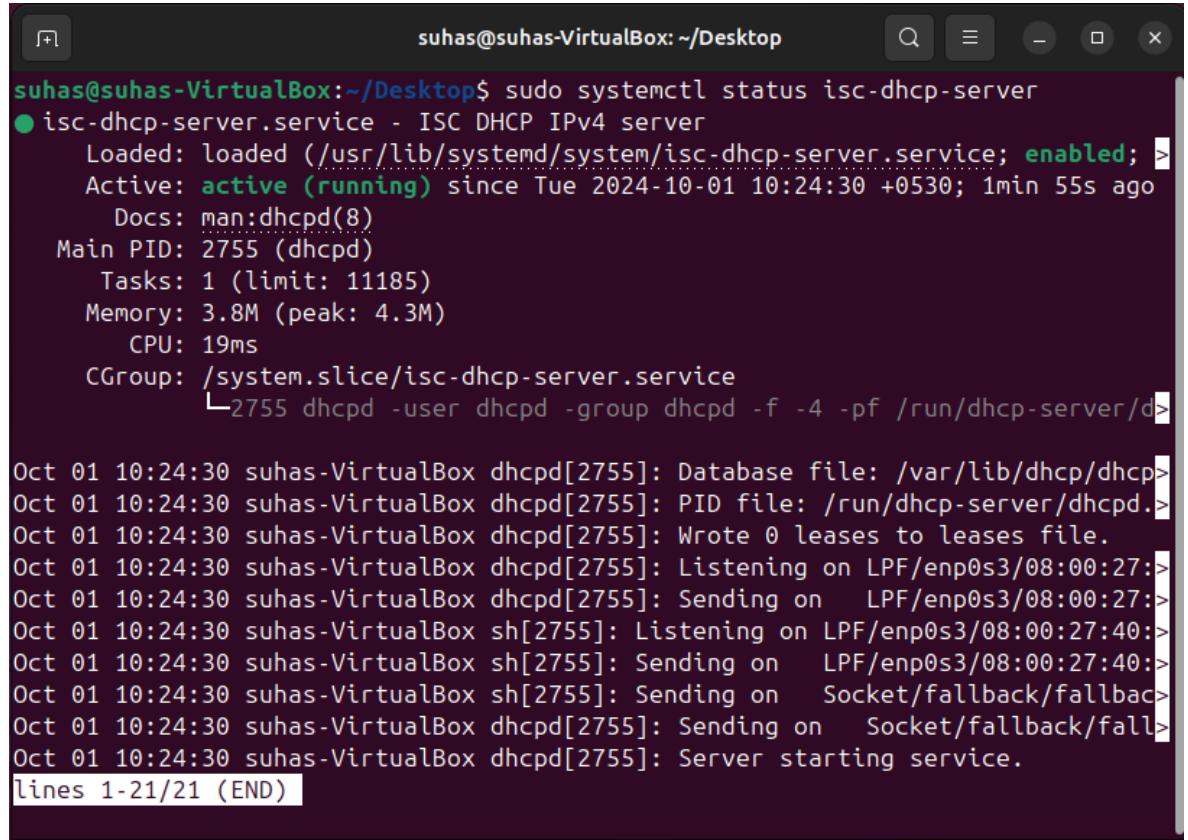
```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl restart isc-dhcp-server
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable isc-dhcp-server
Synchronizing state of isc-dhcp-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable isc-dhcp-server
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 57

7. Verify the Status

You can check if the DHCP server is running properly.

sudo systemctl status isc-dhcp-server



```
suhas@suhas-VirtualBox:~/Desktop$ 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; ➤
      Active: active (running) since Tue 2024-10-01 10:24:30 +0530; 1min 55s ago
        Docs: man:dhcpd(8)
       Main PID: 2755 (dhcpd)
          Tasks: 1 (limit: 11185)
         Memory: 3.8M (peak: 4.3M)
            CPU: 19ms
           CGroup: /system.slice/isc-dhcp-server.service
                   └─2755 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhc>

Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Database file: /var/lib/dhcp/dhc>
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: PID file: /run/dhcp-server/dhcpcd.>
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Wrote 0 leases to leases file.
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Listening on LPF/enp0s3/08:00:27:>
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Sending on   LPF/enp0s3/08:00:27:>
Oct 01 10:24:30 suhas-VirtualBox sh[2755]: Listening on LPF/enp0s3/08:00:27:40:>
Oct 01 10:24:30 suhas-VirtualBox sh[2755]: Sending on   LPF/enp0s3/08:00:27:40:>
Oct 01 10:24:30 suhas-VirtualBox sh[2755]: Sending on   Socket/fallback/fallbac>
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Sending on   Socket/fallback/fall>
Oct 01 10:24:30 suhas-VirtualBox dhcpcd[2755]: Server starting service.
lines 1-21/21 (END)
```

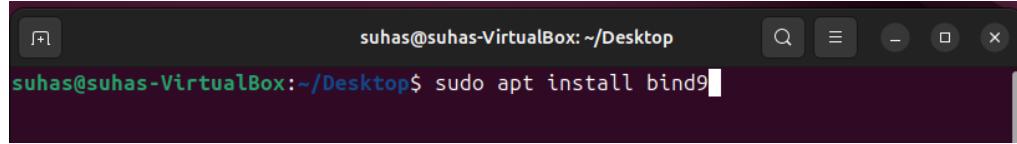
Figure 58

DNS Services Configuration.

1. First, Open the terminal and install bind9

```
sudo apt update
```

```
sudo apt install bind9
```

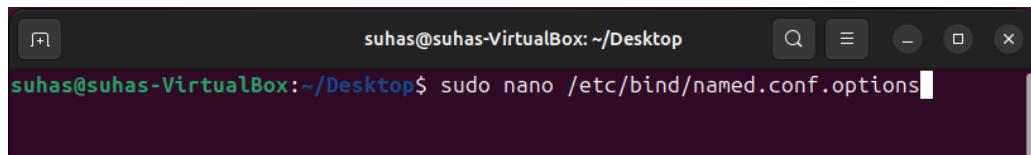


```
suhas@suhas-VirtualBox:~/Desktop$ sudo apt install bind9
```

Figure 59

2. Edit the main configuration file.

```
sudo nano /etc/bind/named.conf.options
```



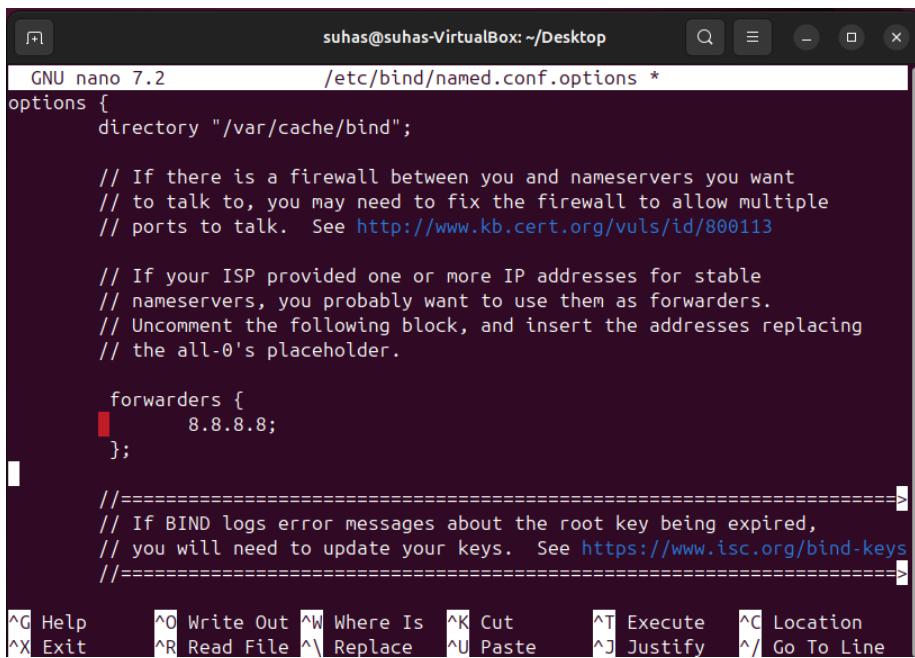
```
suhas@suhas-VirtualBox:~/Desktop$ sudo nano /etc/bind/named.conf.options
```

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



```
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

    // 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
    //=====

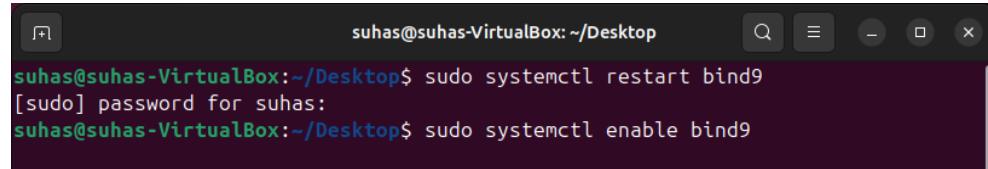
^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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
```



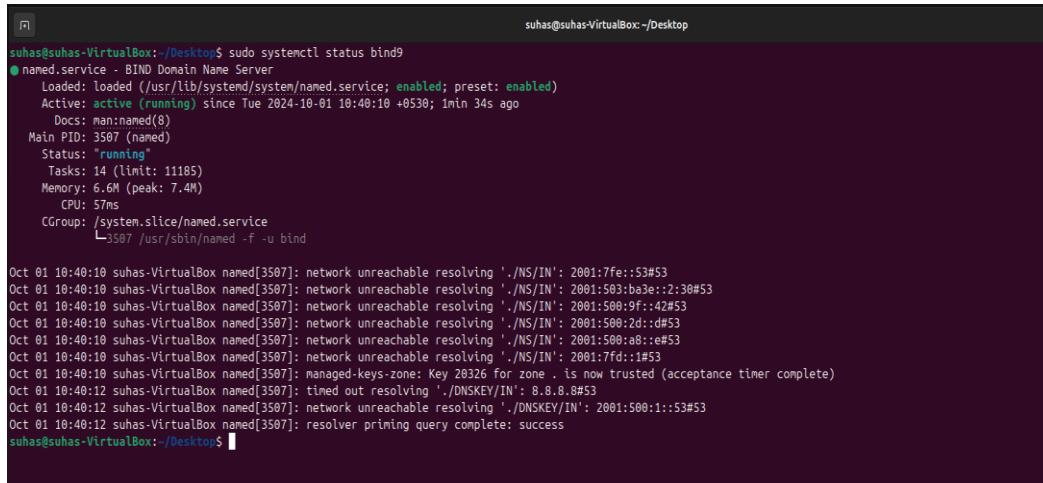
```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl restart bind9  
[sudo] password for suhas:  
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable bind9
```

Figure 62

4. Verify the Status.

You can check if the DNS server is running properly.

```
sudo systemctl status bind9.
```



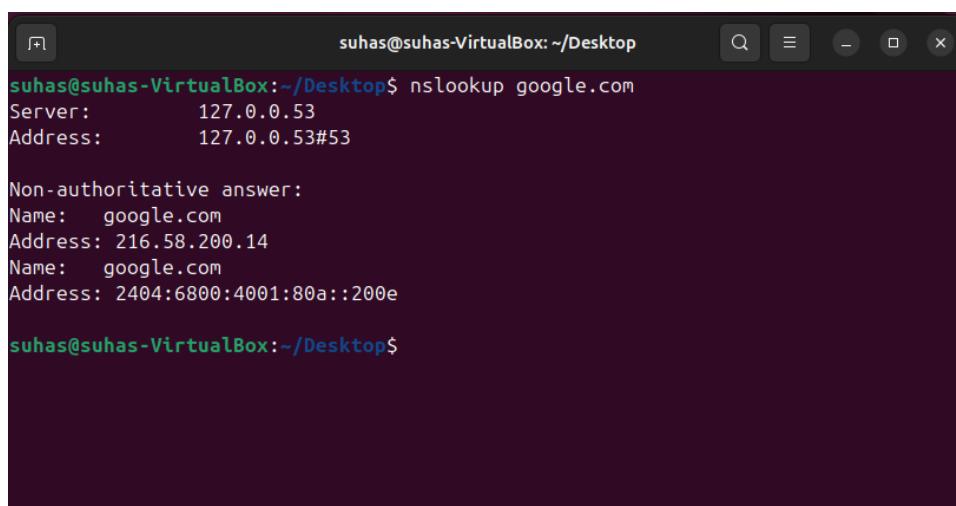
```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl status bind9  
● named.service - BIND Domain Name Server  
  Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)  
  Active: active (running) since Tue 2024-10-01 10:40:10 +0530; 1min 34s ago  
    Docs: man:named(8)  
    Main PID: 3507 (named)  
   Status: "running"  
      Tasks: 14 (limit: 11185)  
     Memory: 6.6M (peak: 7.4M)  
       CPU: 57ms  
      CGroup: /system.slice/named.service  
           └─3507 /usr/sbin/named -f -u bind  
  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:7fe::53#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:500:9f::42#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:500:2d::#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:500:a8::e#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: network unreachable resolving './NS/IN': 2001:7fd::1#53  
Oct 01 10:40:10 suhas-VirtualBox named[3507]: managed-keys-zone: Key 29326 for zone . is now trusted (acceptance timer complete)  
Oct 01 10:40:12 suhas-VirtualBox named[3507]: timed out resolving './DNSKEY/IN': 8.8.8.#53  
Oct 01 10:40:12 suhas-VirtualBox named[3507]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53  
Oct 01 10:40:12 suhas-VirtualBox named[3507]: resolver priming query complete: success  
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 63

5. Test the DNS server.

For this step we need **nslookup** command.

```
nslookup [example.com].
```

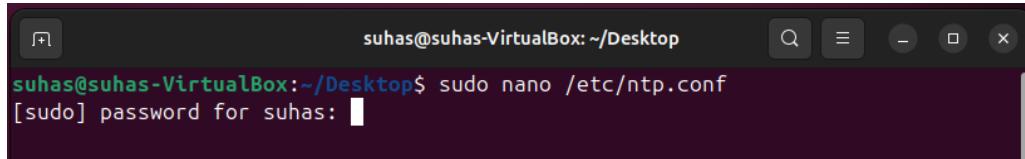


```
suhas@suhas-VirtualBox:~/Desktop$ nslookup google.com  
Server: 127.0.0.53  
Address: 127.0.0.53#53  
  
Non-authoritative answer:  
Name: google.com  
Address: 216.58.200.14  
Name: google.com  
Address: 2404:6800:4001:80a::200e  
  
suhas@suhas-VirtualBox:~/Desktop$
```

NTP Services Configuration.

1. First, Open the terminal and install ntp

```
sudo apt update  
sudo apt install ntp
```

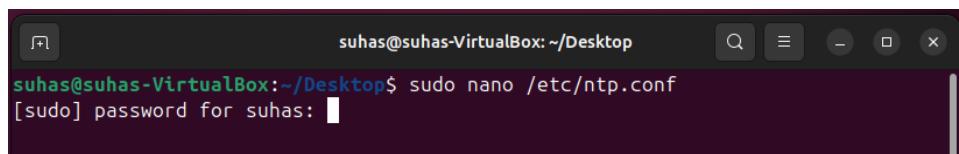


A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The command "sudo nano /etc/ntp.conf" is being typed in. A password prompt "[sudo] password for suhas:" is visible below the command line.

Figure 64

2. Edit the ntp configuring file.

```
sudo nano /etc/ntp.conf
```



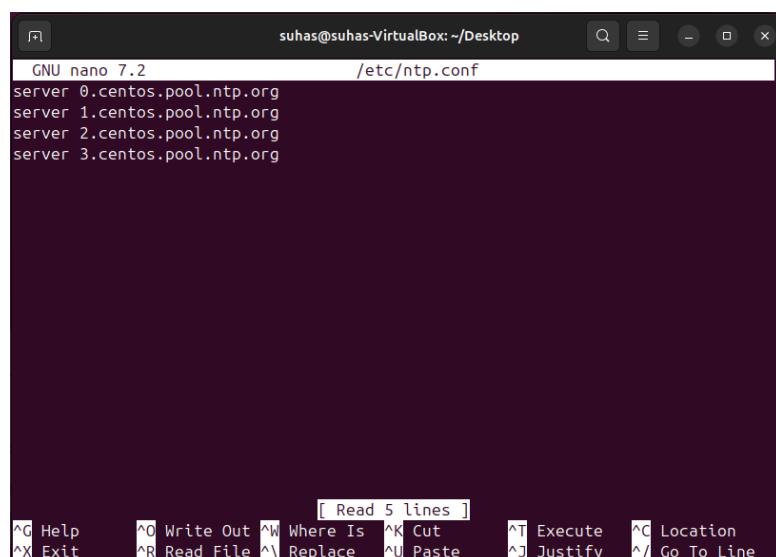
A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The command "sudo nano /etc/ntp.conf" is being typed in. A password prompt "[sudo] password for suhas:" is visible below the command line.

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
```



A screenshot of the nano text editor showing the file "/etc/ntp.conf". The content of the file is:

```
GNU nano 7.2          /etc/ntp.conf  
server 0.centos.pool.ntp.org  
server 1.centos.pool.ntp.org  
server 2.centos.pool.ntp.org  
server 3.centos.pool.ntp.org
```

The bottom of the screen shows the nano command bar with various keyboard shortcuts.

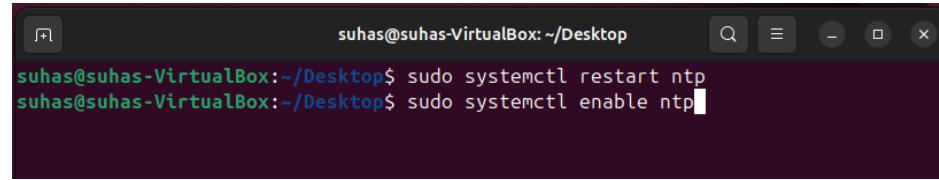
Figure 66

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

3. Restart and enable ntp.

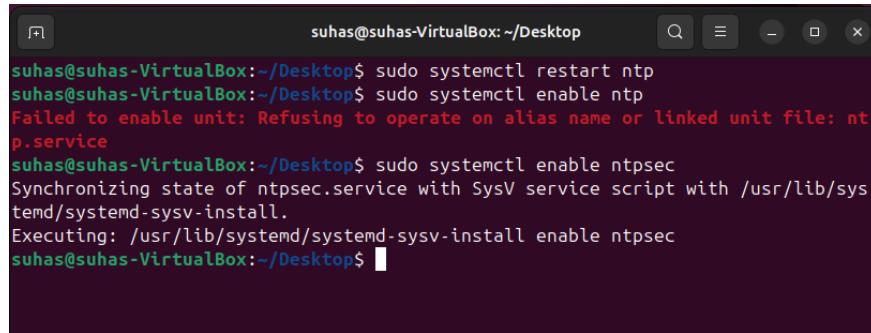
sudo systemctl restart ntp.

sudo systemctl restart ntp.



```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl restart ntp
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable ntp
```

Figure 67



```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl restart ntp
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable ntp
Failed to enable unit: Refusing to operate on alias name or linked unit file: ntp.service
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable ntpsec
Synchronizing state of ntpsec.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ntpsec
suhas@suhas-VirtualBox:~/Desktop$
```

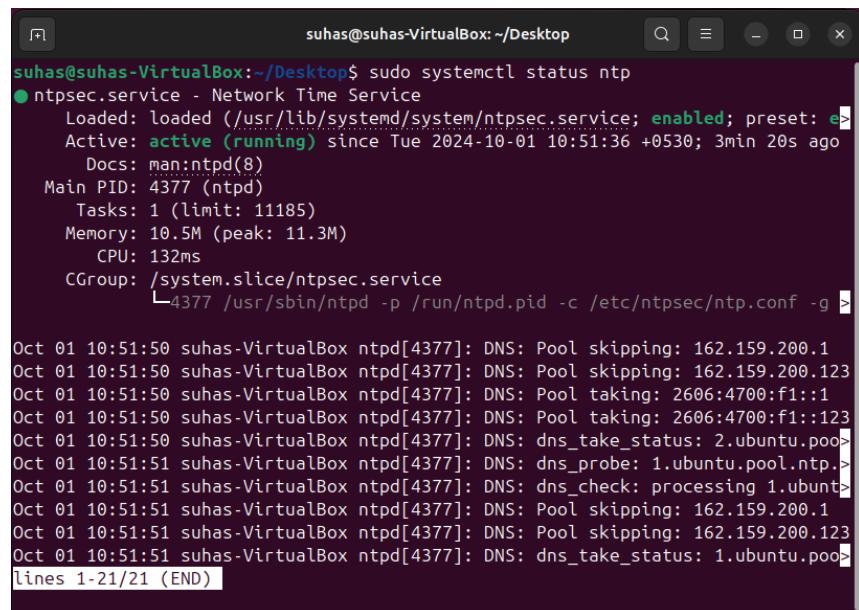
Figure 68

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.



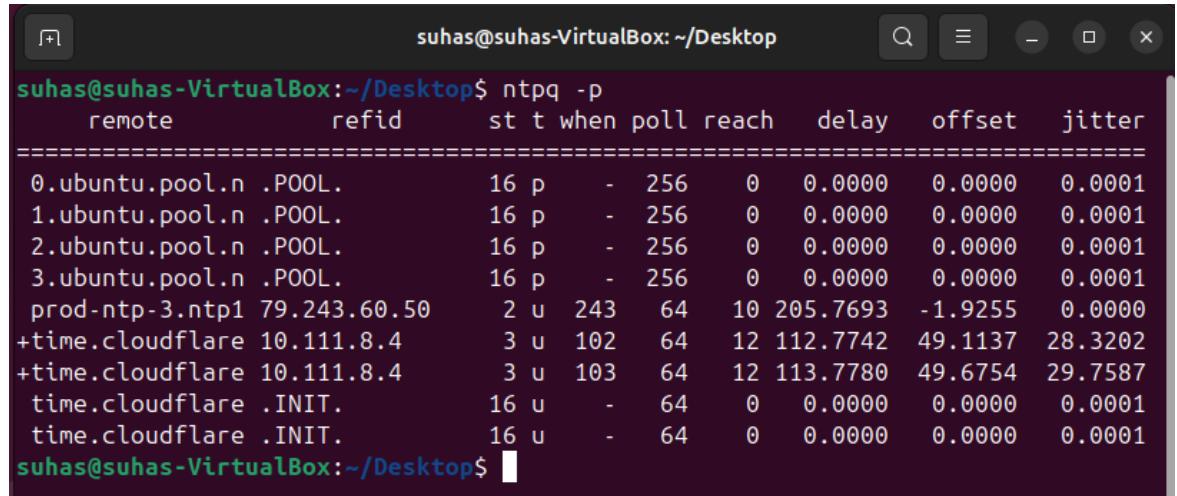
```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl status ntp
● ntpsec.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpsec.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-10-01 10:51:36 +0530; 3min 20s ago
     Docs: man:ntpd(8)
     Main PID: 4377 (ntpd)
        Tasks: 1 (limit: 11185)
       Memory: 10.5M (peak: 11.3M)
          CPU: 132ms
        CGroup: /system.slice/ntpsec.service
                  └─4377 /usr/sbin/ntpd -p /run/ntpd.pid -c /etc/ntpsec/ntp.conf -g

Oct 01 10:51:50 suhas-VirtualBox ntpd[4377]: DNS: Pool skipping: 162.159.200.1
Oct 01 10:51:50 suhas-VirtualBox ntpd[4377]: DNS: Pool skipping: 162.159.200.123
Oct 01 10:51:50 suhas-VirtualBox ntpd[4377]: DNS: Pool taking: 2606:4700:f1::1
Oct 01 10:51:50 suhas-VirtualBox ntpd[4377]: DNS: Pool taking: 2606:4700:f1::123
Oct 01 10:51:50 suhas-VirtualBox ntpd[4377]: DNS: dns_take_status: 2.ubuntu.pool
Oct 01 10:51:51 suhas-VirtualBox ntpd[4377]: DNS: dns_probe: 1.ubuntu.pool.ntp->
Oct 01 10:51:51 suhas-VirtualBox ntpd[4377]: DNS: dns_check: processing 1.ubuntu
Oct 01 10:51:51 suhas-VirtualBox ntpd[4377]: DNS: Pool skipping: 162.159.200.1
Oct 01 10:51:51 suhas-VirtualBox ntpd[4377]: DNS: Pool skipping: 162.159.200.123
Oct 01 10:51:51 suhas-VirtualBox ntpd[4377]: DNS: dns_take_status: 1.ubuntu.pool->
lines 1-21/21 (END)
```

Figure 69

5. Verify that ntp working properly.

```
ntpq -p
```



The screenshot shows a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The command "ntpq -p" is run, displaying the following output:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
0.ubuntu.pool.n	.POOL.	16	p	-	256	0	0.0000	0.0000	0.0001
1.ubuntu.pool.n	.POOL.	16	p	-	256	0	0.0000	0.0000	0.0001
2.ubuntu.pool.n	.POOL.	16	p	-	256	0	0.0000	0.0000	0.0001
3.ubuntu.pool.n	.POOL.	16	p	-	256	0	0.0000	0.0000	0.0001
prod-ntp-3.ntp1	79.243.60.50	2	u	243	64	10	205.7693	-1.9255	0.0000
+time.cloudflare	10.111.8.4	3	u	102	64	12	112.7742	49.1137	28.3202
+time.cloudflare	10.111.8.4	3	u	103	64	12	113.7780	49.6754	29.7587
time.cloudflare	.INIT.	16	u	-	64	0	0.0000	0.0000	0.0001
time.cloudflare	.INIT.	16	u	-	64	0	0.0000	0.0000	0.0001

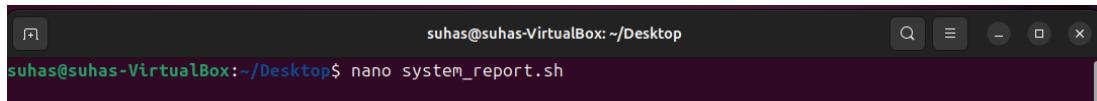
Figure 70

Shell Scripting and Security.

System Details Report Script

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

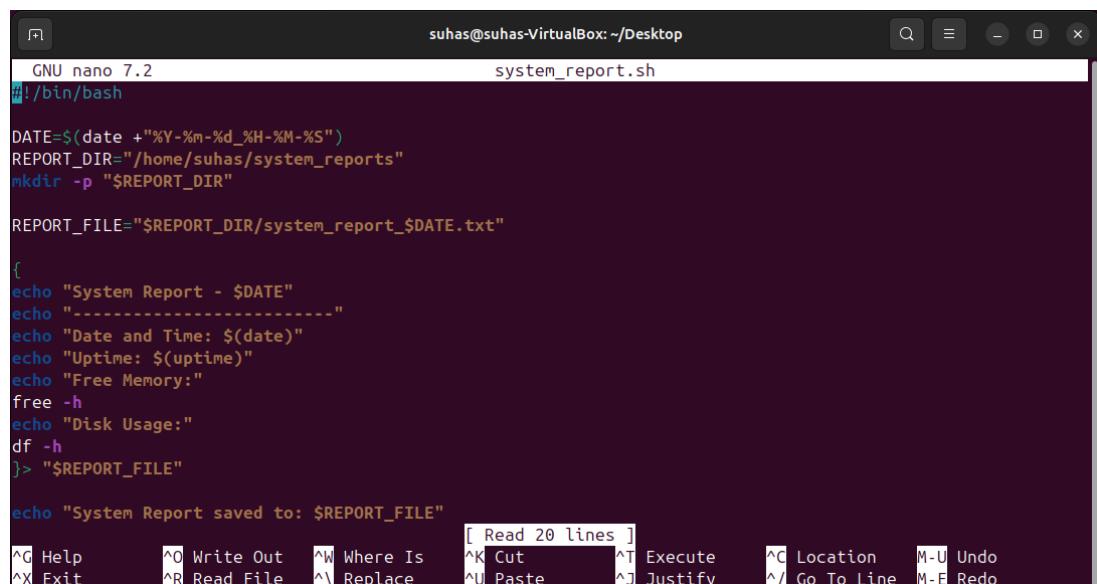
```
nano system_report.sh
```



```
suhas@suhas-VirtualBox:~/Desktop$ nano system_report.sh
```

Figure 71

2. Then type in the file like below mentioned.



```
GNU nano 7.2                                         system_report.sh
#!/bin/bash

DATE=$(date +"%Y-%m-%d_%H-%M-%S")
REPORT_DIR="/home/suhas/system_reports"
mkdir -p "$REPORT_DIR"

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

{
echo "System Report - $DATE"
echo "-----"
echo "Date and Time: $(date)"
echo "Uptime: $(uptime)"
echo "Free Memory:"
free -h
echo "Disk Usage:"
df -h
}> "$REPORT_FILE"

echo "System Report saved to: $REPORT_FILE"
```

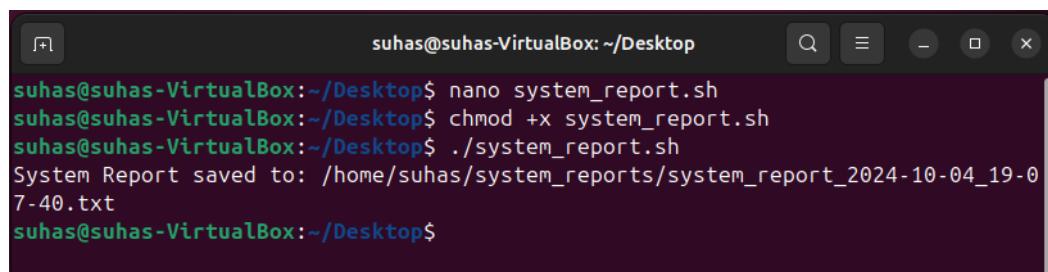
Figure 72

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
```

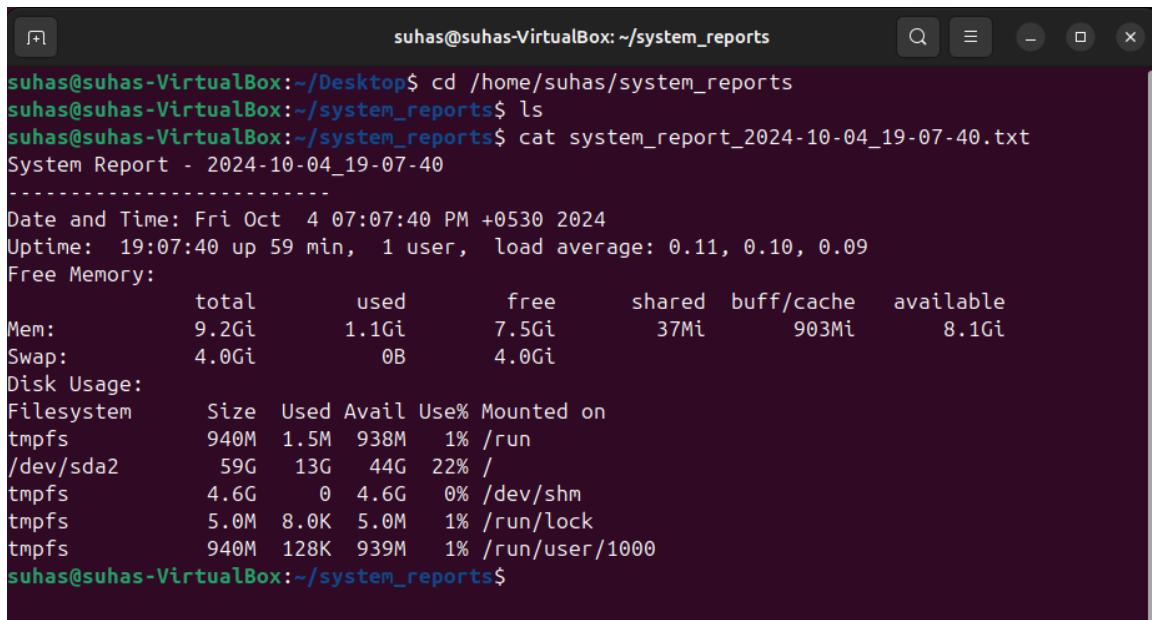


```
suhas@suhas-VirtualBox:~/Desktop$ nano system_report.sh
suhas@suhas-VirtualBox:~/Desktop$ chmod +x system_report.sh
suhas@suhas-VirtualBox:~/Desktop$ ./system_report.sh
System Report saved to: /home/suhas/system_reports/system_report_2024-10-04_19-07-40.txt
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 73

4. View the output file

```
cd /home/suhas/system_reports  
cat system_report_[report file name after created]
```



The screenshot shows a terminal window titled "suhas@suhas-VirtualBox: ~/system_reports". The terminal displays a system report generated by the command "cat system_report_2024-10-04_19-07-40.txt". The report includes the following sections:

- System Report - 2024-10-04_19-07-40**
- Date and Time:** Fri Oct 4 07:07:40 PM +0530 2024
- Uptime:** 19:07:40 up 59 min, 1 user, load average: 0.11, 0.10, 0.09
- Free Memory:**

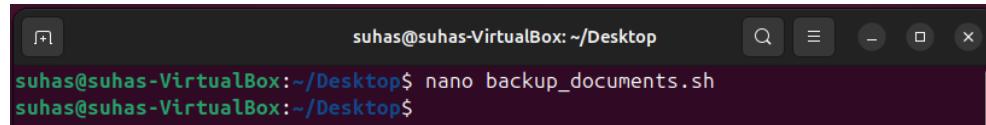
	total	used	free	shared	buff/cache	available
Mem:	9.2Gi	1.1Gi	7.5Gi	37Mi	903Mi	8.1Gi
Swap:	4.0Gi	0B	4.0Gi			
- Disk Usage:**

Filesystem	Size	Used	Avail	Use%	Mounted on
tmpfs	940M	1.5M	938M	1%	/run
/dev/sda2	59G	13G	44G	22%	/
tmpfs	4.6G	0	4.6G	0%	/dev/shm
tmpfs	5.0M	8.0K	5.0M	1%	/run/lock
tmpfs	940M	128K	939M	1%	/run/user/1000

Figure 74

Backup Script

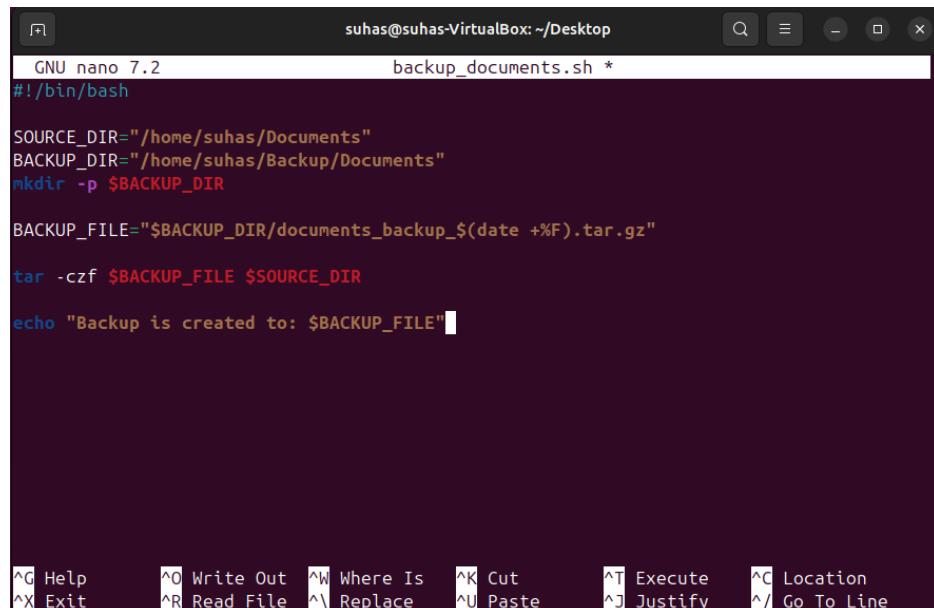
1. Open the terminal and create a new script file using any text editor.
nano backup_documents.sh



```
suhas@suhas-VirtualBox:~/Desktop$ nano backup_documents.sh
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 75

2. Then type in the file like below mentioned.



```
GNU nano 7.2                                backup_documents.sh *
#!/bin/bash

SOURCE_DIR="/home/suhas/Documents"
BACKUP_DIR="/home/suhas/Backup/Documents"
mkdir -p $BACKUP_DIR

BACKUP_FILE="$BACKUP_DIR/documents_backup_$(date +%F).tar.gz"

tar -czf $BACKUP_FILE $SOURCE_DIR

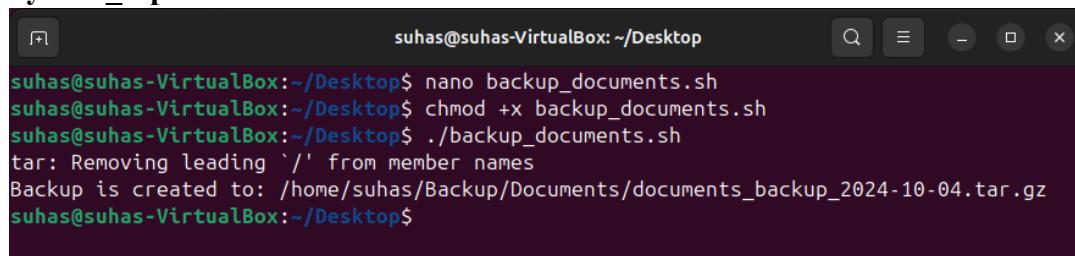
echo "Backup is created to: $BACKUP_FILE"
```

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

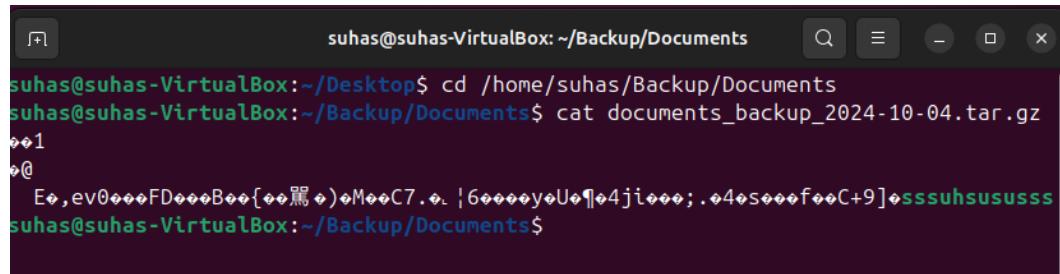


```
suhas@suhas-VirtualBox:~/Desktop$ nano backup_documents.sh
suhas@suhas-VirtualBox:~/Desktop$ chmod +x backup_documents.sh
suhas@suhas-VirtualBox:~/Desktop$ ./backup_documents.sh
tar: Removing leading '//' from member names
Backup is created to: /home/suhas/Backup/Documents/documents_backup_2024-10-04.tar.gz
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 77

4. View the output file.

```
cd /home/suhas/Backup/Documents  
cat documents_backup_[backup file name after created]
```



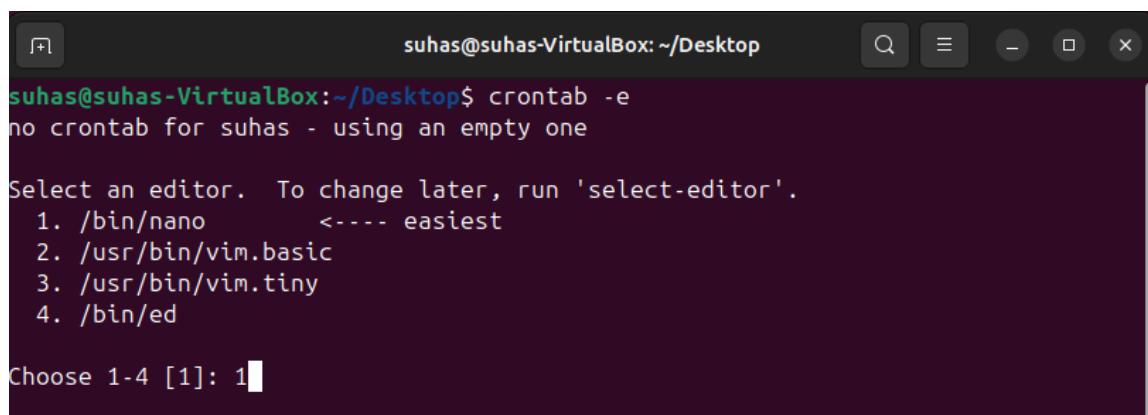
A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Backup/Documents". The terminal shows the command "cat documents_backup_2024-10-04.tar.gz" being run. The output consists of several lines of binary or encoded data, including characters like 'E', 'ev', 'FD', 'B', 'M', 'C7', '6', 'y', 'U', '4', 'j', 'i', '4', 's', 'f', 'C', '9', and 'ssuh'. The terminal has a dark background with light-colored text and standard window controls at the top.

Figure 78

Shell Scripting Scheduling with Cron job

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

```
crontab -e
```



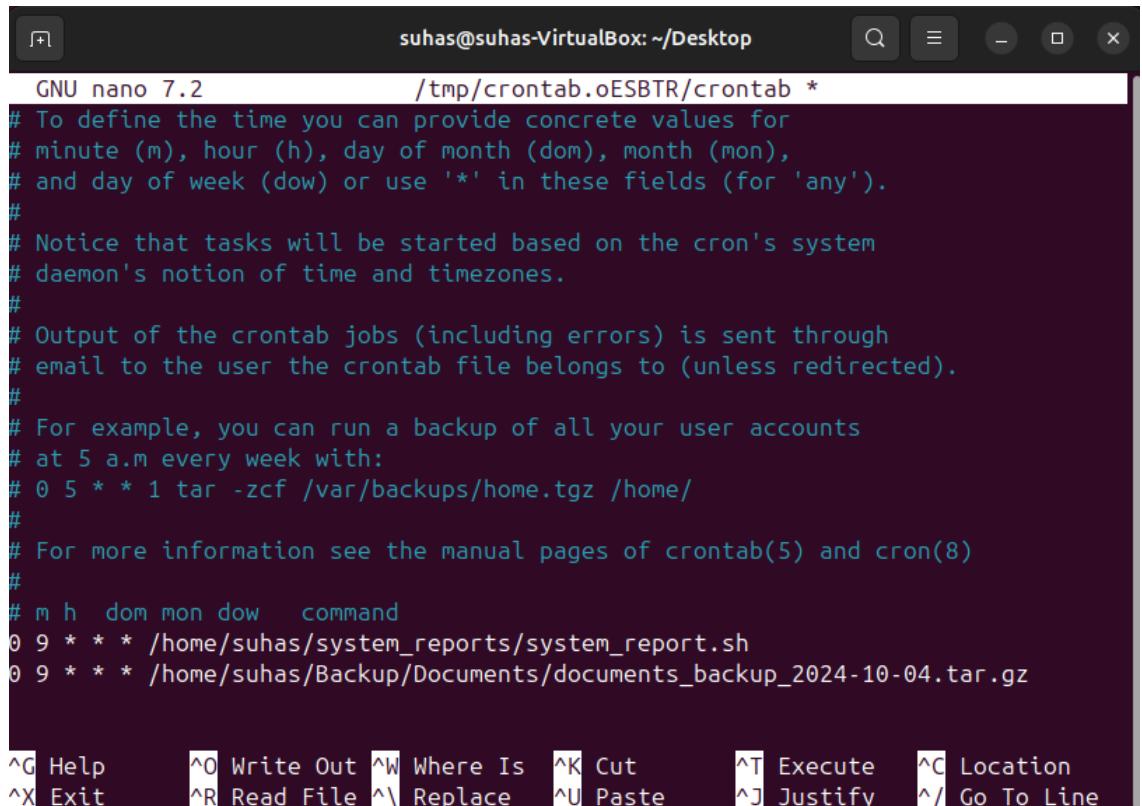
A screenshot of a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The terminal shows the command "crontab -e" being run. It displays a message "no crontab for suhas - using an empty one". It then asks "Select an editor. To change later, run 'select-editor'." followed by a list of four editors: 1. /bin/nano <---- easiest, 2. /usr/bin/vim.basic, 3. /usr/bin/vim.tiny, and 4. /bin/ed. The user is prompted to "Choose 1-4 [1]: 1". The terminal has a dark background with light-colored text and standard window controls at the top.

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.



The screenshot shows a terminal window titled "suhas@suhas-VirtualBox: ~/Desktop". The window contains the crontab file being edited in the GNU nano 7.2 editor. The file includes comments explaining cron syntax and two specific cron entries:

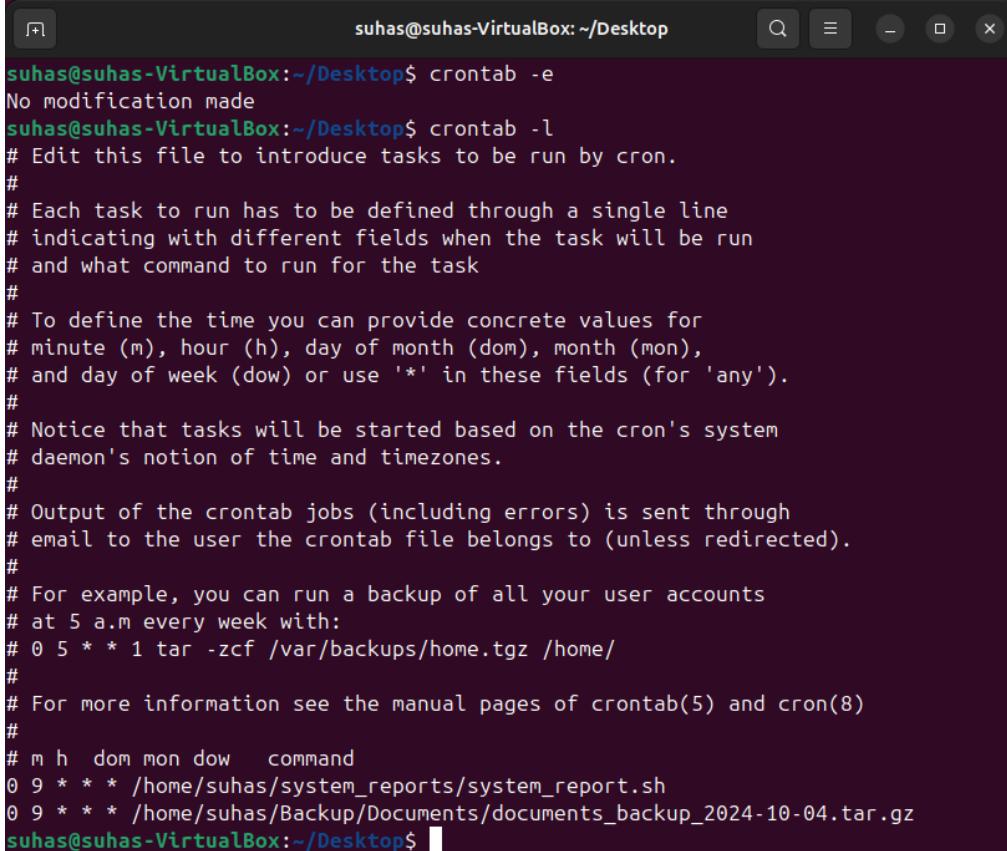
```
GNU nano 7.2          /tmp/crontab.oESBTR/crontab *
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# 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 9 * * * /home/suhas/system_reports/system_report.sh
0 9 * * * /home/suhas/Backup/Documents/documents_backup_2024-10-04.tar.gz
```

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts for navigating and editing the file.

Figure 80

3. Check the cronjobs.

crontab l



```
suhas@suhas-VirtualBox:~/Desktop$ crontab -e
No modification made
suhas@suhas-VirtualBox:~/Desktop$ crontab -l
# 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 9 * * * /home/suhas/system_reports/system_report.sh
0 9 * * * /home/suhas/Backup/Documents/documents_backup_2024-10-04.tar.gz
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 81

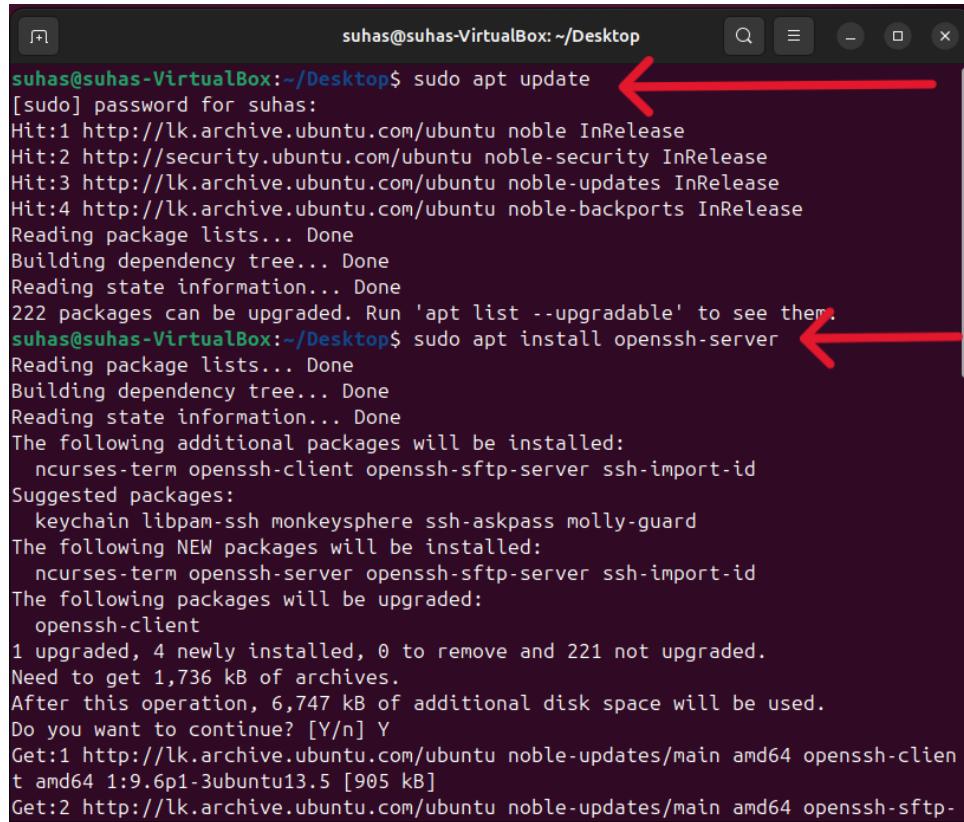
Configuring steps for SSH server, iptables and ACLs

SSH server

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

```
sudo apt update
```

```
sudo apt install openssh-server
```



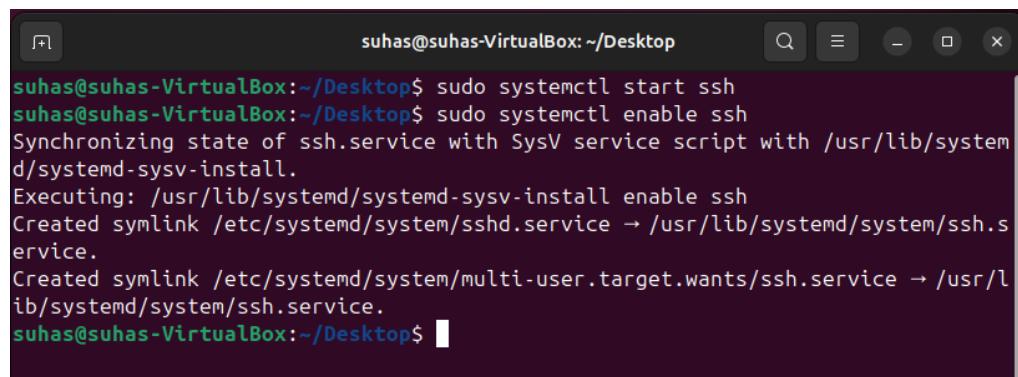
```
suhas@suhas-VirtualBox:~/Desktop$ sudo apt update
[sudo] password for suhas:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
222 packages can be upgraded. Run 'apt list --upgradable' to see them.
suhas@suhas-VirtualBox:~/Desktop$ 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-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 221 not upgraded.
Need to get 1,736 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-client amd64 1:9.6p1-3ubuntu13.5 [905 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-
```

Figure 82

2. Start and enable ssh.

```
sudo systemctl start ssh
```

```
sudo systemctl enable ssh
```

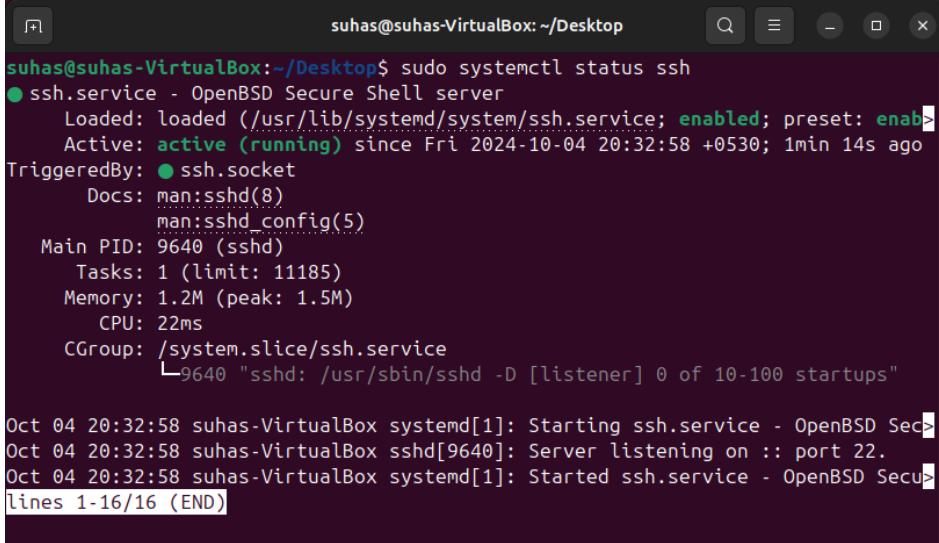


```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl start ssh
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /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.
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 83

3. Check the status of the ssh server.

sudo systemctl status ssh.



```
suhas@suhas-VirtualBox:~/Desktop$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Fri 2024-10-04 20:32:58 +0530; 1min 14s ago
    TriggeredBy: ● ssh.socket
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 9640 (sshd)
     Tasks: 1 (limit: 11185)
    Memory: 1.2M (peak: 1.5M)
       CPU: 22ms
      CGroup: /system.slice/ssh.service
              └─9640 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 04 20:32:58 suhas-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Secu...
Oct 04 20:32:58 suhas-VirtualBox sshd[9640]: Server listening on :: port 22.
Oct 04 20:32:58 suhas-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secu...
lines 1-16/16 (END)
```

Figure 84

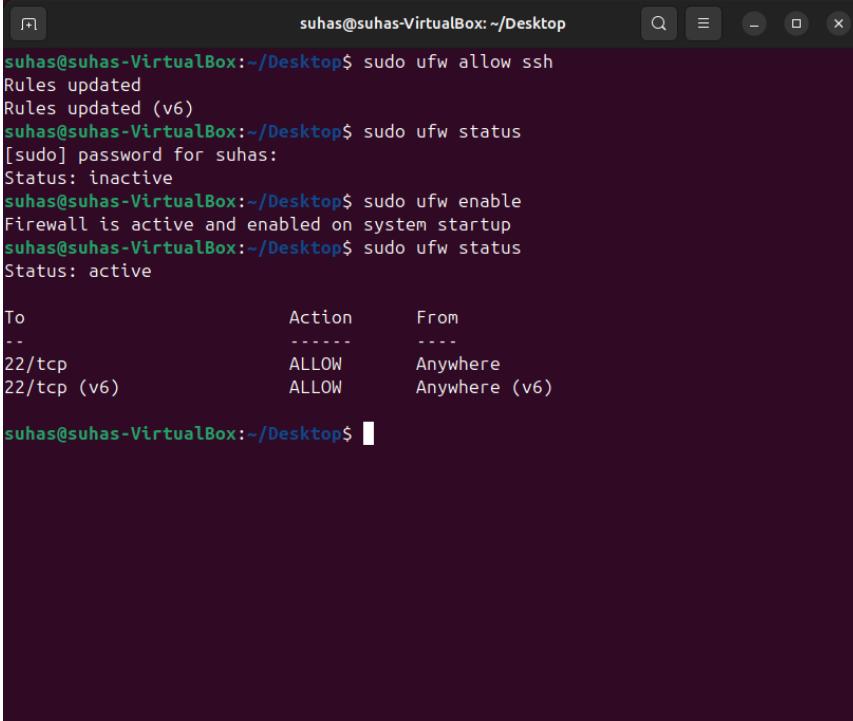
Connecting VM machines using SSH.

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



```
suhas@suhas-VirtualBox:~/Desktop$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
suhas@suhas-VirtualBox:~/Desktop$ sudo ufw status
[sudo] password for suhas:
Status: inactive
suhas@suhas-VirtualBox:~/Desktop$ sudo ufw enable
Firewall is active and enabled on system startup
suhas@suhas-VirtualBox:~/Desktop$ sudo ufw status
Status: active

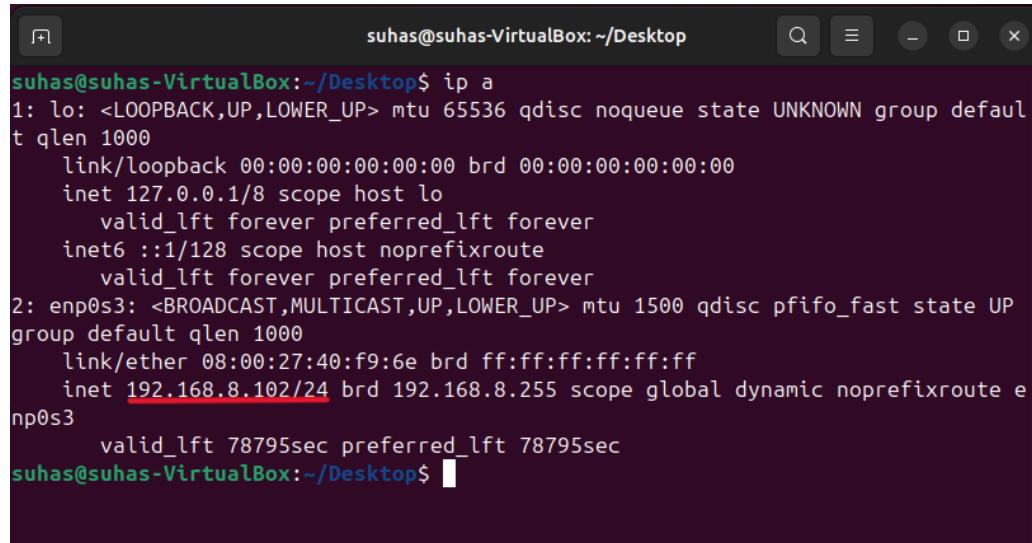
To                         Action      From
--                         --          --
22/tcp                      ALLOW      Anywhere
22/tcp (v6)                  ALLOW      Anywhere (v6)

suhas@suhas-VirtualBox:~/Desktop$
```

Figure 85

2. Find the VMs IP Address.

```
ip a
```



```
suhas@suhas-VirtualBox:~/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 08:00:27:40:f9:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.102/24 brd 192.168.8.255 scope global dynamic noprefixroute enp0s3
        valid_lft 78795sec preferred_lft 78795sec
suhas@suhas-VirtualBox:~/Desktop$
```

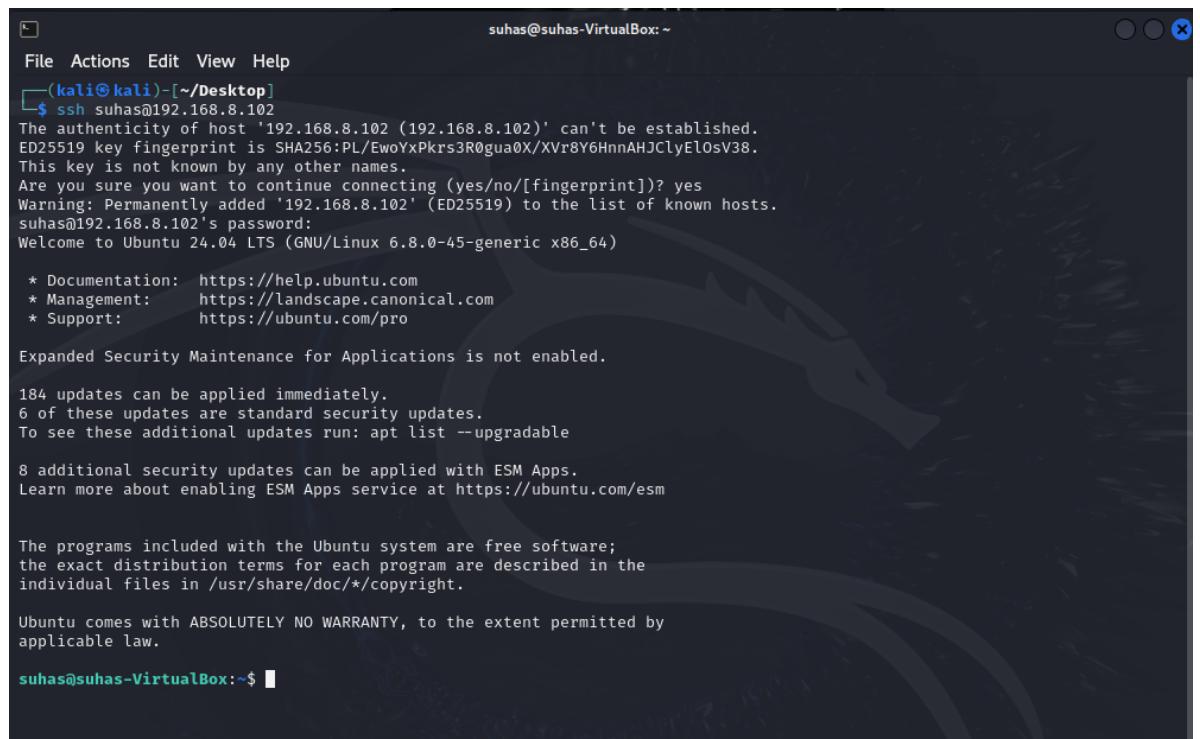
Figure 86

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
```



```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ssh suhas@192.168.8.102
The authenticity of host '192.168.8.102 (192.168.8.102)' can't be established.
ED25519 key fingerprint is SHA256:PL/EwoYxPkrs3R0gua0X/XVr8Y6HnnAHJClyElOsV38.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.102' (ED25519) to the list of known hosts.
suhas@192.168.8.102's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

184 updates can be applied immediately.
6 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

suhas@suhas-VirtualBox:~$
```

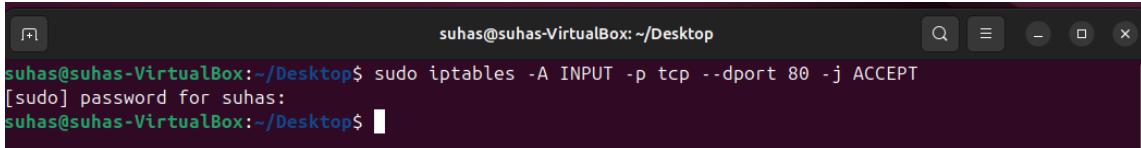
Figure 87

Iptables and ACLs

Web server security.

1. Allow HTTP traffic on port 80.

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

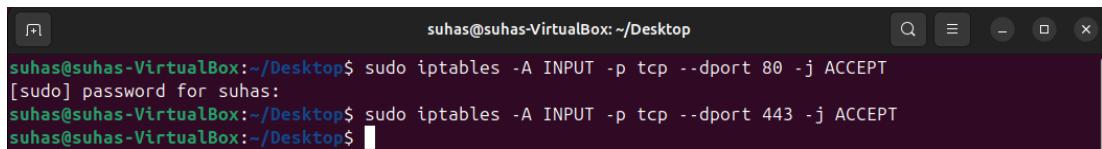


```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[sudo] password for suhas:
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 88

2. Allow HTTPS traffic on port 443.

```
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

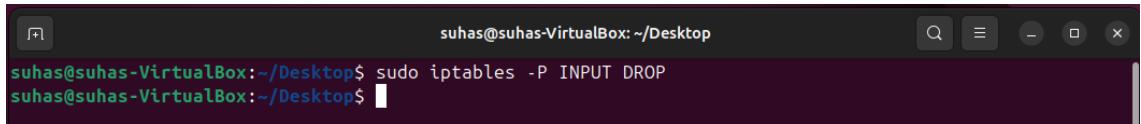


```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[sudo] password for suhas:
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 89

3. Block all other incoming traffic by default.

```
sudo iptables -P INPUT DROP
```



```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -P INPUT DROP
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 90

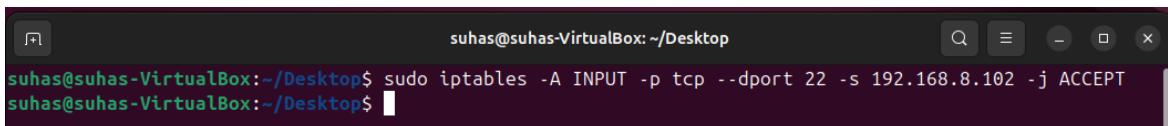
Remote Administration Access.

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
```

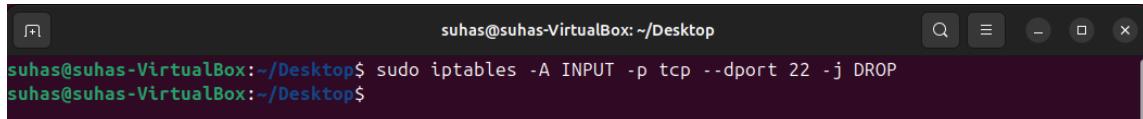


```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.8.102 -j ACCEPT
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 91

2. Block SSH access from all other IP addresses.

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```



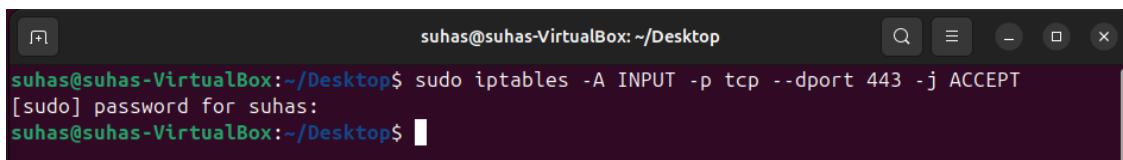
```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
suhas@suhas-VirtualBox:~/Desktop$
```

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
```



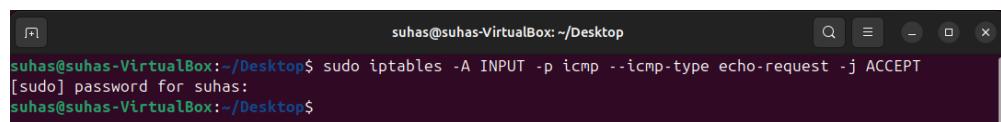
```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
[sudo] password for suhas:
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 93

Allow Pings (ICMP Echo Request)

1. Allow ICMP (ping) request.

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



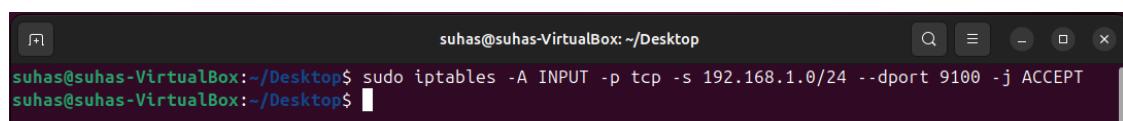
```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
[sudo] password for suhas:
suhas@suhas-VirtualBox:~/Desktop$
```

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
```

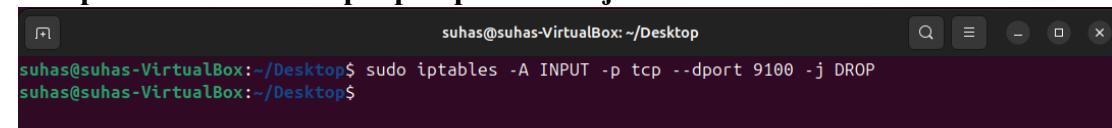


```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 9100 -j ACCEPT
suhas@suhas-VirtualBox:~/Desktop$
```

Figure 95

2. Block external access to the printer server.

```
sudo iptables -A INPUT -p tcp --dport 9100 -j DROP
```



```
suhas@suhas-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 9100 -j DROP
suhas@suhas-VirtualBox:~/Desktop$
```

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).

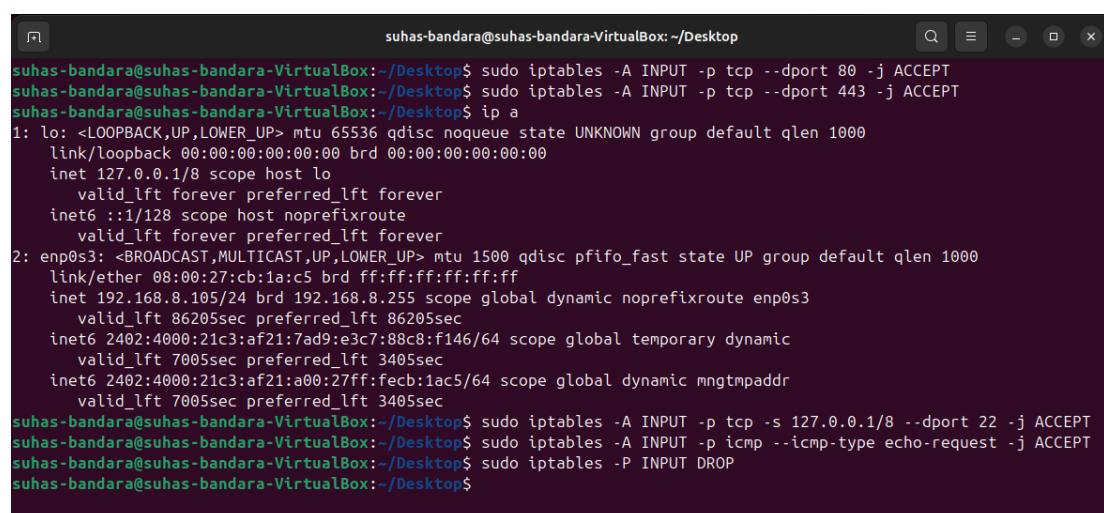
```
sudo iptables -A INPUT -p tcp -s 127.0.0.1/8 --dport 22 -j ACCEPT
```

- 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
```



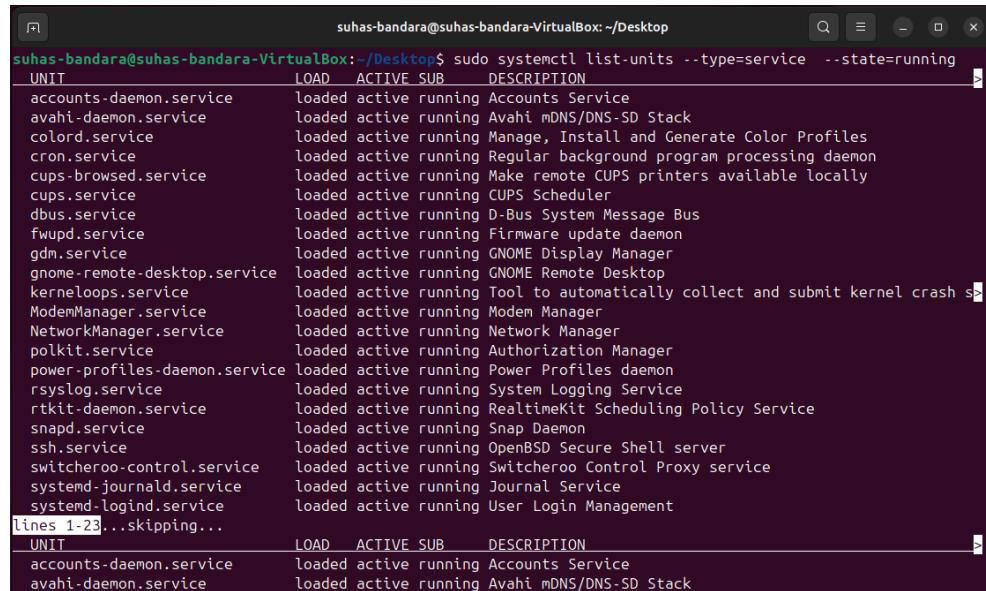
The screenshot shows a terminal window titled "suhas-bandara@suhas-bandara-VirtualBox:~/Desktop". The user has run several commands to set up a basic firewall:

```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
suhas-bandara@suhas-bandara-VirtualBox:~/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 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: 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:cb:1a:c5 brd ff:ff:ff:ff:ff:ff
        inet 192.168.8.105/24 brd 192.168.8.255 scope global dynamic noprefixroute enp0s3
            valid_lft 86205sec preferred_lft 86205sec
        inet6 2402:4000:21c3:af21:7ad9:e3c7:88c8:f146/64 scope global temporary dynamic
            valid_lft 7005sec preferred_lft 3405sec
        inet6 2402:4000:21c3:af21:a00:27ff:fecc:1ac5/64 scope global dynamic mngrtmpaddr
            valid_lft 7005sec preferred_lft 3405sec
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p tcp -s 127.0.0.1/8 --dport 22 -j ACCEPT
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo iptables -P INPUT DROP
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$
```

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

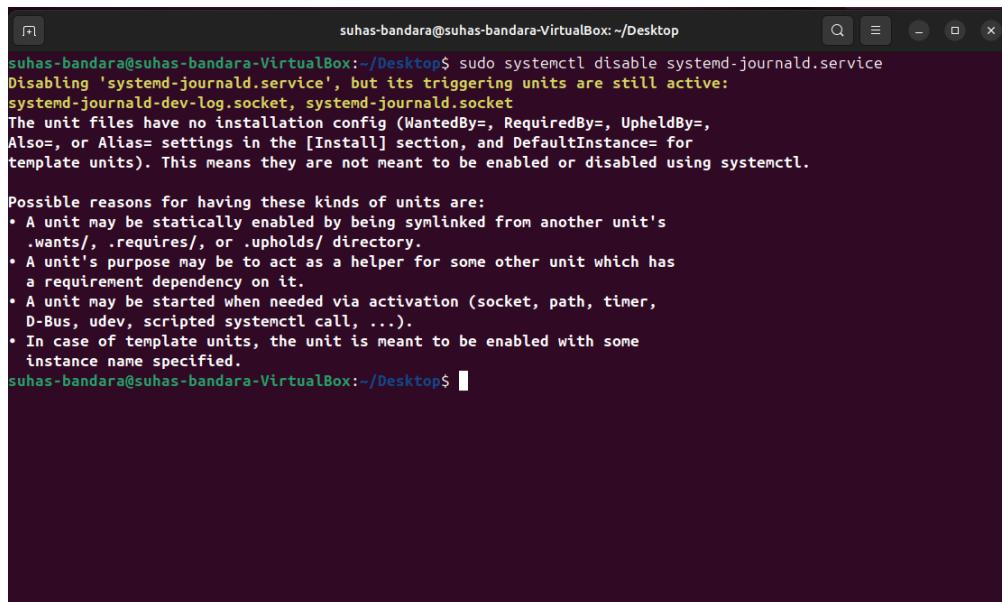


```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo systemctl list-units --type=service --state=running
 _UNIT           LOAD ACTIVE SUB   DESCRIPTION
accounts-daemon.service loaded active running Accounts Service
avahi-daemon.service loaded active running Avahi mDNS/DNS-SD Stack
colord.service    loaded active running Manage, Install and Generate Color Profiles
cron.service     loaded active running Regular background program processing daemon
cups-browsed.service loaded active running Make remote CUPS printers available locally
cups.service      loaded active running CUPS Scheduler
dbus.service      loaded active running D-Bus System Message Bus
fwupd.service     loaded active running Firmware update daemon
gdm.service       loaded active running GNOME Display Manager
gnome-remote-desktop.service loaded active running GNOME Remote Desktop
kerneloops.service loaded active running Tool to automatically collect and submit kernel crash reports
ModemManager.service loaded active running Modem Manager
NetworkManager.service loaded active running Network Manager
polkit.service    loaded active running Authorization Manager
power-profiles-daemon.service loaded active running Power Profiles daemon
rsyslog.service   loaded active running System Logging Service
rtkit-daemon.service loaded active running RealtimeKit Scheduling Policy Service
snapd.service     loaded active running Snap Daemon
ssh.service       loaded active running OpenBSD Secure Shell server
switcheroo-control.service loaded active running Switcheroo Control Proxy service
systemd-journald.service loaded active running Journal Service
systemd-logind.service loaded active running User Login Management
lines 1-23... skipping...
 _UNIT           LOAD ACTIVE SUB   DESCRIPTION
accounts-daemon.service loaded active running Accounts Service
avahi-daemon.service loaded active running Avahi mDNS/DNS-SD Stack
```

Figure 98

Then select and disable services that aren't necessary.

sudo systemctl disable systemd-journald.service



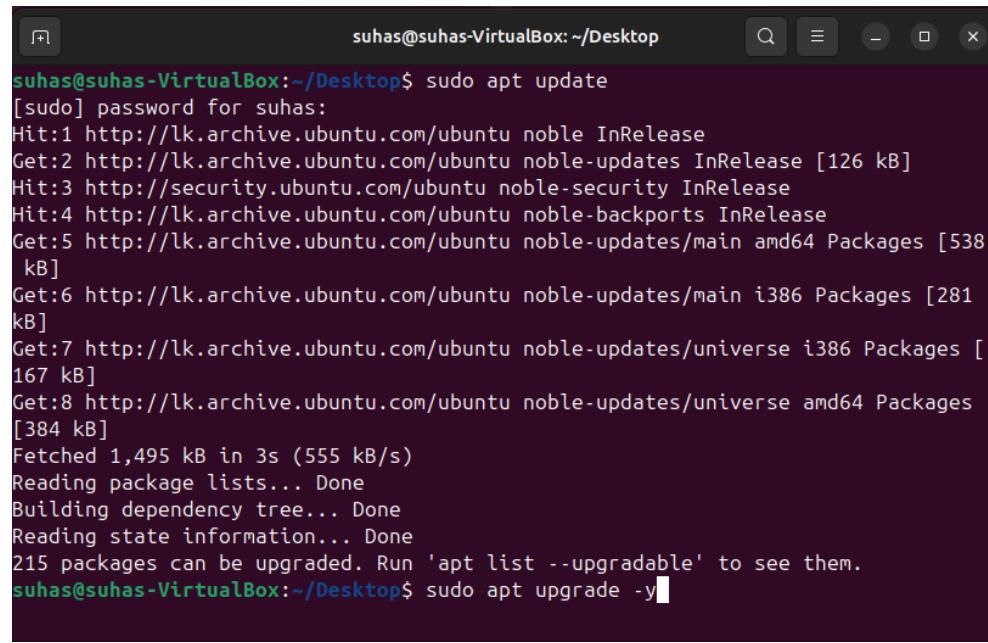
```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo systemctl disable systemd-journald.service
Disabling 'systemd-journald.service', but its triggering units are still active:
systemd-journald-dev-log.socket, systemd-journald.socket
The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=,
Also=, or Alias= settings in the [Install] section, and DefaultInstance= for
template units). This means they are not meant to be enabled or disabled using systemctl.

Possible reasons for having these kinds of units are:
• A unit may be statically enabled by being symlinked from another unit's
.wants/, .requires/, or .upholds/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
instance name specified.
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$
```

Figure 99

3. Keeping Software Updated.

- Update the package lists
sudo apt update
- Upgrade all install packages.
sudo apt upgrade -y

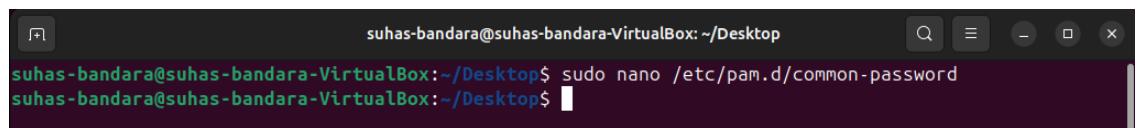


```
suhas@suhas-VirtualBox:~/Desktop$ sudo apt update
[sudo] password for suhas:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [538 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main i386 Packages [281 kB]
Get:7 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe i386 Packages [167 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [384 kB]
Fetched 1,495 kB in 3s (555 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
215 packages can be upgraded. Run 'apt list --upgradable' to see them.
suhas@suhas-VirtualBox:~/Desktop$ 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

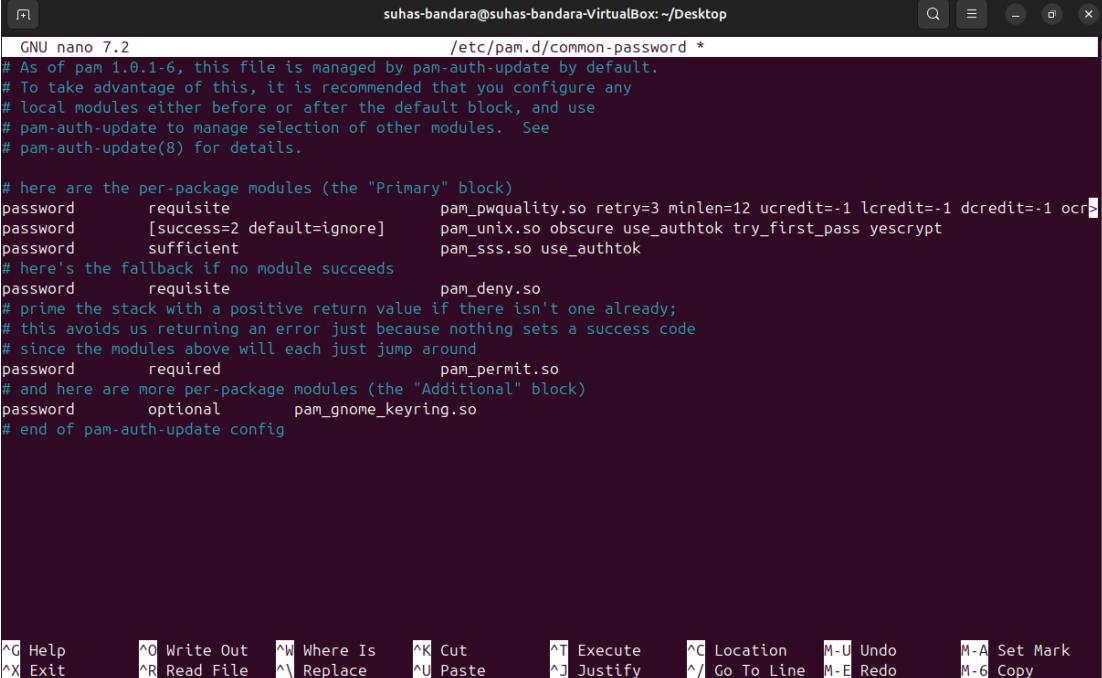


```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo nano /etc/pam.d/common-password
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$
```

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
```



```
GNU nano 7.2          /etc/pam.d/common-password *
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite      pam_pwquality.so retry=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password      [success=2 default=ignore]    pam_unix.so obscure use_authtok try_first_pass yescrypt
password      sufficient    pam_sss.so use_authtok
# here's the fallback if no module succeeds
password      requisite    pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required     pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional     pam_gnome_keyring.so
# end of pam-auth-update config
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-A Set Mark
M-6 Copy

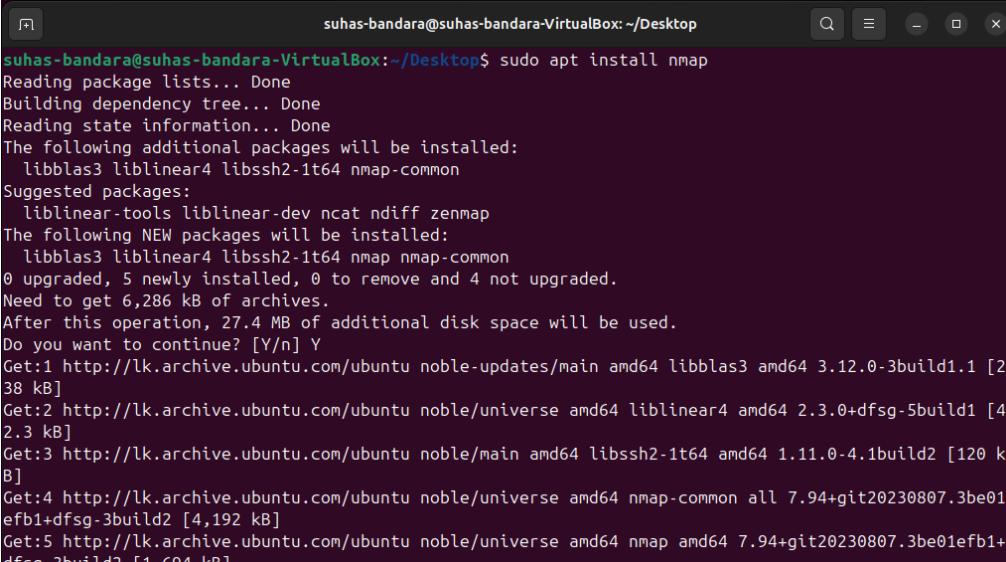
Figure 102

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
```

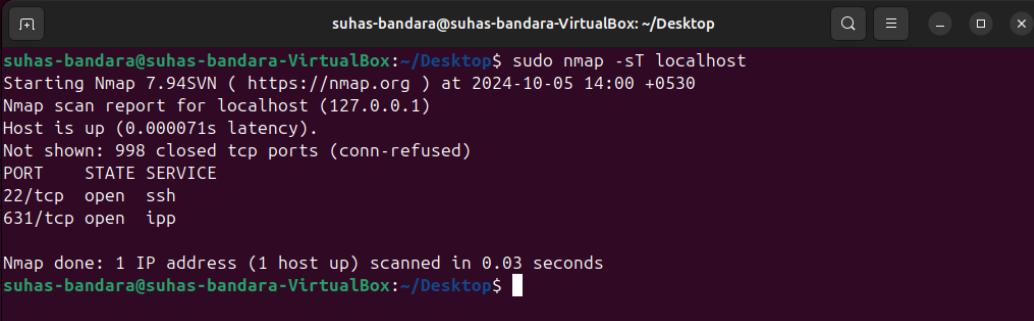


```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 4 not upgraded.
Need to get 6,286 kB of archives.
After this operation, 27.4 MB 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 libblas3 amd64 3.12.0-3build1.1 [2838 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.0+dfsg-5build1 [42.3 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0-4.1build2 [120 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-3build2 [4,192 kB]
Get:5 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-3build2 [1,694 kB]
```

Figure 103

- Scan open ports on the local machine.

```
sudo nmap -sT localhost
```



A terminal window titled "suhas-bandara@suhas-bandara-VirtualBox: ~/Desktop". The window contains the output of a sudo nmap -sT localhost command. The output shows the host is up with 0 latency. It lists two open TCP ports: 22/tcp (ssh) and 631/tcp (ipp). The scan took 0.03 seconds.

```
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$ sudo nmap -sT localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 14:00 +0530
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
suhas-bandara@suhas-bandara-VirtualBox:~/Desktop$
```

Figure 104