



## **IE2012 - System and Network Programming**

**Assignment - 2025 (Feb/June)**

H.M. Buddhima Herath  
Y2S1

# 1. Basics of Linux Environment.

## 1.1. Virtual Machine Setup:

The following steps will successfully be implemented virtual machine software and Linux Distribution.

### Step 01: Select one software to run virtual machine.

- Download VMware Workstation Player from official website:  
<https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html>
- Download VirtualBox from the official website: <https://www.virtualbox.org/wiki/Downloads>

### Step 02: Download an .iso file from the Ubuntu or CentOS website.

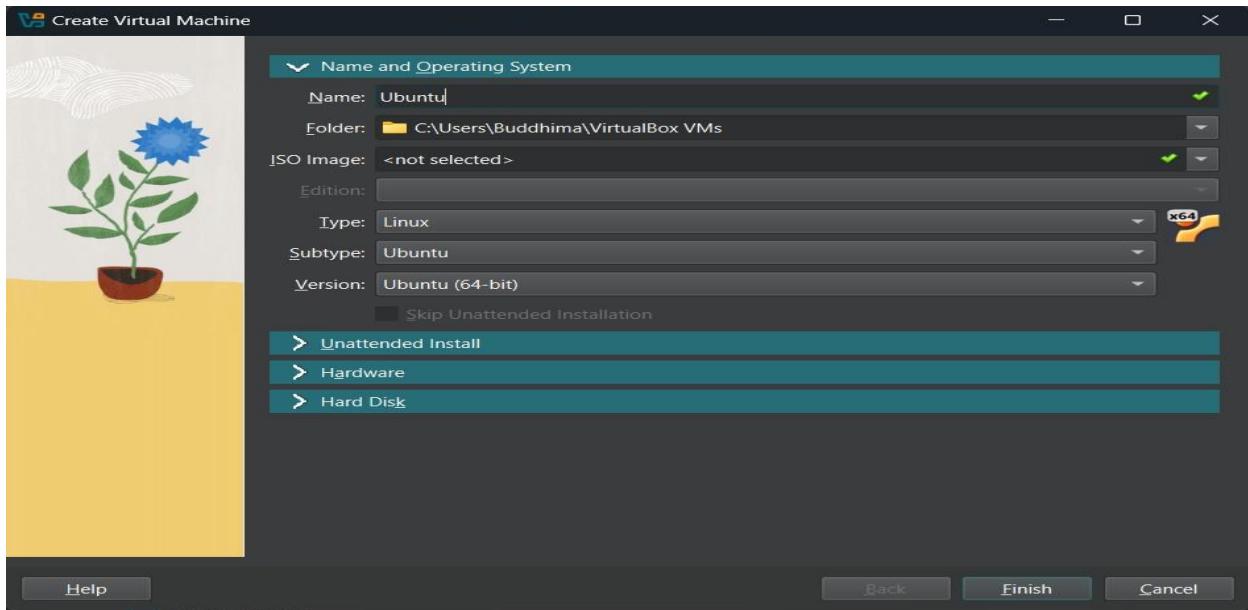
- Ubuntu: (<https://ubuntu.com/download/desktop>)
- CentOS: (<https://www.centos.org/download/>)

### Step 03:

Open the Virtual Machine software and follow the guidelines below, In  
VirtualBox:

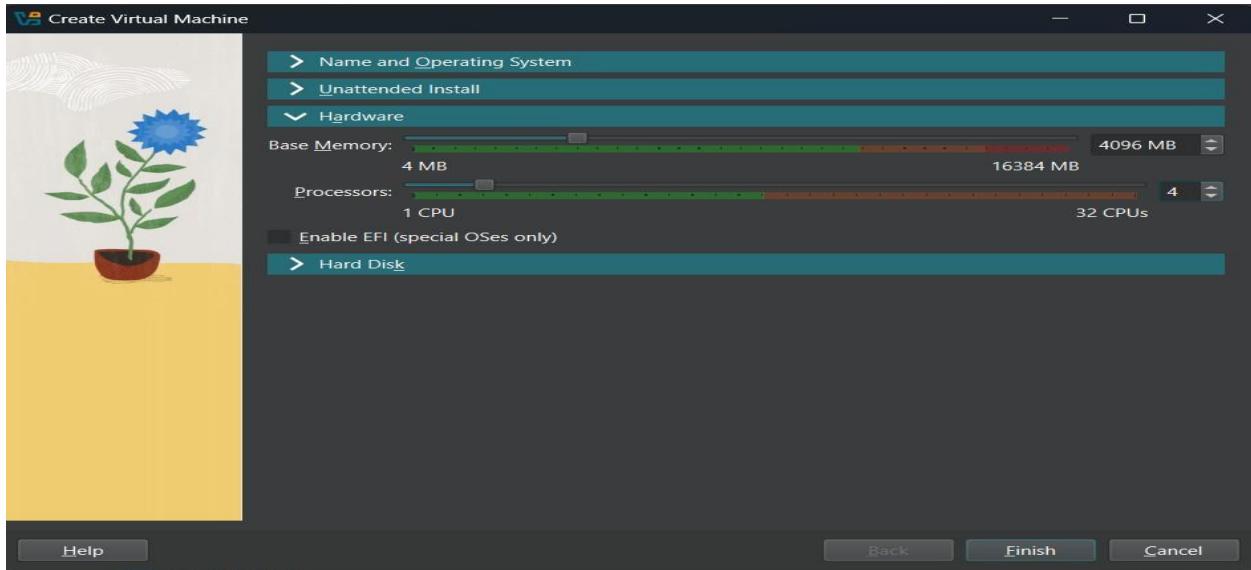
Open the VirtualBox software to create a new virtual machine.

1. Create a new virtual machine click on NEW icon.
2. Name: Ubuntu
3. Set the type and version as Linux and Ubuntu (64-bit)



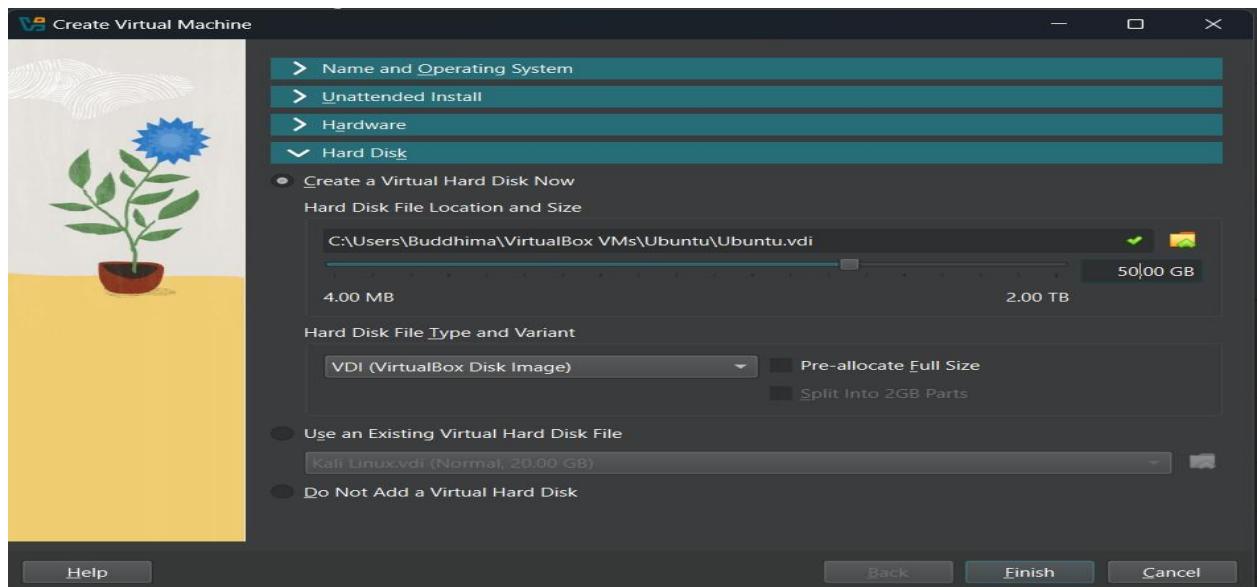
4. Click on Hardware

- Base Memory (RAM): 4096 MB
- Processor: 4



5. Click on Hard Disk

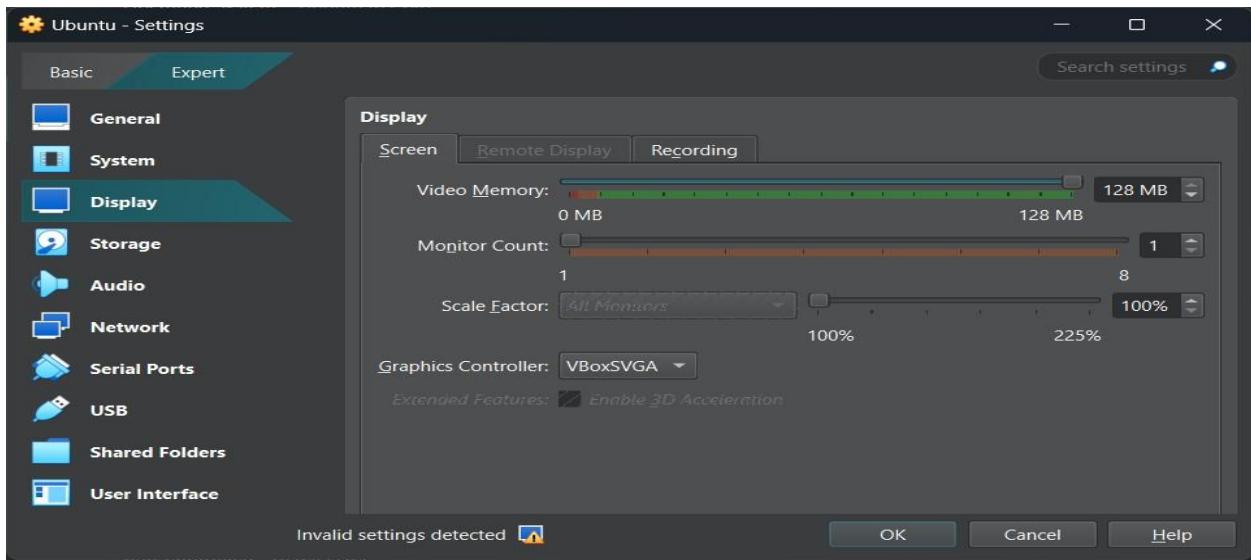
- Change the size of the Hard Disk File Location into 50 GB



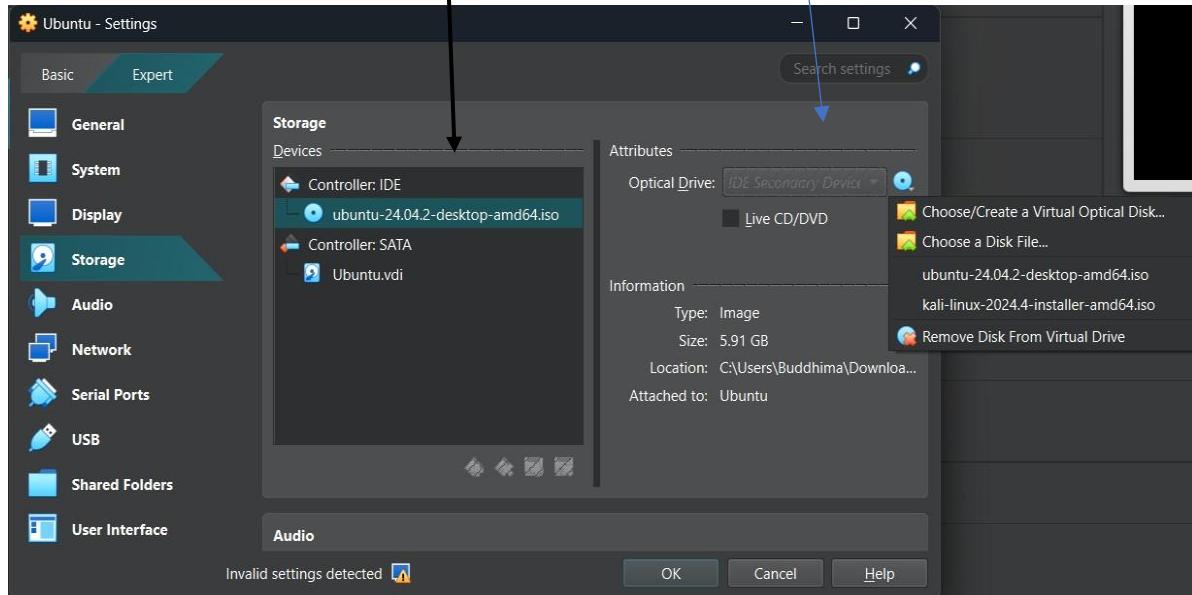
6. Open Ubuntu settings,

- Change the display video memory size into 128 MB.

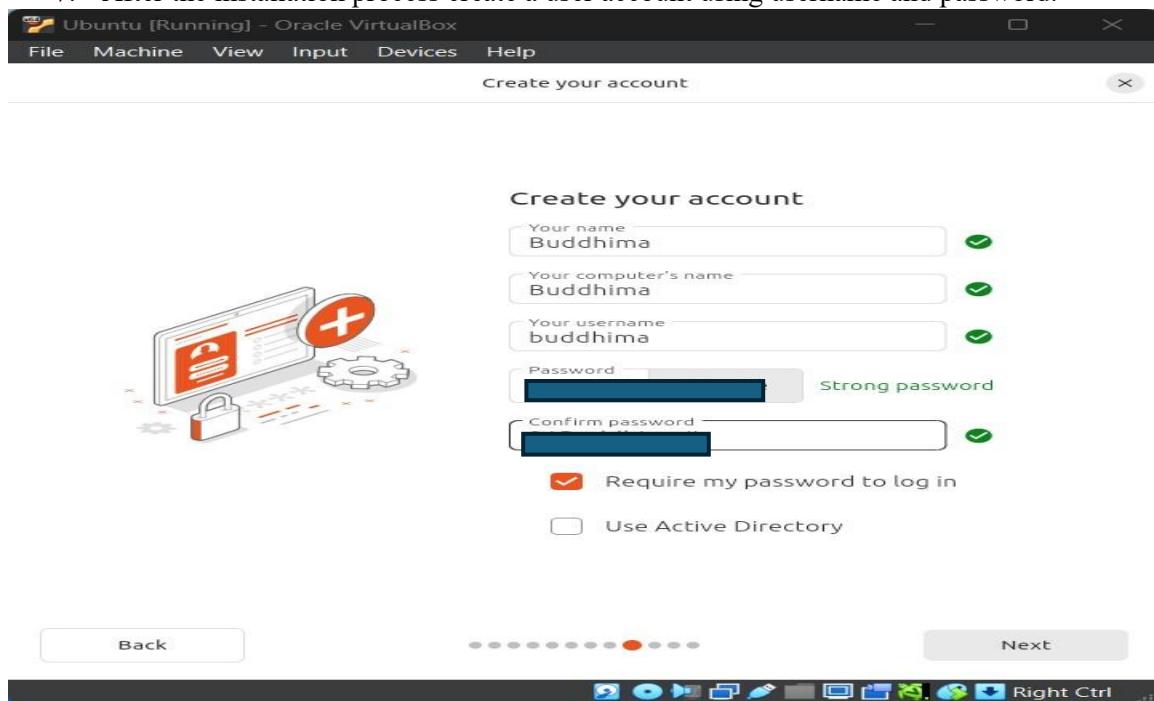
- Change the display Graphics Controller to VBoxSVGA.



- Change the Optical Drive as IDE Secondary Device 0
- Attach the downloaded ISO file to the empty controller IDE (ubuntu-24.04.2-desktop-amd64.iso)



7. After the installation process create a user account using username and password.



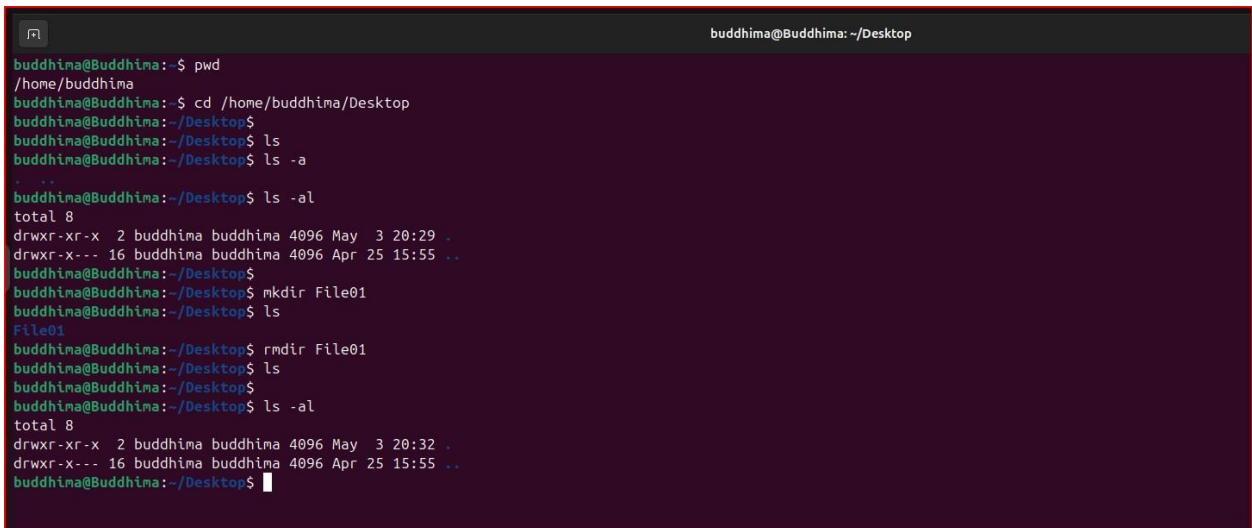
8. Login with the user credentials after rebooting the Virtual Machine.



## 1.2. Command Line Introduction.

The following commands will be interacted with the Linux system to navigate the Linux environment effectively.

Navigation Commands:	
<b>1.<code>pwd</code></b>	<ul style="list-style-type: none"><li>• This command will print the current working directory.</li></ul>
<b>2.<code>ls</code></b> <b>-a</b> <b>-al</b>	<ul style="list-style-type: none"><li>• This command will list files and directories.</li><li>• This command will list files and directories with hidden files. This command will list all files and directories with size, permission, date.</li></ul>
<b>3.<code>mkdir</code></b>	<ul style="list-style-type: none"><li>• This command will create a directory.</li></ul>
<b>4.<code>rmdir</code></b>	<ul style="list-style-type: none"><li>• This command removes directory with all contents.</li></ul>



A screenshot of a terminal window titled "Terminal". The window shows a session on a Linux system named "buddhima@Buddhima". The user runs several commands to demonstrate file navigation:

```
buddhima@Buddhima: ~$ pwd
/home/buddhima
buddhima@Buddhima: ~$ cd /home/buddhima/Desktop
buddhima@Buddhima: ~/Desktop$ 
buddhima@Buddhima: ~/Desktop$ ls
buddhima@Buddhima: ~/Desktop$ ls -a
.
..
buddhima@Buddhima: ~/Desktop$ ls -al
total 8
drwxr-xr-x 2 buddhima buddhima 4096 May  3 20:29 .
drwxr-xr-x 16 buddhima buddhima 4096 Apr 25 15:55 ..
buddhima@Buddhima: ~/Desktop$ 
buddhima@Buddhima: ~/Desktop$ mkdir File01
buddhima@Buddhima: ~/Desktop$ ls
File01
buddhima@Buddhima: ~/Desktop$ rmdir File01
buddhima@Buddhima: ~/Desktop$ ls
buddhima@Buddhima: ~/Desktop$ 
buddhima@Buddhima: ~/Desktop$ ls -al
total 8
drwxr-xr-x 2 buddhima buddhima 4096 May  3 20:32 .
drwxr-xr-x 16 buddhima buddhima 4096 Apr 25 15:55 ..
buddhima@Buddhima: ~/Desktop$ 
```

File Manipulation Commands.	
<b>5.<code>cd</code> –</b> <b>cd ..</b> –	<ul style="list-style-type: none"><li>• This command will change the working directory. This command will move one directory up.</li></ul>
<b>6.<code>cp</code> –</b>	<ul style="list-style-type: none"><li>• This command will copy file.</li></ul>
<b>7.<code>mv</code> –</b>	<ul style="list-style-type: none"><li>• This command will move or rename file.</li></ul>
<b>8.<code>touch</code> –</b>	<ul style="list-style-type: none"><li>• This command will create an empty file.</li></ul>
<b>9.<code>rm</code> –</b>	<ul style="list-style-type: none"><li>• This command will remove file.</li></ul>

```
buddhima@Buddhima:~/Desktop$ cp file.txt File1
buddhima@Buddhima:~/Desktop$ cd File1
buddhima@Buddhima:~/Desktop/File1$ ls
file.txt
buddhima@Buddhima:~/Desktop/File1$ mv file.txt newfile.txt
buddhima@Buddhima:~/Desktop/File1$ ls
newfile.txt
buddhima@Buddhima:~/Desktop/File1$ 
buddhima@Buddhima:~/Desktop/File1$ cat newfile.txt
Hello
buddhima@Buddhima:~/Desktop/File1$ 
buddhima@Buddhima:~/Desktop/File1$ touch file1.txt
buddhima@Buddhima:~/Desktop/File1$ ls
file1.txt  newfile.txt
buddhima@Buddhima:~/Desktop/File1$ rm file1.txt
buddhima@Buddhima:~/Desktop/File1$ ls
newfile.txt
buddhima@Buddhima:~/Desktop/File1$
```

### 1.3. System Information and User Management.

Can retrieve the system information of computer's hardware, software and performance. Explore the user management commands, checking system status, and troubleshooting.

User Management Commands:	
10.whoami –	<ul style="list-style-type: none"><li>This command will Shows the current username.</li></ul>
11.id –	<ul style="list-style-type: none"><li>This command will show user ID and group ID.</li></ul>

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

System Information Commands:	
12. <b>cat /proc/version</b> — <b>cat</b> —	<ul style="list-style-type: none"> <li>This command will show Linux version information by reading the /proc/version file.</li> <li>This command will show the content of a file.</li> </ul>
13. <b>uname -a</b> —	<ul style="list-style-type: none"> <li>This command will confirm the version of Linux running. (print the kernel name, version, machine type and OS)</li> </ul>
14. <b>df -h</b> —	<ul style="list-style-type: none"> <li>This command will show the disk space usage of all mounted filesystem. (In a human-readable format – GB/MB)</li> </ul>
15. <b>free -h</b> —	<ul style="list-style-type: none"> <li>This command will show memory usage and available memory. (In a human-readable format.)</li> </ul>

```
buddhima@Buddhima:~/Desktop$ cat /proc/version
Linux version 6.11.0-24-generic (build0@lcy02-amd64-034) (x86_64-linux-gnu-gcc-13 (Ubuntu 13.3.0-6ubuntu2-24.04) 13.3.0, GNU ld (GNU Binutils for Ubuntu) 2.42)
REEMPT_DYNAMIC Tue Mar 25 20:14:34 UTC 2
buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$ uname -a
Linux Buddhima 6.11.0-24-generic #24-24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Tue Mar 25 20:14:34 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs          392M   1M  391M  1% /run
/dev/sda2        49G   1G   37G  23% /
tmpfs          2.0G    0   2.0G  0% /dev/shm
tmpfs          5.0M  8.0K  5.0M  1% /run/lock
tmpfs          392M  132K  392M  1% /run/user/1000
buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$ free -h
              total        used        free      shared  buff/cache   available
Mem:       3.8Gi       1.3Gi      1.7Gi      34Mi       1.1Gi      2.5Gi
Swap:      3.8Gi         0B      3.8Gi
buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$
```

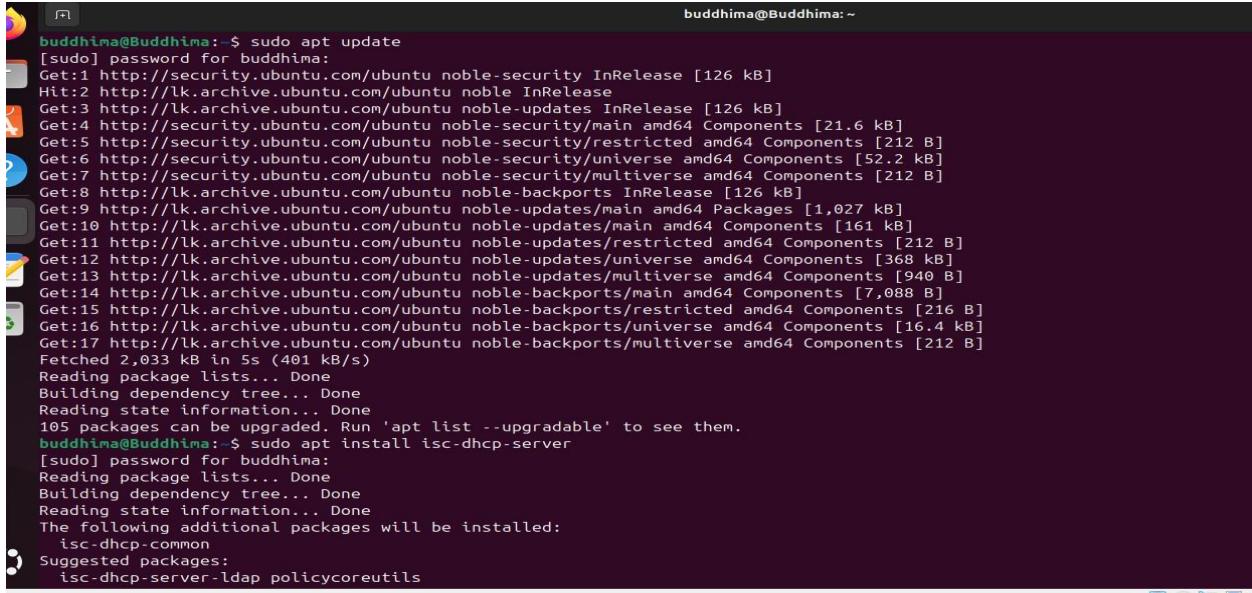
## 2. DHCP, DNS and NTP Services.

### 2.1. DHCP (Dynamic Host Configuration Protocol) Network Service:

DHCP Network Service assigns automatically IP addresses, subnet masks gateway and configures other networks like DNS servers to devices in a network. It helps to manage IP addresses without manually assigning them.

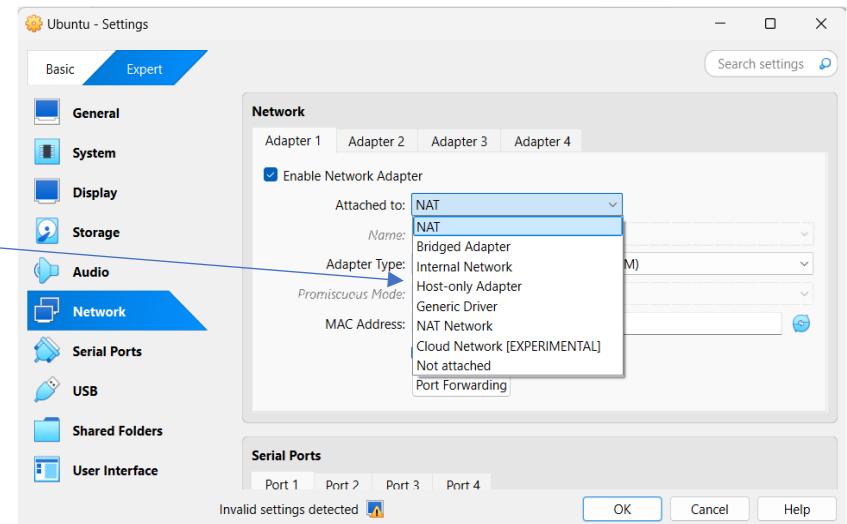
Step 01: Install the DHCP server using the commands below.

- **sudo apt update** (update the list of packages that are available and the version)
- **sudo apt install isc-dhcp-server** (install the ISC DHCP server and it allows assign IP addresses)



```
buddhima@Buddhima: ~
[buddhima@Buddhima: ~]$ sudo apt update
[sudo] password for buddhima:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:9 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,027 kB]
Get:10 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [161 kB]
Get:11 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 kB]
Get:12 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [368 kB]
Get:13 http://lk.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 kB]
Get:14 http://lk.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,088 kB]
Get:15 http://lk.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 kB]
Get:16 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [16.4 kB]
Get:17 http://lk.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 kB]
Fetched 2,033 kB in 5s (401 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
105 packages can be upgraded. Run 'apt list --upgradable' to see them.
[buddhima@Buddhima: ~]$ sudo apt install isc-dhcp-server
[sudo] password for buddhima:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  isc-dhcp-common
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
```

After the installation of DHCP should change the network setting from NAT to Host-Only, cause NAT is used for internet access and Host-Only used to create private network between Local host and the VMs.



- **dpkg -l | grep isc-dhcp-server** – check DHCP is installed successfully.

```

buddhima@Buddhima: ~
buddhima@Buddhima: $ dpkg -l | grep isc-dhcp-server
ii  isc-dhcp-server          4.4.3-P1-4ubuntu2      buddhima@Buddhima: ~
[sudo] password for buddhima:
buddhima@Buddhima: $ sudo nano /etc/dhcp/dhcpd.conf
buddhima@Buddhima: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 431sec preferred_lft 431sec
    inet6 fe80::a00:27ff:fec1:db05/64 scope link
        valid_lft forever preferred_lft forever
buddhima@Buddhima: ~
buddhima@Buddhima: $ sudo nano /etc/dhcp/dhcpd.conf
[sudo] password for buddhima:
buddhima@Buddhima: $ sudo nano /etc/default/isc-dhcp-server
buddhima@Buddhima: $ 

```

## Step 02: Configure DHCP

- sudo nano /etc/dhcp/dhcpd.conf - Using nano editor open dhcpd.conf file.
- Inside the dhcpd.conf file- change **option domain-name** as “buddhima.local” and **optional domain-name-server** as 1.1.1.1, 8.8.8.8.

```

buddhima@Buddhima: ~
buddhima@Buddhima: ~
GNU nano 7.2
# /etc/dhcp/dhcpd.conf
#
# Sample configuration file for ISC dhcpcd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
#
# option definitions common to all supported networks...
option domain-name "buddhima.local";
option domain-name-servers 1.1.1.1, 8.8.8.8;

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

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {

```

File menu    Edit menu    Insert menu    View menu    Search menu    Help menu

Help    Write Out    Where Is    Cut    Execute    Location    Undo    Set Mark    To Bracket    Previous

```

buddhima@Buddhima: ~
buddhima@Buddhima: ~
buddhima@Buddhima: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
            valid_lft 426sec preferred_lft 426sec
        inet6 fe80::a00:27ff:fe1:db05/64 scope link
            valid_lft forever preferred_lft forever
buddhima@Buddhima: $ 

```

- Add below command to the configuration file, subnet 192.168.56.0 netmask 255.255.255.0 { range 192.168.56.100 192.168.56.200; option routers 192.168.56.1; option domain-name-servers 8.8.8.8; default-lease-time 600; max-lease-time 7200; }

Above mentioned commands define the network range, subnet mask, domain name server and max lease time.

- **Ip a** – using IP a command shows all the interface of network, and the IP address details also.

```

buddhima@Buddhima: ~
buddhima@Buddhima: ~
GNU nano 7.2
/etc/dhcp/dhcpd.conf *

# This is a very basic subnet declaration.

subnet 10.254.239.0 netmask 255.255.255.224 {
# range 10.254.239.10 10.254.239.20;
# option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

subnet 10.254.239.32 netmask 255.255.255.224 {
# 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 192.168.56.0 netmask 255.255.255.0 {
    range 192.168.56.150 192.168.56.200;
    option domain-name-servers 8.8.8.8;
    option domain-name "buddhima.local";
    option subnet-mask 255.255.255.0;
    option routers 192.168.56.1;
    option broadcast-address 192.168.56.255;
    default-lease-time 600;
    max-lease-time 7200;
}

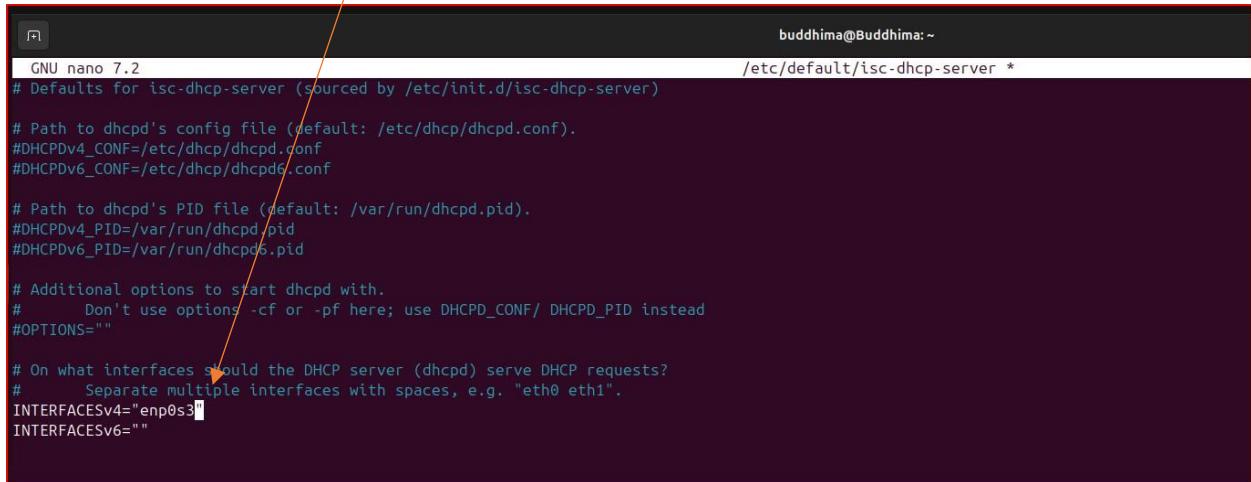
# Hosts which require special configuration options can be listed in
# host statements. If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information

```

### Step 03: Set the interface of DHCP Server

- **sudo nano /etc/default/isc-dhcp-server**- Set the network interface that already find from ip a command.
- Set as **INTERFACESv4="enp0s3"**

Network interfaces tell the DHCP to operate on the enp0s3 interface (Host-Only mode in VirtualBox)



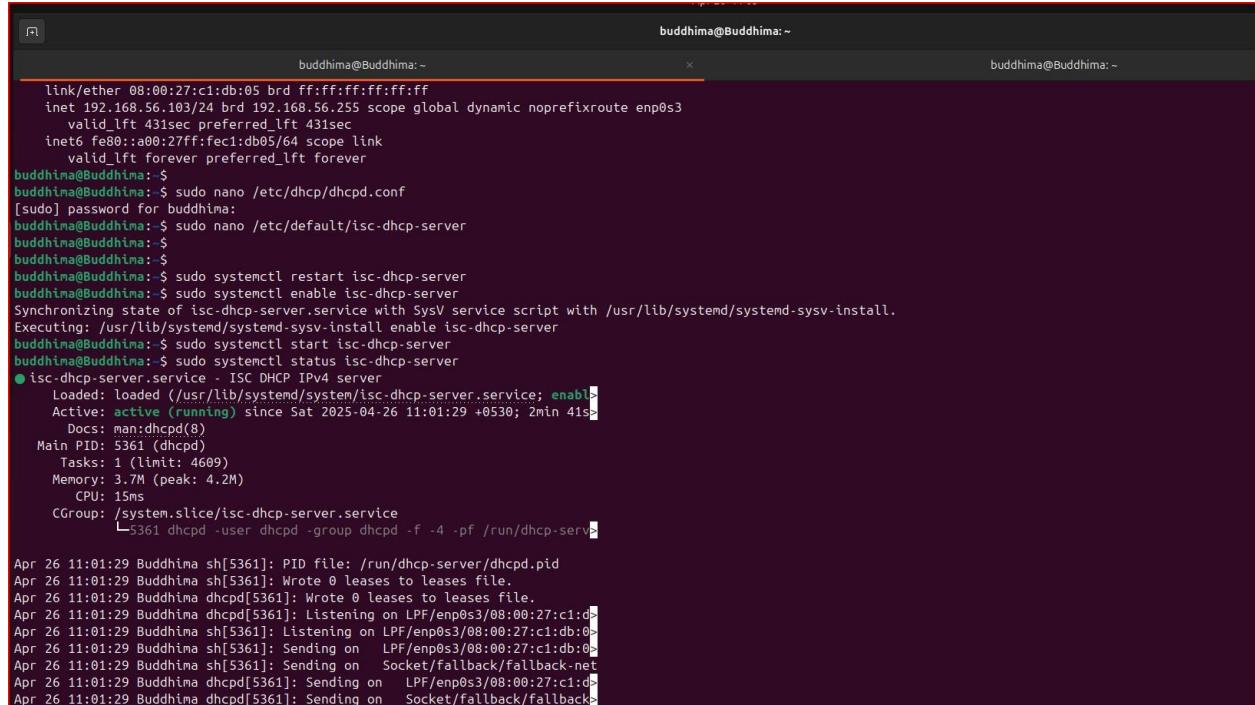
```
GNU nano 7.2                                buddhima@Buddhima:~
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpcd.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpcd.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=""
```

### Step 04: Restart and Enable the DHCP server.



```
buddhima@Buddhima:~          buddhima@Buddhima:~          buddhima@Buddhima:~
link/ether 08:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
    valid_lft 431sec preferred_lft 431sec
    inet6 fe80::a00:27ff:fe:c1:db%enp0s3/64 scope link
        valid_lft forever preferred_lft forever
buddhima@Buddhima:~ $          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
buddhima@Buddhima:~ $ sudo nano /etc/dhcp/dhcpcd.conf          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
[sudo] password for buddhima:          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
buddhima@Buddhima:~ $          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
buddhima@Buddhima:~ $ sudo systemctl restart isc-dhcp-server          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
buddhima@Buddhima:~ $ sudo systemctl enable isc-dhcp-server          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
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
buddhima@Buddhima:~ $ sudo systemctl start isc-dhcp-server          buddhima@Buddhima:~ $          buddhima@Buddhima:~ $
buddhima@Buddhima:~ $ 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 Sat 2025-04-26 11:01:29 +0530; 2min 41s ago
     Docs: man:dhcpcd(8)
     Main PID: 5361 (dhcpcd)
        Tasks: 1 (limit: 4609)
       Memory: 3.7M (peak: 4.2M)
          CPU: 15ms
         CGroup: /system.slice/isc-dhcp-server.service
             └─ 5361 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server.pid

Apr 26 11:01:29 Buddhima sh[5361]: PID file: /run/dhcp-server/dhcpcd.pid
Apr 26 11:01:29 Buddhima sh[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpcd[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpcd[5361]: Listening on LPF/enp0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima sh[5361]: Listening on LPF/enp0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima dhcpcd[5361]: Sending on   LPF/enp0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima sh[5361]: Sending on   Socket/fallback/fallback-net
Apr 26 11:01:29 Buddhima dhcpcd[5361]: Sending on   LPF/enp0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima dhcpcd[5361]: Sending on   Socket/fallback/fallback
```

- **sudo systemctl restart isc-dhcp-server** – This command restarts the DHCP server applying any changes that made in conf file.
- **sudo systemctl enable isc-dhcp-server** - This command enables the DHCP server to start automatically.

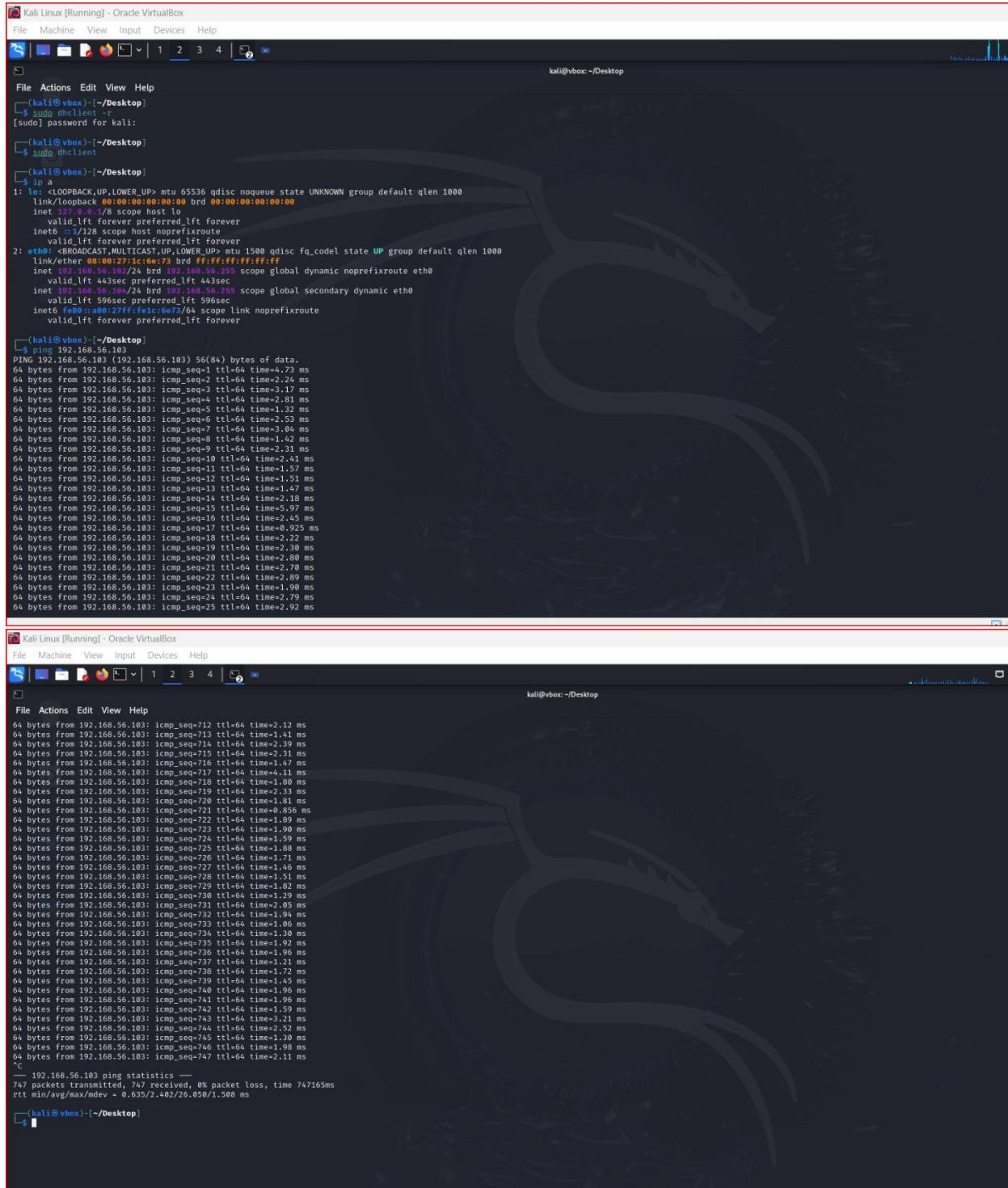
Step 05: Check the system status.

- **Sudo systemctl status isc-dhcp-server-** check the current status of ISC DHCP server whether it's active or fail.

```
buddhima@Buddhima: ~
buddhima@Buddhima: ~
Apr 26 11:01:29 Buddhima sh[5361]: PID file: /run/dhcp-server/dhcpd.pid
Apr 26 11:01:29 Buddhima sh[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpd[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpd[5361]: Listening on LPF/epn0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima sh[5361]: Listening on LPF/epn0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima sh[5361]: Sending on   LPF/epn0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   Socket/fallback/fallback-net
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   LPF/epn0s3/08:00:27:c1:db:05
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   Socket/fallback/fallback-net
Apr 26 11:01:29 Buddhima dhcpd[5361]: Server starting service.
lines 1-21/21 (END)...skipping...
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-04-26 11:01:29 +0530; 2min 41s ago
    Docs: man:dhcpd(8)
   Main PID: 5361 (dhcpd)
     Tasks: 1 (limit: 4609)
    Memory: 3.7M (peak: 4.2M)
      CPU: 15ms
     CGroup: /system.slice/isc-dhcp-server.service
           └─5361 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp0s3

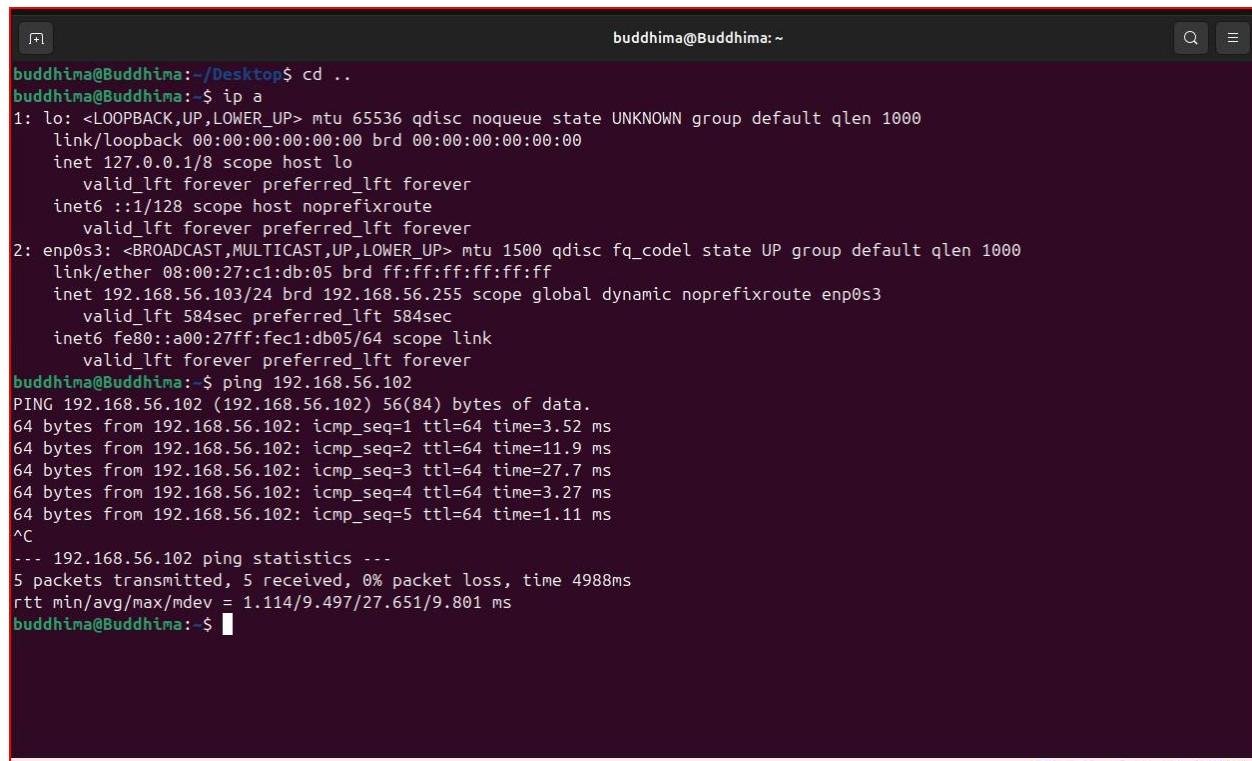
Apr 26 11:01:29 Buddhima sh[5361]: PID file: /run/dhcp-server/dhcpd.pid
Apr 26 11:01:29 Buddhima sh[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpd[5361]: Wrote 0 leases to leases file.
Apr 26 11:01:29 Buddhima dhcpd[5361]: Listening on LPF/epn0s3/08:00:27:c1:db:05/192.168.56.0/24
Apr 26 11:01:29 Buddhima sh[5361]: Listening on LPF/epn0s3/08:00:27:c1:db:05/192.168.56.0/24
Apr 26 11:01:29 Buddhima sh[5361]: Sending on   LPF/epn0s3/08:00:27:c1:db:05/192.168.56.0/24
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   Socket/fallback/fallback-net
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   LPF/epn0s3/08:00:27:c1:db:05/192.168.56.0/24
Apr 26 11:01:29 Buddhima dhcpd[5361]: Sending on   Socket/fallback/fallback-net
Apr 26 11:01:29 Buddhima dhcpd[5361]: Server starting service.
-
-
-
-
```

Ping <ubuntu ip address> - can check successfully data packets are transferring properly.



```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿vbox) ~/Desktop
$ sudo dhclient -r
[sudo] password for kali:
(kali㉿vbox) ~/Desktop
$ sudo dhclient
(kali㉿vbox) ~/Desktop
$ ls
1LOORBACK_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 brd 127.255.255.255 scope host lo
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:27:1c:e7:73 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
    valid_lft forever preferred_lft forever
    inet6 fe80::a00c27ff:fe1ce7:73/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali㉿vbox) ~/Desktop
$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=4.73 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=2.94 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=3.17 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=2.85 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=2.01 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=2.94 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=1.42 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=2.34 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=2.41 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=1.57 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=64 time=1.51 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=64 time=1.49 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=64 time=2.16 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=64 time=5.97 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=64 time=2.45 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=64 time=0.925 ms
64 bytes from 192.168.56.103: icmp_seq=18 ttl=64 time=2.22 ms
64 bytes from 192.168.56.103: icmp_seq=19 ttl=64 time=2.30 ms
64 bytes from 192.168.56.103: icmp_seq=20 ttl=64 time=2.80 ms
64 bytes from 192.168.56.103: icmp_seq=21 ttl=64 time=1.78 ms
64 bytes from 192.168.56.103: icmp_seq=22 ttl=64 time=2.05 ms
64 bytes from 192.168.56.103: icmp_seq=23 ttl=64 time=1.98 ms
64 bytes from 192.168.56.103: icmp_seq=24 ttl=64 time=2.79 ms
64 bytes from 192.168.56.103: icmp_seq=25 ttl=64 time=2.92 ms
(kali㉿vbox) ~/Desktop
$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=2.12 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.41 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=2.39 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=2.31 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.47 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=1.88 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=1.00 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=2.33 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=1.81 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=0.856 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=1.89 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=64 time=1.99 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=64 time=1.89 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=64 time=1.88 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=64 time=1.71 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=64 time=1.46 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=64 time=1.51 ms
64 bytes from 192.168.56.103: icmp_seq=18 ttl=64 time=1.85 ms
64 bytes from 192.168.56.103: icmp_seq=19 ttl=64 time=1.69 ms
64 bytes from 192.168.56.103: icmp_seq=20 ttl=64 time=2.05 ms
64 bytes from 192.168.56.103: icmp_seq=21 ttl=64 time=1.95 ms
64 bytes from 192.168.56.103: icmp_seq=22 ttl=64 time=1.05 ms
64 bytes from 192.168.56.103: icmp_seq=23 ttl=64 time=1.39 ms
64 bytes from 192.168.56.103: icmp_seq=24 ttl=64 time=1.95 ms
64 bytes from 192.168.56.103: icmp_seq=25 ttl=64 time=1.85 ms
64 bytes from 192.168.56.103: icmp_seq=26 ttl=64 time=1.21 ms
64 bytes from 192.168.56.103: icmp_seq=27 ttl=64 time=1.72 ms
64 bytes from 192.168.56.103: icmp_seq=28 ttl=64 time=1.45 ms
64 bytes from 192.168.56.103: icmp_seq=29 ttl=64 time=1.96 ms
64 bytes from 192.168.56.103: icmp_seq=30 ttl=64 time=1.98 ms
64 bytes from 192.168.56.103: icmp_seq=31 ttl=64 time=1.49 ms
64 bytes from 192.168.56.103: icmp_seq=32 ttl=64 time=3.21 ms
64 bytes from 192.168.56.103: icmp_seq=33 ttl=64 time=2.52 ms
64 bytes from 192.168.56.103: icmp_seq=34 ttl=64 time=1.30 ms
64 bytes from 192.168.56.103: icmp_seq=35 ttl=64 time=1.98 ms
64 bytes from 192.168.56.103: icmp_seq=36 ttl=64 time=2.11 ms
(kali㉿vbox) ~/Desktop
$ ping 192.168.56.103
ping statistics --
747 packets transmitted, 747 received, 0% packet loss, time 747165ms
rtt min/avg/max/mdev = 0.635/2.402/26.050/1.506 ms
```

**Ping <kali ip address>** - can check successfully data packets are transferring.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it displays the command prompt "buddhima@Buddhima:~". Below the prompt, the user runs the command "cd .." followed by "ip a". The output shows the kernel's view of the network interfaces:

```
buddhima@Buddhima:~/Desktop$ cd ..
buddhima@Buddhima:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 584sec preferred_lft 584sec
    inet6 fe80::a00:27ff:fec1:db05/64 scope link
        valid_lft forever preferred_lft forever
buddhima@Buddhima:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=3.52 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=11.9 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=27.7 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=3.27 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=1.11 ms
^C
--- 192.168.56.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4988ms
rtt min/avg/max/mdev = 1.114/9.497/27.651/9.801 ms
buddhima@Buddhima:~$
```

## 2.2. DNS (Domain Name System) Network Service:

DNS can translate human readable domain names into IP addresses. Without DNS it will be very difficult to identify every website.

Step 01: Install DNS server (bind9)

- **Sudo apt update**
- **sudo apt install bind9 bind9utils bind9-doc** - manage the DNS server

```
buddhima@Buddhima: ~$ sudo apt update
[sudo] password for buddhima:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [782 kB]
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,028 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [147 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [191 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [833 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.3 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 kB]
Get:14 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [224 kB]
Get:15 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [161 kB]
Get:16 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Icons (48x48) [34.7 kB]
Get:17 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Icons (64x64) [49.6 kB]
Get:18 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [199 kB]
Get:19 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 kB]
Get:20 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,059 kB]
Get:21 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [268 kB]
Get:22 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [376 kB]
Get:23 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Icons (48x48) [226 kB]
Get:24 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Icons (64x64) [350 kB]
Get:25 http://lk.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 kB]
Get:26 http://lk.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,076 kB]
Get:27 http://lk.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 kB]
Get:28 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [16.4 kB]
Get:29 http://lk.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 kB]
Fetched 6,406 kB in 6s (998 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
122 packages can be upgraded. Run 'apt list --upgradable' to see them.
buddhima@Buddhima: ~$
```

**bind9**- DNS server software. **Bind9utils**- help to manage and troubleshoot. **bind9-doc**- documentation files for bind9.

```
buddhima@Buddhima: ~$ sudo apt install bind9 bind9utils bind9-doc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils
0 upgraded, 4 newly installed, 0 to remove and 122 not upgraded.
Need to get 3,669 kB of archives.
After this operation, 9,244 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-utils amd64 1:9.18.30-0ubuntu0.24.04.2 [159 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9 amd64 1:9.18.30-0ubuntu0.24.04.2 [254 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-doc all 1:9.18.30-0ubuntu0.24.04.2 [3,252 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 bind9utils all 1:9.18.30-0ubuntu0.24.04.2 [3,680 B]
Fetched 3,669 kB in 6s (568 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 149257 files and directories currently installed.)
Preparing to unpack .../bind9-utils_1%3a9.18.30-0ubuntu0.24.04.2_amd64.deb ...
Unpacking bind9-utils (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.18.30-0ubuntu0.24.04.2_amd64.deb ...
Unpacking bind9 (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9-doc.
Preparing to unpack .../bind9-doc_1%3a9.18.30-0ubuntu0.24.04.2_all.deb ...
Unpacking bind9-doc (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.18.30-0ubuntu0.24.04.2_all.deb ...
Unpacking bind9utils (1:9.18.30-0ubuntu0.24.04.2) ...
Setting up bind9-doc (1:9.18.30-0ubuntu0.24.04.2) ...
Setting up bind9-utils (1:9.18.30-0ubuntu0.24.04.2) ...
Setting up bind9 (1:9.18.30-0ubuntu0.24.04.2) ...
Info: Selecting CPIO from source 100 to 200
```

### Step 03: Configure the DNS zone files .

```
buddhima@Buddhima:~$ sudo nano /etc/bind/named.conf.local
[sudo] password for buddhima:
buddhima@Buddhima:~$
```

- **sudo nano /etc/bind/named.conf.local**- using nano editor view the DNS config file,
- Add this part into DNS zone file, **zone "mydomain.local" { type master;**  
**file "/etc/bind/db.mydomain.local";**  
**};**

```
GNU nano 7.2
buddhima@Buddhima:~$ /etc/bind/named.conf.local *
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "mydomain.local"{
    type master;
    file "/etc/bind/db.mydomain.local";
};
```

- zone “mydomain.local”- defines new DNS zone for the domain.
- Type master: define DNS is the primary server for this zone.
- file "/etc/bind/db.mydomain.local": points the DNSS zone file that stores the actual DN records..

### Step 04: Create DNS zone file.

- **sudo cp /etc/bind/db.local /etc/bind/db.mydomain.local**- copy the default DNS zone file to db.mydomain.local file.

```
buddhima@Buddhima:~$ sudo nano /etc/bind/named.conf.local
[sudo] password for buddhima:
buddhima@Buddhima:~$ sudo cp /etc/bind/db.local /etc/bind/db.mydomain.local
[sudo] password for buddhima:
buddhima@Buddhima:~$ sudo nano /etc/bind/db.mydomain.local
buddhima@Buddhima:~$
```

- **sudo nano /etc/bind/db.mydomain.local**- This command explain how DNS server resolve names in mydomain.local.

```

GNU nano 7.2                                buddhima@Buddhima:~ /etc/bind/db.mydomain.local *

;
; BIND data file for local loopback interface
;

$TTL    604800
@       IN      SOA     ns1.mydomain.local. admin.mydomain.local. (
                        3           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                      604800 )    ; Negative Cache TTL
;
@       IN      NS      ns1.mydomain.local.
ns1    IN      A       192.168.56.1
www   IN      A       192.168.56.100

```

- SOA- Identify the primary DNS server.
- NS- Define the domain name server.
- A- Map IP address.

Step 05: Check the errors restart and enable the bind9.

```

buddhima@Buddhima: $ sudo nano /etc/bind/named.conf.local
[sudo] password for buddhima:
buddhima@Buddhima: $
buddhima@Buddhima: $ sudo cp /etc/bind/db.local /etc/bind/db.mydomain.local
[sudo] password for buddhima:
buddhima@Buddhima: $ sudo nano /etc/bind/db.mydomain.local
buddhima@Buddhima: $
buddhima@Buddhima: $ sudo named-checkconf
buddhima@Buddhima: $ sudo named-checkzone mydomain.local /etc/bind/db.mydomain.local
zone mydomain.local/IN: loaded serial 3
OK
buddhima@Buddhima: $
buddhima@Buddhima: $ sudo systemctl restart bind9
buddhima@Buddhima: $ sudo systemctl enable bind9
Failed to enable unit: Refusing to operate on alias name or linked unit file: bind9.service
buddhima@Buddhima: $ 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 Wed 2025-04-30 17:00:14 +0530; 1min 32s ago
     Docs: man:named(8)
 Main PID: 3046 (named)
    Status: "running"
   Tasks: 14 (limit: 4609)
  Memory: 6.8M (peak: 7.6M)
    CPU: 87ms
   CGroup: /system.slice/named.service
           └─3046 /usr/sbin/named -f -u bind

Apr 30 17:00:14 Buddhima named[3046]: zone 0.in-addr.arpa/IN: loaded serial 1
Apr 30 17:00:14 Buddhima named[3046]: zone 255.in-addr.arpa/IN: loaded serial 1
Apr 30 17:00:14 Buddhima named[3046]: zone 127.in-addr.arpa/IN: loaded serial 1
Apr 30 17:00:14 Buddhima named[3046]: zone mydomain.local/IN: loaded serial 3
Apr 30 17:00:14 Buddhima named[3046]: zone localhost/IN: loaded serial 2
Apr 30 17:00:14 Buddhima named[3046]: all zones loaded
Apr 30 17:00:14 Buddhima systemd[1]: Started named.service - BIND Domain Name Server
Apr 30 17:00:14 Buddhima named[3046]: running
Apr 30 17:00:24 Buddhima named[3046]: managed-keys-zone: Unable to fetch DNSKEY set
Apr 30 17:00:24 Buddhima named[3046]: resolver priming query complete: timed out
lines 1-22/22 (END)...skipping...

```

- **Sudo named-checkconf**- check the syntax of bind9 DNS server and make sure there is no mistakes before the server restarts.
- **sudo systemctl restart bind9**- restart it applying any changes that are made in DNS zone file.

- **sudo systemctl enable bind9**- enable bind9 to start automatically.

#### Step 07: Resolve the hostname

- **nslookup db.mydomain.local**- used to resolve the hostname db.mydomain.local into an IP address using DNS
- If it properly configured zone file, bind9 server is running without errors like following output.

```
Server: 192.168.56.10
Address: 192.168.56.10#53
```

```
Name: db.mydomain.local
Address: 192.168.56.10
```

```
~
~
lines 1-22/22 (END)
buddhima@Buddhima: ~ nslookup db.mydomain.local
;; Got SERVFAIL reply from 127.0.0.53
Server:      127.0.0.53
Address:     127.0.0.53#53

** server can't find db.mydomain.local: SERVFAIL
buddhima@Buddhima: ~
```

## 2.3. NTP (Network Time Protocol) Network Service:

Network Time Protocol (NTP) can synchronize the system clock of computer devices. It makes all devices set the same and correct constant time.

Step 01: Install the NTP server.

```
buddhima@Buddhima: $ sudo apt install ntpsec
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-ntp
Suggested packages:
  certbot ntpsec-doc ntpsec-ntpviz
The following packages will be REMOVED:
  systemd-timesyncd
The following NEW packages will be installed:
  ntpsec python3-ntp
0 upgraded, 2 newly installed, 1 to remove and 123 not upgraded.
Need to get 434 kB of archives.
After this operation, 1,032 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 python3-ntp amd64 1.2.2+dfsg1-4build2 [91.2 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntpsec amd64 1.2.2+dfsg1-4build2 [343 kB]
Fetched 434 kB in 6s (76.4 kB/s)
(Reading database ... 149409 files and directories currently installed.)
Removing systemd-timesyncd (255.4-1ubuntu8.5) ...
Selecting previously unselected package python3-ntp.
(Reading database ... 149393 files and directories currently installed.)
Preparing to unpack .../python3-ntp_1.2.2+dfsg1-4build2_amd64.deb ...
Unpacking python3-ntp (1.2.2+dfsg1-4build2) ...
Selecting previously unselected package ntpsec.
Preparing to unpack .../ntpsec_1.2.2+dfsg1-4build2_amd64.deb ...
Unpacking ntpsec (1.2.2+dfsg1-4build2) ...
Setting up python3-ntp (1.2.2+dfsg1-4build2) ...
Setting up ntpsec (1.2.2+dfsg1-4build2) ...

Created symlink /etc/systemd/system/timers.target.wants/ntpsec-rotate-stats.timer → /usr/lib/systemd/system/ntpsec-rotate-stats.timer.
Created symlink /etc/systemd/system/network-pre.target.wants/ntpsec-systemd-netif.path → /usr/lib/systemd/system/ntpsec-systemd-netif.path.
Created symlink /etc/systemd/system/ntp.service → /usr/lib/systemd/system/ntpsec.service.
Created symlink /etc/systemd/system/ntpdp.service → /usr/lib/systemd/system/ntpsec.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ntpsec.service → /usr/lib/systemd/system/ntpsec.service.
Processing triggers for dbus (1.14.10-4ubuntu4.1) ...
Processing triggers for man-db (2.12.0-4ubuntu2) ... #####
buddhima@Buddhima: $
```

- **sudo apt install ntp-** download the NTP package that can automatically sync computer system with internet time servers.

Step 02: Edit the NAT configuration file.

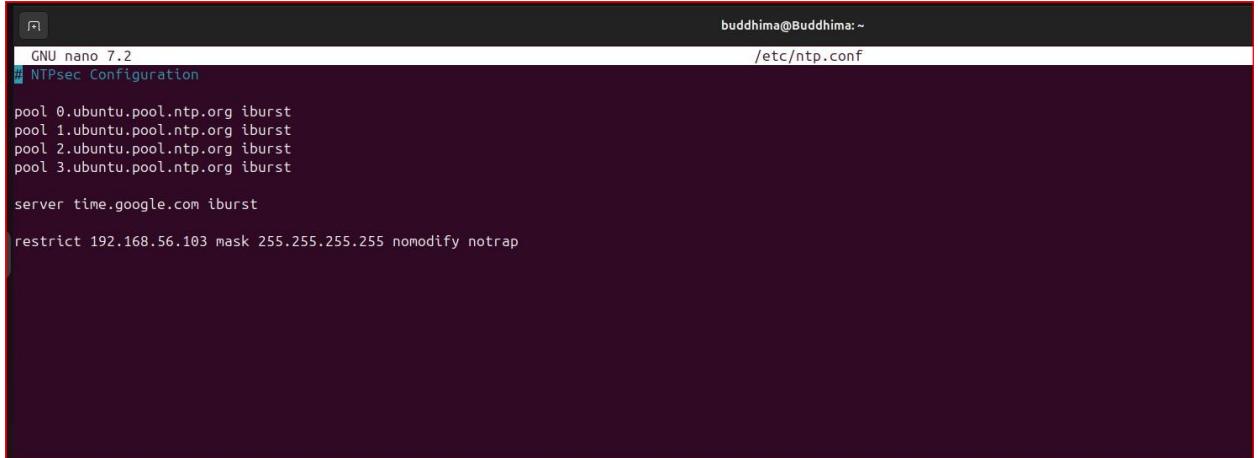
- **sudo nano /etc/ntp.conf-** using nano editor, view the configuration file.

```
buddhima@Buddhima: $ sudo nano /etc/ntp.conf
[sudo] password for buddhima:
buddhima@Buddhima: $
```

- Set NTP servers,  
Server- add each line to, NTP from ubuntu time server pool.  
Iburst- increase the time speed of system sending a burst of packets.

```
server 0.ubuntu.pool.ntp.org iburst server
      1.ubuntu.pool.ntp.org iburst server
      0.ubuntu.pool.ntp.org iburst server
      1.ubuntu.pool.ntp.org iburst
```

- **server time.google.com iburst-** Google public NTP used to set sync the system time.



```

GNU nano 7.2
buddhima@Buddhima: ~
/etc/ntp.conf

pool 0.ubuntu.pool.ntp.org iburst
pool 1.ubuntu.pool.ntp.org iburst
pool 2.ubuntu.pool.ntp.org iburst
pool 3.ubuntu.pool.ntp.org iburst

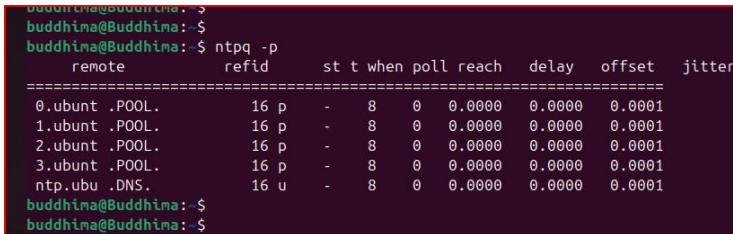
server time.google.com iburst

restrict 192.168.56.103 mask 255.255.255.255 nomodify notrap

```

Step 03: Check the status of NTP server.

- **ntpq -p-** shows a list of sync time with their status.



```

buddhima@Buddhima: ~
buddhima@Buddhima: ~$ ntpq -p
      remote         refid    st t when poll reach   delay    offset  jitter
===== 
 0.ubunt .POOL.        16 p  -  8  0  0.0000  0.0000  0.0001
 1.ubunt .POOL.        16 p  -  8  0  0.0000  0.0000  0.0001
 2.ubunt .POOL.        16 p  -  8  0  0.0000  0.0000  0.0001
 3.ubunt .POOL.        16 p  -  8  0  0.0000  0.0000  0.0001
ntp.ubu .DNS.        16 u  -  8  0  0.0000  0.0000  0.0001
buddhima@Buddhima: ~
buddhima@Buddhima: ~$ 

```

- remote- Hostname or IP of NTP server.
- refid- Sync NTP server.
- st- shows how close the server is to the actual time source
- t- type of connection
- when- seconds since last poll
- poll-polling interval in seconds
- reach- shows success of recent contact attempts
- delay-Round-trip-time
- offset-time difference
- jitter-variability in delay

Step 04: Restart and check the status of NTP.

- **sudo systemctl restart ntpd**- restart the DNS server.
- **sudo systemctl status ntpd**- check the DNS server status is active or failed. If it is active NTP server is running correctly.

```
buddhima@Buddhima:~$  
buddhima@Buddhima:~$ sudo systemctl restart ntpd  
buddhima@Buddhima:~$ sudo systemctl status ntpd  
● ntpsec.service - Network Time Service  
    Loaded: loaded (/usr/lib/systemd/system/ntpsec.service; enabled; priori>  
    Active: active (running) since Thu 2025-05-01 01:56:11 +0530; 26s >  
      Docs: man:ntpd(8)  
    Process: 3799 ExecStart=/usr/libexec/ntpsec/ntp-systemd-wrapper (co>  
   Main PID: 3803 (ntpd)  
     Tasks: 2 (limit: 4609)  
    Memory: 10.8M (peak: 11.3M)  
      CPU: 212ms  
     CGroup: /system.slice/ntpsec.service  
             └─3803 /usr/sbin/ntpd -p /run/ntpd.pid -c /etc/ntpsec/ntp.>  
  
May 01 01:56:31 Buddhima ntpd[3803]: DNS: dns_check: DNS error: -3, Temp>  
May 01 01:56:31 Buddhima ntpd[3803]: DNS: dns_take_status: 3.ubuntu.poo>  
May 01 01:56:32 Buddhima ntpd[3803]: DNS: dns_probe: ntp.ubuntu.com, ca>  
May 01 01:56:32 Buddhima ntpd[3803]: DNS: dns_check: processing ntp.uba>  
May 01 01:56:32 Buddhima ntpd[3803]: DNS: dns_check: DNS error: -3, Temp>  
May 01 01:56:32 Buddhima ntpd[3803]: DNS: dns_take_status: ntp.ubuntu.c>  
lines 2-18
```

Step 05: check the current time.

- **timedatectl**- This command will show the current time status, date, whether its synchronized or not.

```
buddhima@Buddhima:~$  
buddhima@Buddhima:~$  
buddhima@Buddhima:~$ timedatectl  
          Local time: Wed 2025-04-30 23:04:56 +0530  
          Universal time: Wed 2025-04-30 17:34:56 UTC  
            RTC time: Wed 2025-04-30 17:34:56  
          Time zone: Asia/Colombo (+0530, +0530)  
System clock synchronized: yes  
          NTP service: n/a  
RTC in local TZ: no  
buddhima@Buddhima:~$
```

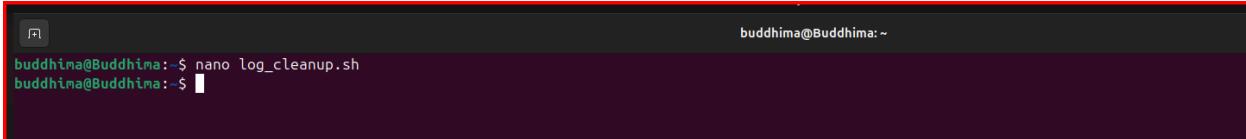
### 3. Security and Other Servers.

#### 3.1. Shell Scripting:

In this section learn the basics of shell scripting syntax creating a shell script file.

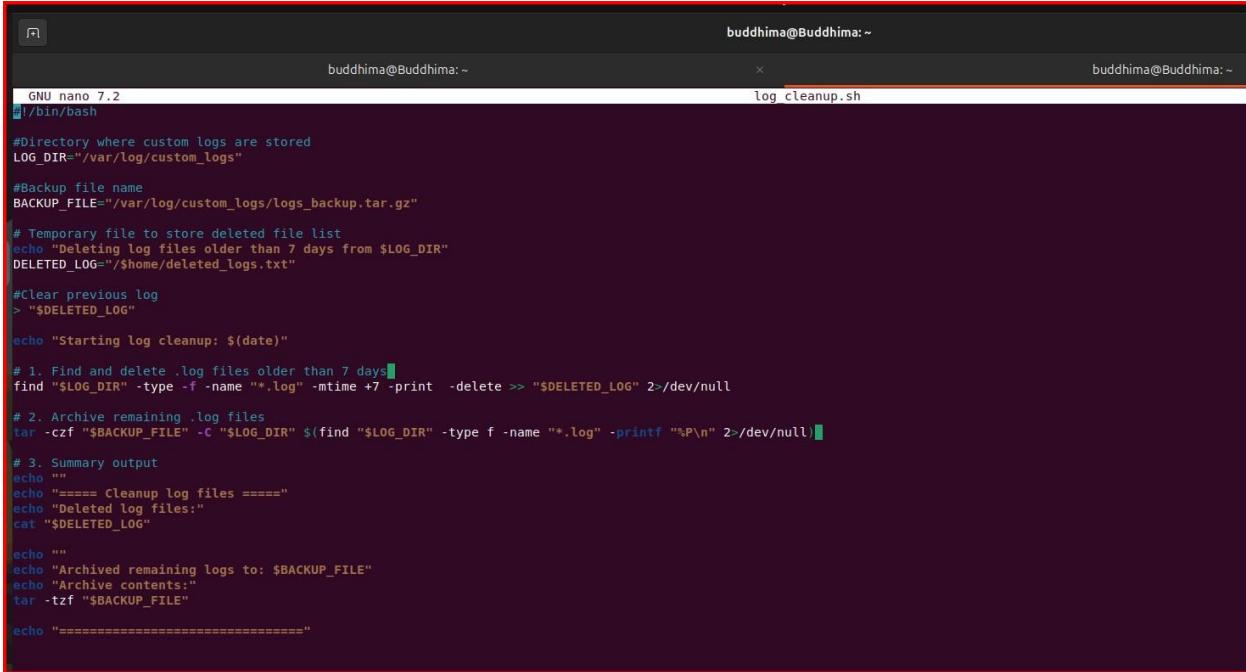
- i. Step 01: Create a script file (`log_cleanup.sh`) to write the bash script.

- **nano log\_cleanup.sh** – create using nano text editor.



```
buddhima@Buddhima:~$ nano log_cleanup.sh
buddhima@Buddhima:~$
```

- Write the script as follows:



```
GNU nano 7.2
#!/bin/bash

#Directory where custom logs are stored
LOG_DIR="/var/log/custom_logs"

#Backup file name
BACKUP_FILE="/var/log/custom_logs/logs_backup.tar.gz"

# Temporary file to store deleted file list
echo "Deleting log files older than 7 days from $LOG_DIR"
DELETED_LOG="/$home/deleted_logs.txt"

#Clear previous log
> "$DELETED_LOG"

echo "Starting log cleanup: $(date)"

# 1. Find and delete .log files older than 7 days
find "$LOG_DIR" -type -f -name "*.log" -mtime +7 -print -delete >> "$DELETED_LOG" 2>/dev/null

# 2. Archive remaining .log files
tar -czf "$BACKUP_FILE" -C "$LOG_DIR" $(find "$LOG_DIR" -type f -name "*.log" -printf "%P\n" 2>/dev/null)

# 3. Summary output
echo ""
echo "===== Cleanup log files ====="
echo "Deleted log files:"
cat "$DELETED_LOG"

echo ""
echo "Archived remaining logs to: $BACKUP_FILE"
echo "Archive contents:"
tar -tzf "$BACKUP_FILE"

echo "=====
```

- This Bash script automatically deletes old log files, archives current logs, and prints a summary to manage disk space efficiently, and is scheduled to run weekly using cron.

**LOG\_DIR="/var/log/custom\_logs"** – Set LOG\_DIR variable to store the custom logs files.

**BACKUP\_FILE="/var/log/custom\_logs/logs\_backup.tar.gz"** – Set BACKUP\_FILE variable to save compressed archived file (.tar.gz) in the same custom log directory.

**DELETED\_LOG="/\$home/deleted\_logs.txt"** – Set TEMP\_DELETED variable to store a list of deleted files.

- `find "$LOG_DIR" -type f -name "*.log" -mtime +7 -print -delete >> "$TEMP_DELETED"`  
`2>/dev/null`

`find`- search for files and directories.

`"$LOG_DIR` – find inside the directory stored in this variable.(path is /var/log/custom\_logs) **type**

**f**- filter that used to find the file type, search to regular files only.

**name "\*.log"** – match the extension that have .log **-mtime**

**+7**- find files that were created 7 days ago.

**-print** – print the full path of matches files.

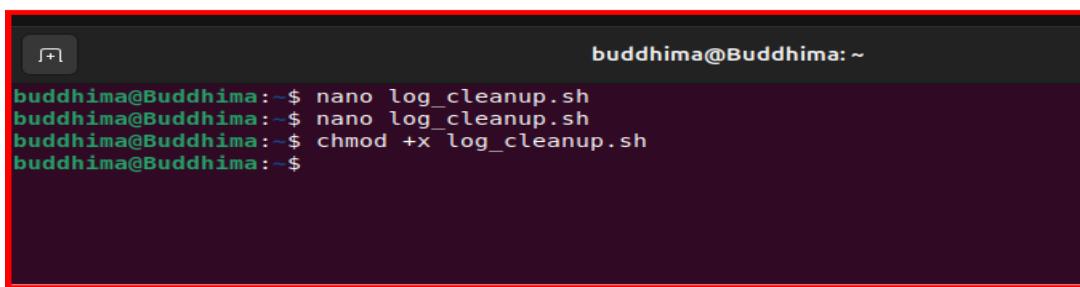
**-delete**- delete the matched file after determining more than 7 days old files.

**>> "\$TEMP\_DELETED"**- display in summary what was deleted previously.

**2>/dev/null**- hide or ignore the error messages.

- `chmod +x log_cleanup.sh` – make the log\_cleanup.sh file executable.

•



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "buddhima@Buddhima: ~". The user has run three commands:

```
buddhima@Buddhima:~$ nano log_cleanup.sh
buddhima@Buddhima:~$ nano log_cleanup.sh
buddhima@Buddhima:~$ chmod +x log_cleanup.sh
buddhima@Buddhima:~$
```

Step 02: Create several dummy files in custom\_logs directory in “/var/log/custom\_logs” .

- **sudo mkdir -p /var/log/custom\_logs** – create a directory using mkdir as **custom\_logs**
- **for i in {1..5}; do sudo touch /var/log/custom\_logs/test\_\$i.log**  
- create 5 dummy log files using for loop done

```
buddhima@Buddhima:~$ sudo mkdir -p /var/log/custom_logs
[sudo] password for buddhima:
buddhima@Buddhima:~$ for i in {1..5}; do
> sudo touch /var/log/custom_logs/test_$i.log
> sudo touch /var/log/custom_logs/test_$i.log
> done
buddhima@Buddhima:~$ cd -p /var/log/custom_logs
bash: cd: -p: invalid option
cd: usage: cd [-L][-P [-e]] [-@J] [dir]
buddhima@Buddhima:~$ cd /var/log/custom_logs
buddhima@Buddhima:/var/log/custom_logs$ ls
test_1.log test_2.log test_3.log test_4.log test_5.log
buddhima@Buddhima:/var/log/custom_logs$
```

- **cd -p /var/log/custom\_logs** - move into **custom\_logs** directory.
- **Ls** – using Ls , to check dummy files are created properly.

Step 03: Test the log\_cleanup.sh file manually.

```
=====
buddhima@Buddhima:~$ sudo ./log_cleanup.sh
Deleting log files older than 7 days from /var/log/custom_logs
Starting log cleanup: Mon May  5 04:46:17 PM +0530 2025

===== Cleanup log files =====
Deleted log files:

Archived remaining logs to: /var/log/custom_logs/logs_backup.tar.gz
Archive contents:
test_5.log
test_3.log
test_1.log
test_4.log
test_2.log
=====
buddhima@Buddhima:~$
```

- **sudo ./log\_cleanup.sh** - using this command test it manually.

#### Step 04: Schedule the script with corn job.

- sudo crontab -e → open the corntab editor.

```
buddhima@Buddhima:~$  
buddhima@Buddhima:~$ sudo crontab -e  
[sudo] password for buddhima:  
no crontab for root - using an empty one  
  
Select an editor. To change later, run 'select-editor'.  
1. /bin/nano <---- easiest  
2. /usr/bin/vim.tiny  
3. /bin/ed  
  
Choose 1-3 [1]: 1  
crontab: installing new crontab  
buddhima@Buddhima:~$ sudo crontab -
```

- **0 0 \* \* 0 /path/to/log\_cleanup.sh** – add this line as mentioned below.

```
buddhima@Buddhima:~$  
buddhima@Buddhima:~$  
GNU nano 7.2  
# 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 0 * * 0 /var/log/log_cleanup.sh  
# Minute 0, Hour 0, Anby day, any month, Day 0 (sunday) is what is implemented
```

- **0 0 \* \* 0** - This part schedule corn runs at 12 A.M every Sunday.
- **/var/log/log\_cleanup.sh** – This part replace with the path of log\_cleanup.sh

```
buddhima@Buddhima:~/Desktop$ cd ..  
buddhima@Buddhima: $ cd /var/log/custom_logs  
buddhima@Buddhima:/var/log/custom_logs$ ls -l  
total 4  
-rw-r--r-- 1 root root 150 May 5 16:46 logs_backup.tar.gz  
-rw-r--r-- 1 root root 0 May 5 15:03 test_1.log  
-rw-r--r-- 1 root root 0 May 5 15:03 test_2.log  
-rw-r--r-- 1 root root 0 May 5 15:03 test_3.log  
-rw-r--r-- 1 root root 0 May 5 15:03 test_4.log  
-rw-r--r-- 1 root root 0 May 5 15:03 test_5.log  
buddhima@Buddhima:/var/log/custom_logs$
```

## 3.2. SSH (Secure Shell):

To configure an SSH server on a Ubuntu for secure remote login using tools like openssh and connect to client machine (kali) remotely.

Step 01: Install the openssh server.

- **sudo apt update**
- **sudo apt install openssh-server -y**

Step 02: Check the status of SSH service.

- **sudo systemctl status ssh – check the status of SSH service is active or fail.**

```
buddhima@Buddhima: $ sudo apt update
[sudo] password for buddhima:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,060 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [228 kB]
Get:7 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [161 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:9 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,061 kB]
Get:10 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [268 kB]
Get:11 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [376 kB]
Get:12 http://lk.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:13 http://lk.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,076 B]
Get:14 http://lk.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Get:15 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [16,4 kB]
Get:16 http://lk.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 3,432 kB in 4s (801 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
131 packages can be upgraded. Run 'apt list --upgradable' to see them.
buddhima@Buddhima: $ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.6p1-3ubuntu13.11).
0 upgraded, 0 newly installed, 0 to remove and 131 not upgraded.
buddhima@Buddhima: $
buddhima@Buddhima: $ 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 Tue 2025-05-06 00:47:31 +0530; 11min ago
    TriggeredBy: ● ssh.socket
      Docs: man:sshd(8)
             man:sshd_config(5)
     Main PID: 1002 (sshd)
        Tasks: 1 (limit: 4609)
       Memory: 2.1M (peak: 2.4M)
          CPU: 267ms
         CGroup: /system.slice/ssh.service
                   └─1002 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 06 00:47:30 Buddhima systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 06 00:47:31 Buddhima sshd[1002]: Server listening on :: port 22.
May 06 00:47:31 Buddhima systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
buddhima@Buddhima: $
```

### Step 03: Verify the connectivity of both server (ubuntu) and client (kali).

```

buddhima@Buddhima: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 527sec preferred_lft 527sec
    inet6 fe80::a00:27ff:fe:c1db%6 scope link
        valid_lft forever preferred_lft forever
buddhima@Buddhima: $
buddhima@Buddhima: $ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=6.28 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=3.06 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=3.02 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=2.82 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=2.70 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=1.70 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=3.82 ms
^C
--- 192.168.56.102 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 7232ms
rtt min/avg/max/mdev = 1.700/3.343/6.275/1.330 ms
buddhima@Buddhima: $
buddhima@Buddhima: $ sudo systemctl status ssh
[sudo] password for buddhima:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset:>)
  Active: active (running) since Tue 2025-05-06 01:02:02 +0530; 14min ago
  TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 959 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUC>
 Main PID: 968 (sshd)
   Tasks: 1 (limit: 4609)
     Memory: 4.1M (peak: 5.4M)
       CPU: 243ms
      CGroup: /system.slice/ssh.service
              └─968 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup"

May 06 01:02:01 Buddhima systemd[1]: Starting ssh.service - OpenBSD Secure Shell...
May 06 01:02:02 Buddhima sshd[968]: Server listening on :: port 22.

```

- ip a – find the IP address. (192.168.56.103)
- ping 192.168.56.102 – If successfully transfer and response confirm bidirectional communication.

```

(kali㉿vbox)-[~/Desktop]
└─$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=2.84 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=1.79 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=1.64 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=2.79 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=2.40 ms
^C
--- 192.168.56.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 1.643/2.202/2.841/0.496 ms

(kali㉿vbox)-[~/Desktop]
└─$ 

```

- ping 192.168.56.103 – If successful response confirms client can access the server.

Step 04:Check the remote connection using SSH client.

- ssh [buddhima@192.168.56.103](mailto:buddhima@192.168.56.103) – Initiate a SSH connection to the machine 192.168.56.103

```
—(kali㉿vbox)-[~/Desktop]
$ 

—(kali㉿vbox)-[~/Desktop]
$ ssh buddhima@192.168.56.103
The authenticity of host '192.168.56.103' (192.168.56.103) can't be established.
ED25519 key fingerprint is SHA256:VMGwI6D5HSrAxhwrerAzKULkEq5Z31EUmjIZpsDgnFM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
buddhima@192.168.56.103's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-24-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.

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

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting
s

Last login: Tue May  6 00:34:41 2025 from 192.168.56.103
buddhima@Buddhima:~$ which ssh
/usr/bin/ssh
buddhima@Buddhima:~$ hostname
Buddhima
buddhima@Buddhima:~$ whoami
buddhima
buddhima@Buddhima:~$ 
```

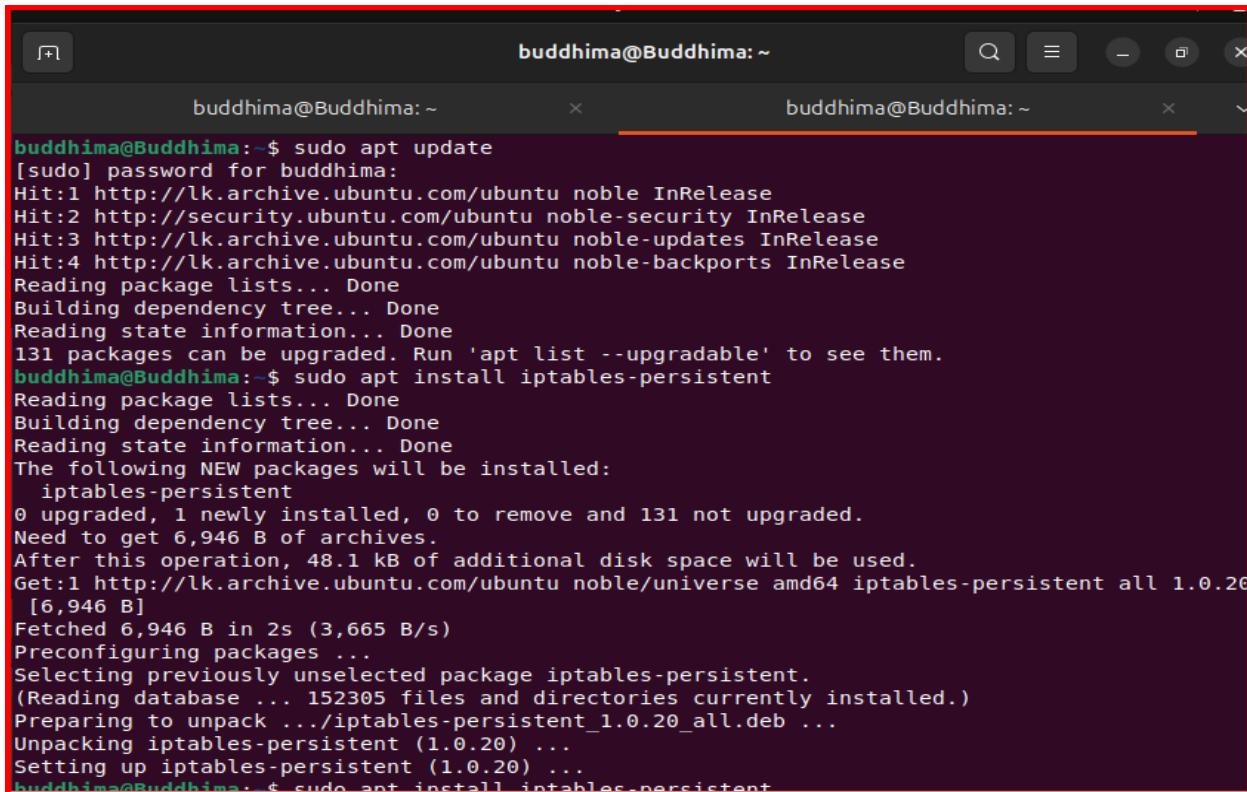
- which ssh- shows the full path of the ssh
- hostname- name of the machine that logged into (ubuntu hostname)
- whoami – user name that currently login , and it confirms the identity of remote machine(ubuntu).

### 3.3. Iptables and ACLs:

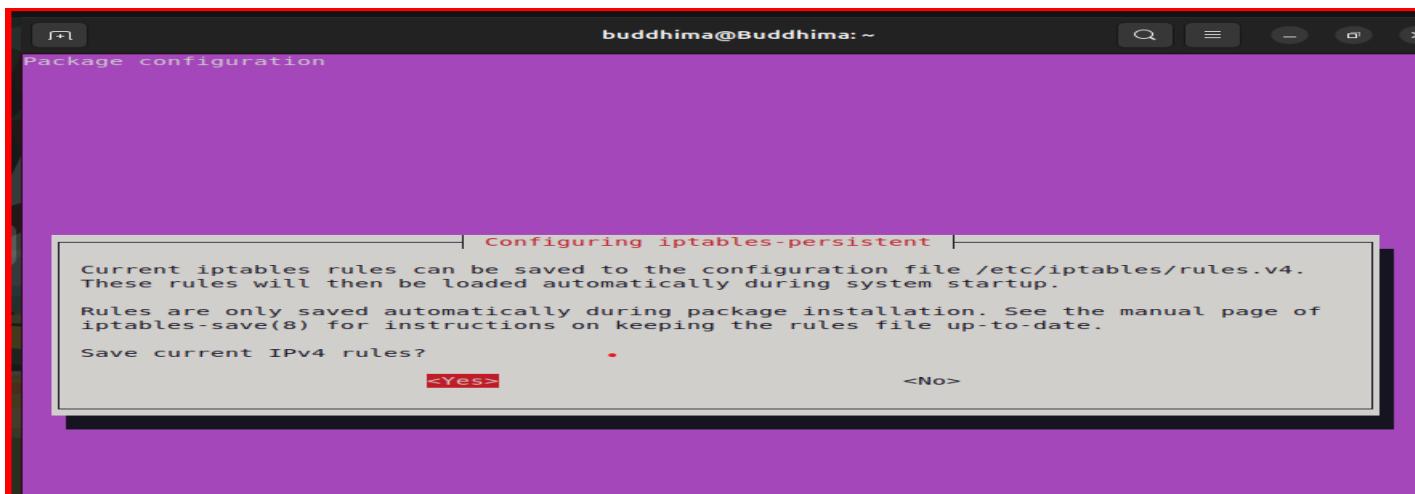
Using firewalls and iptables rules, managing the network traffic. In this section block social media websites like facebook, Instagram and twitter. And block HTTP (port 80) traffic and allow only (port 443) HTTPS and ensure the security of network by defining iptables rules to implement these security services.

Step 01: Install and update

- Sudo apt update
- Sudo apt install iptables-persistent - save iptables rules



```
buddhima@Buddhima:~$ sudo apt update
[sudo] password for buddhima:
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
131 packages can be upgraded. Run 'apt list --upgradable' to see them.
buddhima@Buddhima:~$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  iptables-persistent
0 upgraded, 1 newly installed, 0 to remove and 131 not upgraded.
Need to get 6,946 B of archives.
After this operation, 48.1 kB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 iptables-persistent all 1.0.20
 [6,946 B]
Fetched 6,946 B in 2s (3,665 B/s)
Preconfiguring packages ...
Selecting previously unselected package iptables-persistent.
(Reading database ... 152305 files and directories currently installed.)
Preparing to unpack .../iptables-persistent_1.0.20_all.deb ...
Unpacking iptables-persistent (1.0.20) ...
Setting up iptables-persistent (1.0.20) ...
buddhima@Buddhima:~$ sudo apt install iptables-persistent
```



Step 02: Create iptables rules to block HTTP (port 80) and allow HTTPS (443) .

- **sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT**
- **sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT**

```
buddhima@Buddhima: $  
buddhima@Buddhima: $  
buddhima@Buddhima: $ sudo iptables -A OUTPUT -p tcp --dport 80 -j REJECT  
buddhima@Buddhima: $ sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT  
buddhima@Buddhima: $
```

Step 03: Create iptables rules to block (facebook, Instagram, twitter) specific IP addresses.

- **sudo iptables -A OUTPUT -p tcp -d 157.240.22.35 --dport 443 -j REJECT # Facebook**
- **sudo iptables -A OUTPUT -p tcp -d 31.13.71.36 --dport 443 -j REJECT # Instagram**
- **sudo iptables -A OUTPUT -p tcp -d 104.244.42.129 --dport 443 -j REJECT # Twitter**

```
buddhima@Buddhima: $ sudo iptables -A OUTPUT -p tcp -d 157.240.22.35 --dport 443 -j REJECT  
buddhima@Buddhima: $ sudo iptables -A OUTPUT -d 157.240.0.0/16 -j DROP  
buddhima@Buddhima: $ sudo iptables -A OUTPUT -d 31.13.0.0/16 -j DROP  
buddhima@Buddhima: $ sudo iptables -A OUTPUT -d 104.244.42.0/24 -j DROP  
buddhima@Buddhima: $
```

- **sudo iptables-save > /etc/iptables/rules.v4 – Ensure iptables rules are persist after using this command.**

- **Sudo iptables-save | sudo tee /etc/iptables/rules.v4 >/dev/null** – current iptables rules pipe into tee /etc/iptables/rules.v4

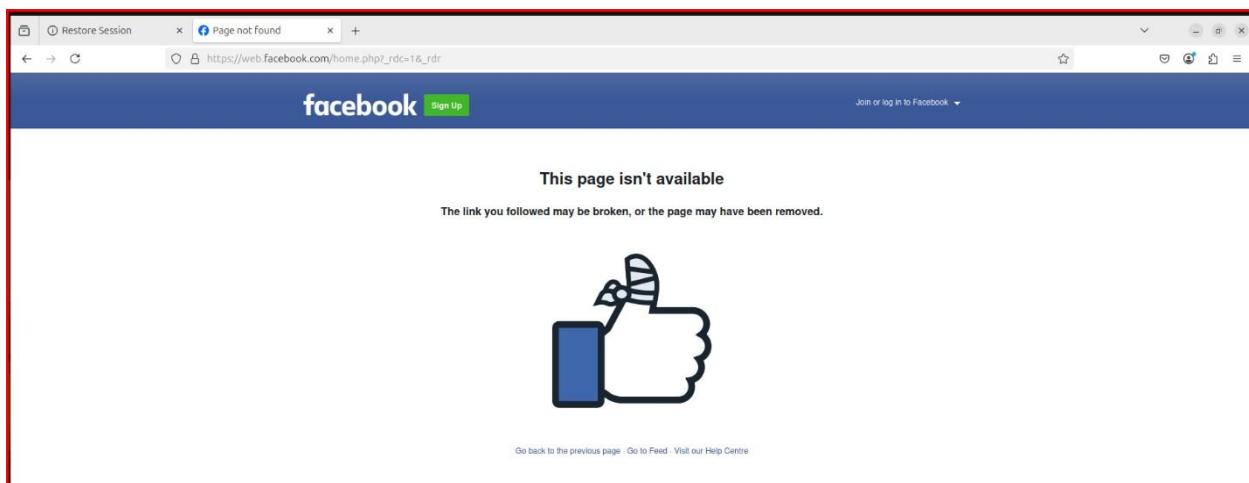
Steps 04: List iptables rules.

- **sudo iptables -L -v -n**  
 -L – List all current rules.  
 -v – Shows detailed output.  
 -n – Prevent DNS lookups for IP addresses and ports.

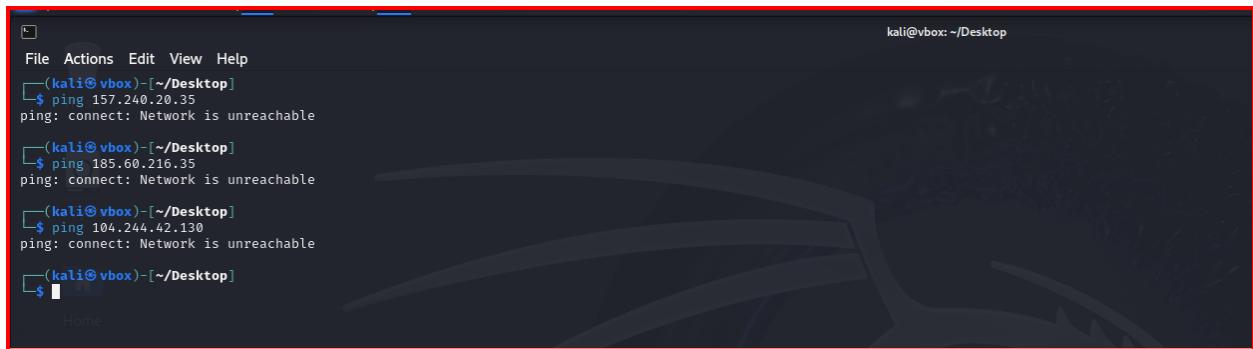
```
buddhima@Buddhima:~$ 
buddhima@Buddhima:~$ sudo iptables-save | sudo tee /etc/iptables/rules.v4 > /dev/null
buddhima@Buddhima:~$ 
buddhima@Buddhima:~$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
Chain OUTPUT (policy ACCEPT 5492 packets, 422K bytes)
pkts bytes target     prot opt in     out    source          destination
  0   0 DROP       6  -- *   *   0.0.0.0/0
  0   0 ACCEPT     6  -- *   *   0.0.0.0/0
  0   0 DROP       0  -- *   *   0.0.0.0/0
buddhima@Buddhima:~$
```

Step 05: Check the IP address are blocked successfully in the server.

- Surfing the browser and try to login [www.facebook.com](https://www.facebook.com)



- Can check it in terminal also.



```
kali@vbox: ~/Desktop
File Actions Edit View Help
(kali㉿vbox) [~/Desktop]
$ ping 157.240.20.35
ping: connect: Network is unreachable

(kali㉿vbox) [~/Desktop]
$ ping 185.60.216.35
ping: connect: Network is unreachable

(kali㉿vbox) [~/Desktop]
$ ping 104.244.42.130
ping: connect: Network is unreachable

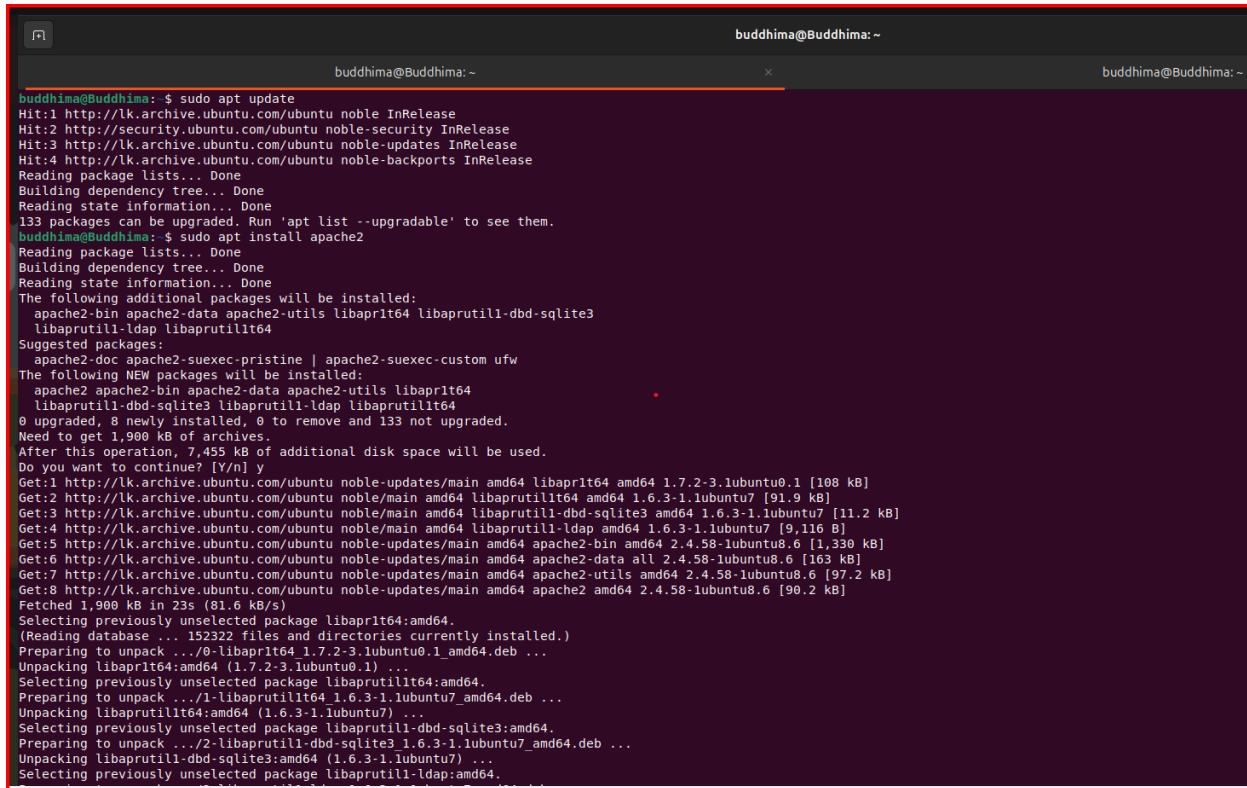
(kali㉿vbox) [~/Desktop]
$
```

### 3.4. WEB Server (Apache):

WEB Server (Apache) is used to deliver web content to clients through the internet. It can handle HTTP/HTTPS requests from clients and respond to it. In this section create a simple web page and configure the web server to serve it in VM using Apache software.

Step 01: Install apache2 and update.

- **sudo apt update**
- **sudo apt install apache2** – Install apache2 sever.



```
buddhima@Buddhima: ~
buddhima@Buddhima: ~
buddhima@Buddhima: $ sudo apt update
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
133 packages can be upgraded. Run 'apt list --upgradable' to see them.
buddhima@Buddhima: $ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
0 upgraded, 8 newly installed, 0 to remove and 133 not upgraded.
Need to get 1,900 kB of archives.
After this operation, 7,455 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 libaprutil1t64 amd64 1.7.2-3.lubuntu0.1 [108 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.lubuntu7 [91.9 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.lubuntu7 [11.2 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.lubuntu7 [9,116 kB]
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-lubuntu8.6 [1,330 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-lubuntu8.6 [163 kB]
Get:7 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-lubuntu8.6 [97.2 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-lubuntu8.6 [90.2 kB]
Fetched 1,900 kB in 23s (81.6 kB/s)
Selecting previously unselected package libapr1t64:amd64.
(Reading database ... 152322 files and directories currently installed.)
Preparing to unpack .../0-libapr1t64 1.7.2-3.lubuntu0.1_amd64.deb ...
Unpacking libapr1t64:amd64 (1.7.2-3.lubuntu0.1) ...
Selecting previously unselected package libaprutil1t64:amd64.
Preparing to unpack .../1-libaprutil1t64_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1t64:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../2-libaprutil1-dbd-sqlite3_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
```

## Step 02: Check the Apache server status

- **sudo systemctl status apache2 – check the Apache server status is successfully activated or fail.**

```
buddhima@Buddhima:/var/www/html$ 
buddhima@Buddhima:/var/www/html$ sudo systemctl status apache2
[sudo] password for buddhima:
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
    Active: active (running) since Tue 2025-05-06 21:06:37 +0530; 4min 22s ago
      Docs: https://httpd.apache.org/docs/2.4/
   Process: 1032 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1117 (apache2)
     Tasks: 55 (limit: 4609)
    Memory: 7.7M (peak: 8.2M)
       CPU: 112ms
      CGroup: /system.slice/apache2.service
              └─1117 /usr/sbin/apache2 -k start
                  ├─1119 /usr/sbin/apache2 -k start
                  ├─1120 /usr/sbin/apache2 -k start

May 06 21:06:37 Buddhima systemd[1]: Starting apache2.service - The Apache HTTP Server.>
May 06 21:06:37 Buddhima apachectl[1087]: AH00558: apache2: Could not reliably determin>
May 06 21:06:37 Buddhima systemd[1]: Started apache2.service - The Apache HTTP Server.
[lines 1-17/17 (END)]
buddhima@Buddhima:/var/www/html$
```

## Step 03: Create a simple web page.

- **cd /var/www/html/ - navigate to root directory of Apache document.**
- **ls – using ls can list the directory and find index.html file.**
- **sudo nano index.html – create index1.html using nano text editor.**

```
buddhima@Buddhima:~$ cd /var/www/html
buddhima@Buddhima:/var/www/html$ ls
index.html
buddhima@Buddhima:/var/www/html$ sudo nano index1.html
[sudo] password for buddhima:
```

- Add the html coding part to create a simple web page.



GNU nano 7.2 index1.html \*

```
<!DOCTYPE html>
<html>
  <head>
    <title>MY Apache Page</title>
  </head>
  <body>
    <h1>Hello from my web server!</h1>
  </body>
</html>
```

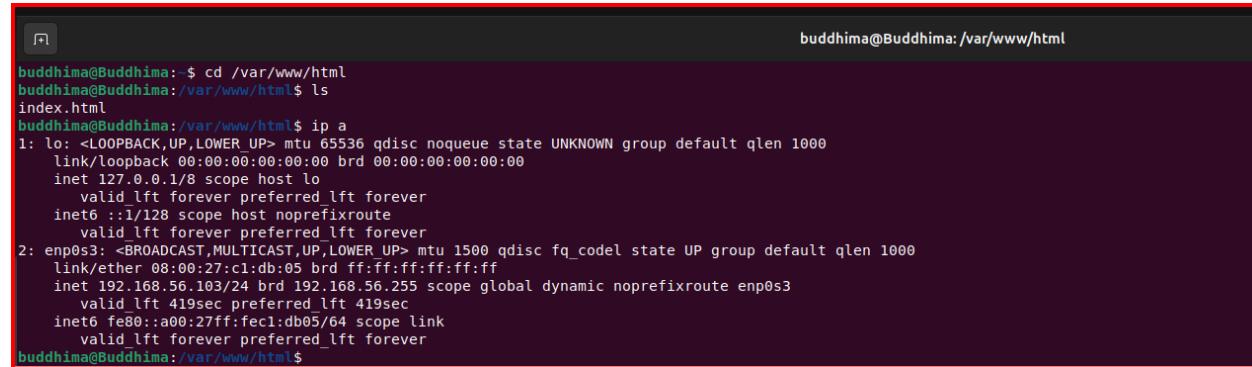
Press CTRL + O to save.

Press Enter to confirm.

Press CTRL + X to exit.

#### Step 04: Check the IP address of server (ubuntu IP address)

- ip a - select the IP address under enp0s3



```
buddhima@Buddhima: ~$ cd /var/www/html
buddhima@Buddhima: /var/www/html$ ls
index.html
buddhima@Buddhima:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:db:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 419sec preferred_lft 419sec
        inet6 fe80::a00:27ff:fed1:db05/64 scope link
            valid_lft forever preferred_lft forever
buddhima@Buddhima:/var/www/html$
```

Step 05: Test in the browser.

- Using <http://192.168.56.103> IP address to test in browser.

A screenshot of a web browser window titled "Index of /". The address bar shows "192.168.56.103". The page content is a table with one row, showing a file named "index1.html" with a size of 154 bytes. A blue arrow points from this screenshot down to the second screenshot.

Name	Last modified	Size	Description
index1.html	2025-05-07 11:16	154	

Apache/2.4.58 (Ubuntu) Server at 192.168.56.103 Port 80

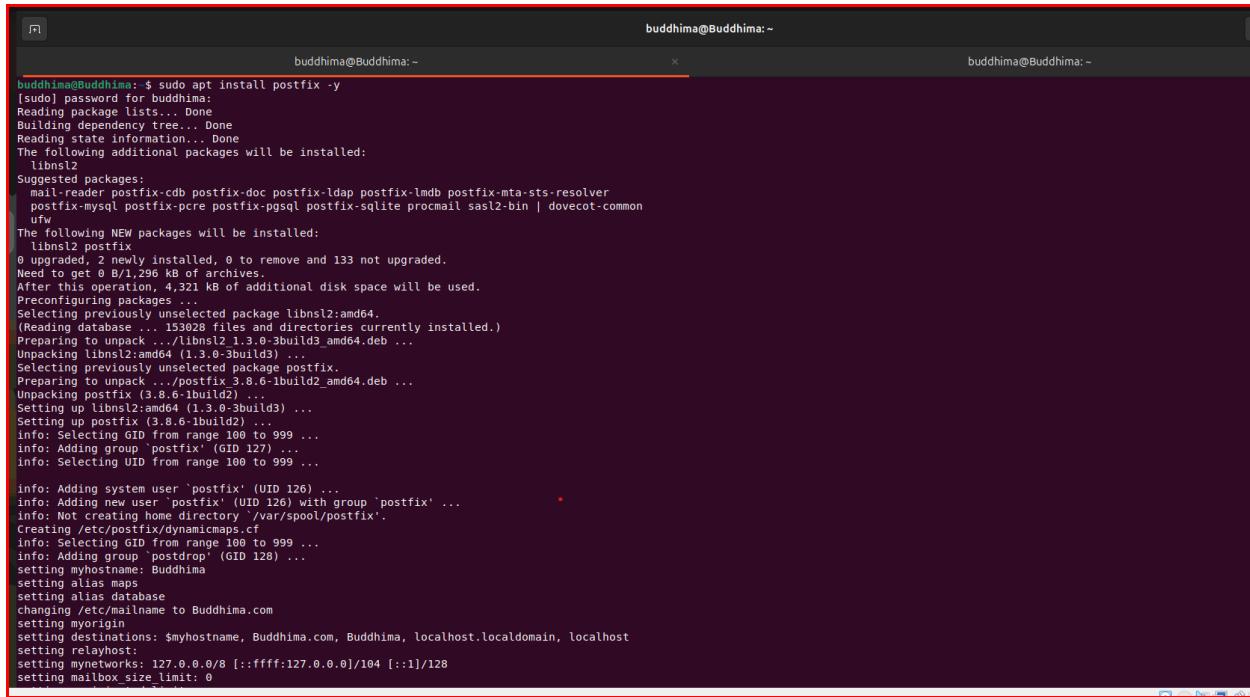
A screenshot of a web browser window titled "MY Apache Page". The address bar shows "192.168.56.103/index1.html". The page content displays the text "Hello from my web server!".

### 3.5. Email Server (postfix):

Email Server is a system where messages can be sent, receives, stores between users. In this section handle send and receive emails.

Step 01: Install postfix server.

- **sudo apt install postfix -y** – Install postfix with its required packages.



```
buddhima@Buddhima:~$ sudo apt install postfix -y
[sudo] password for buddhima:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libns12
Suggested packages:
mail-reader postfix-cdb postfix-doc postfix-ldap postfix-lmdb postfix-mta-sts-resolver
postfix-mysql postfix-pcre postfix-psql postfix-sqlite procmail sasl2-bin | dovecot-common
lswf
The following NEW packages will be installed:
libns12 postfix
0 upgraded, 2 newly installed, 0 to remove and 133 not upgraded.
Need to get 0 B/1,296 kB of archives.
After this operation, 4,321 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package libns12:amd64.
(Reading database ... 153028 files and directories currently installed.)
Preparing to unpack .../libns12_1.3.0-3build3_amd64.deb ...
Unpacking libns12:amd64 (1.3.0-3build3) ...
Selecting previously unselected package postfix.
Preparing to unpack .../postfix_3.8.6-1build2_amd64.deb ...
Unpacking postfix (3.8.6-1build2) ...
Setting up libns12:amd64 (1.3.0-3build3) ...
Setting up postfix (3.8.6-1build2) ...
info: Selecting GID from range 100 to 999 ...
info: Adding group 'postfix' (GID 127) ...
info: Selecting UID from range 100 to 999 ...
info: Adding system user "postfix" (UID 126) ...
info: Adding user "postfix" (UID 126) with group 'postfix' ...
info: Not creating home directory '/var/spool/postfix'.
Creating /etc/postfix/dynamicmaps.cf
info: Selecting GID from range 100 to 999 ...
info: Adding group 'postdrop' (GID 128) ...
setting myhostname: Buddhima
setting alias maps
setting alias database
changing /etc/mailname to Buddhima.com
setting myorigin
setting destinations: $myhostname, Buddhima.com, Buddhima, localhost.localdomain, localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0

```

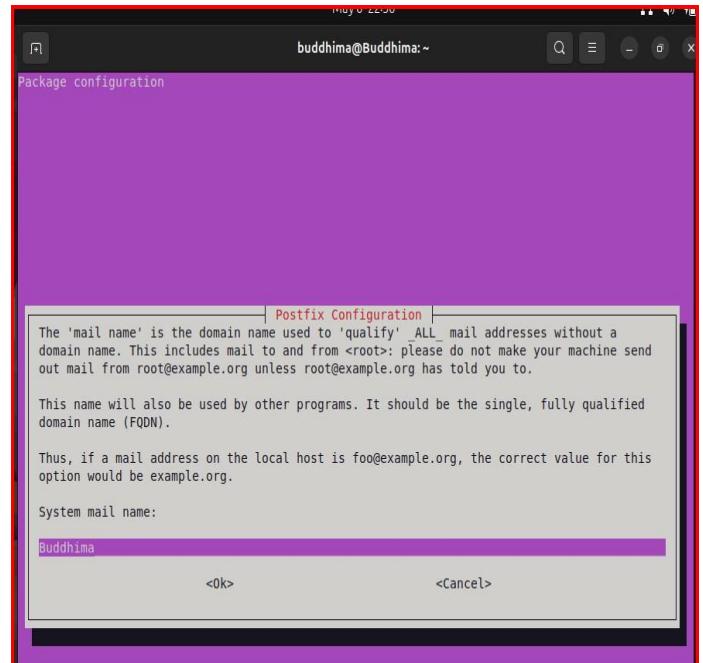
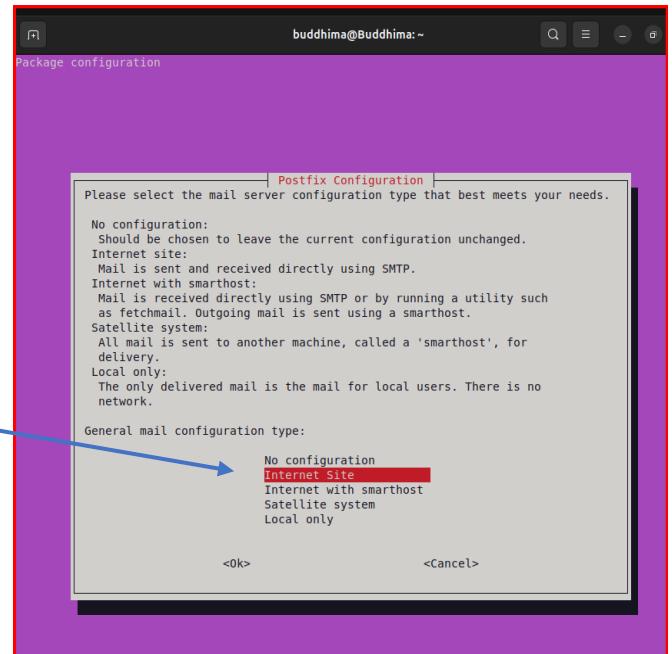
- During the installation,

postfix configurations ask to select the **type of Mail configuration**,

- Select - Internet Site

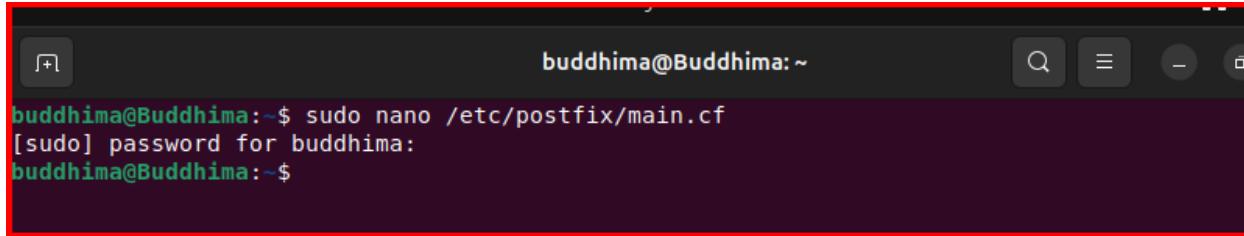
Afterwards there is another selector asking to enter the **System mail name**,

- Enter: Buddhima.com



Step 02: Verify the configuration of postfix.

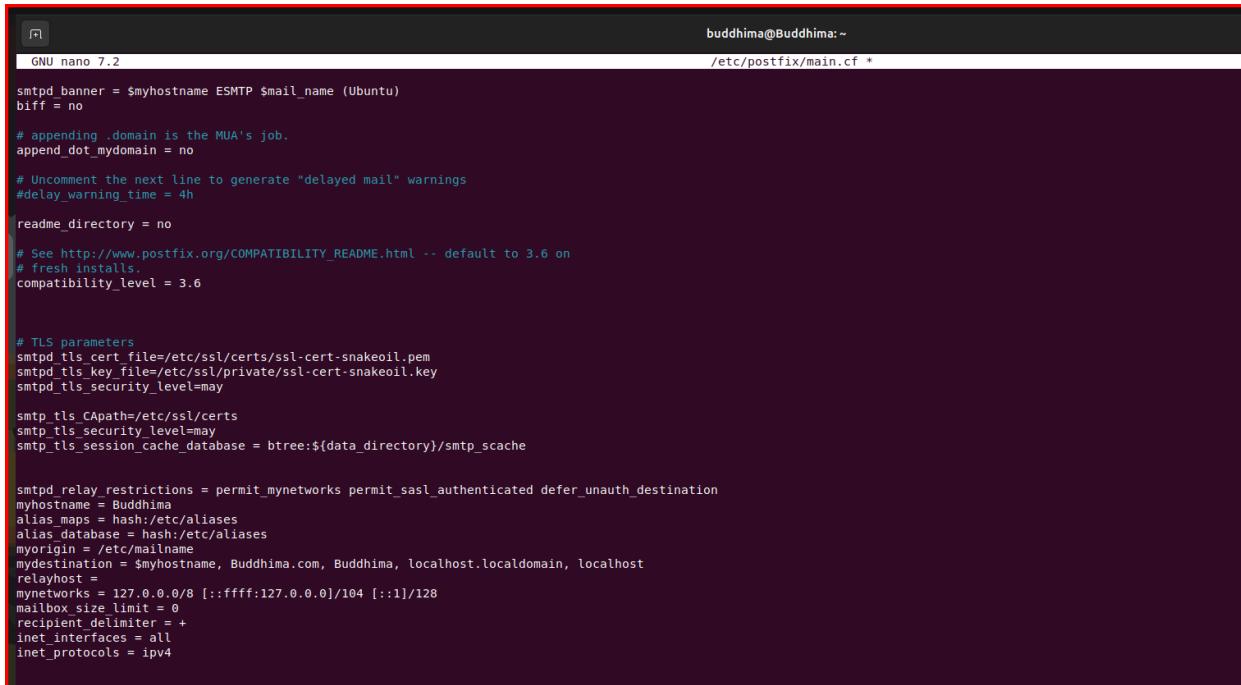
- **sudo nano /etc/postfix/main.cf** – open postfix configuration file using nano text editor.



```
buddhima@Buddhima:~$ sudo nano /etc/postfix/main.cf
[sudo] password for buddhima:
buddhima@Buddhima:~$
```

- Check following lines are modified during the configuration.

```
myhostname = Buddhima.com myorigin
= /etc/mailname
mydestination = $myhostname, localhost.$mydomain, localhost inet_interfaces
= all
inet_protocols = ipv4
```



```
GNU nano 7.2
buddhima@Buddhima:~ /etc/postfix/main.cf *

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
# appending _domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
readme_directory = no
# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

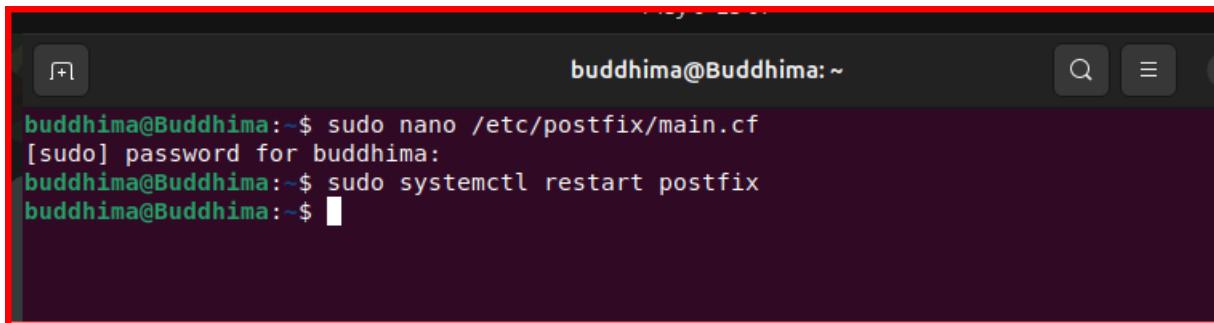
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = Buddhima
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, Buddhima.com, Buddhima, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
```

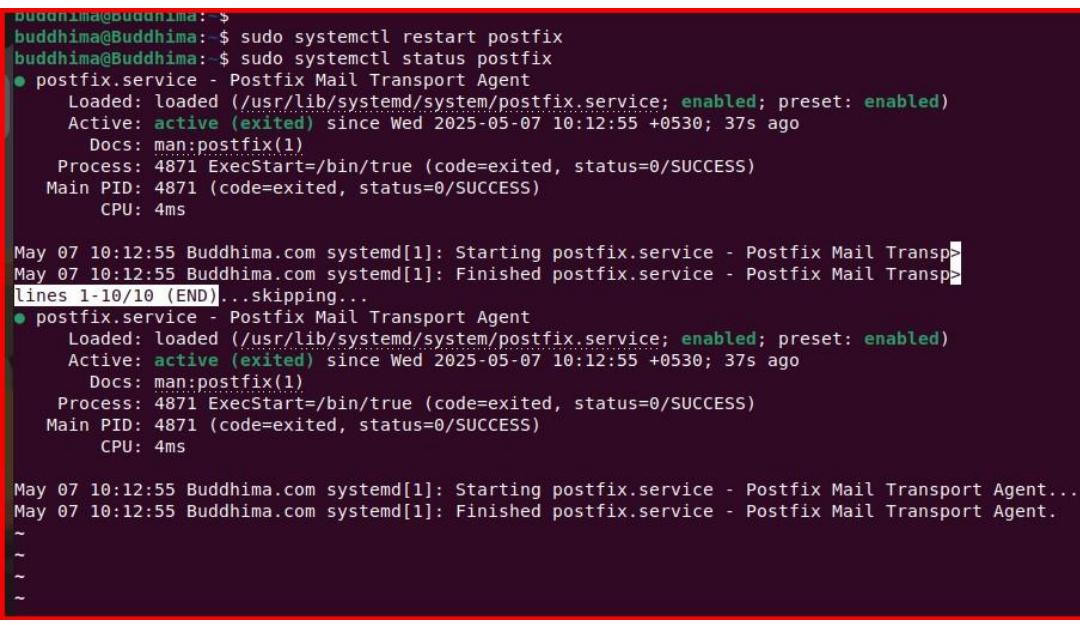
Step 03: Restart and status check of postfix.

- **sudo systemctl restart postfix**



```
buddhima@Buddhima:~$ sudo nano /etc/postfix/main.cf
[sudo] password for buddhima:
buddhima@Buddhima:~$ sudo systemctl restart postfix
buddhima@Buddhima:~$ █
```

- **sudo systemctl status postfix** – check the status of postfix whether it is activated successfully or fail.



```
buddhima@Buddhima:~$ sudo systemctl restart postfix
buddhima@Buddhima:~$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
  Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: enabled)
  Active: active (exited) since Wed 2025-05-07 10:12:55 +0530; 37s ago
    Docs: man:postfix(1)
   Process: 4871 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 4871 (code=exited, status=0/SUCCESS)
    CPU: 4ms

May 07 10:12:55 Buddhima.com systemd[1]: Starting postfix.service - Postfix Mail Transp>
May 07 10:12:55 Buddhima.com systemd[1]: Finished postfix.service - Postfix Mail Transp>
lines 1-10/10 (END)...skipping...
● postfix.service - Postfix Mail Transport Agent
  Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: enabled)
  Active: active (exited) since Wed 2025-05-07 10:12:55 +0530; 37s ago
    Docs: man:postfix(1)
   Process: 4871 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 4871 (code=exited, status=0/SUCCESS)
    CPU: 4ms

May 07 10:12:55 Buddhima.com systemd[1]: Starting postfix.service - Postfix Mail Transport Agent...
May 07 10:12:55 Buddhima.com systemd[1]: Finished postfix.service - Postfix Mail Transport Agent.
~
~
~
~
```

#### Step 04: Install mailutils.

- **sudo apt install mailutils -y** – Installing this server allows to test email from terminal.

```
buddhima@Buddhima:~$ sudo apt install mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl18 libgssglue1 libmailutils9t64 libmysqlclient21
  libntlm0 libpq5 mailutils-common mysql-common
Suggested packages:
  mailutils-mh mailutils-doc
The following NEW packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl18 libgssglue1 libmailutils9t64 libmysqlclient21
  libntlm0 libpq5 mailutils-common mysql-common
0 upgraded, 12 newly installed, 0 to remove and 133 not upgraded.
Need to get 10.3 MB of archives.
After this operation, 67.5 MB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 gsasl-common all 2.2.1-1willsync1build2 [5,056 B]
Get:2 http://lk.archive.ubuntu.com/ubuntu/noble/main amd64 libgc1 amd64 1:8.2.6-1build1 [90.3 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 guile-3.0-libs amd64 3.0.9-1build2 [7,630 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu/noble/main amd64 libgssglue1 amd64 0.9-1build1 [20.7 kB]
Get:5 http://lk.archive.ubuntu.com/ubuntu/noble/main amd64 libntlm0 amd64 1.7-1build1 [19.4 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu/noble/main amd64 libgsasl18 amd64 2.2.1-1willsync1build2 [72.8 kB]
Get:7 http://lk.archive.ubuntu.com/ubuntu/noble/universe amd64 mailutils-common all 1:3.17-1.1build3 [389 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu/noble/main amd64 mysql-common all 5.8+1.1.0build1 [6,746 B]
Get:9 http://lk.archive.ubuntu.com/ubuntu/noble-updates/main amd64 libmysqlclient21 amd64 8.0.42-0ubuntu0.24.04.1 [1,254 kB]
Get:10 http://lk.archive.ubuntu.com/ubuntu/noble-updates/main amd64 libpq5 amd64 16.8-0ubuntu0.24.04.1 [142 kB]
Get:11 http://lk.archive.ubuntu.com/ubuntu/noble/universe amd64 libmailutils9t64 amd64 1:3.17-1.1build3 [514 kB]
Get:12 http://lk.archive.ubuntu.com/ubuntu/noble/universe amd64 mailutils amd64 1:3.17-1.1build3 [127 kB]
Fetched 10.3 MB in 9s (1,151 kB/s)
Selecting previously unselected package gsasl-common.
(Reading database ... 153231 files and directories currently installed.)
Preparing to unpack .../00-gsasl-common_2.2.1-1willsync1build2_all.deb ...
Unpacking gsasl-common (2.2.1-1willsync1build2) ...
Selecting previously unselected package libgc1:amd64.
Preparing to unpack .../01-libgc1_1%3a8.2.6-1build1_amd64.deb ...
Unpacking libgc1:amd64 (1:8.2.6-1build1) ...
Selecting previously unselected package guile-3.0-libs:amd64.
Preparing to unpack .../02-guile-3.0-libs_3.0.9-1build2_amd64.deb ...
```

#### Step 05: Add a new user.

- **sudo adduser testuser**

```
buddhima@Buddhima:~$ 
buddhima@Buddhima:~$ sudo adduser testuser
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1001) ...
info: Adding new user `testuser' (1001) with group `testuser (1001)' ...
info: Creating home directory `/home/testuser' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n] y
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Adding user `testuser' to group `users' ...
buddhima@Buddhima:~$
```

Step 06: Send a test email.

- **echo "Hello from Postfix!" | mail -s "Test Email" testuser** – send a email to testuser
- **sudo su – testuser** – switch user (switch to testuser)

Step 07: Check the testuser's mailbox.

- **mail** – using this command can read the message.
- **q** – press q to exit
- **exit** – to logout from new user account.

```
buddhima@Buddhima:~$ echo "Hello from Postfix!" | mail -s "Test Email" testuser
buddhima@Buddhima:~$ sudo su - testuser
testuser@Buddhima:~$ mail
"/var/mail/testuser": 1 message 1 new
>N 1 Buddhima             Wed May  7 11:03 13/444  Test Email
?
Interrupt
? q
Held 1 message in /var/mail/testuser
You have mail in /var/mail/testuser
testuser@Buddhima:~$ exit
logout
buddhima@Buddhima:~$ █
```

## 4. Linux GDB.

This section focuses on **analyzing the behavior of an executable program using GNU Debugger (GDB)** and **monitoring its impact on the file system**. The goal is to understand how the program executes, what files it creates or modifies, and how it generates and processes output data.

**Download the Executable file from here -**

[https://drive.google.com/drive/folders/19didjVba\\_W49b6RyrXOKHIEHmiAmGrk6?usp=drive\\_link](https://drive.google.com/drive/folders/19didjVba_W49b6RyrXOKHIEHmiAmGrk6?usp=drive_link)

Step 01: Check your system architecture

First, the system architecture was identified using the uname -m command. Based on the detected architecture (such as x86\_64, i686, or arm), the appropriate executable file was selected from the provided assignment files to ensure compatibility.

- **uname -m - x86\_64, choose the 64-bit executable.**
- **Cd /home/Buddhima/Download – navigate to this directory and give ls command**
- **Cd Executable - navigate to Execute directory and ls**
- **Cd Executable - navigate to Executable directory and give ls command**
- **Chmod +x x86\_64 – execute x86\_64**
- **Sudo ./x86\_64 – run this file**
- **Then it rename it usin IT236 [REDACTED]**

```

buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$ uname -m
x86_64
buddhima@Buddhima:~/Desktop$ cd /home/buddhima/Downloads
buddhima@Buddhima:~/Downloads$ ls
Executables 'Executables(1).zip' Executables.zip
buddhima@Buddhima:~/Downloads$ cd Executables
buddhima@Buddhima:~/Downloads/Executables$ ls
Executables _MACOSX
buddhima@Buddhima:~/Downloads/Executables$ cd Executables
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM x86_64
buddhima@Buddhima:~/Downloads/Executables$ chmod +x x86_64
buddhima@Buddhima:~/Downloads/Executables$ sudo ./x86_64
Enter the student IT number: IT23611788
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM IT23611788
buddhima@Buddhima:~/Downloads/Executables$ sudo ./IT23611788
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM data.txt IT23611788
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM data.txt IT23611788
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
WM[buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ xxd data.txt
00000000: 0d57 4d5b .WM[
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ gdb ./IT23611788
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY to the extent permitted by law.

```

### Step 02: Run the Selected Executable

- The selected executable was run with **root privileges**. During execution, the program prompted for an IT number.  
`sudo ./IT23611788`
- After providing the IT number, the program generated a **new executable file named after the entered IT number**.

### Step 3: Analyze the Generated Executable

The newly created executable was executed. This execution resulted in the creation of a text file named **data.txt**.

The contents of this file were examined to identify patterns, encoded data, suspicious outputs, or hidden information.

Run the new executable:

- `./IT23611788`

Analyze data.txt:

```

buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
WM[buddhima@Buddhima:~/Downloads/Executables$ 

```

## Step 04: Debug the New Executable Using GDB

Start GDB:

gdb ./IT23

```
uddhima@Buddhima: ~/Downloads/Executables$  
uddhima@Buddhima: ~/Downloads/Executables$ Executables$  
uddhima@Buddhima: ~/Downloads/Executables$ Executables$ gdb ./IT23 [REDACTED]  
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git  
Copyright (C) 2024 Free Software Foundation, Inc.  
.license GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>  
.this is free software: you are free to change and redistribute it.  
.there is NO WARRANTY to the extent permitted by law.
```

Analyze the flow of execution:

(gdb) run- Start running the program within GDB:

(gdb) break main- Set a breakpoint at the start:

```
buddhima@Buddhima: ~/Downloads/Executables/Executables
```

```
GNU gdb (Ubuntu 15.0.50-20240403-0ubuntu1) 15.0.50-20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
  <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for symbols related to "word"...
Reading symbols from ./IT23
(gdb) run
Starting program: /home/buddhima/Downloads/Executables/Executables/IT23

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Download separate debug info for system-supplied DSO at 0x7ffff7fc3000
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching after vfork from child process 4851]
[sudo] password for buddhima:
Error creating data.txt!
[Inferior 1 (process 4847) exited with code 01]
(gdb) break main
Breakpoint 1 at 0x5555555552f: file IT23.c, line 13.
(gdb) run
Starting program: /home/buddhima/Downloads/Executables/Executables/IT23
```

(Gdb) disassemble

```

Quit
(gdb) disassemble main
Dump of assembler code for function main:
0x0000555555552f0 <+0>:    endbr64
0x0000555555552f4 <+4>:    push   %rbp
0x0000555555552f5 <+5>:    mov    %rsp,%rbp
0x0000555555552f8 <+8>:    sub    $0x60,%rsp
0x0000555555552fc <+12>:   mov    %fs:0x28,%rax
0x000055555555305 <+21>:   mov    %rax,-0x8(%rbp)
0x000055555555309 <+25>:   xor    %eax,%eax
=> 0x00005555555530b <+27>:   lea    0xcf6(%rip),%rax      # 0x555555556008
0x000055555555312 <+34>:   mov    %rax,%rsi
0x000055555555315 <+37>:   lea    0xcf4(%rip),%rax      # 0x555555556010
0x00005555555531c <+44>:   mov    %rax,%rdi
0x00005555555531f <+47>:   call   0x55555555160 <open@plt>
0x000055555555324 <+52>:   mov    %rax,-0x58(%rbp)
0x000055555555328 <+56>:   cmpq   $0x0,-0x58(%rbp)
0x00005555555532d <+61>:   jne    0x55555555348 <main+88>
0x00005555555532f <+63>:   lea    0xd02(%rip),%rax      # 0x555555556038
0x000055555555336 <+70>:   mov    %rax,%rdi
0x000055555555339 <+73>:   call   0x555555550e0 <puts@plt>
0x00005555555533e <+78>:   mov    $0x1,%eax
0x000055555555343 <+83>:   jmp    0x55555555400 <main+272>
0x000055555555348 <+88>:   mov    -0x58(%rbp),%rdx
0x00005555555534c <+92>:   lea    -0x40(%rbp),%rax
0x000055555555350 <+96>:   mov    $0x32,%esi
0x000055555555355 <+101>:  mov    %rax,%rdi
0x000055555555358 <+104>:  call   0x55555555150 <fgets@plt>
0x00005555555535d <+109>:  mov    -0x58(%rbp),%rax
0x000055555555361 <+113>:  mov    %rax,%rdi
0x000055555555364 <+116>:  call   0x55555555120 <pclose@plt>
0x000055555555369 <+121>:  lea    -0x40(%rbp),%rax
0x00005555555536d <+125>:  lea    0xcda(%rip),%rdx      # 0x55555555604e
0x000055555555374 <+132>:  mov    %rdx,%rsi
0x000055555555377 <+135>:  mov    %rax,%rdi
0x00005555555537a <+138>:  call   0x55555555140 <strcspn@plt>
0x00005555555537f <+143>:  movb   $0x0,-0x40(%rbp,%rax,1)
0x000055555555384 <+148>:  lea    0xcc5(%rip),%rax      # 0x555555556050
0x00005555555538b <+155>:  mov    %rax,-0x50(%rbp)
0x00005555555538f <+159>:  mov    -0x50(%rbp),%rdx
0x000055555555393 <+163>:  lea    -0x40(%rbp),%rax
0x000055555555397 <+167>:  mov    %rdx,%rsi
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
(gdb) exit

```

Step 05: Determine the Contents of data.txt

```
Birth: 2025-05-07 13:13:54.236630593 +0530
buddhima@Buddhima:~/Downloads/Executables/Executables$ sudo ./IT23 [REDACTED]
[sudo] password for buddhima:
buddhima@Buddhima:~/Downloads/Executables/Executables$ stat data.txt
  File: data.txt
  Size: 4          Blocks: 8          IO Block: 4096   regular file
Device: 8,2      Inode: 1577942      Links: 1
Access: (0644/-rw-r--r--) Uid: (    0/  root)  Gid: (    0/  root)
Access: 2025-05-07 13:17:59.003019236 +0530
Modify: 2025-05-07 14:13:42.730991373 +0530
Change: 2025-05-07 14:13:42.730991373 +0530
 Birth: 2025-05-07 13:13:54.236630593 +0530
buddhima@Buddhima:~/Downloads/Executables/Executables$ ls -l
total 96
-rw-rw-r-- 1 buddhima buddhima 70824 Mar 17 06:26 ARM
-rw-r--r-- 1 root      root      4 May  7 14:13 data.txt
-rwxr-xr-x 1 root      root     20368 May  7 13:08 IT23 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables/Executables$ cat data.txt
WM[buddhima@Buddhima:~/Downloads/Executables/Executables$]
buddhima@Buddhima:~/Downloads/Executables/Executables$ base64 -d data.txt
base64: invalid input
buddhima@Buddhima:~/Downloads/Executables/Executables$ xxd data.txt
00000000: 0d57 4d5b .WM[
buddhima@Buddhima:~/Downloads/Executables/Executables$ hexdump -C data.txt
00000000  0d 57 4d 5b                                | .WM[ |
00000004
buddhima@Buddhima:~/Downloads/Executables/Executables$ strings ./IT23 [REDACTED]
/lib64/ld-linux-x86-64.so.2
fgets
```

## Step 07:

### 1. Execution Process:

```
buddhima@Buddhima:~/Desktop$ 
buddhima@Buddhima:~/Desktop$ uname -m
x86_64
buddhima@Buddhima:~/Desktop$ cd /home/buddhima/Downloads
buddhima@Buddhima:~/Downloads$ ls
Executables 'Executables(1).zip' Executables.zip
buddhima@Buddhima:~/Downloads$ cd Executables
buddhima@Buddhima:~/Downloads/Executables$ ls
Executables _MACOSX
buddhima@Buddhima:~/Downloads/Executables$ cd Executables
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM x86_64
buddhima@Buddhima:~/Downloads/Executables$ chmod +x x86_64
buddhima@Buddhima:~/Downloads/Executables$ sudo ./x86_64
Enter the student IT number: IT2 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM IT23 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables$ sudo ./IT23 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM data.txt IT23 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
buddhima@Buddhima:~/Downloads/Executables$ ls
ARM data.txt IT23 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables$ cat data.txt
[REDACTED]@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ xxd data.txt
00000000: 0d57 4d5b .WMI
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ 
buddhima@Buddhima:~/Downloads/Executables$ gdb ./IT23 [REDACTED]
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY to the extent permitted by law.
```

### 2. Debugging Process:

System calls- **puts@plt** - Calls the puts() function (prints a null-terminated string with a newline to stdout).

**fgets@plt** - Calls fgets() (reads a line from a file or stdin into a buffer, up to a given size).

**popen@plt** - Calls popen() (opens a process by creating a pipe, used for running shell commands and reading their output).

**strcspn@plt** -Calls strcspn() (calculates the length of the initial segment of a string that does **not** contain any characters from another string).

This refers to the instruction located 88 bytes (or so) into the main() function. This is used **main+88** in debugging to refer to a specific location inside a function.

Similarly, this is the offset 272 bytes into main(). GDB might show breakpoints or **main+272** execution state here.

```
Quit
(gdb) disassemble main
Dump of assembler code for function main:
0x000055555552f0 <+0>:    endbr64
0x000055555552f4 <+4>:    push   %rbp
0x000055555552f5 <+5>:    mov    %rsp,%rbp
0x000055555552f8 <+8>:    sub    $0x60,%rsp
0x000055555552fc <+12>:   mov    %fs:0x28,%rax
0x00005555555305 <+21>:   mov    %rax,-0x8(%rbp)
0x00005555555309 <+25>:   xor    %eax,%eax
=>0x0000555555530b <+27>:   lea    0xcf6(%rip),%rax      # 0x555555556008
0x00005555555312 <+34>:   mov    %rax,%rsi
0x00005555555315 <+37>:   lea    0xcf4(%rip),%rax      # 0x555555556010
0x0000555555531c <+44>:   mov    %rax,%rdi
0x0000555555531f <+47>:   call   0x555555555160 <popen@plt>
0x00005555555324 <+52>:   mov    %rax,-0x58(%rbp)
0x00005555555328 <+56>:   cmpq   $0x0,-0x58(%rbp)
0x0000555555532d <+61>:   jne    0x55555555348 <main+88>
0x0000555555532f <+63>:   lea    0xd02(%rip),%rax      # 0x555555556038
0x00005555555336 <+70>:   mov    %rax,%rdi
0x00005555555339 <+73>:   call   0x5555555550e0 <puts@plt>
0x0000555555533e <+78>:   mov    $0x1,%eax
0x00005555555343 <+83>:   jmp    0x55555555400 <main+272>
0x00005555555348 <+88>:   mov    -0x58(%rbp),%rdx
0x0000555555534c <+92>:   lea    -0x40(%rbp),%rax
0x00005555555350 <+96>:   mov    $0x32,sesi
0x00005555555355 <+101>:  mov    %rax,%rdi
0x00005555555358 <+104>:  call   0x55555555150 <fgets@plt>
0x0000555555535d <+109>:  mov    -0x58(%rbp),%rax
0x00005555555361 <+113>:  mov    %rax,%rdi
0x00005555555364 <+116>:  call   0x55555555120 <pclose@plt>
0x00005555555369 <+121>:  lea    -0x40(%rbp),%rax
0x0000555555536d <+125>:  lea    0xcda(%rip),%rdx      # 0x55555555604e
0x00005555555374 <+132>:  mov    %rdx,%rsi
0x00005555555377 <+135>:  mov    %rax,%rdi
0x0000555555537a <+138>:  call   0x55555555140 <strcspn@plt>
0x0000555555537f <+143>:  movb  $0x0,-0x40(%rbp,%rax,1)
0x00005555555384 <+148>:  lea    0xcc5(%rip),%rax      # 0x555555556050
0x0000555555538b <+155>:  mov    %rax,-0x50(%rbp)
0x0000555555538f <+159>:  mov    -0x50(%rbp),%rdx
0x00005555555393 <+163>:  lea    -0x40(%rbp),%rax
0x00005555555397 <+167>:  mov    %rdx,%rsi
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
(gdb) exit
```

### 3.File System Analysis

- Stat data.txt – shows static data of data.txt file.

```
buddhima@Buddhima:~/Downloads/Executables/Executables$ 
buddhima@Buddhima:~/Downloads/Executables/Executables$ stat data.txt
  File: data.txt
  Size: 4          Blocks: 8          IO Block: 4096   regular file
Device: 8,2      Inode: 1577942      Links: 1
Access: (0644/-rw-r--r--) Uid: (    0/      root)  Gid: (    0/      root)
Access: 2025-05-07 13:17:59.003019236 +0530
Modify: 2025-05-07 13:13:54.236630593 +0530
Change: 2025-05-07 13:13:54.236630593 +0530
 Birth: 2025-05-07 13:13:54.236630593 +0530
buddhima@Buddhima:~/Downloads/Executables/Executables$ 
buddhima@Buddhima:~/Downloads/Executables/Executables$ sudo ./IT236 [REDACTED]
[sudo] password for buddhima:
buddhima@Buddhima:~/Downloads/Executables/Executables$ stat data.txt
  File: data.txt
  Size: 4          Blocks: 8          IO Block: 4096   regular file
Device: 8,2      Inode: 1577942      Links: 1
Access: (0644/-rw-r--r--) Uid: (    0/      root)  Gid: (    0/      root)
Access: 2025-05-07 13:17:59.003019236 +0530
Modify: 2025-05-07 14:13:42.730991373 +0530
Change: 2025-05-07 14:13:42.730991373 +0530
 Birth: 2025-05-07 13:13:54.236630593 +0530
buddhima@Buddhima:~/Downloads/Executables/Executables$ ls -l
total 96
-rw-rw-r-- 1 buddhima buddhima 70824 Mar 17 06:26 ARM
-rw-r--r-- 1 root      root      4 May  7 14:13 data.txt
-rwxr-xr-x 1 root      root     20368 May  7 13:08 IT236 [REDACTED]
buddhima@Buddhima:~/Downloads/Executables/Executables$
```

- Hexdump -C data.txt – convert into hexa value

```
buddhima@Buddhima:~/Downloads/Executables/Executables$ 
buddhima@Buddhima:~/Downloads/Executables/Executables$ hexdump -C data.txt
00000000  0d 57 4d 5b  |.WM[|
00000004
buddhima@Buddhima:~/Downloads/Executables/Executables$ 
buddhima@Buddhima:~/Downloads/Executables/Executables$ strings ./IT236 [REDACTED]
/lib64/ld-linux-x86-64.so.2
fgets
stack_chk_fail
```

#### 4. Analysis of "data.txt"

- Cat data.txt = display the encrypt message.

```
buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ cat data.txt  
WM[buddhima@Buddhima:~/Downloads/Executables/Executables$
```

- Source of the contents of data.txt

```
Birth: 2025-05-07 13:13:54.236630593 +0530  
buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ sudo ./IT23  
[sudo] password for buddhima:  
buddhima@Buddhima:~/Downloads/Executables/Executables$ stat data.txt  
  File: data.txt  
  Size: 4          Blocks: 8          IO Block: 4096   regular file  
Device: 8,2      Inode: 1577942      Links: 1  
Access: (0644/-rw-r--r--) Uid: (     0/    root)  Gid: (     0/    root)  
Access: 2025-05-07 13:17:59.003019236 +0530  
Modify: 2025-05-07 14:13:42.730991373 +0530  
Change: 2025-05-07 14:13:42.730991373 +0530  
 Birth: 2025-05-07 13:13:54.236630593 +0530  
buddhima@Buddhima:~/Downloads/Executables/Executables$ ls -l  
total 96  
-rw-rw-r-- 1 buddhima buddhima 70824 Mar 17 06:26 ARM  
-rw-r--r-- 1 root      root      4 May  7 14:13 data.txt  
-rwxr-xr-x 1 root      root     20368 May  7 13:08 IT23  
buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ cat data.txt  
WM[buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ base64 -d data.txt  
base64: invalid input  
buddhima@Buddhima:~/Downloads/Executables/Executables$ xxd data.txt  
00000000: 0d57 4d5b .WM[  
buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ hexdump -C data.txt  
00000000  0d 57 4d 5b | .WM[]  
00000004  
buddhima@Buddhima:~/Downloads/Executables/Executables$  
buddhima@Buddhima:~/Downloads/Executables/Executables$ strings ./IT23  
/lib64/ld-linux-x86-64.so.2  
fgets
```

- Any decoded/processed information

String ./IT2E [REDACTED] - identifying encoded information inside executables.

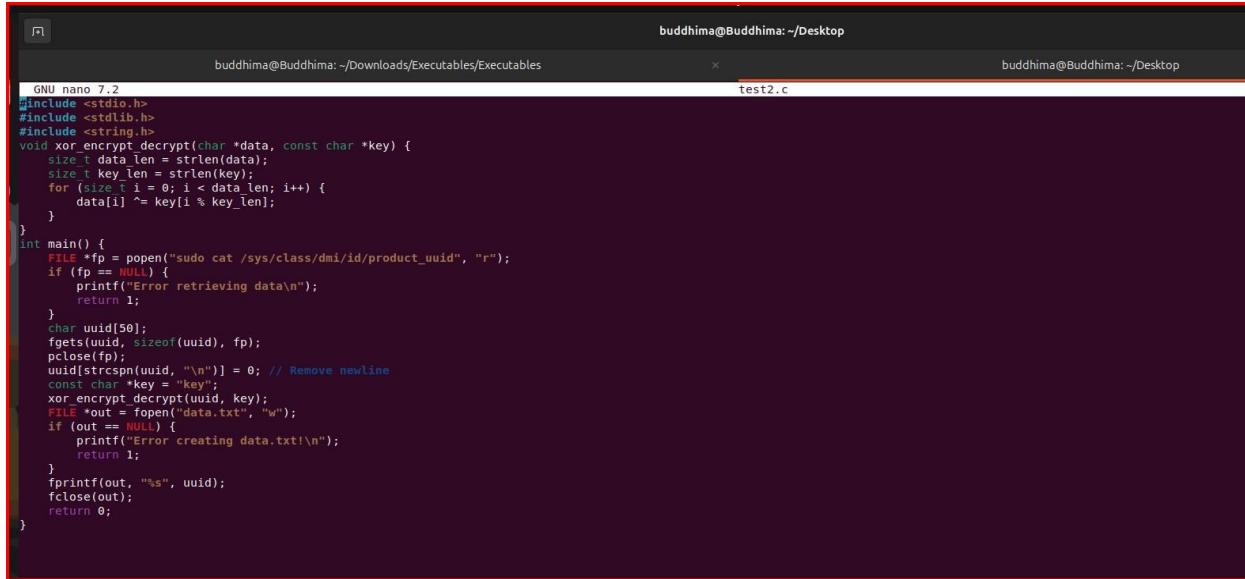
```
buddhima@Buddhima:~/Downloads/Executables/Executables$ hexdump -C data.txt
00000000  0d 57 4d 5b                                |.WM[|
00000004
buddhima@Buddhima:~/Downloads/Executables/Executables$ strings ./IT2E [REDACTED]
/lib64/ld-linux-x86-64.so.2
fgets
_stack_chk_fail
fopen
strlen
strcspn
pclose
__libc_start_main
__cxa_finalize
popen
fclose
fputs
libc.so.6
GLIBC_2.4
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
_gmon_start_
_ITM_registerTMCloneTable
PTE1
u+UH
sudo cat /sys/class/dmi/id/product_uuid
Error retrieving data
data.txt
Error creating data.txt!
9*35"
GCC: (Ubuntu 13.3.0-6ubuntu2~24.04) 13.3.0
_off_t
_IO_read_ptr
_chain
_size_t
_shortbuf
_IO_buf_base
long long unsigned int
long long int
fileno
```

Nano test2.c -Check decrypted code

Copy the source code into test.c file

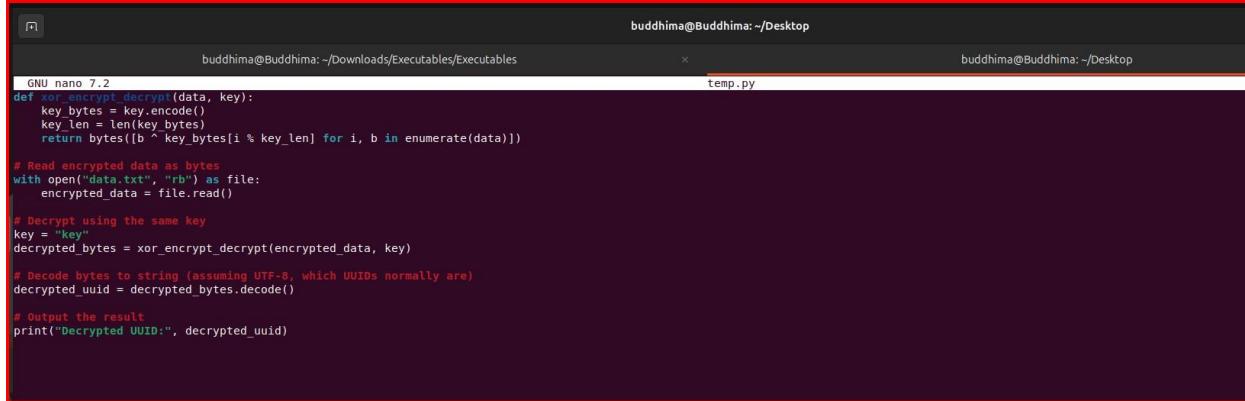
```
buddhima@Buddhima:~/Desktop$ nano test2.c
buddhima@Buddhima:~/Desktop$ nano temp.py
buddhima@Buddhima:~/Desktop$
```

This program extracts the system's hardware UUID, encrypts it using XOR encryption, and stores the encrypted value in data.txt for later decryption.



```
buddhima@Buddhima: ~/Downloads/Executables/Executables test2.c
GNU nano 7.2
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
void xor_encrypt_decrypt(char *data, const char *key) {
    size_t data_len = strlen(data);
    size_t key_len = strlen(key);
    for (size_t i = 0; i < data_len; i++) {
        data[i] ^= key[i % key_len];
    }
}
int main() {
    FILE *fp = fopen("sudo cat /sys/class/dmi/id/product_uuid", "r");
    if (fp == NULL) {
        printf("Error retrieving data\n");
        return 1;
    }
    char uuid[50];
    fgets(uuid, sizeof(uuid), fp);
    pclose(fp);
    uuid[strcspn(uuid, "\n")] = 0; // Remove newline
    const char *key = "key";
    xor_encrypt_decrypt(uuid, key);
    FILE *out = fopen("data.txt", "w");
    if (out == NULL) {
        printf("Error creating data.txt!\n");
        return 1;
    }
    fprintf(out, "%s", uuid);
    fclose(out);
    return 0;
}
```

Nano temp.py – create a python code to execute



```
buddhima@Buddhima: ~/Downloads/Executables/Executables temp.py
GNU nano 7.2
def xor_encrypt_decrypt(data, key):
    key_bytes = key.encode()
    key_len = len(key_bytes)
    return bytes([b ^ key_bytes[i % key_len] for i, b in enumerate(data)])

# Read encrypted data as bytes
with open("data.txt", "rb") as file:
    encrypted_data = file.read()

# Decrypt using the same key
key = "key"
decrypted_bytes = xor_encrypt_decrypt(encrypted_data, key)

# Decode bytes to string (assuming UTF-8, which UUIDs normally are)
decrypted_uuid = decrypted_bytes.decode()

# Output the result
print("Decrypted UUID:", decrypted_uuid)
```

This Python script decrypts XOR-encrypted binary data from data.txt using a predefined key and reveals the original UUID stored in the file.

```
buddhima@Buddhima: ~/Downloads/Executables/Executables
buddhima@Buddhima: ~/Desktop

IO write base
/home/buddhima/Downloads/Executables/Executables
IT23611788.c
/usr/lib/gcc/x86_64-linux-gnu/13/include
/usr/include/x86_64-linux-gnu/bits
/usr/include/x86_64-linux-gnu/bits/types
/usr/include
stddef.h
types.h
struct_FILE.h
stdio.h
string.h
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
void xor_encrypt_decrypt(char *data, const char *key) {
    size_t data_len = strlen(data);
    size_t key_len = strlen(key);
    for (size_t i = 0; i < data_len; i++) {
        data[i] ^= key[i % key_len];
    }
}
int main() {
    FILE *fp = fopen("sudo cat /sys/class/dmi/id/product_uuid", "r");
    if (fp == NULL) {
        printf("Error retrieving data\n");
        return 1;
    }
    char uuid[50];
    fgets(uuid, sizeof(uuid), fp);
    pclose(fp);
    uuid[strcspn(uuid, "\n")] = 0; // Remove newline
    const char *key = "key";
    xor_encrypt_decrypt(uuid, key);
    FILE *out = fopen("data.txt", "w");
    if (out == NULL) {
        printf("Error creating data.txt!\n");
        return 1;
    }
    fprintf(out, "%s", uuid);
    fclose(out);
    return 0;
}
Scrtl.o
abi_tag
```

Decrypted messeg

```
buddhima@Buddhima:~/Desktop$ python3 temp.py
Decrypted UUID: f240
buddhima@Buddhima:~/Desktop$ sudo cat /sys/class/dmi/id/product_uuid
f240e105-e3ec-9845-95e3-6ae83e906e2e
```

Only a partial UUID (f240) was recovered because XOR encryption generated NULL bytes, causing the encrypted string to be truncated when written to data.txt using string-based file output