Sri Lanka Institute of Information Technology

IE2012: System and Network Programming

Year 2 Semester 1

Assignment

IT23839274 - P.B.U.R. WICKRAMASINGHE

Table of Contents

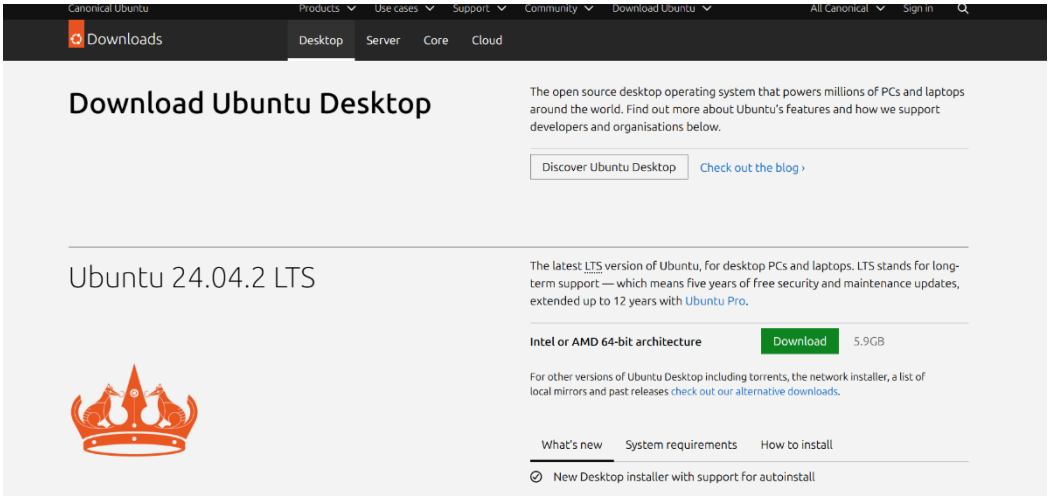
1. Basic of Linux Environments

1.1 Documentation of the Virtual Machine Setup

Step to Install Virtual Machine

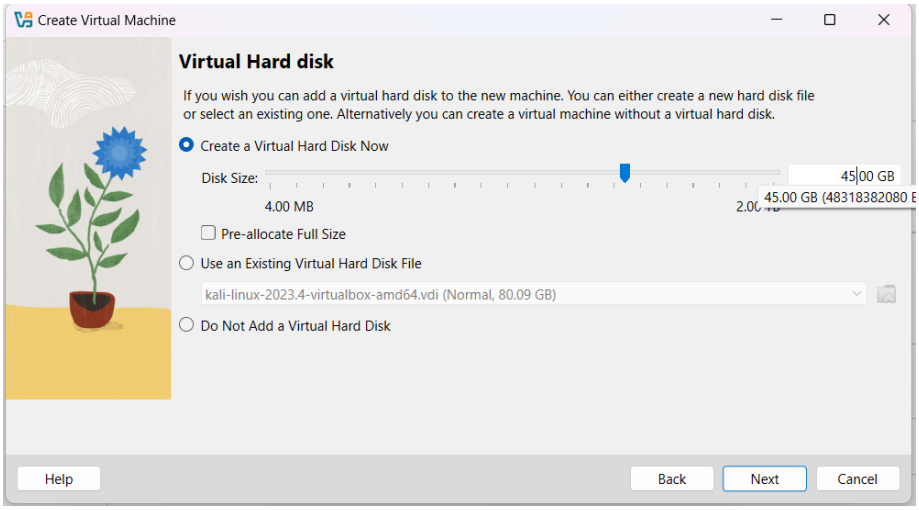
1) Download and install VirtualBox or VMware Workstation Player. (Already Installed)

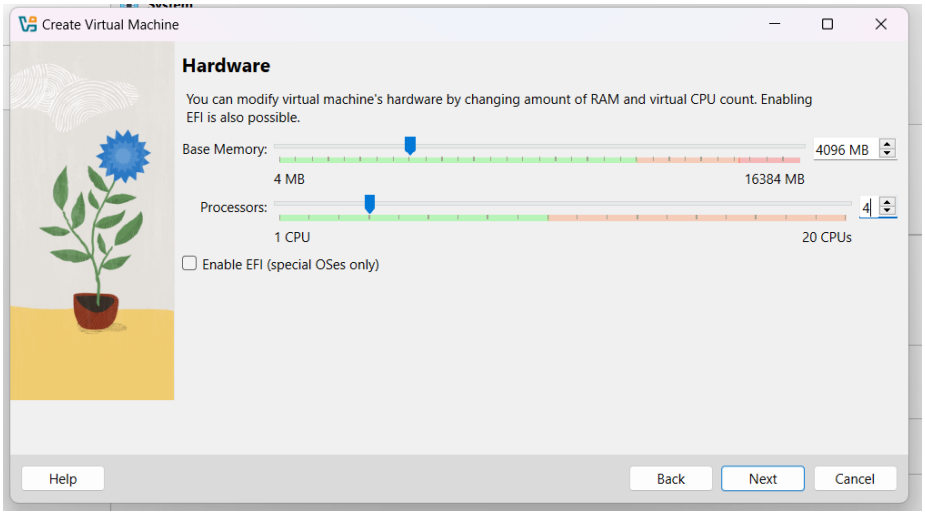
2) Download Ubuntu from ‘Ubuntu Official Site’ or CentOS from ‘CentOS Official’ Site.



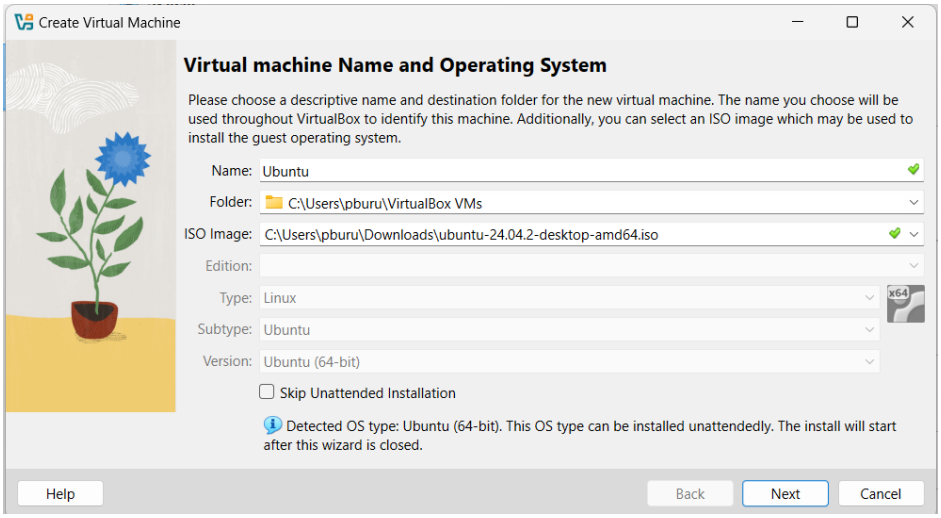
3) Open VirtualBox and create a new virtual machine.

4) Allocate resources:
    a. **RAM**: Minimum 4GB.
    b. **Storage**: Minimum 20GB.





5) Attached the downloaded ISO file to the virtual machine.



6) Install the Linux distribution following on screen instruction.
7) Set up a Username and password for authentication.
8) Restart and log into the Linux system.

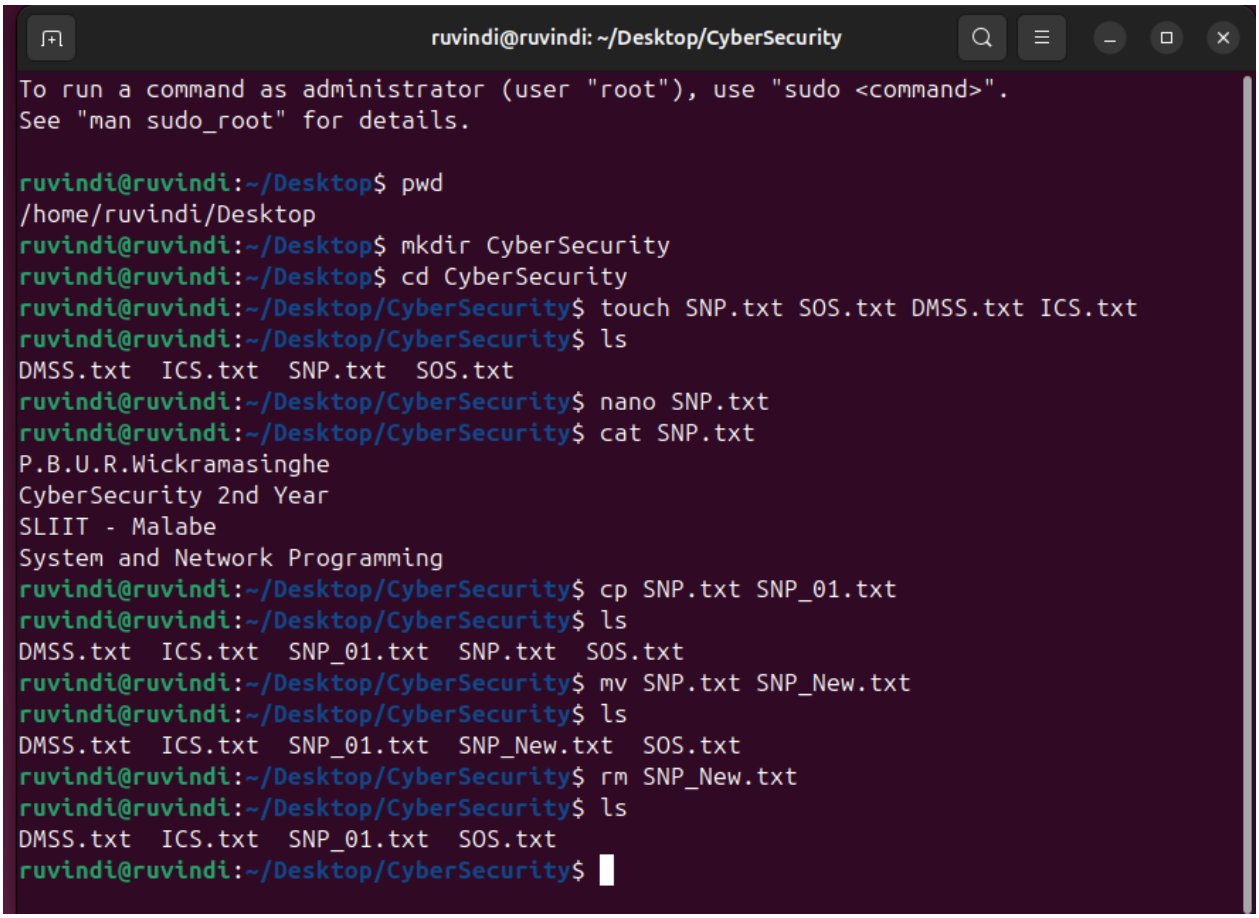
1.2 Command Line Introduction

Basic Navigation Commands

Command	Functionality
pwd	Prints the current working directory
cd	Changes the current directories
ls	List the files and directories
mkdir	Creates a new directory
rmdir	Removes an empty directory
cat	View content of a file

File Manipulation Commands

cp	Copies files or directories
mv	Moves or rename files
cat	Displays files contents
rm	Deletes a file
touch	Create a new empty file
nano	Edit texter



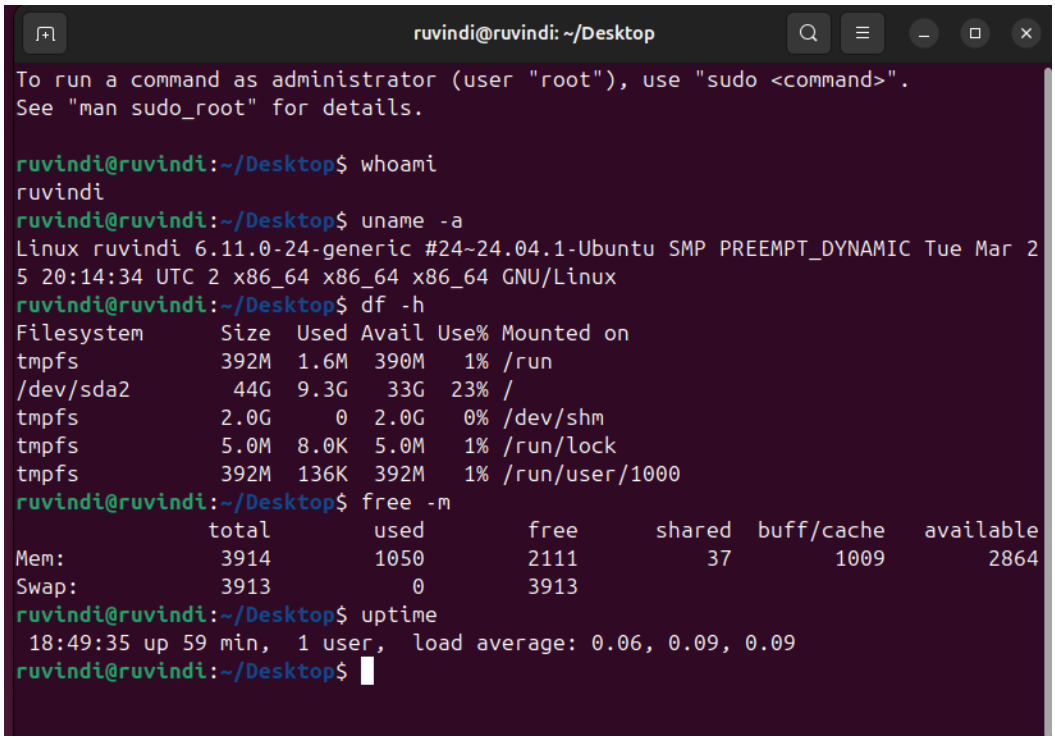
1.3 System Information and User Management

System Information Commands

uname -a	Displays information system
df -h	Shows disk space usage
Free -m	Displays memory usage
uptime	Shows system uptime

User Management Commands

whoami	Displays the current user
id	Shows user and group id
useradd	Adds a new user
passwd	Change user password



2. DHCP, DNS and NTP Services

2.1 DHCP Configuration

1) Install DHCP Server

This command updates the package list from all software repositories.
It connects to the package repositories and download the least package lists.

"sudo apt update"

This command installs the **ISC DHCP Server**, which is the software that will assign IP addresses to devices in the network.

"sudo apt install isc-dhcp-server"

2) Edit the DHCP Configuration File

This opens the main configuration file of the DHCP server in the nano text editor.

"sudo nano /etc/dhcp/dhcpd.conf"

3) Add the Subnet details

This block defines a DHCP scope for the subnet 192.168.1.0/24

"Subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.100 192.168.1.200;
option routers 10.0.2.1;
option domain-name-servers 8.8.8.8, 8.8.4.4;
}"

Save the configuration and exit the editor.

- Subnet 192.168.1.0 netmask 255.255.255.0: - Specifies the network for which the DHCP server will assign IPs.
- range 192.168.1.100 192.168.1.200: - Defines the Ip address range that server can assign to client.
- option routers 10.0.2.1: - Set the default gateway that clients will use to access other networks.
- option domain-name-servers 8.8.8.8, 8.8.4.4: Tells clients which DNS servers to use — in this case, Google's public DNS servers.

4) Restart the DHCP Server

This command restarts the DHCP server so it applies the new settings from the dhcpd.conf file.

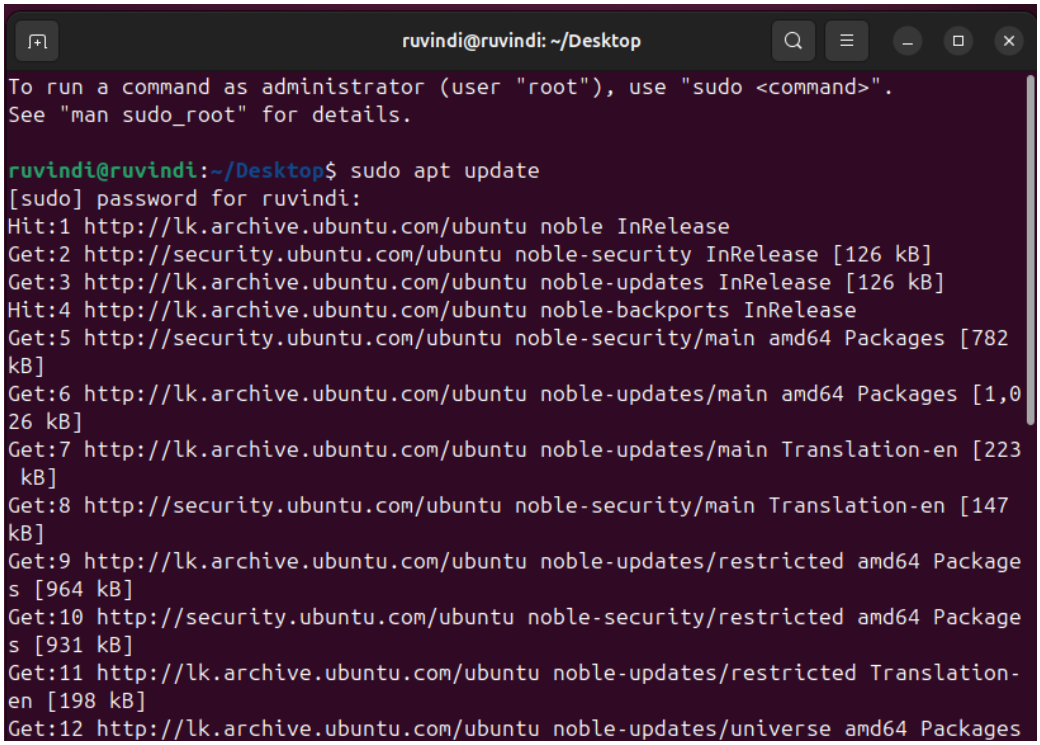
If the configuration is correct, the service will start running and devices in the subnet will start receiving IP addresses automatically.

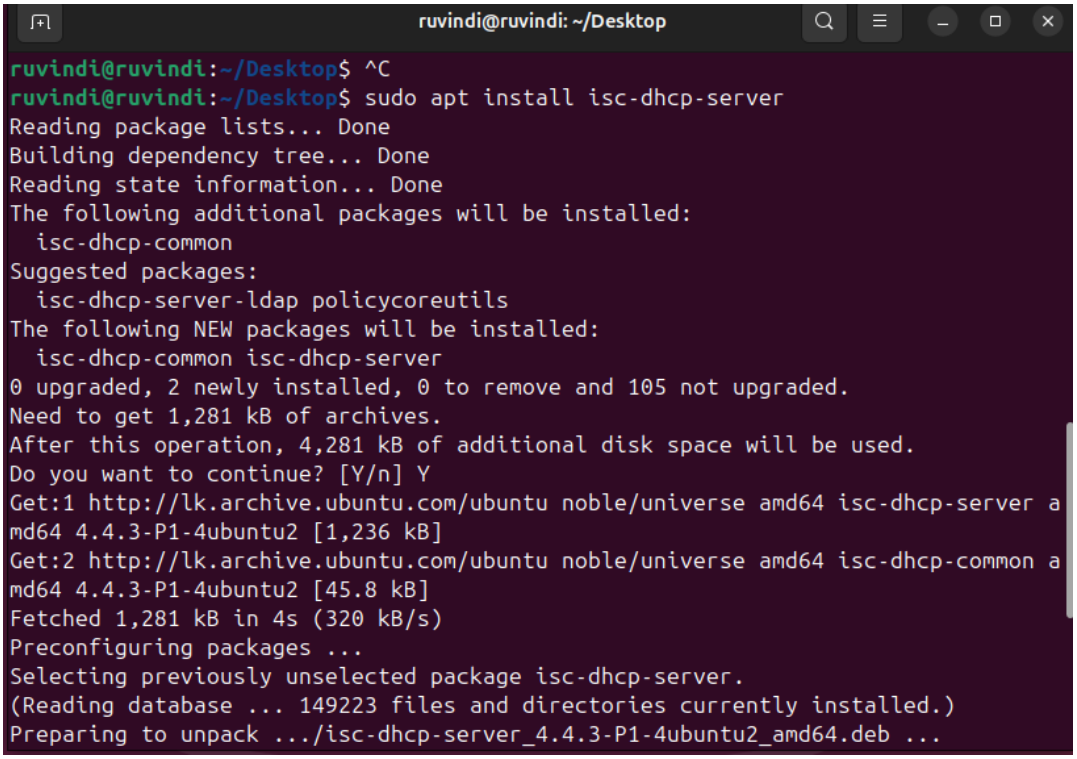
"sudo systemctl restart isc-dhcp-server"

"sudo systemctl status isc-dhcp-server"

- sudo systemctl status isc-dhcp-server: - Shows the current status of the DHCP service.

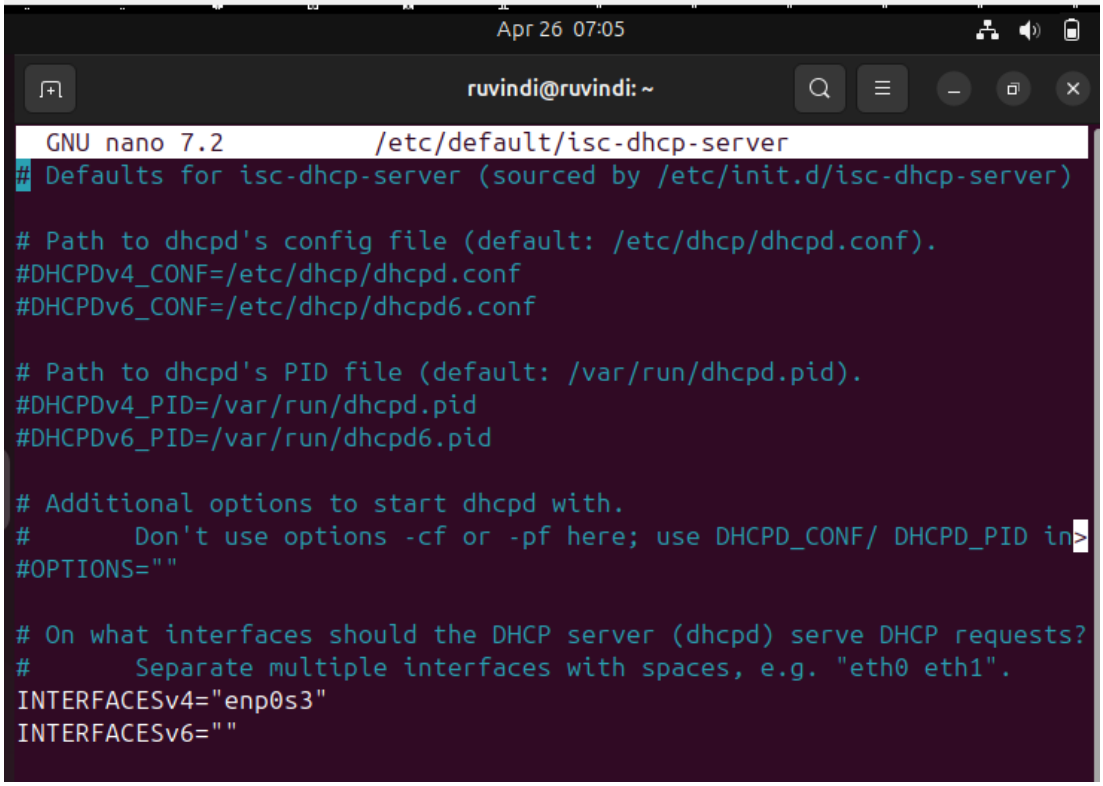
2.2.1 Screenshots of the DHCP Configuration

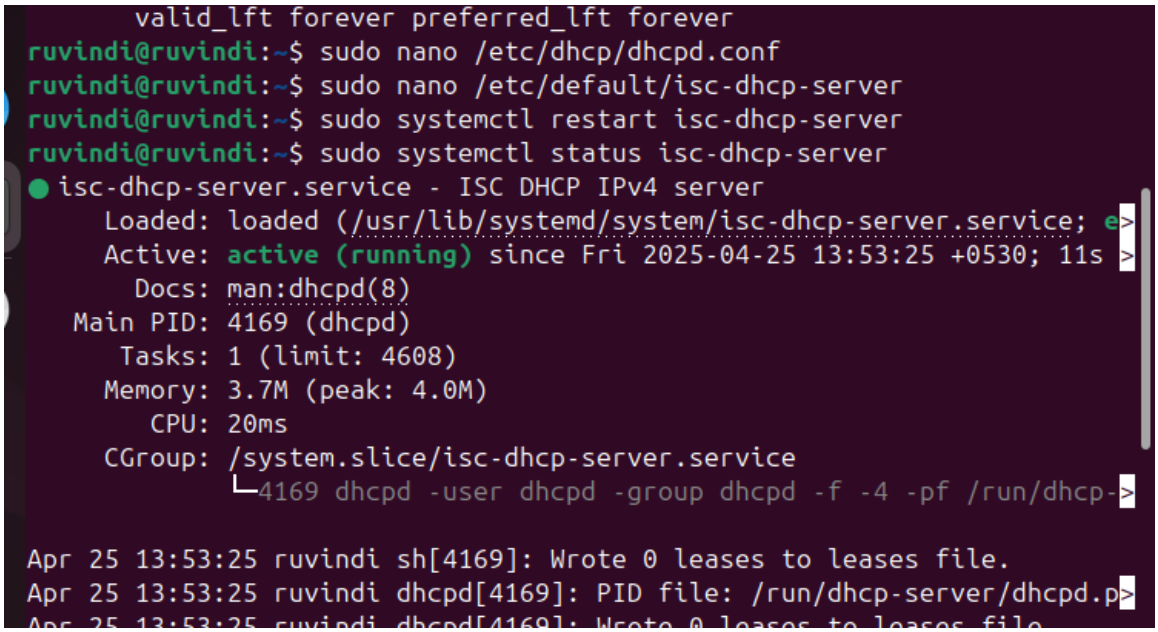




```
ruvindi@ruvindi:~$ sudo nano /etc/default/isc-dhcp-server
ruvindi@ruvindi:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN grou
p default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft 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 sta
te UP group default qlen 1000
    link/ether 08:00:27:d1:9c:50 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
enp0s3
       valid_lft 82043sec preferred_lft 82043sec
    inet6 fd00::5937:c094:fd99:9c3a/64 scope global temporary dynamic
       valid_lft 86159sec preferred_lft 14159sec
    inet6 fd00::a00:27ff:fed1:9c50/64 scope global dynamic mngtmpaddr
```

```
  GNU nano 7.2                  /etc/dhcp/dhcpd.conf
# The ddns-updates-style parameter controls whether or not the server w>
# attempt to do a DNS update when a lease is confirmed. We default to t>
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

subnet 10.0.2.0 netmask 255.255.255.0 {
  range 10.0.2.100 10.0.2.200;
  option routers 10.0.2.1;
  option domain-name-servers 8.8.8.8, 8.8.4.4;
}
# 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;
```


Apr 26 07:05
ruvindi@ruvindi: ~
GNU nano 7.2 /etc/default/isc-dhcp-server
Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf
Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid
Additional options to start dhcpd with.
Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID in
#OPTIONS=""
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""


valid_lft forever preferred_lft forever
ruvindi@ruvindi:~$ sudo nano /etc/dhcp/dhcpd.conf
ruvindi@ruvindi:~$ sudo nano /etc/default/isc-dhcp-server
ruvindi@ruvindi:~$ sudo systemctl restart isc-dhcp-server
ruvindi@ruvindi:~$ sudo systemctl status isc-dhcp-server
isc-dhcp-server.service - ISC DHCP IPv4 server
Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; e
Active: active (running) since Fri 2025-04-25 13:53:25 +0530; 11s
Docs: man:dhcpd(8)
Main PID: 4169 (dhcpd)
Tasks: 1 (limit: 4608)
Memory: 3.7M (peak: 4.0M)
CPU: 20ms
CGroup: /system.slice/isc-dhcp-server.service
└4169 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-
Apr 25 13:53:25 ruvindi sh[4169]: Wrote 0 leases to leases file.
Apr 25 13:53:25 ruvindi dhcpd[4169]: PID file: /run/dhcp-server/dhcpd.p

2.2 DNS Configuration (BIND)

1) Update the package list

"sudo apt update"

Update the package list to verify we're using the most recent version.

2) Install the DNS Server

"sudo apt install bind9"

Using your package manager, install a DNS server, such as BIND (Berkeley Internet Name Domain).

3) Configure the BIND DNS Server

"Sudo nano /etc/bind/named.conf.local"

Configure DNS zones by editing the BIND configuration file (/etc/bind/named.conf).

Add DNS zone configurations to the text editor.

```
zone "ruvindi.local" {
type master;
file "/etc/bind/zones/db.example.local";
};
```

Save the file and exit the editor.

- **zone "ruvindi.local"**: This defines a domain or zone named ruvindi.local.
- **type master**: This DNS server is the **primary (master)** for this zone, meaning it **stores the original zone file**.
- **file**: Points to the file where the DNS records for this domain are stored.

4) Create the Zone Directory and File

"sudo mkdir /etc/bind/zones"

Create a directory for storing zone files.

"sudo nano /etc/bind/zones/db.ruvindi.local"

Create a zone file for domain.

Add the zone file content

```
$TTL    604800
@       IN      SOA     ns1.ruvindi.local. admin.ruvindi.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
```

- **$TTL 604800**: Sets the default Time-To-Live for records (in seconds). Here, 604800 seconds = 7 days.

- **SOA (Start of Authority)**: Declares authoritative information about the zone:
- The numbers control DNS caching and zone refresh:
  - **Serial**: Used by secondary servers to know when to update.
  - **Refresh**: How often a secondary should check for updates.
  - **Retry**: Wait time before retrying a failed update.
  - **Expire**: Time after which the zone is no longer authoritative if refresh fails.
  - **Negative Cache TTL**: How long to cache a "non-existent domain" response.

@ IN NS ns1.ruvindi.local.

ns1 IN A 192.168.1.10

www IN A 192.168.1.20

- @ IN NS ns1.ruvindi.local.: Declares the **name server** for the domain.
- ns1 IN A 192.168.1.10: Binds ns1.ruvindi.local to IP address 192.168.1.10.
- www IN A 192.168.1.20: Maps www.ruvindi.local to 192.168.1.20.

5) Check Configuration and Restart BIND

Checks the **main BIND configuration files** for syntax errors

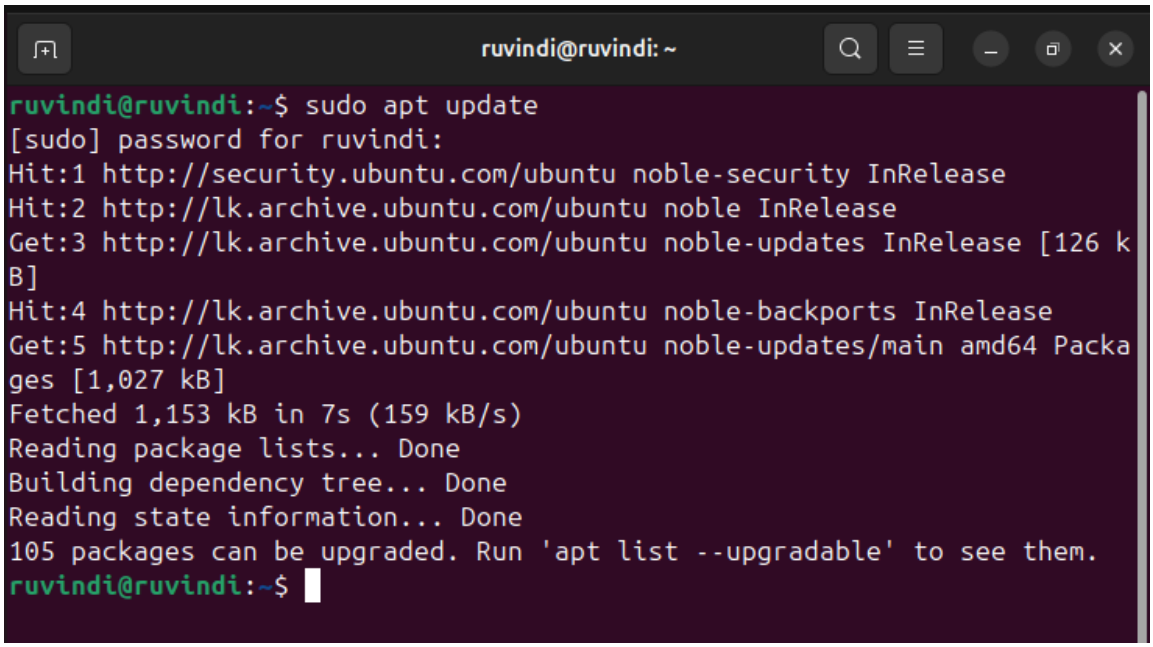
"sudo named-checkconf"

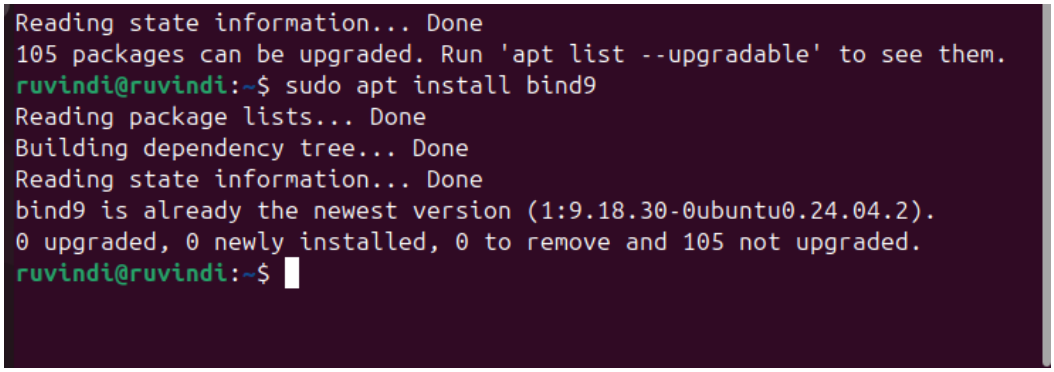
Checks the **syntax and correctness of the zone file**.

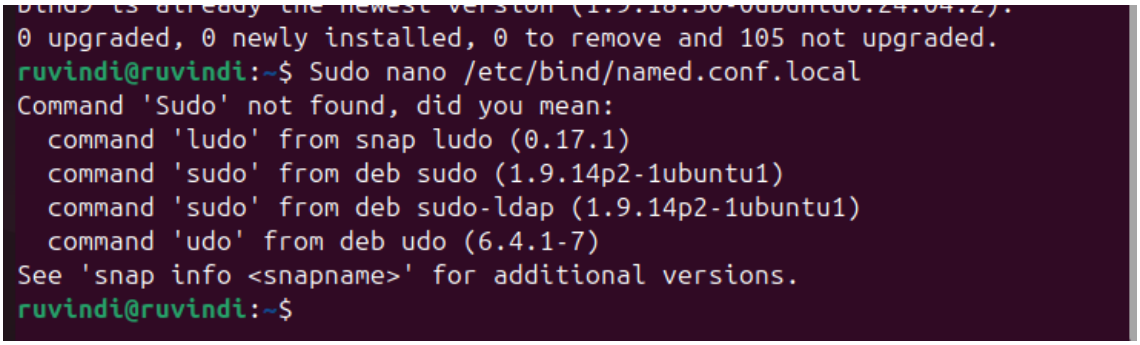
"sudo named-checkzone ruvindi.local /etc/bind/zones/db.ruvindi.local"

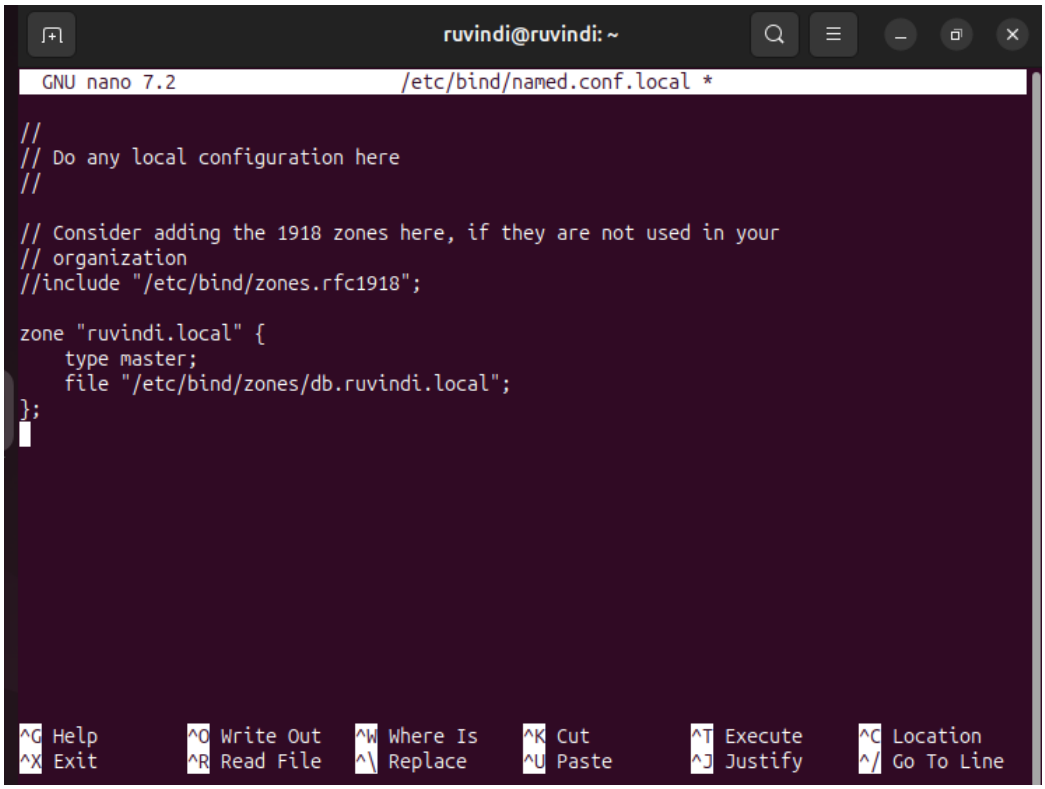
Before restarting the Bind9 service, inspect the configuration for syntax problem.

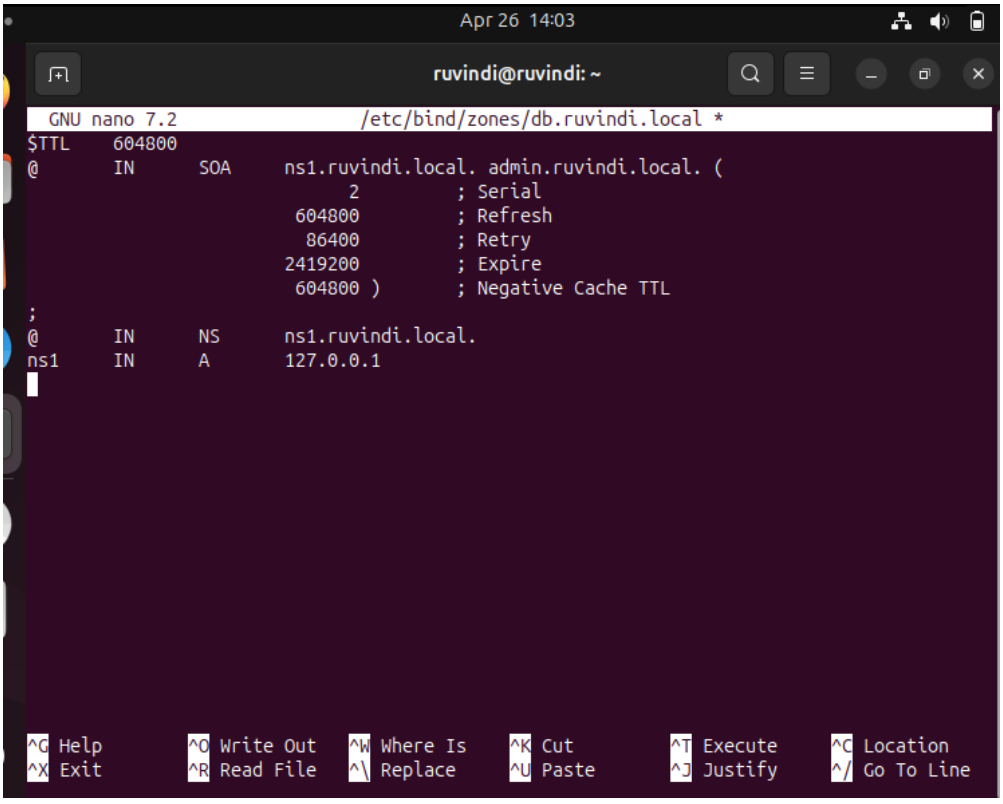
2.2.2 Screenshots of the DNS Configuration

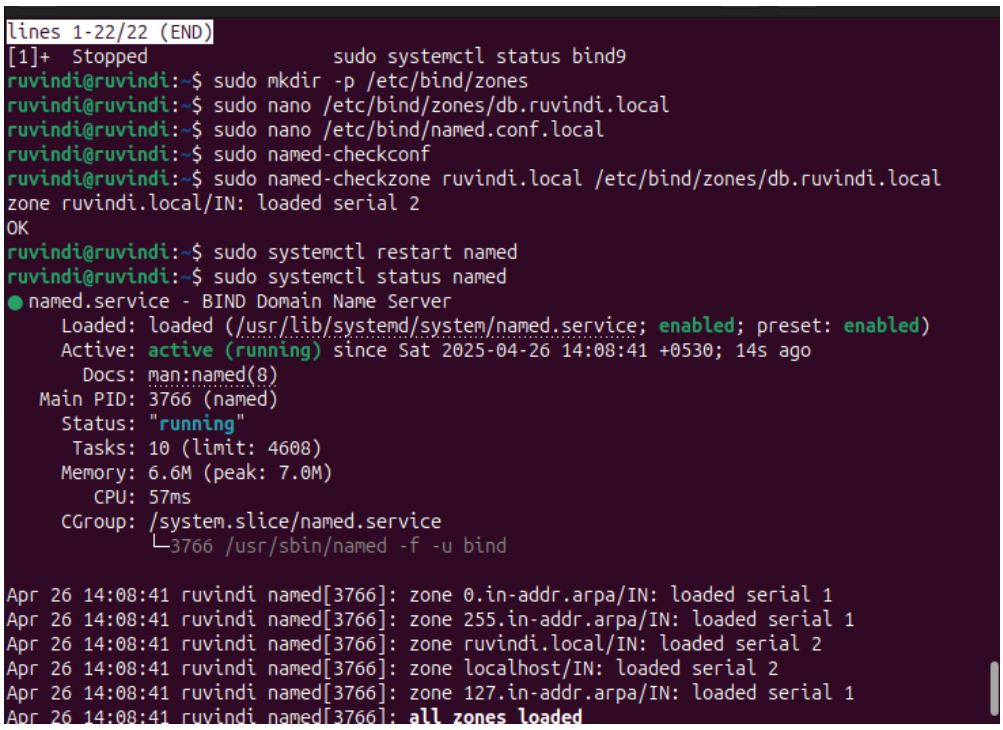







ruvindi@ruvindi: ~
GNU nano 7.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "ruvindi.local" {
type master;
file "/etc/bind/zones/db.ruvindi.local";
};
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line


Apr 26 14:03
ruvindi@ruvindi: ~
GNU nano 7.2 /etc/bind/zones/db.ruvindi.local *
$TTL 604800
@ IN SOA ns1.ruvindi.local. admin.ruvindi.local. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
@ IN NS ns1.ruvindi.local.
ns1 IN A 127.0.0.1
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line



2.3 NTP Configuration

1) Update & Install an NTP Client

Update the package list using same command and Install the NTP server software from your package manager.

"sudo apt update"

"sudo apt install ntp -y"

- The **-y** flag auto-confirms the installation without prompting.

2) Configure NTP Server

Edit the NTP Configuration File

"sudo nano /etc/ntp.conf"

Within the file, you can add or change server entries in the "pool" or "server" sections to point to your preferred NTP servers.

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

- These lines tell your system to use **public NTP servers from the pool.ntp.org network**, which distributes requests across many time servers.
- The keyword iburst speeds up the initial synchronization by sending a burst of packets if the server is unreachable at first.

3) Start and Enable the NTP Service

Start the NTP service

"sudo systemctl start ntp"

Enable it to start automatically at boot

"sudo systemctl enable ntp"

4) **Verify the NTP Synchronization**

You should see a list of NTP servers and synchronization details.

"ntpq -p"

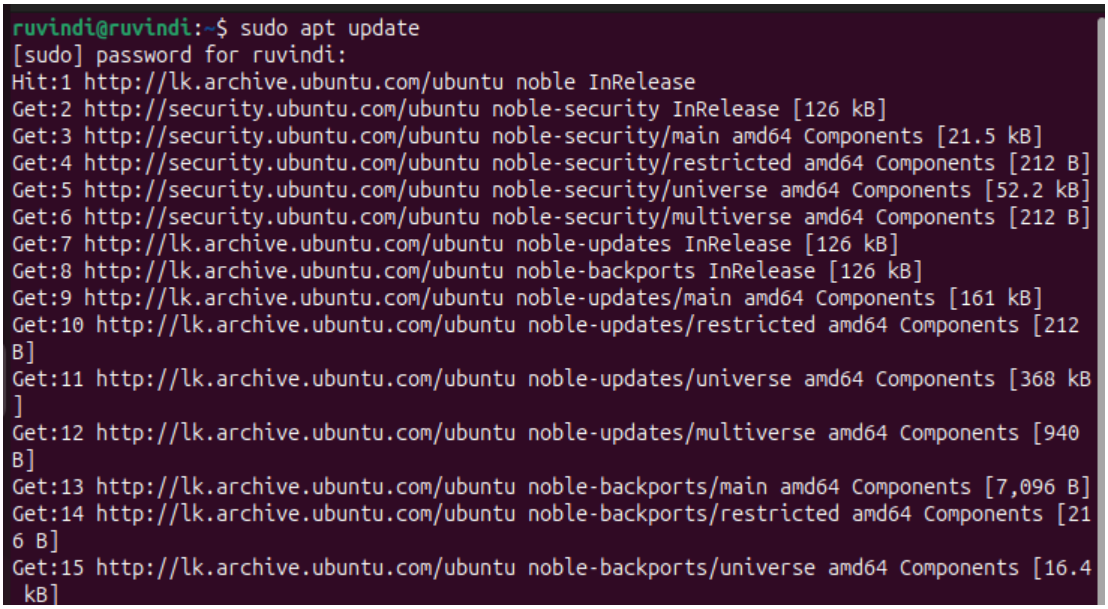
Shows details such as:

- Server addresses
- Delay
- Offset (time difference)
- Jitter (stability)

"timedatectl status"

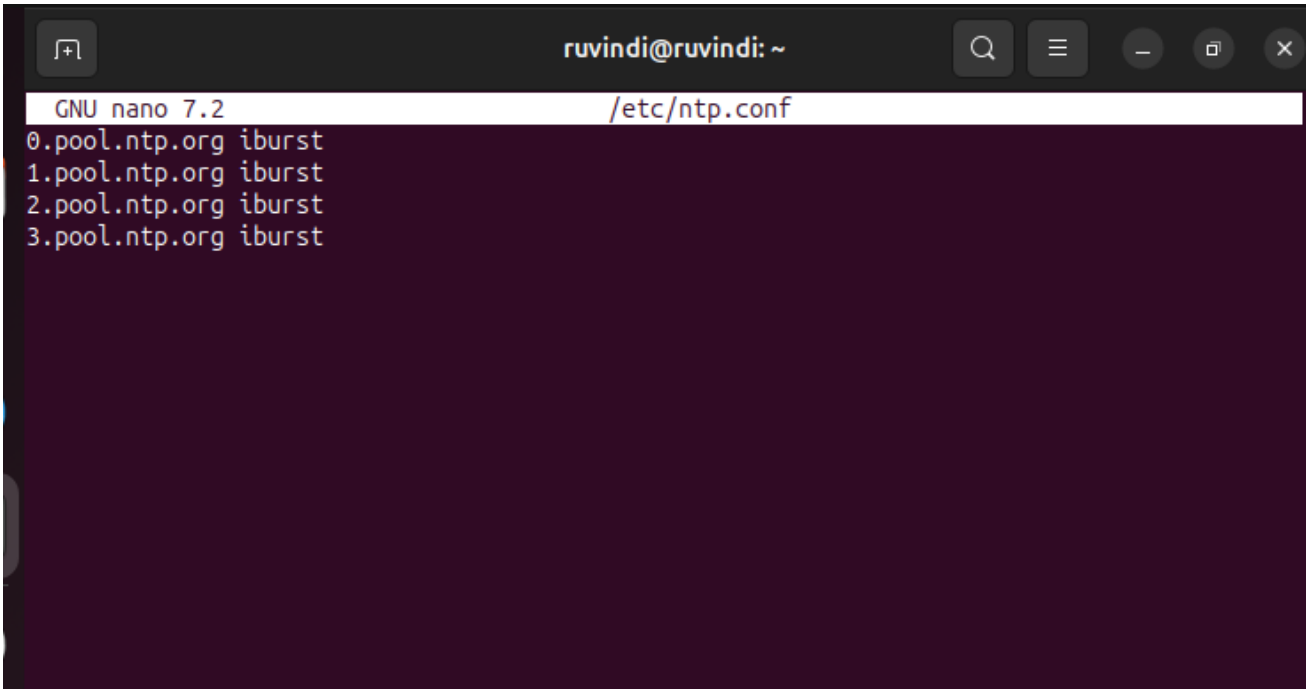
- Shows the **system clock status**, including:
  - Local time
  - UTC time
  - RTC time (hardware clock)
  - NTP synchronization status (System clock synchronized: yes if successful)

2.3.3 Screenshots of the NTP Configuration



```
ruvindi@ruvindi:~$ sudo apt install ntp -y

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ntpsec python3-ntp
Suggested packages:
  certbot ntpsec-doc ntpsec-ntpviz
The following NEW packages will be installed:
  ntp ntpsec python3-ntp
0 upgraded, 3 newly installed, 0 to remove and 104 not upgraded.
Need to get 450 kB of archives.
After this operation, 1,308 kB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 python3-ntp amd64 1.2.2+dfs
g1-4build2 [91.2 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntpsec amd64 1.2.2+dfsg1-4b
uild2 [343 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntp all 1:4.2.8p15+dfsg-2~1
.2.2+dfsg1-4build2 [15.7 kB]
Fetched 450 kB in 4s (112 kB/s)
Selecting previously unselected package python3-ntp.
(Reading database ... 151499 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) ...
Selecting previously unselected package ntp.
```

```
Created symlink /etc/systemd/system/ntpd.service → /usr/lib/systemd/system/ntpsec.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ntpsec.service → /usr/lib/syst
emd/system/ntpsec.service.
Setting up ntp (1:4.2.8p15+dfsg-2~1.2.2+dfsg1-4build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
ruvindi@ruvindi:~$ sudo nano /etc/ntp.conf
```




```
ruvindi@ruvindi:~$ sudo systemctl start ntp.service
ruvindi@ruvindi:~$ sudo systemctl status ntp.service
● ntpsec.service - Network Time Service
     Loaded: loaded (/usr/lib/systemd/system/ntpsec.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-04-26 16:17:10 +0530; 3h 57min ago
       Docs: man:ntpd(8)
    Process: 5516 ExecStart=/usr/libexec/ntpsec/ntp-systemd-wrapper (code=exited, status=>
   Main PID: 5519 (ntpd)
      Tasks: 1 (limit: 4608)
     Memory: 11.4M (peak: 11.9M)
        CPU: 1.148s
     CGroup: /system.slice/ntpsec.service
             └─5519 /usr/sbin/ntpd -p /run/ntpd.pid -c /etc/ntpsec/ntp.conf -g -N -u ntps>

Apr 26 20:12:35 ruvindi ntpd[5519]: DNS: Pool skipping: 162.159.200.1
Apr 26 20:12:35 ruvindi ntpd[5519]: DNS: Pool skipping: 222.165.180.134
Apr 26 20:12:35 ruvindi ntpd[5519]: DNS: Pool skipping: 162.159.200.123
Apr 26 20:12:35 ruvindi ntpd[5519]: DNS: dns_take_status: 1.ubuntu.pool.ntp.org=>good, 8
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: dns_probe: 3.ubuntu.pool.ntp.org, cast_flags:8, >
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: dns_check: processing 3.ubuntu.pool.ntp.org, 8, >
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: Pool skipping: 162.159.200.1
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: Pool skipping: 222.165.180.134
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: Pool skipping: 162.159.200.123
Apr 26 20:12:37 ruvindi ntpd[5519]: DNS: dns_take_status: 3.ubuntu.pool.ntp.org=>good, 8
lines 1-22/22 (END)
```

```
ruvindi@ruvindi:~$ ntpq -p
     remote                       refid      st t when poll reach   delay   offset   jitter
==============================================================================
 0.ubuntu.pool.ntp.org      .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 1.ubuntu.pool.ntp.org      .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 2.ubuntu.pool.ntp.org      .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 3.ubuntu.pool.ntp.org      .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
-prod-ntp-4.ntp4.ps5.canon 17.253.28.251    2 u  239  256  373 155.8524  12.3709  68.0060
*ntp.sltidc.lk             216.239.35.4     2 u  108  256  377  13.7541 -74.3318  94.1798
+time.cloudflare.com       10.120.8.100     3 u  222  256  373  11.8640  25.8415  55.9912
+time.cloudflare.com       10.195.8.4       3 u   70  256  377  11.8799  24.4307  44.0599
+time.cloudflare.com       10.111.8.4       3 u  738  256  354  11.2444 -22.5365  46.4006
-time.cloudflare.com       10.111.8.4       3 u  50m  256  370  10.6127  59.6849  90.0838
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ timedatectl status
               Local time: Sat 2025-04-26 20:22:49 +0530
           Universal time: Sat 2025-04-26 14:52:49 UTC
                 RTC time: Sat 2025-04-26 14:52:36
                Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
              NTP service: n/a
          RTC in local TZ: no
ruvindi@ruvindi:~$
```

3. Security and Other Servers

3.1 Shell Scripting

Automate Log Management Script

1) Create the script File

Opened a new script file using nano editor.

"nano log_cleanup.sh"

2) Write the Script

```
#!/bin/bash

# Define the log directory
log_dir="$HOME/logs/custom_logs"

# Define the backup directory
backup_dir="$HOME/logs/logs_backup"

# Create the backup directory if it does not exist
mkdir -p "$backup_dir"

# Find and delete .log files older than 7 days
find "$log_dir" -name "*.log" -type f -mtime +7 -exec rm -v {} \; > deleted_logs.txt

# Archive remaining .log files
tar -czvf "$backup_dir/logs_backup_$(date +%Y%m%d).tar.gz" "$log_dir"/*.log

# Print summary
echo "Deleted files:"
cat deleted_logs.txt
echo "Remaining files archived at $backup_dir/logs_backup_$(date +%Y%m%d).tar.gz"
```

Save the script and exit from the file.

Script Explanation:

- #!/bin/bash: Shebang line – tells the system to execute this script with the Bash shell.
- backup_dir=...: Sets the path where backups will be stored.
- mkdir -p "$backup_dir": Creates the backup directory if it doesn't already exist (-p avoids errors if it does).
- find ... -mtime +7 -exec rm -v {} \;: Finds .log files older than 7 days and deletes them; logs the deleted files to deleted_logs.txt.
- tar -czvf ...: Archives (compresses) the remaining .log files into a .tar.gz file named with the current date.
- echo and cat: Print out the deleted files and location of the backup archive.

3) Make the Script Executable

"chmod +x log_cleanup.sh"

Grants **execute permission** to the script, allowing it to be run like a program.

4) Run the Script

"./log_cleanup.sh"

Executes the script.

5) Set up the Cron Job

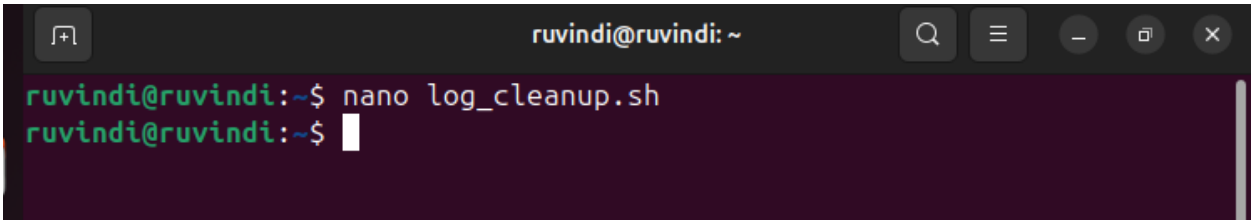
"crontab -e"

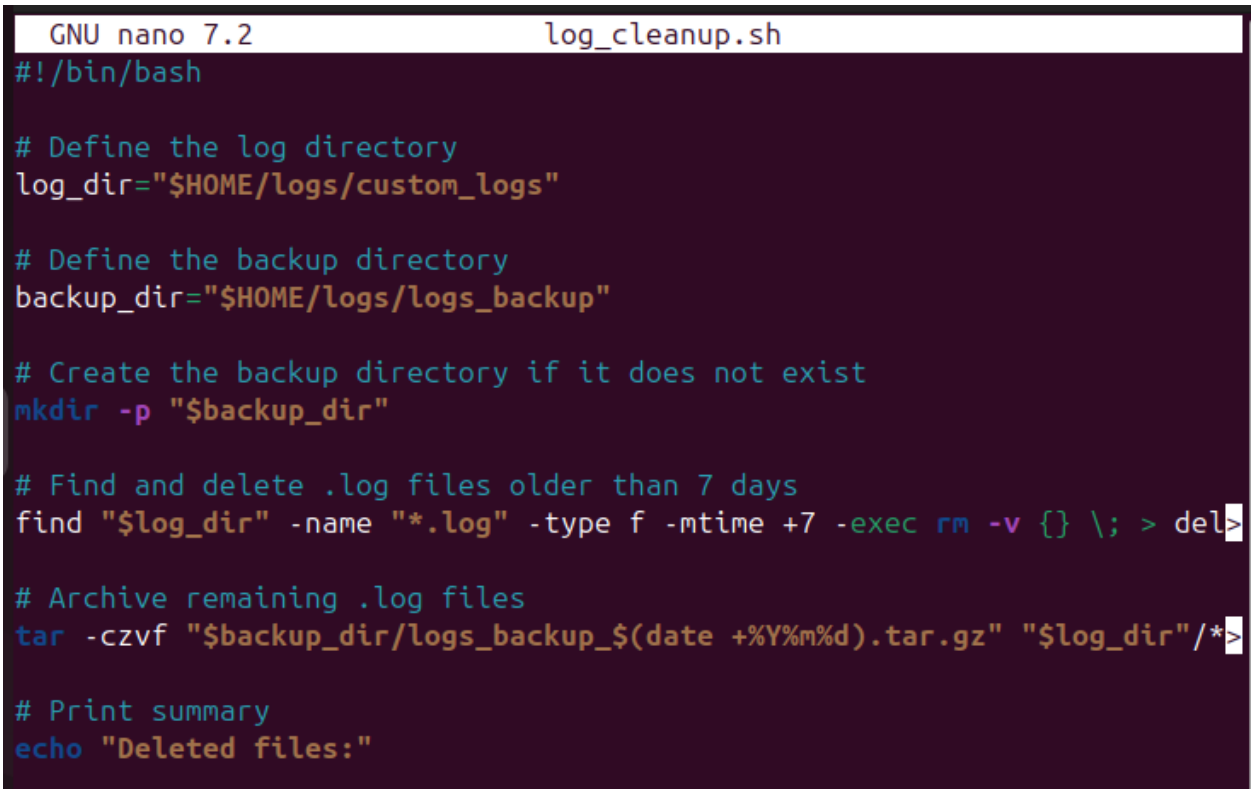
Added this line to schedule it every **Sunday at 12:00 AM**:

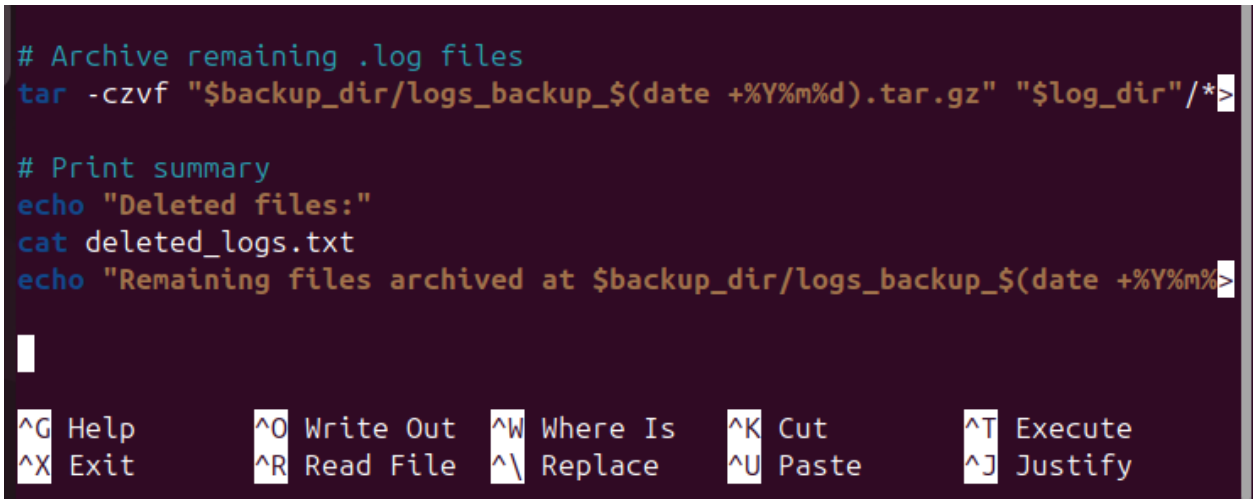
*"0 0 * * 0 /path/to/log_cleanup.sh"*

- 0 0 * * 0: Run the script **every Sunday at 12:00 AM**.
- /path/to/log_cleanup.sh: Replace this with the **full absolute path** to your script.

3.1.1 Screenshots of the Shell Scripting

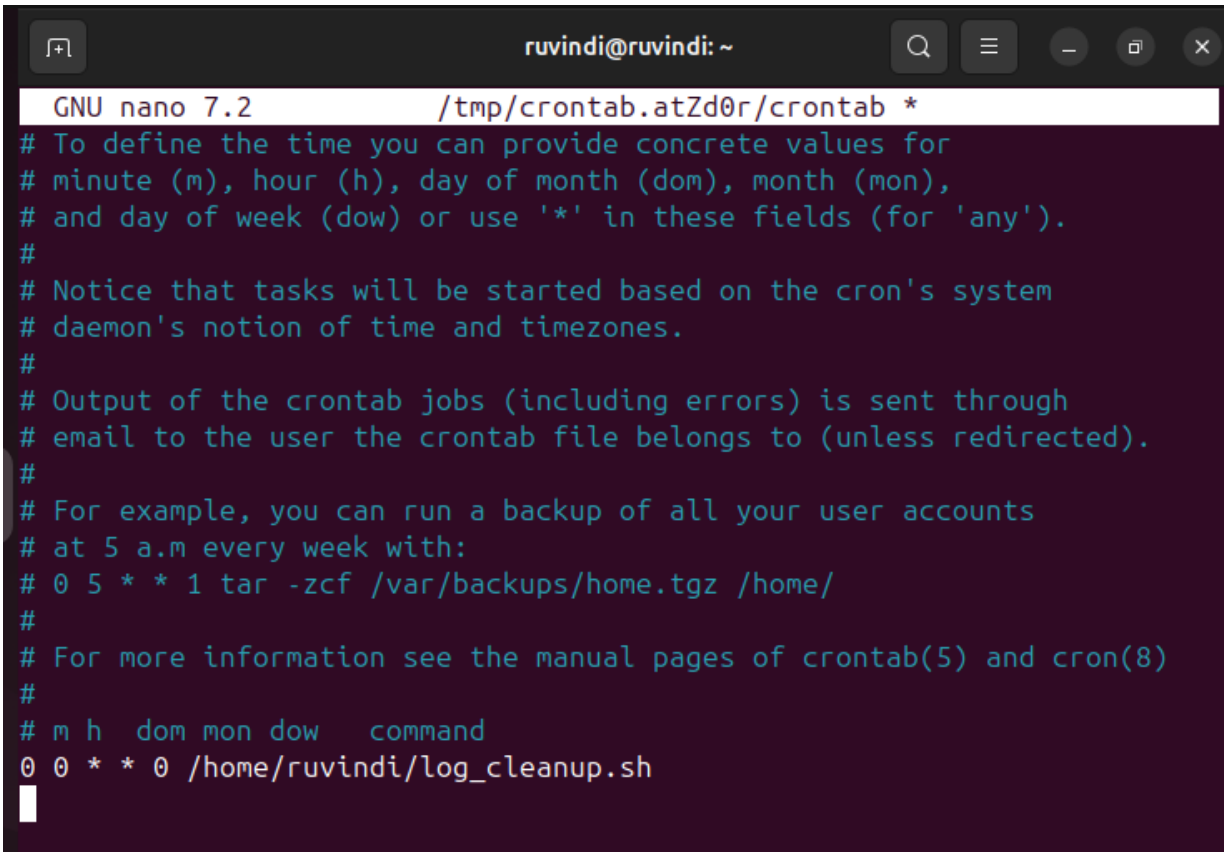






```
ruvindi@ruvindi:~$ chmod +x log_cleanup.sh
ruvindi@ruvindi:~$ ./log_cleanup.sh
tar: Removing leading `/' from member names
/home/ruvindi/logs/custom_logs/test1.log
tar: Removing leading `/' from hard link targets
/home/ruvindi/logs/custom_logs/test2.log
Deleted files:
Remaining files archived at /home/ruvindi/logs/logs_backup/logs_backup_2
0250429.tar.gz
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$ crontab -e
no crontab for ruvindi - 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
ruvindi@ruvindi:~$
```



3.2 SSH Server Setup

1) **Update the package index**

   Update the package with the same command that we used previously.

   "sudo apt update"

2) **Install OpenSSH Server**

   Install OpenSSH using the following command.

   "sudo apt install openssh-server"

3) **Check SSH Service Status**

   After installation, SSH should start automatically. We may check its status with the following command.

   "sudo systemctl status ssh"

- Confirmed that SSH service is active.

4) **Configure SSH Settings**

   "sudo nano /etc/ssh/sshd_config"

5) **Edit SSH Configuration**

   - Change the default port from 22
   - Set "PermitRootLogin no"
   - Ensure PasswordAuthentication yes.

6) **Restart the SSH Service**

   After making changes save the file and restart the SSH Service.
   "sudo systemctl restart ssh"

7) Firewall Configuration

"Sudo ufw allow ssh"

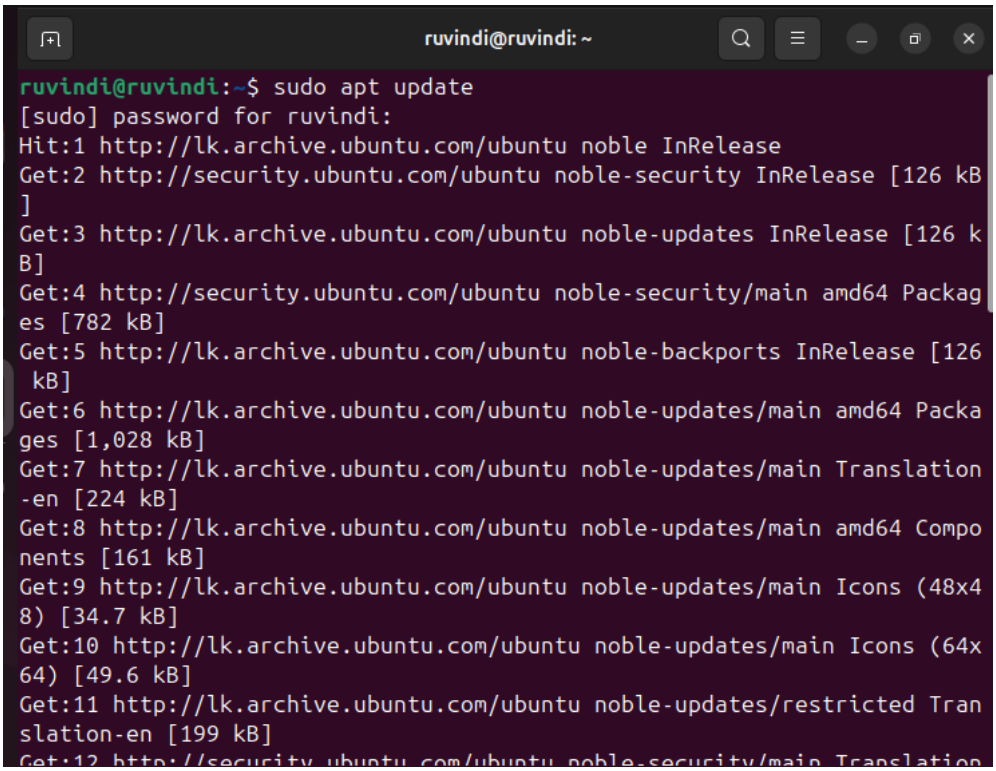
6) Connect to SSH Server Remotely

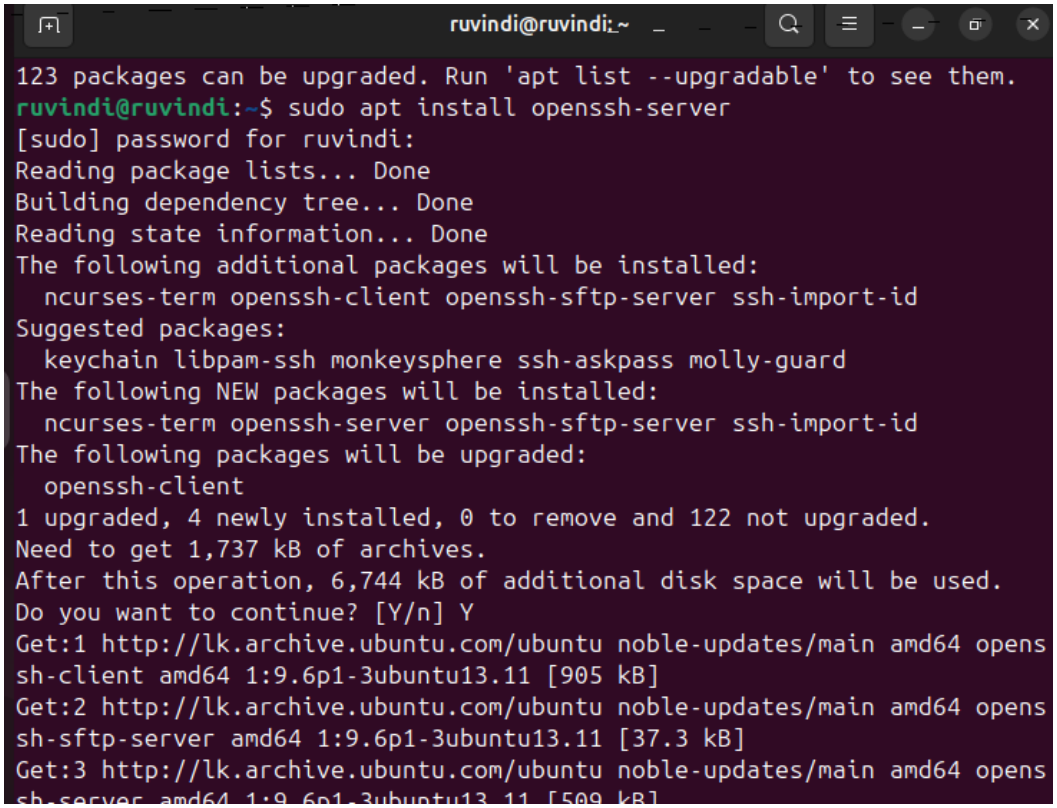
On another machine:
"ssh username@server_ip"
Entered the password and logged in successfully.

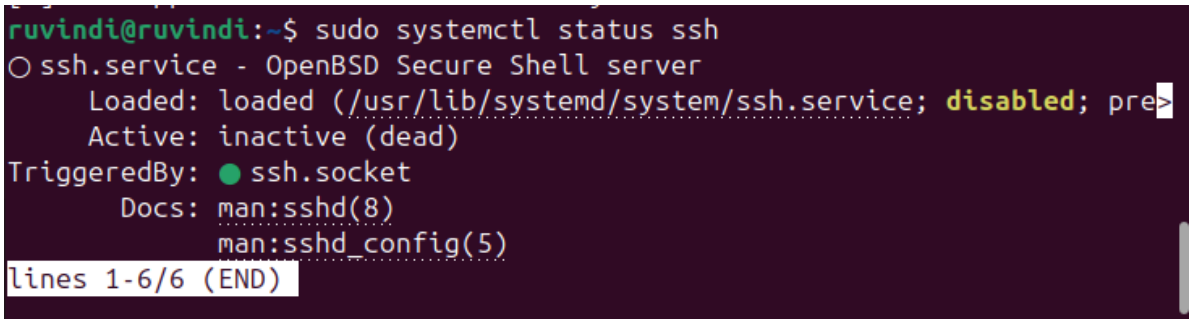
7) Check Status

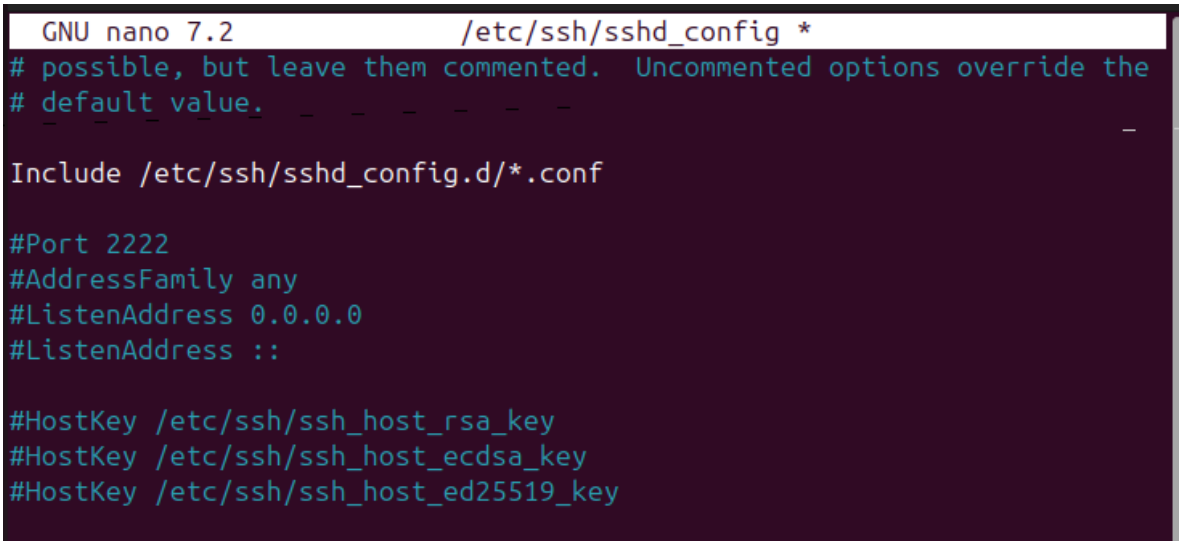
Use the following command to determine whether it is active or inactive.
"sudo systemctl status ssh".

3.2.2 Screenshots of the SSH Server Configuration



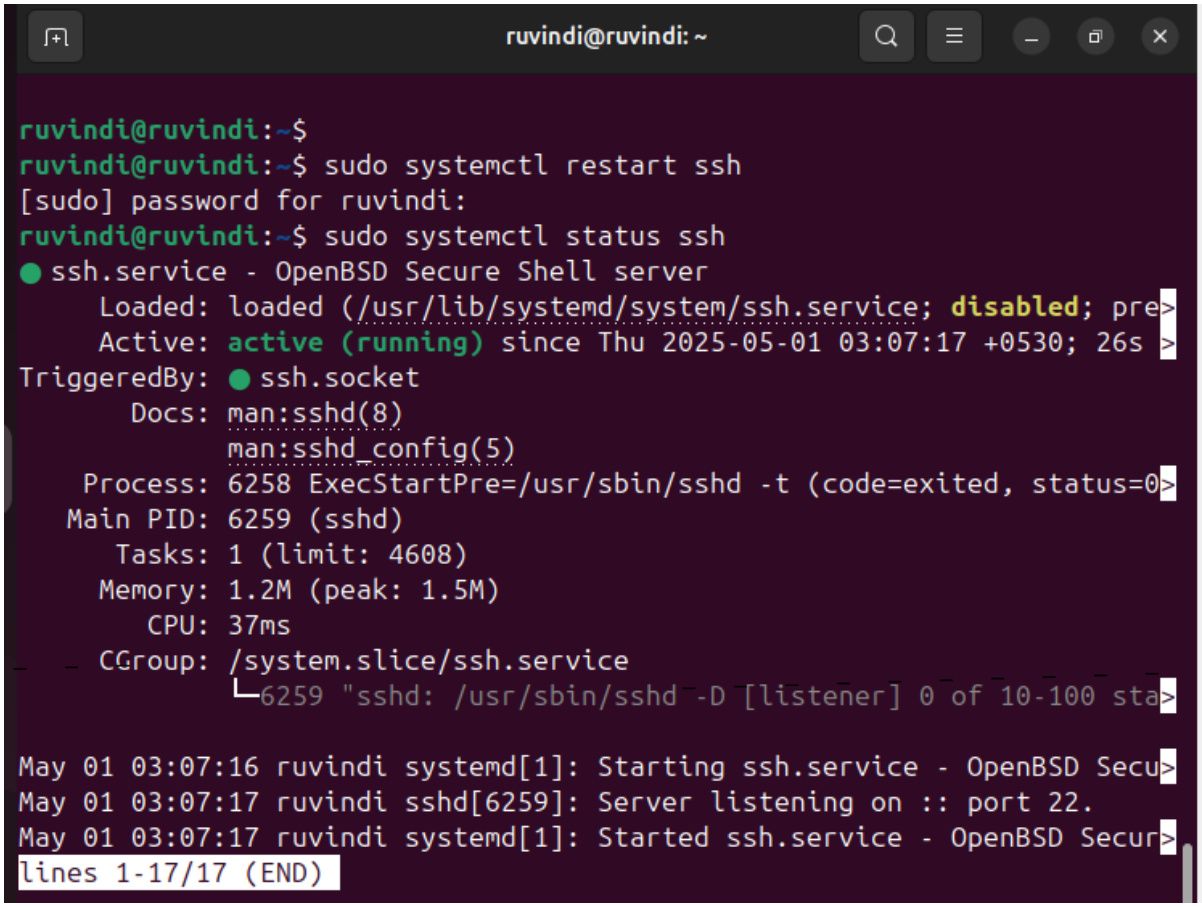

ruvindi@ruvindi: ~
123 packages can be upgraded. Run 'apt list --upgradable' to see them.
ruvindi@ruvindi:~$ sudo apt install openssh-server
[sudo] password for ruvindi:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
openssh-client
1 upgraded, 4 newly installed, 0 to remove and 122 not upgraded.
Need to get 1,737 kB of archives.
After this operation, 6,744 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 opens
sh-client amd64 1:9.6p1-3ubuntu13.11 [905 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 opens
sh-sftp-server amd64 1:9.6p1-3ubuntu13.11 [37.3 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 opens


ruvindi@ruvindi:~$ sudo systemctl status ssh
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; pre>
Active: inactive (dead)
TriggeredBy: ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
lines 1-6/6 (END)


GNU nano 7.2 /etc/ssh/sshd_config *
possible, but leave them commented. Uncommented options override the
default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

```
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
```

```
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
ruvindi@ruvindi:~$ ssh ruvindi@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:YLYw8Yin52E2z4eW5Mc/FejF5h9ZHqwnd9mMQp
efc9Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known ho
sts.
ruvindi@10.0.2.15'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
```



3.3 Firewall (iptables)

A) iptables Configuration

1) Update the package index

Update the package with the same command that we used previously.

"sudo apt update"

2) Install iptables

Install the iptables using following command.

"sudo apt install iptables"

3) Allow SSH Access

Allow SSH (remote access) to server.

"sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT"

- –A INPUT: Append this rule to the INPUT chain (incoming traffic).
- -p tcp: Match TCP protocol.
- --dport 22: Match destination port 22 (used for SSH).
- -j ACCEPT: Allow the connection.

Purpose: Ensures you don't get locked out of your server when applying firewall rules.

4) Allow Only Secure Browsing (HTTPS) (Block HTTP)

Allow HTTPS (Port 443):

"iptables -A FORWARD -p tcp --dport 443 -j ACCEPT"

Permits forwarding of traffic to secure websites (port 443).

Block HTTP (Port 80):

"iptables -A FORWARD -p tcp --dport 80 -j REJECT"

Denies forwarding of unencrypted web traffic (port 80).

5) Block Social Media Websites

Blocks Facebook-related traffic:

"sudo iptables -A OUTPUT -d 157.240.0.0/16 -j REJECT"

Blocks Instagram-related traffic

"sudo iptables -A FORWARD -d 31.13.64.0/18 -j REJECT"

6) Allow Ping (ICMP Echo Request)

Allow the server to respond to pings.

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

7) Allow Web Server Access (HTTP/HTTPS)

Allow web server traffic (website hosting)

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

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

8) Save and Make iptables Rules Persistent

Saved rules so they survive reboot.

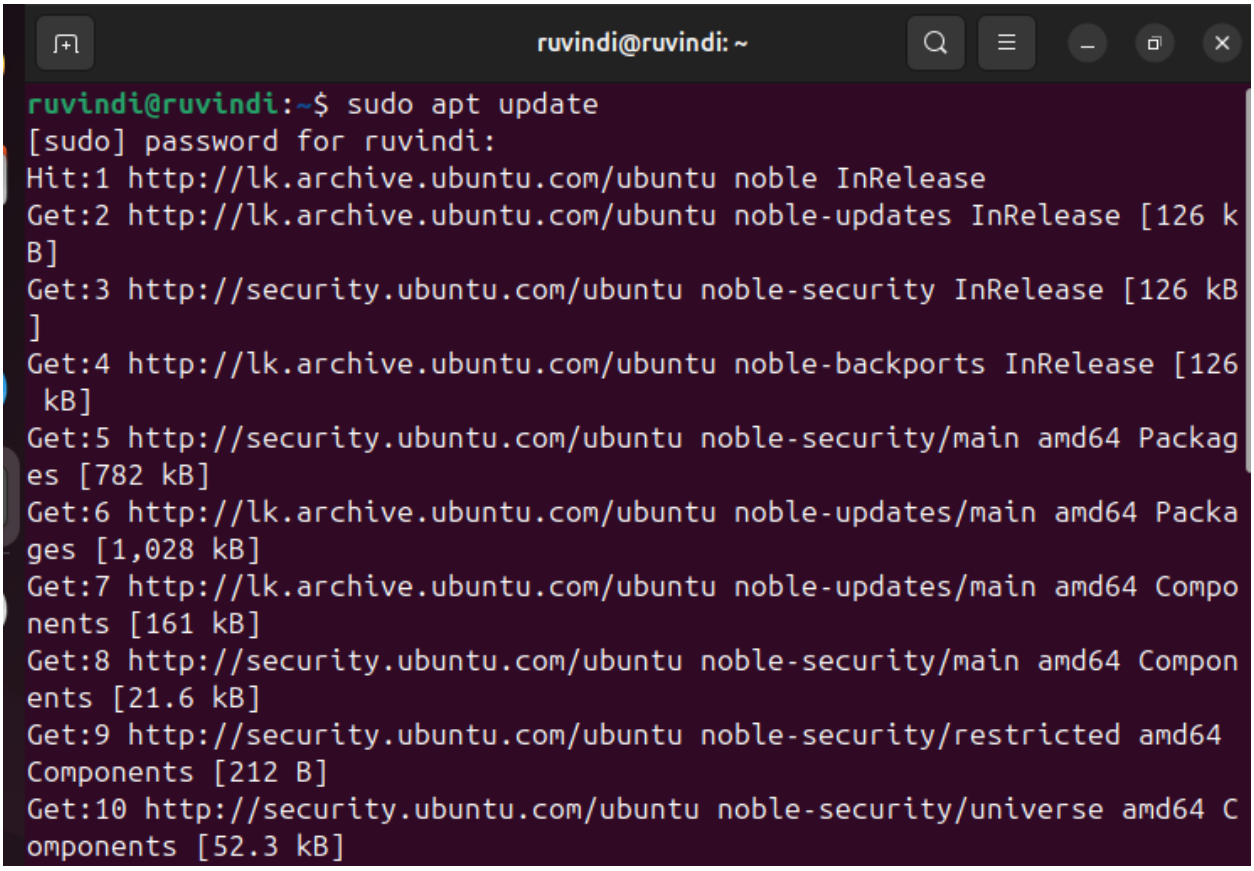
"sudo apt install iptables-persistent"

iptables-persistent: A package that saves your current iptables rules and reloads them automatically on reboot.

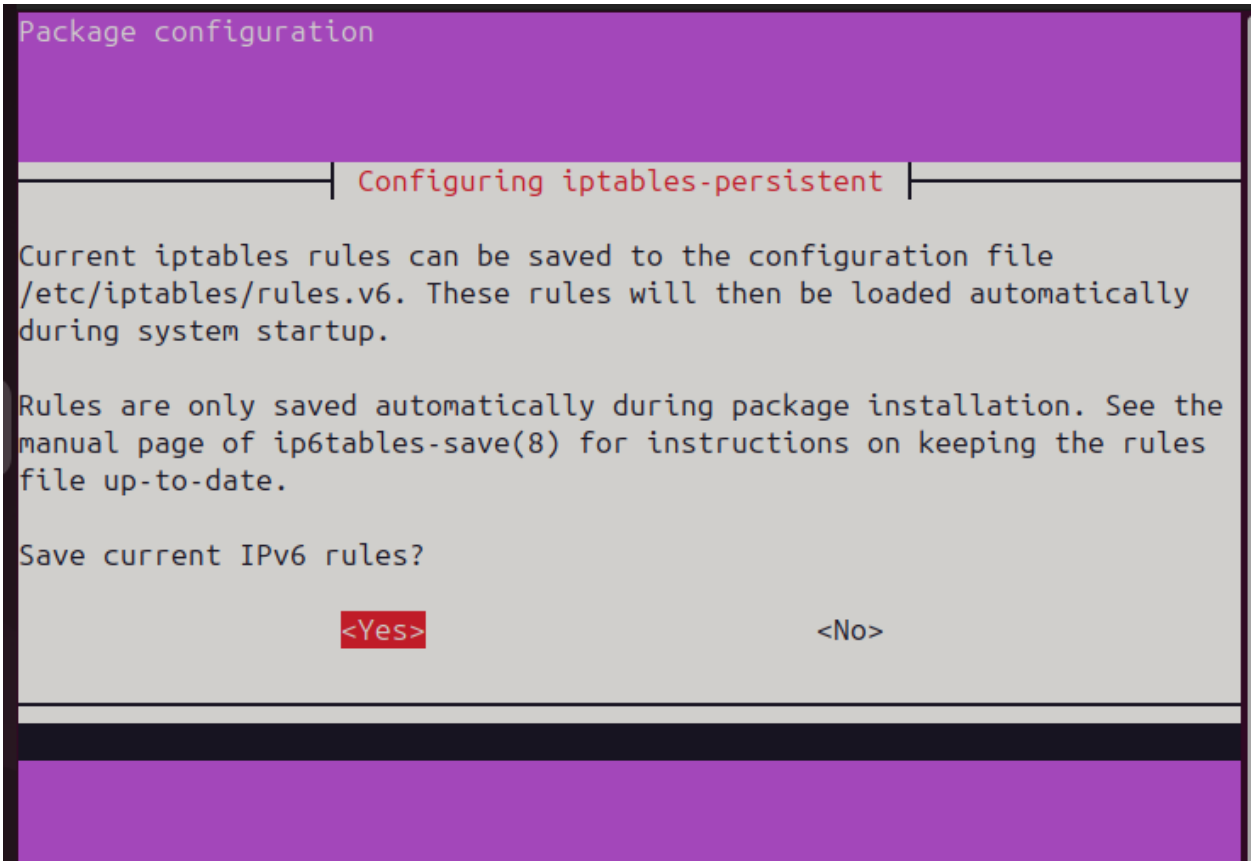
"sudo netfilter-persistent save"

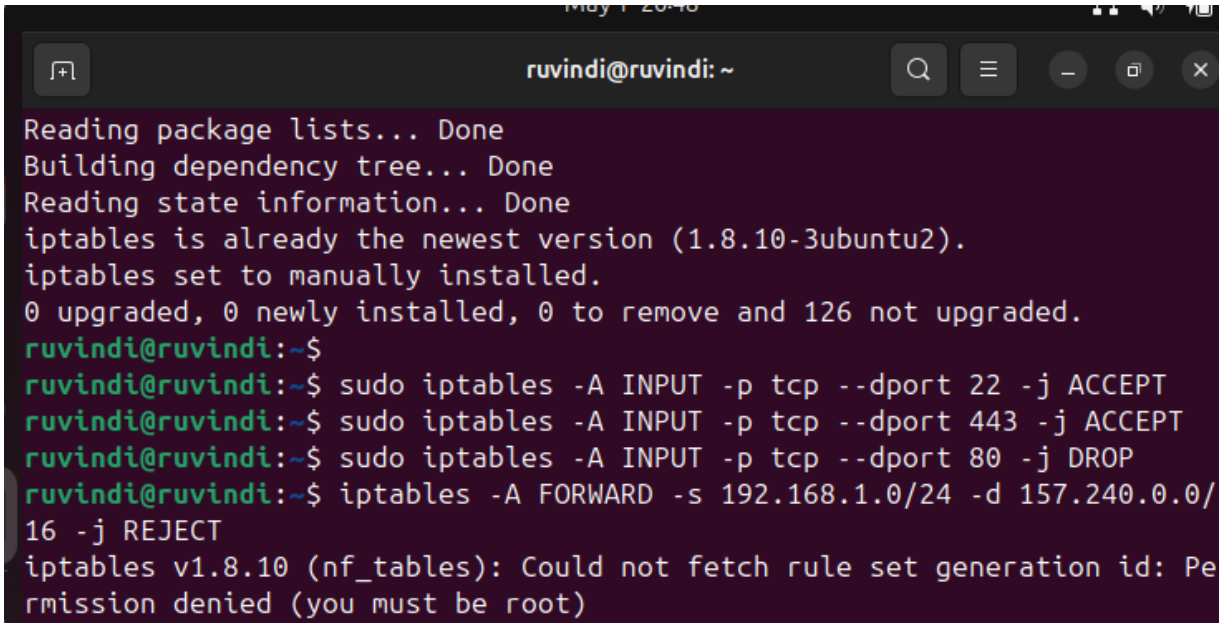
netfilter-persistent save: Saves current active rules to disk.

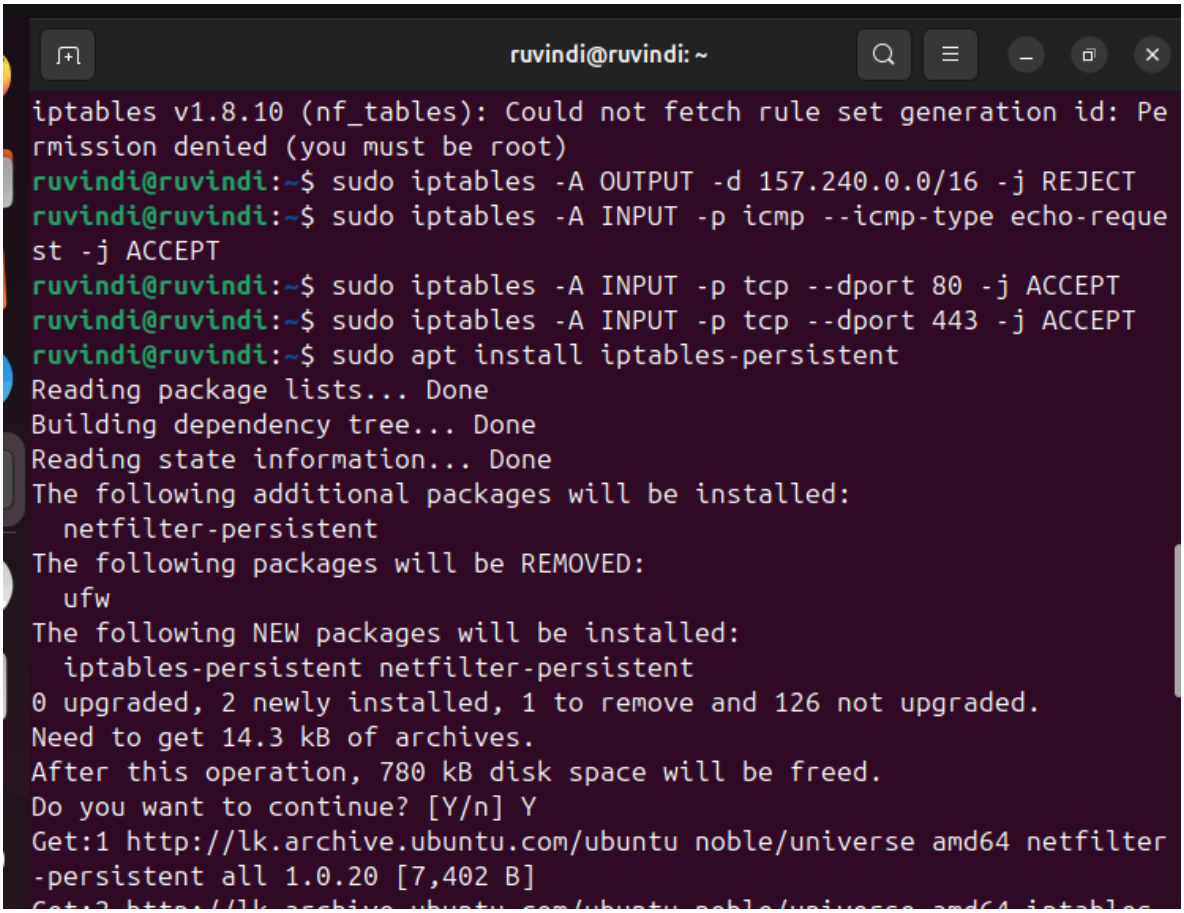
3.3.3 Screenshots of iptables Configuration



```
Reading state information... Done
126 packages can be upgraded. Run 'apt list --upgradable' to see them.
ruvindi@ruvindi:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 126 not upgraded.
ruvindi@ruvindi:~$
```




ruvindi@ruvindi: ~
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 126 not upgraded.
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
ruvindi@ruvindi:~$ iptables -A FORWARD -s 192.168.1.0/24 -d 157.240.0.0/
16 -j REJECT
iptables v1.8.10 (nf_tables): Could not fetch rule set generation id: Pe
rmission denied (you must be root)


ruvindi@ruvindi: ~
iptables v1.8.10 (nf_tables): Could not fetch rule set generation id: Pe
rmission denied (you must be root)
ruvindi@ruvindi:~$ sudo iptables -A OUTPUT -d 157.240.0.0/16 -j REJECT
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-reque
st -j ACCEPT
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
ruvindi@ruvindi:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
ruvindi@ruvindi:~$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
netfilter-persistent
The following packages will be REMOVED:
ufw
The following NEW packages will be installed:
iptables-persistent netfilter-persistent
0 upgraded, 2 newly installed, 1 to remove and 126 not upgraded.
Need to get 14.3 kB of archives.
After this operation, 780 kB disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 netfilter
-persistent all 1.0.20 [7,402 B]

```
Preparing to unpack .../iptables-persistent_1.0.20_all.deb ...
Unpacking iptables-persistent (1.0.20) ...
Setting up netfilter-persistent (1.0.20) ...
Created symlink /etc/systemd/system/iptables.service → /usr/lib/systemd/
system/netfilter-persistent.service.
Created symlink /etc/systemd/system/ip6tables.service → /usr/lib/systemd
/system/netfilter-persistent.service.
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-pe
rsistent.service → /usr/lib/systemd/system/netfilter-persistent.service.
Setting up iptables-persistent (1.0.20) ...
Processing triggers for man-db (2.12.0-4build2) ...
ruvindi@ruvindi:~$ sudo netfilter-persistent save
[sudo] password for ruvindi:
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tab
les save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tab
les save
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi: ~
ruvindi@ruvindi:~$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 496 packets, 122K bytes)
 pkts bytes target     prot opt in     out     source               dest
ination
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.
0.0/0            tcp dpt:22
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.
0.0/0            tcp dpt:443
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.
0.0/0            tcp dpt:80
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.
0.0/0            icmptype 8
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.
0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.
0.0/0            tcp dpt:443

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               dest
ination

Chain OUTPUT (policy ACCEPT 484 packets, 75606 bytes)
 pkts bytes target     prot opt in     out     source               dest
ination
```

B) ACLs (Access Control Lists)

1) Update the package index

Update the package with the same command that we used previously.

"sudo apt update"

2) Install the ACL Tool

Install the iptables using following command.

"sudo apt install acl"

3) Mount Filesystem with ACL Support

Remounted root filesystem with ACL support.

"sudo mount -o remount,acl /"

4) Create a test folder (if you don't have one)

This creates a folder in your home directory named test_acl_folder

"mkdir -p ~/test_acl_folder"

5) Set ACL on a Directory

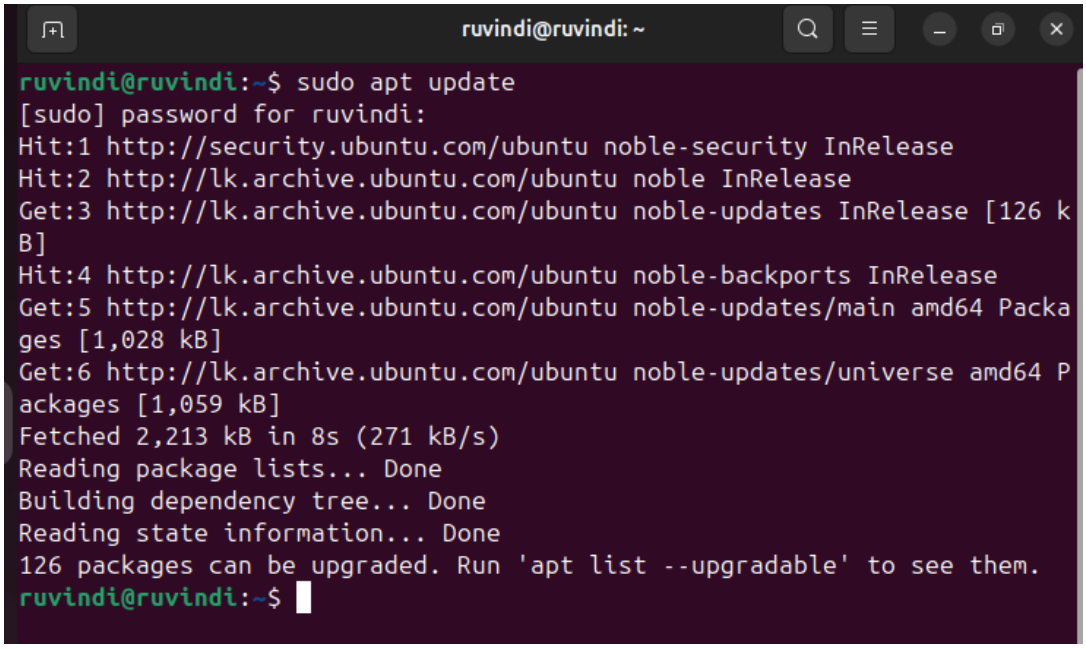
"sudo setfacl -m u:username:rwx /path/to/directory"

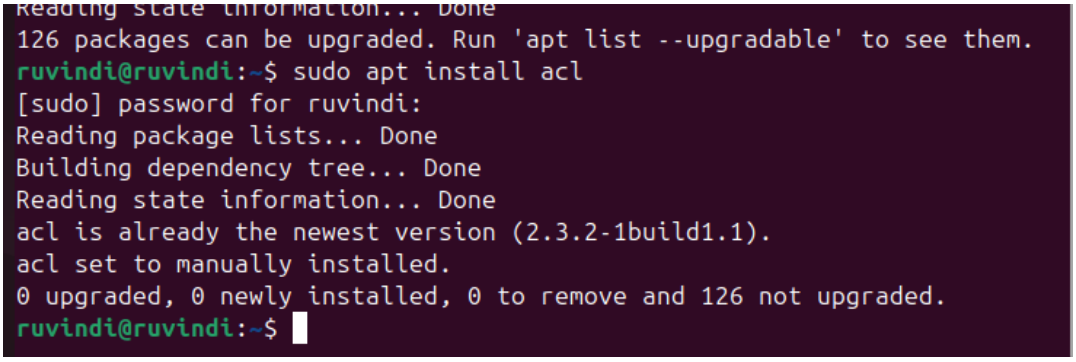
6) Check ACL Permissions

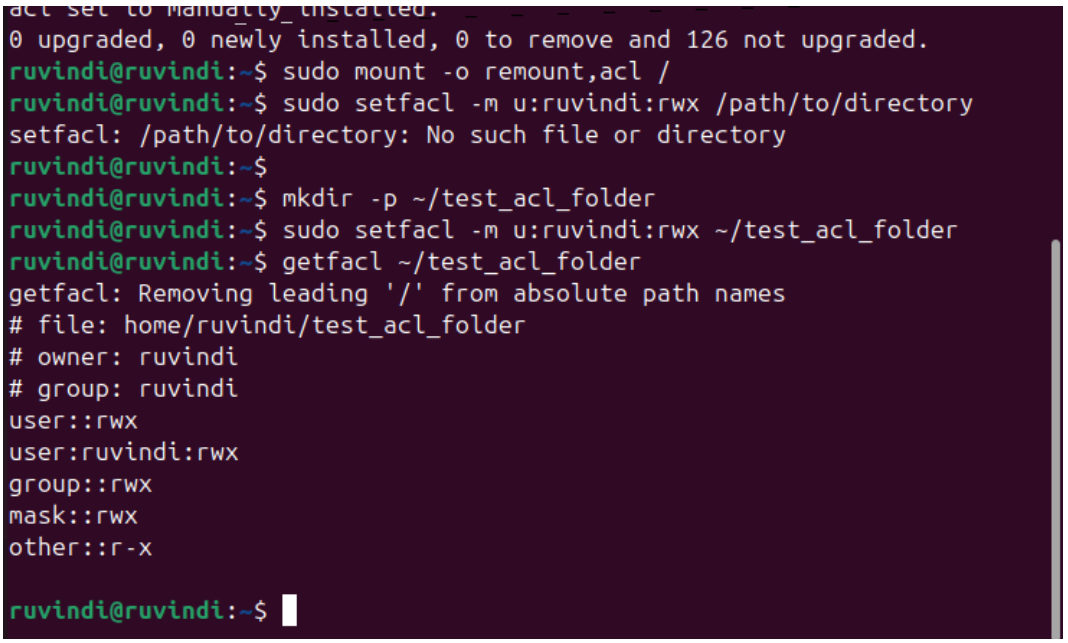
Verified the applied ACLs.

"getfacl /path/to/directory"

3.3.4 Screen Shots of ACLs Setup







3.4 Web Server (Apache) Installation and Setup

1) **Install Apache**

"sudo apt update"
"sudo apt install apache2 -y"

2) **Start and Enable Apache**

"sudo systemctl start apache2"
"sudo systemctl enable apache2"

3) **Verify Apache is Running**

You should see active (running).
"sudo systemctl ststus apache2"

4) **Create a Simple Web Page**

You can also manually edit it:
"sudo nano /var/www/html/index.html"

5) **Get your Virtual Box IP Address**
"ip a"

6) **Access Web Page from Another Machine**

Open a browser and enter:
"http://10.0.2.15"

You should see your custom web page.

3.4.4 Screenshots of the Web Server Installation

```
ruvindi@ruvindi:~$ sudo apt update
[sudo] password for ruvindi:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble 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.
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$ sudo apt install apache2 -y
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 libapr1t64 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 131 not upgraded.
Need to get 1,900 kB of archives.
After this operation, 7,455 kB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.
1 [108 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.
9 kB]
```

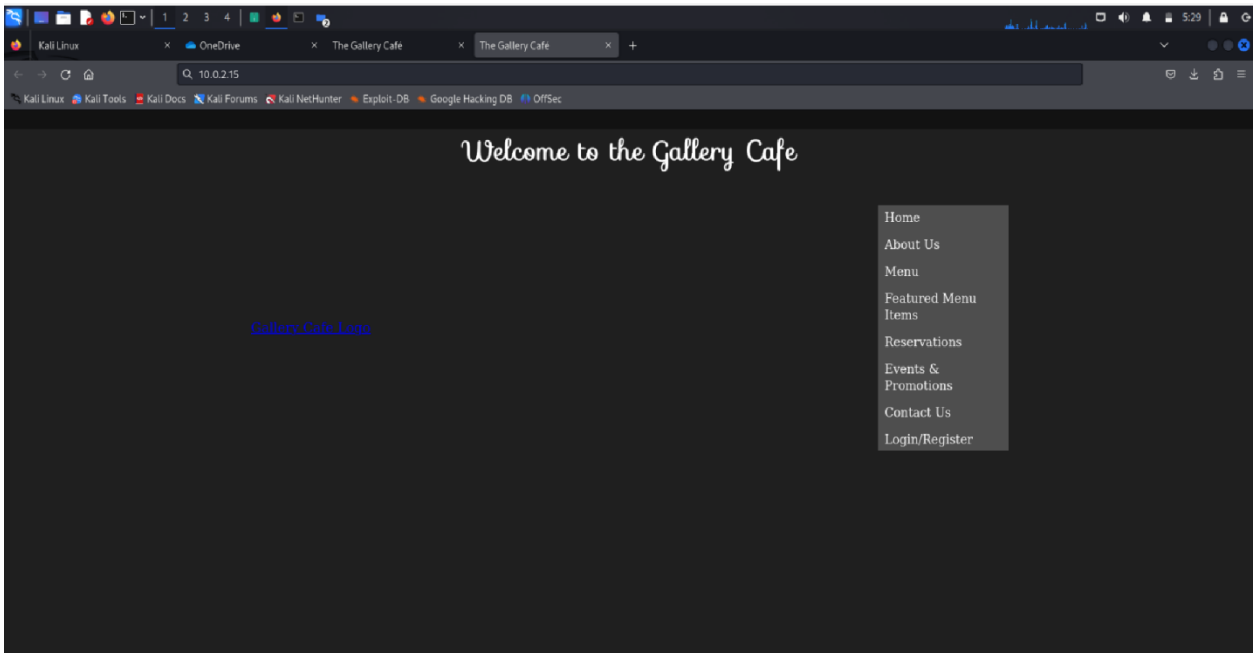
```
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
ruvindi@ruvindi:~$ sudo systemctl start apache2
ruvindi@ruvindi:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-in
stall.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ruvindi@ruvindi:~$
```

```
stall.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ruvindi@ruvindi:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-02 11:47:31 +0530; 19min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 7606 (apache2)
      Tasks: 55 (limit: 4608)
     Memory: 5.5M (peak: 6.0M)
        CPU: 197ms
     CGroup: /system.slice/apache2.service
             ├─7606 /usr/sbin/apache2 -k start
             ├─7608 /usr/sbin/apache2 -k start
             └─7609 /usr/sbin/apache2 -k start

May 02 11:47:31 ruvindi systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 02 11:47:31 ruvindi apachectl[7605]: AH00558: apache2: Could not reliably determine the server's>
May 02 11:47:31 ruvindi systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-16/16 (END)
[1]+  Stopped                 sudo systemctl status apache2
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi: ~
 GNU nano 7.2                          /var/www/html/GalleryCafe.html *
    <link rel="stylesheet" href="styles.css">
    <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Sofia">
</head>
<body>
    <header>
        <h1>Welcome to the Gallery Cafe</h1>
        <div class="container">
            <div class="logo">
                <a href="index.html"><img src="Images/Logo.png" alt="Gallery Cafe Logo"></a>
            </div>
            <nav class="nav-menu">
                <ul>
                    <li><a href="index.html">Home</a></li>
                    <li><a href="about.html">About Us</a></li>
                    <li><a href="menu.html">Menu</a></li>
                    <li><a href="featured.html">Featured Menu Items</a></li>
                    <li><a href="reservations.html">Reservations</a></li>
                    <li><a href="events.html">Events & Promotions</a></li>
                    <li><a href="contact.html">Contact Us</a></li>
                    <li class="active"><a href="auth.html">Login/Register</a></li>
                </ul>
            </nav>
            <div class="menu-toggle">
                <span class="bar"></span>
                <span class="bar"></span>
                <span class="bar"></span>

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

```
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo nano /var/www/html/GalleryCafe.html
[sudo] password for ruvindi:
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$ 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:d1:9c:50 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 70544sec preferred_lft 70544sec
    inet6 fd00::b229:8a3f:957d:ca86/64 scope global temporary dynamic
       valid_lft 86339sec preferred_lft 14339sec
    inet6 fd00::a00:27ff:fed1:9c50/64 scope global dynamic mngtmpaddr
       valid_lft 86339sec preferred_lft 14339sec
    inet6 fe80::a00:27ff:fed1:9c50/64 scope link
       valid_lft forever preferred_lft forever
ruvindi@ruvindi:~$
```



3.5 Email Server Setup

1) Update System

"sudo apt update"
Refreshes the package lists to get the latest versions.

"sudo apt upgrade -y"
Installs all available upgrades for the system packages without prompting for confirmation.

2) Install Postfix

During installation, you will see a configuration screen:

- Choose **"Internet Site"**
- For **"System mail name"**, enter your hostname (e.g., yourdomain.com or localhost if for testing)

"sudo apt install postfix -y"

3) Configure Postfix (Basic)

"sudo nano /etc/postfix/main.cf"

Ensure these values are present (adjust your hostname/domain as needed):

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

- myhostname: Fully Qualified Domain Name (FQDN) of your server.
- myorigin: Sets the domain name Postfix uses in outgoing mail.
- mydestination: Specifies what domains the mail server will receive emails for.
- inet_interfaces = all: Makes Postfix listen on all available network interfaces.

- inet_protocols = ipv4: Ensures Postfix uses IPv4 only (can avoid issues if IPv6 isn't configured).

Then restart Postfix:

"sudo systemctl restart postfix"
"sudo systemctl enable postfix"

4) Send a Test Email

Install the mail command:

"sudo apt install mailutils -y"

Then send a test email:

"echo "This is a test email" | mail -s "Test Subject" yourusername@localhost"

Check local mail:

"mail"

Use Enter to navigate and q to quit.

5) Check Port Listening

Ensure Postfix is listening on port 25 (SMTP):

"sudo ss -tuln | grep :25"

6) Check Mail Logs

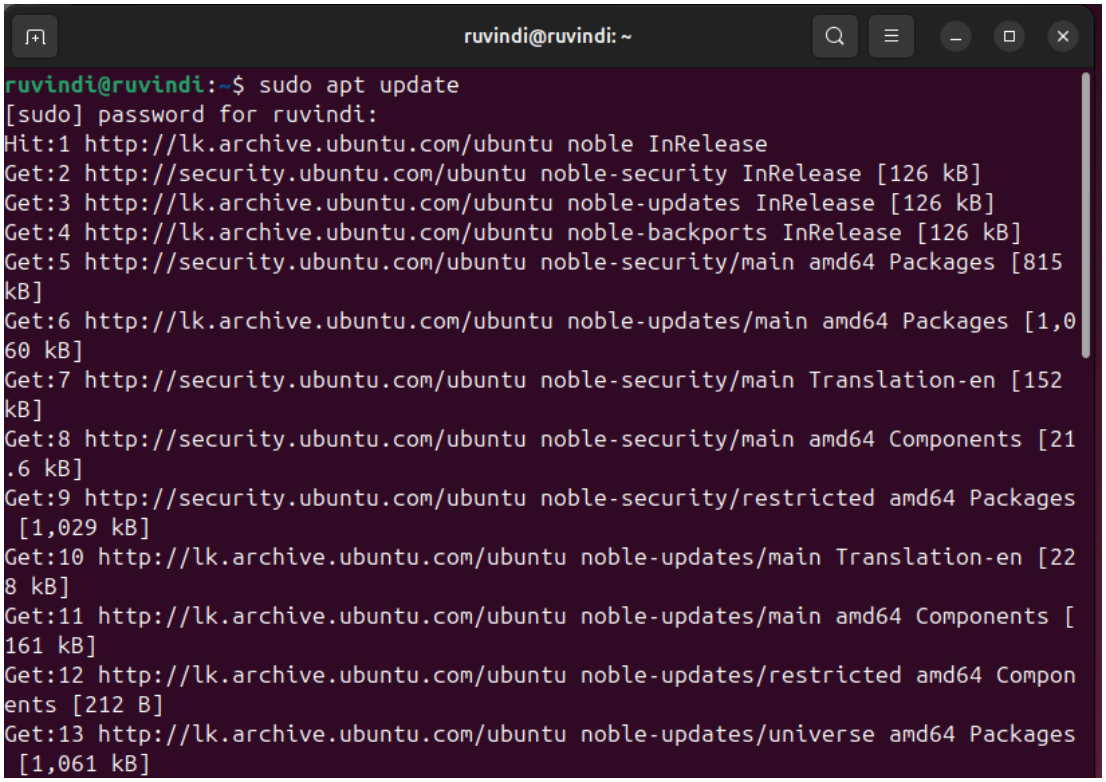
Check logs to verify if emails were sent:

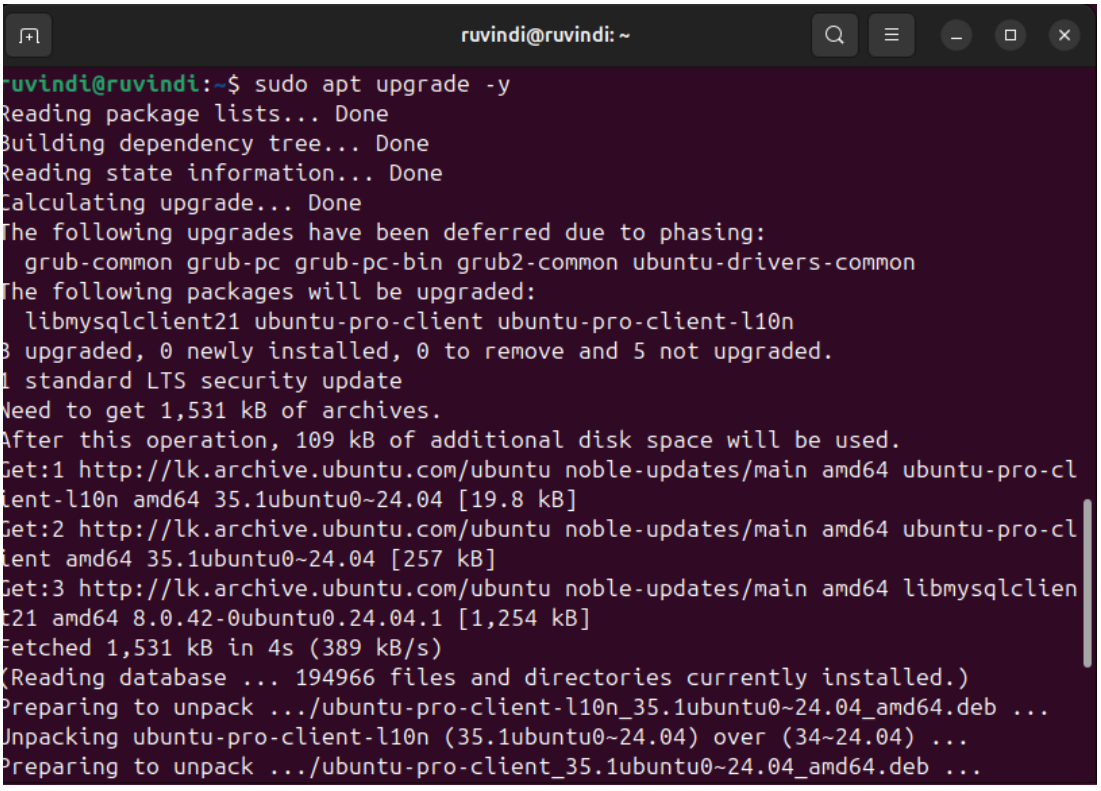
"sudo tail -f /var/log/mail.log"

7) Enable Postfix at Boot

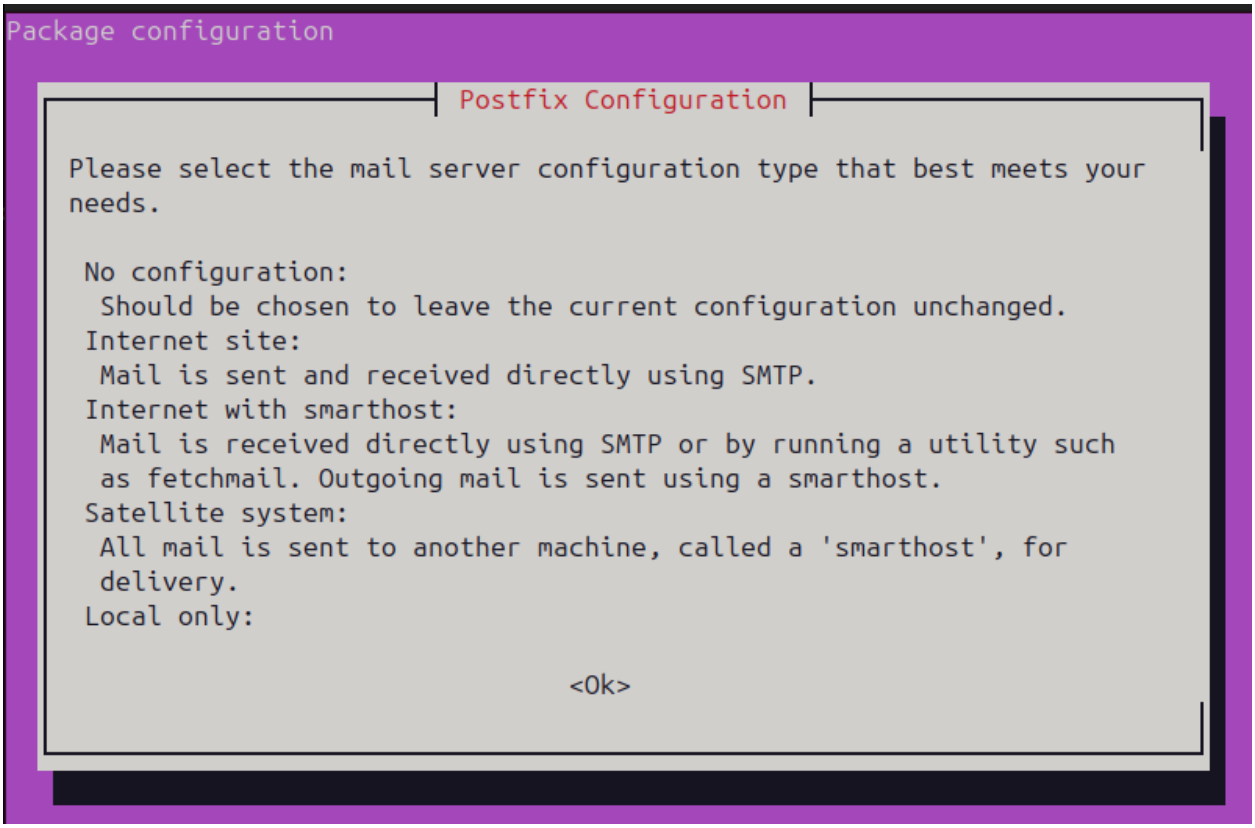
"sudo systemctl enable postfix"

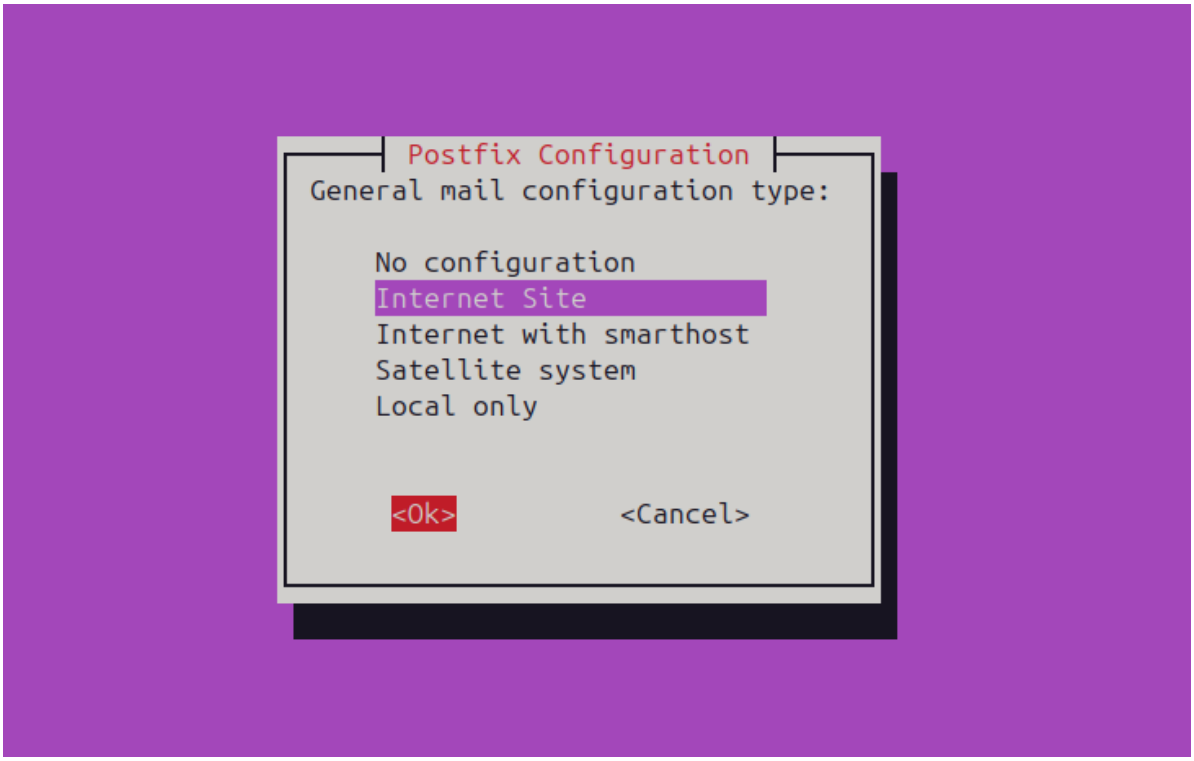
3.5.5 Screen Shots of the Email Server Setup

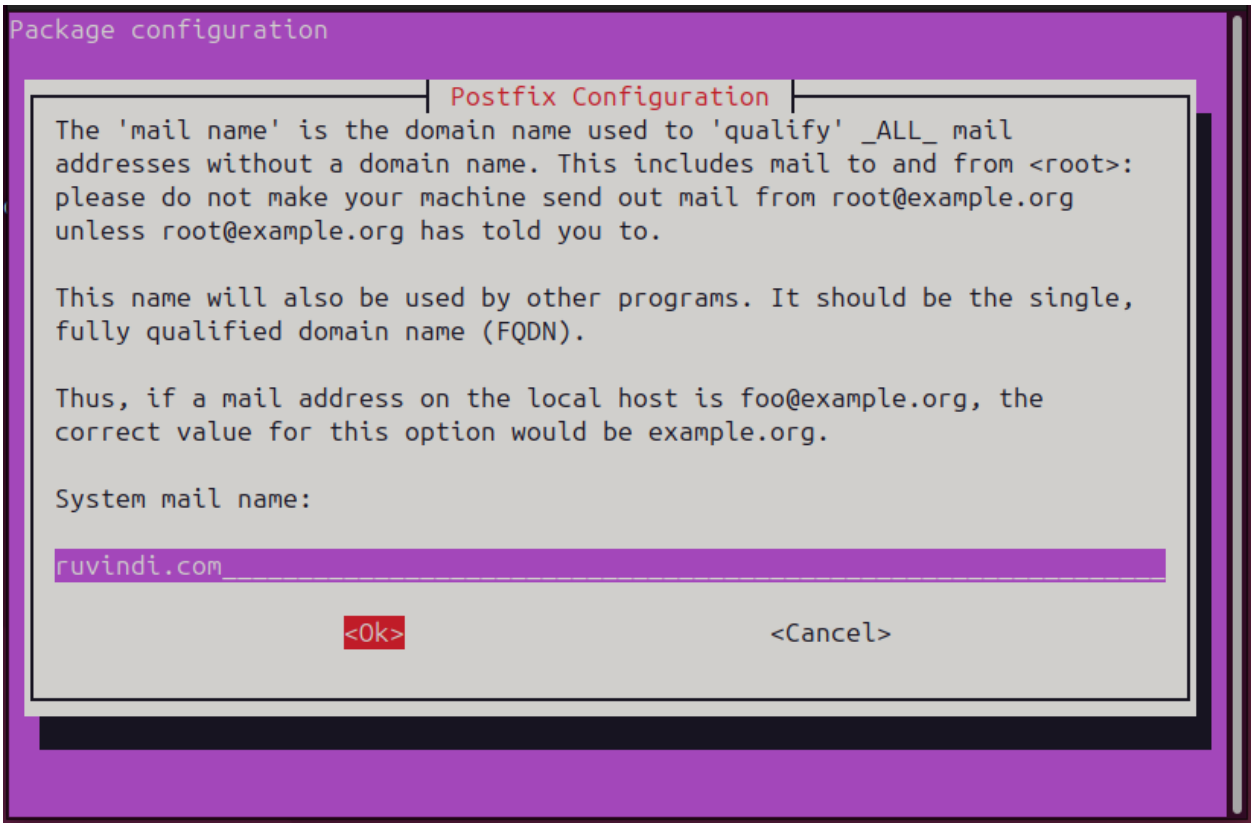


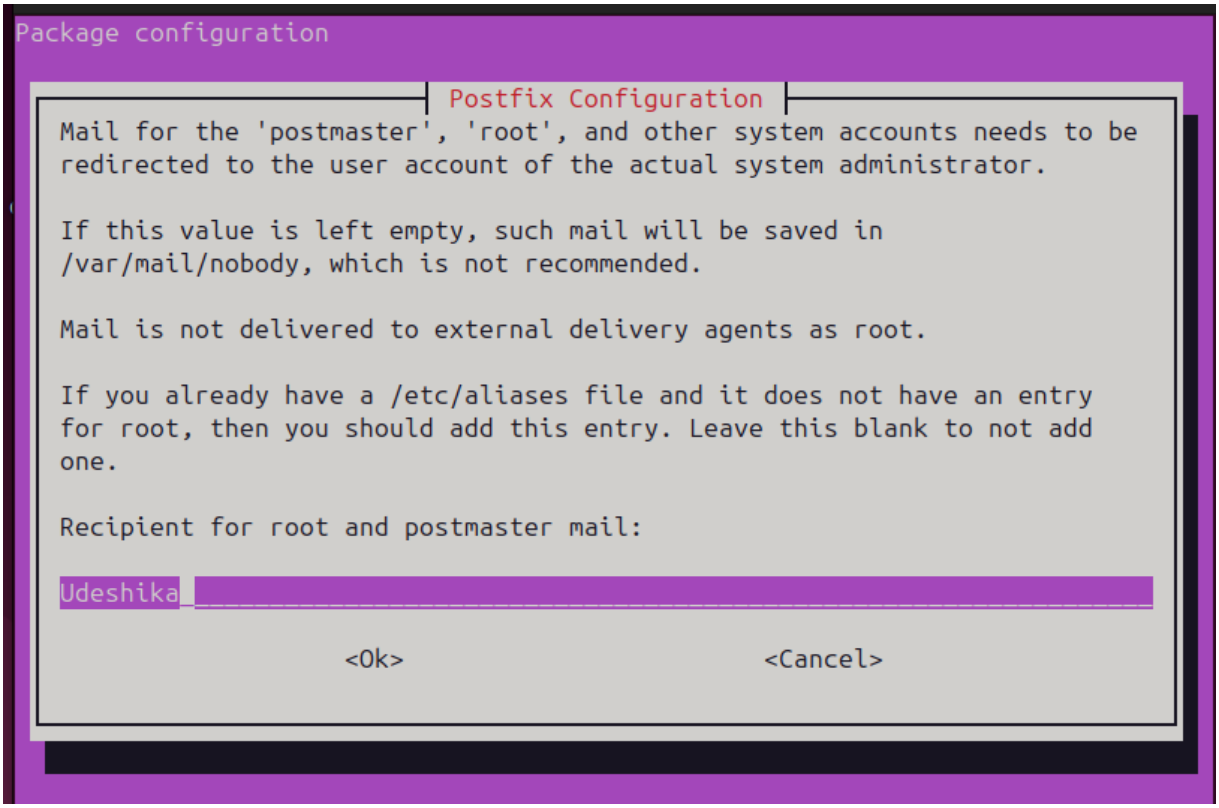


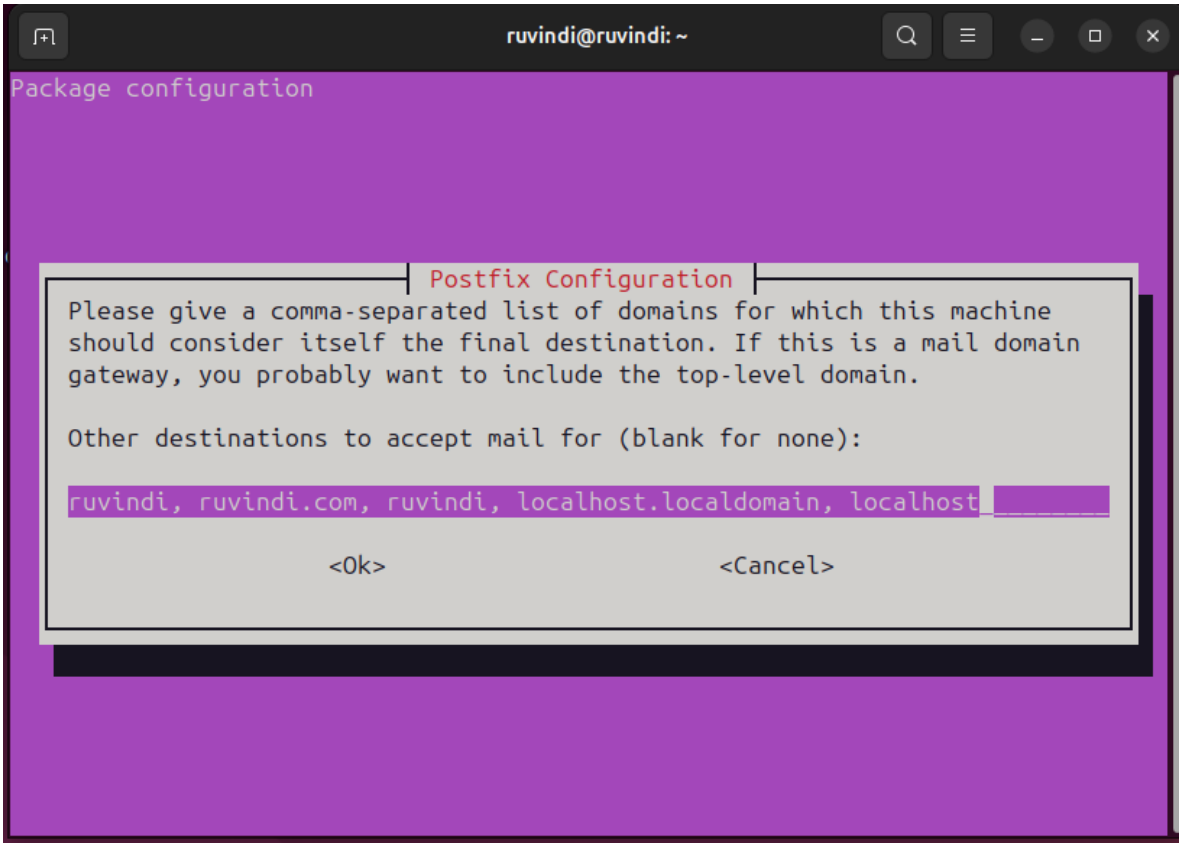
```
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo apt install postfix -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
postfix is already the newest version (3.8.6-1build2).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
ruvindi@ruvindi:~$
```

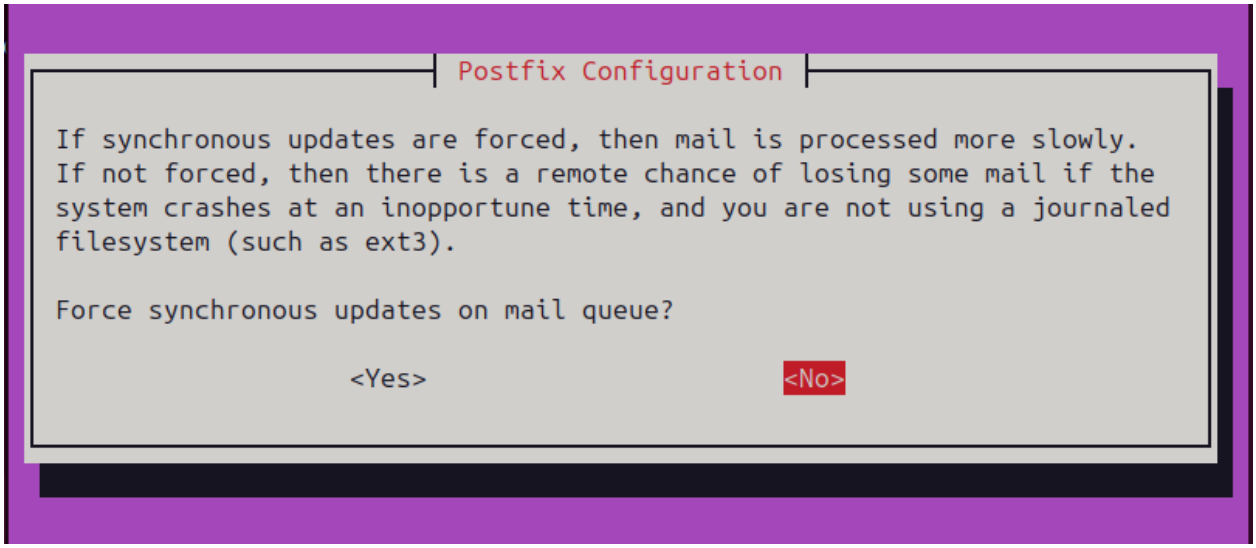


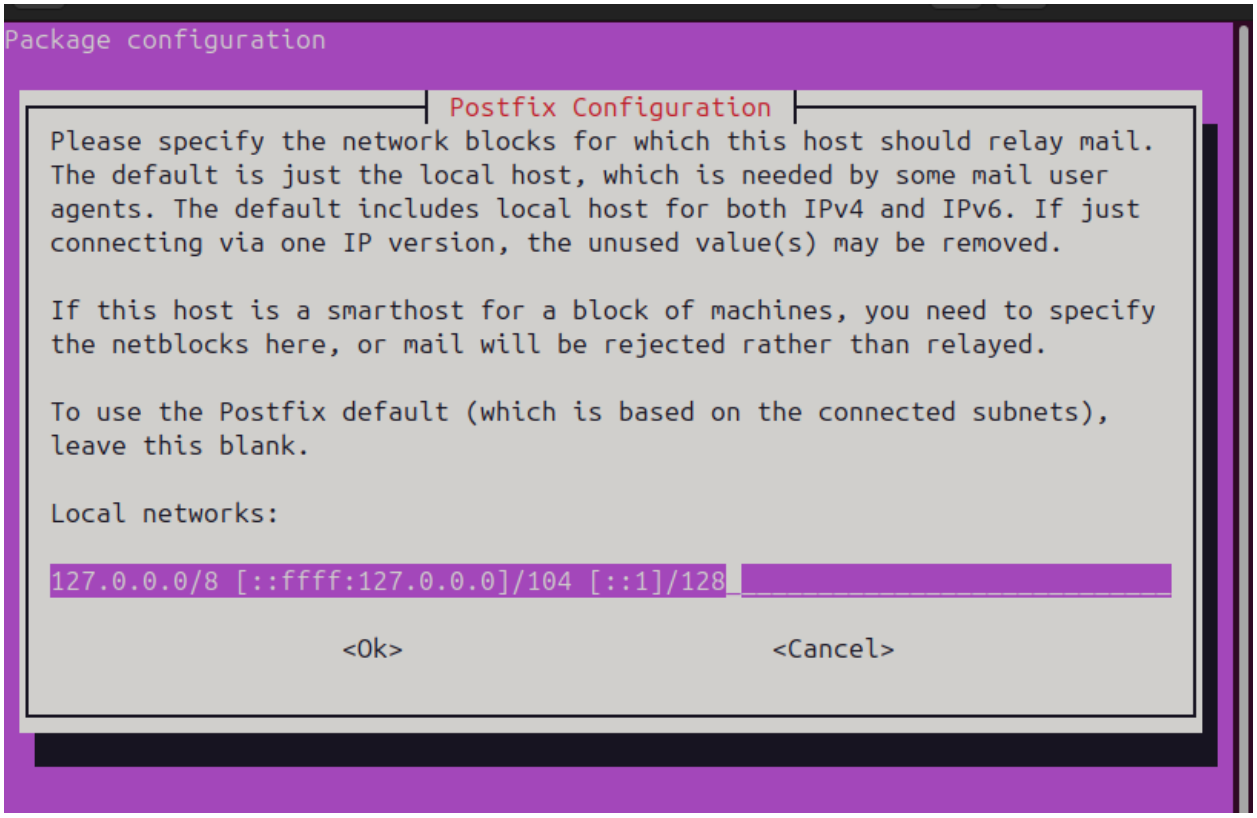

Postfix Configuration
General mail configuration type:
No configuration
Internet Site
Internet with smarthost
Satellite system
Local only
<Ok>
<Cancel>

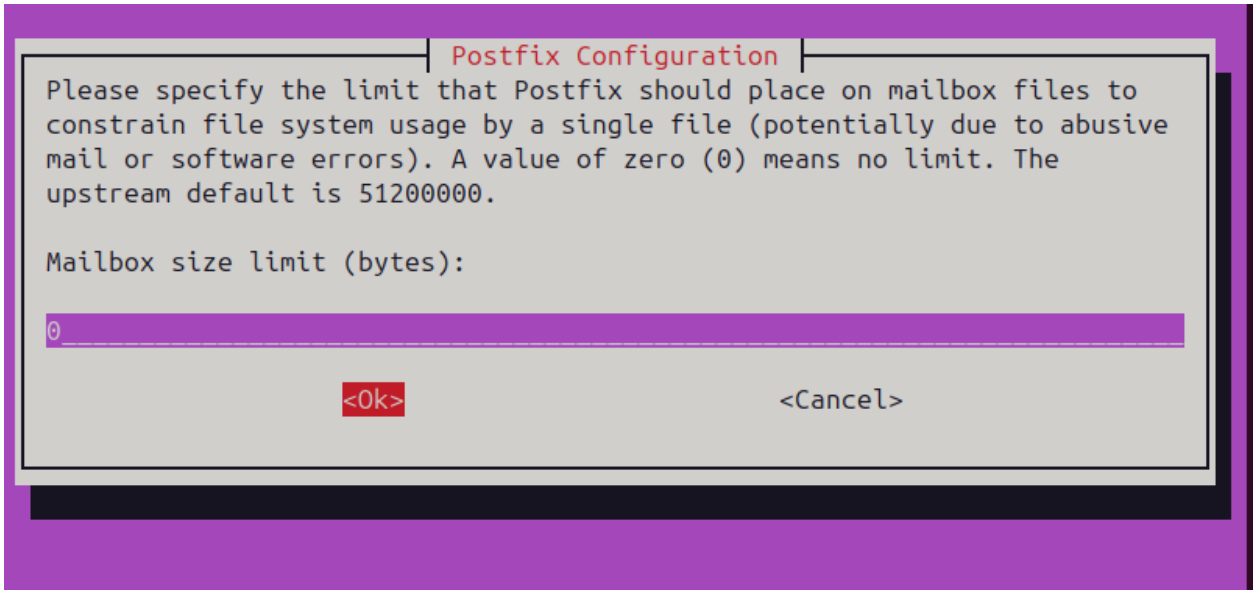

Package configuration
Postfix Configuration
The 'mail name' is the domain name used to 'qualify' _ALL_ mail addresses without a domain name. This includes mail to and from <root>: please do not make your machine send out mail from root@example.org unless root@example.org has told you to.
This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).
Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.
System mail name:
ruvindi.com
<Ok>
<Cancel>

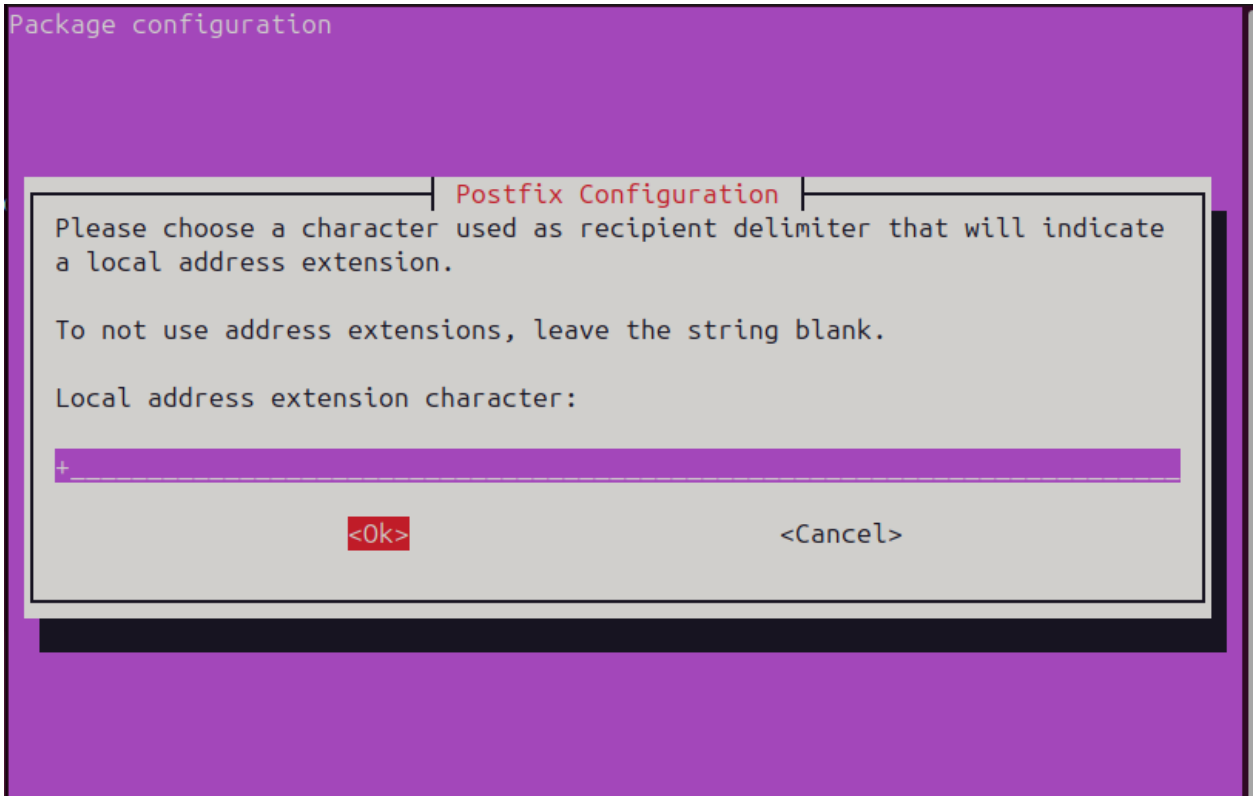

Package configuration
Postfix Configuration
Mail for the 'postmaster', 'root', and other system accounts needs to be redirected to the user account of the actual system administrator.
If this value is left empty, such mail will be saved in /var/mail/nobody, which is not recommended.
Mail is not delivered to external delivery agents as root.
If you already have a /etc/aliases file and it does not have an entry for root, then you should add this entry. Leave this blank to not add one.
Recipient for root and postmaster mail:
Udeshika
<Ok>
<Cancel>

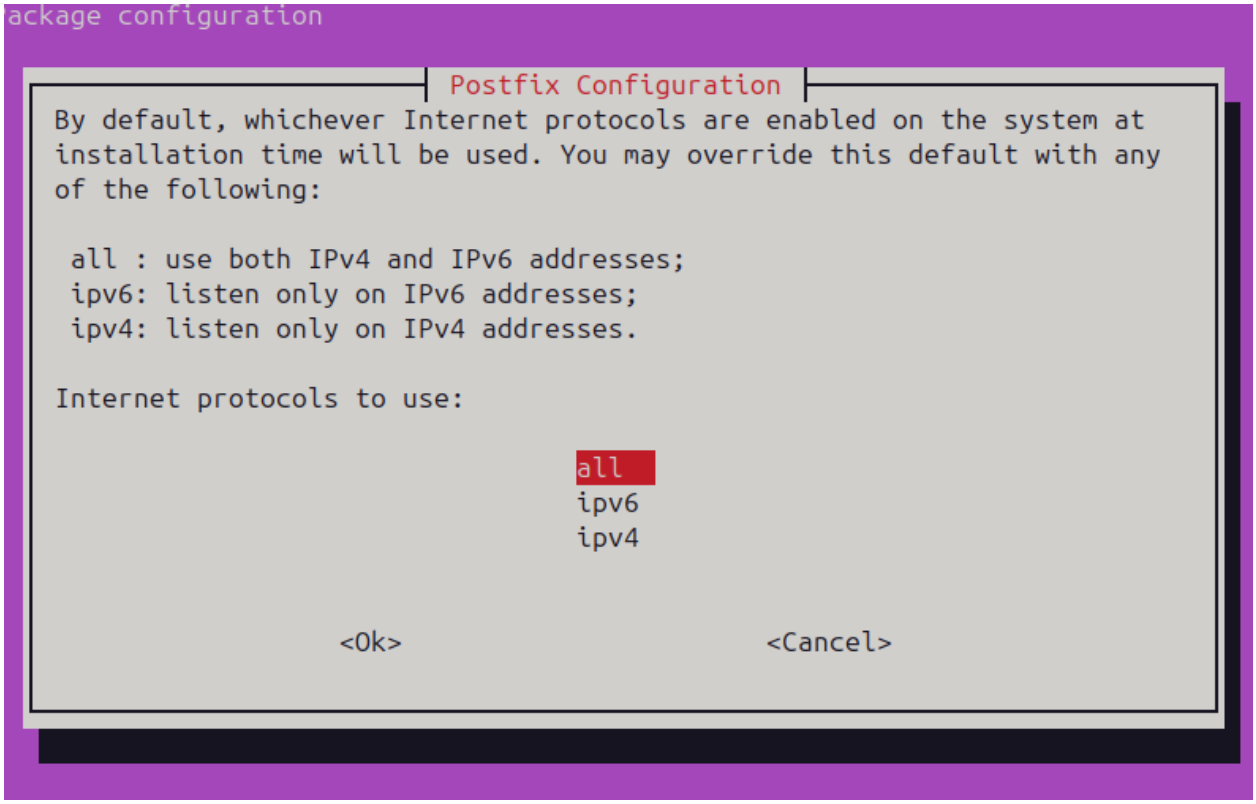

ruvindi@ruvindi: ~
Package configuration
Postfix Configuration
Please give a comma-separated list of domains for which this machine should consider itself the final destination. If this is a mail domain gateway, you probably want to include the top-level domain.
Other destinations to accept mail for (blank for none):
ruvindi, ruvindi.com, ruvindi, localhost.localdomain, localhost
<Ok>
<Cancel>


Postfix Configuration
If synchronous updates are forced, then mail is processed more slowly.
If not forced, then there is a remote chance of losing some mail if the
system crashes at an inopportune time, and you are not using a journaled
filesystem (such as ext3).
Force synchronous updates on mail queue?
<Yes>
<No>


Package configuration
Postfix Configuration
Please specify the network blocks for which this host should relay mail.
The default is just the local host, which is needed by some mail user
agents. The default includes local host for both IPv4 and IPv6. If just
connecting via one IP version, the unused value(s) may be removed.
If this host is a smarthost for a block of machines, you need to specify
the netblocks here, or mail will be rejected rather than relayed.
To use the Postfix default (which is based on the connected subnets),
leave this blank.
Local networks:
127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
<Ok>
<Cancel>


Postfix Configuration
Please specify the limit that Postfix should place on mailbox files to constrain file system usage by a single file (potentially due to abusive mail or software errors). A value of zero (0) means no limit. The upstream default is 51200000.
Mailbox size limit (bytes):
0
<Ok>
<Cancel>


Package configuration
Postfix Configuration
Please choose a character used as recipient delimiter that will indicate a local address extension.
To not use address extensions, leave the string blank.
Local address extension character:
+
<Ok>
<Cancel>




```
After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo nano /etc/postfix/main.cf
```

```
 GNU nano 7.2                    /etc/postfix/main.cf *
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_un>
myhostname = ruvindi
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = ruvindi, ruvindi.com, ruvindi, 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

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

```
^Z
[1]+  Stopped                 sudo tail -f /var/log/mail.log
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo systemctl status postfix
[sudo] password for ruvindi:
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: enable>
     Active: active (exited) since Tue 2025-05-06 18:17:09 +0530; 4h 3min ago
       Docs: man:postfix(1)
   Main PID: 9847 (code=exited, status=0/SUCCESS)
        CPU: 1ms

May 06 18:17:09 ruvindi systemd[1]: Starting postfix.service - Postfix Mail Transport>
May 06 18:17:09 ruvindi systemd[1]: Finished postfix.service - Postfix Mail Transport>
lines 1-9/9 (END)
[2]+  Stopped                 sudo systemctl status postfix
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$ echo "This is a test mail from Postfix" | mail -s "Test Mail" ruvin
di@localhost
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ mail
"/var/mail/ruvindi": 2 messages 1 new 1 unread
 U   1 Ruvindi            Sat May  3 00:37  16/490   Test Subject
>N   2 Ruvindi            Tue May  6 18:32  13/436   Test Mail
? q
Held 2 messages in /var/mail/ruvindi
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo tail -f /var/log/mail.log
[sudo] password for ruvindi:
2025-05-06T15:25:44.987453+05:30 ruvindi postfix/master[7308]: daemon started -- versi
on 3.8.6, configuration /etc/postfix
2025-05-06T18:17:08.235622+05:30 ruvindi postfix/postfix-script[9514]: stopping the Po
stfix mail system
2025-05-06T18:17:08.239924+05:30 ruvindi postfix/master[7308]: terminating on signal 1
5
2025-05-06T18:17:09.088538+05:30 ruvindi postfix/postfix-script[9841]: starting the Po
```

```
ruvindi@ruvindi:~$ sudo systemctl restart postfix
[sudo] password for ruvindi:
ruvindi@ruvindi:~$ sudo systemctl enable postfix
Synchronizing state of postfix.service with SysV service script with /usr/lib/systemd/
systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable postfix
ruvindi@ruvindi:~$
```

```
ruvindi@ruvindi:~$
ruvindi@ruvindi:~$ sudo ss -tuln | grep :25
[sudo] password for ruvindi:
tcp   LISTEN 0      100                                0.0.0.0:25         0.0.0.0:*

tcp   LISTEN 0      100                                   [::]:25            [::]:*

ruvindi@ruvindi:~$
```

4. Linux GDB

Step-by-Step Instructions

i. Identify System Architecture

"uname -m"

Common outputs:

- x86_64 → 64-bit
- i686 → 32-bit
- arm* → ARM-based

Based on the output, select the correct executable from the provided ZIP file.

ii. Run the Selected Executable

Make the file executable:
"chmod +x x86_64"
Grants execute permissions to the file so it can be run as a program.

Run it with root privileges:
"sudo ./x86_64"
Executes the file with root privileges.

iii. Run the New Executable

"sudo ./IT23839274"

- This should create a file named data.txt.
- Check for its presence:

"ls -l"

Lists files and their details

"cat data.txt"

Displays the content of data.txt.

Look for any **encoded or suspicious content** in data.txt.

iv. Analyze with GDB

Launch GDB:

"gdb ./IT12345678"

In GDB:

```
break main        # Set breakpoint at main
run               # Start the program
step              # Steps into the next function line by line.
next              # Executes the next line without entering any functions.
print <variable>  # Print variables
info registers    # View CPU registers
x/s <address>     # Shows the string stored at a specific memory address.
```

v. Monitor File System Changes

Before running the executable:

"ls -lhtr"

Lists files sorted by **modification time**, oldest to newest, with human-readable sizes

Run it again:

"sudo ./IT23839274"

After:

"ls -lhtr" # Look for new/modified files

“stat data.txt”

Look for encoded/hidden patterns or keywords

“strings data.txt”

“hexdump -C data.txt”

File Content Analysis

- Used tools:
  - strings data.txt
  - hexdump -C data.txt
  - base64 decoding (if needed)

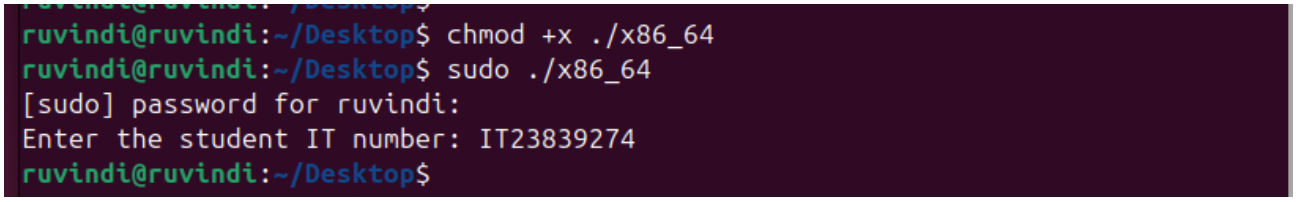
- Provides a **hexadecimal and ASCII view** of the file's binary contents, useful for detecting patterns or signs of encoding (e.g., base64, shellcode).

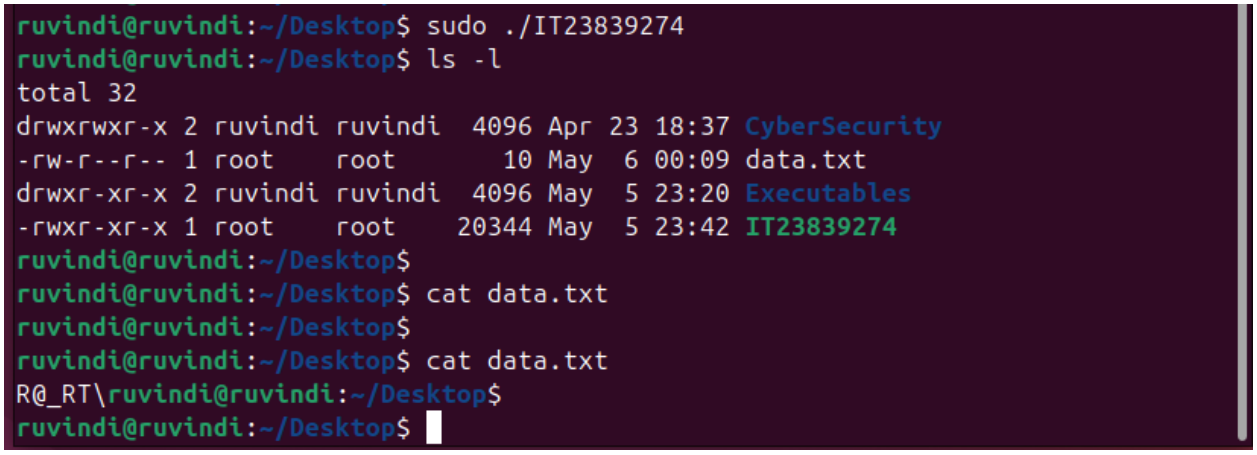
vi. Analyze data.txt

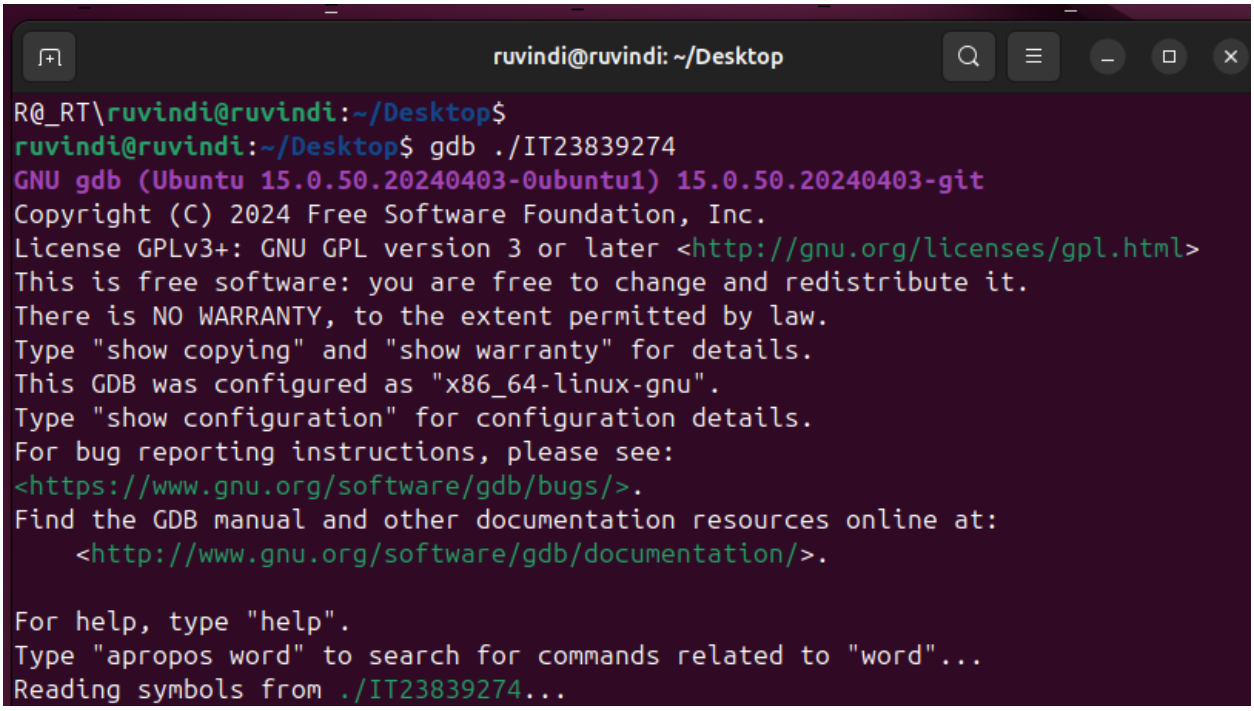
“strings data.txt”

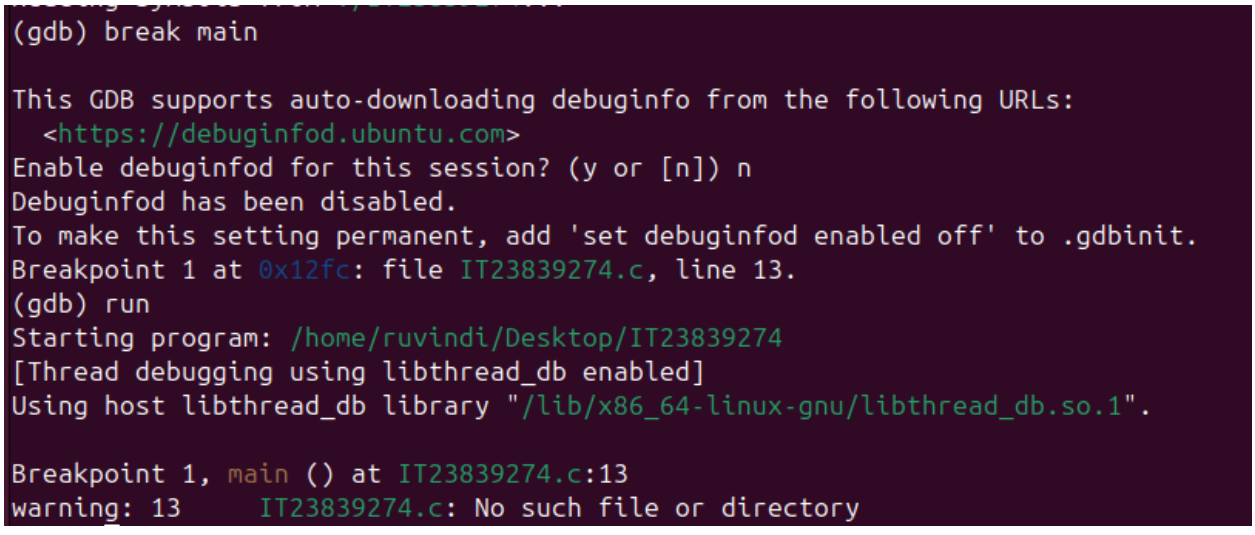
“hexdump -C data.txt”

Screen Shots of the Linux GDB Analysis





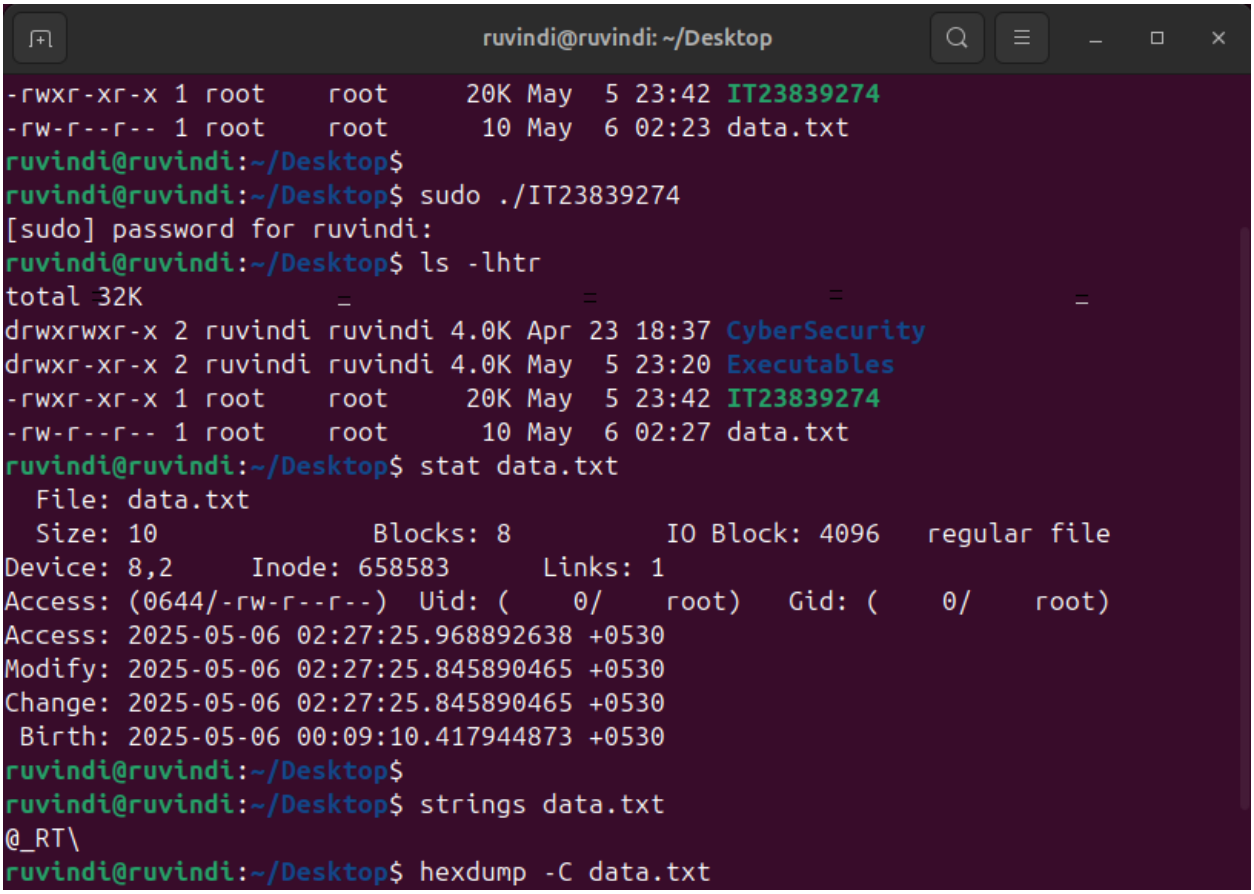

ruvindi@ruvindi: ~/Desktop
R@_RT\ruvindi@ruvindi:~/Desktop$
ruvindi@ruvindi:~/Desktop$ gdb ./IT23839274
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This 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 commands related to "word"...
Reading symbols from ./IT23839274...

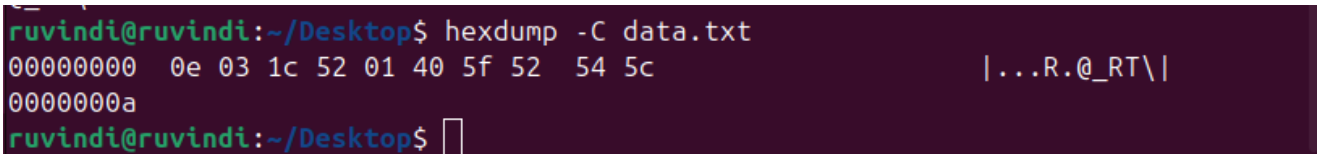

(gdb) break main
This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Breakpoint 1 at 0x12fc: file IT23839274.c, line 13.
(gdb) run
Starting program: /home/ruvindi/Desktop/IT23839274
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Breakpoint 1, main () at IT23839274.c:13
warning: 13 IT23839274.c: No such file or directory

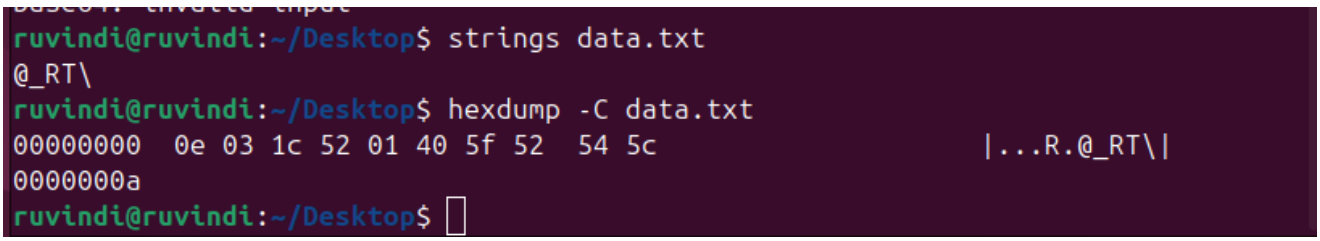

Breakpoint 1, main () at IT23839274.c:13
warning: 13 IT23839274.c: No such file or directory
(gdb) disassemble main
Dump of assembler code for function main:
0x00005555555552f0 <+0>: endbr64
0x00005555555552f4 <+4>: push %rbp
0x00005555555552f5 <+5>: mov %rsp,%rbp
0x00005555555552f8 <+8>: sub $0x60,%rsp
=> 0x00005555555552fc <+12>: mov %fs:0x28,%rax
0x0000555555555305 <+21>: mov %rax,-0x8(%rbp)
0x0000555555555309 <+25>: xor %eax,%eax
0x000055555555530b <+27>: lea 0xcf6(%rip),%rax # 0x555555556008
0x0000555555555312 <+34>: mov %rax,%rsi
0x0000555555555315 <+37>: lea 0xcf4(%rip),%rax # 0x555555556010
0x000055555555531c <+44>: mov %rax,%rdi
0x000055555555531f <+47>: call 0x555555555160 <popen@plt>
0x0000555555555324 <+52>: mov %rax,-0x58(%rbp)
0x0000555555555328 <+56>: cmpq $0x0,-0x58(%rbp)
0x000055555555532d <+61>: jne 0x555555555348 <main+88>
0x000055555555532f <+63>: lea 0xd02(%rip),%rax # 0x555555556038
0x0000555555555336 <+70>: mov %rax,%rdi
0x0000555555555339 <+73>: call 0x5555555550e0 <puts@plt>
0x000055555555533e <+78>: mov $0x1,%eax
0x0000555555555343 <+83>: jmp 0x555555555400 <main+272>

```
       Inferior 1 [process 7002] will be killed.

Quit anyway? (y or n) y
ruvindi@ruvindi:~/Desktop$ strings ./IT23839274
/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
```

```
ruvindi@ruvindi:~/Desktop$ ls -lhtr
total 32K
drwxrwxr-x 2 ruvindi ruvindi 4.0K Apr 23 18:37 CyberSecurity
drwxr-xr-x 2 ruvindi ruvindi 4.0K May  5 23:20 Executables
-rwxr-xr-x 1 root    root     20K May  5 23:42 IT23839274
-rw-r--r-- 1 root    root      10 May  6 00:09 data.txt
ruvindi@ruvindi:~/Desktop$
```


ruvindi@ruvindi: ~/Desktop
-rwxr-xr-x 1 root root 20K May 5 23:42 IT23839274
-rw-r--r-- 1 root root 10 May 6 02:23 data.txt
ruvindi@ruvindi:~/Desktop$
ruvindi@ruvindi:~/Desktop$ sudo ./IT23839274
[sudo] password for ruvindi:
ruvindi@ruvindi:~/Desktop$ ls -lhtr
total 32K
drwxrwxr-x 2 ruvindi ruvindi 4.0K Apr 23 18:37 CyberSecurity
drwxr-xr-x 2 ruvindi ruvindi 4.0K May 5 23:20 Executables
-rwxr-xr-x 1 root root 20K May 5 23:42 IT23839274
-rw-r--r-- 1 root root 10 May 6 02:27 data.txt
ruvindi@ruvindi:~/Desktop$ stat data.txt
File: data.txt
Size: 10 Blocks: 8 IO Block: 4096 regular file
Device: 8,2 Inode: 658583 Links: 1
Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)
Access: 2025-05-06 02:27:25.968892638 +0530
Modify: 2025-05-06 02:27:25.845890465 +0530
Change: 2025-05-06 02:27:25.845890465 +0530
Birth: 2025-05-06 00:09:10.417944873 +0530
ruvindi@ruvindi:~/Desktop$
ruvindi@ruvindi:~/Desktop$ strings data.txt
@_RT\
ruvindi@ruvindi:~/Desktop$ hexdump -C data.txt


ruvindi@ruvindi:~/Desktop$ hexdump -C data.txt
00000000 0e 03 1c 52 01 40 5f 52 54 5c |...R.@_RT\|
0000000a
ruvindi@ruvindi:~/Desktop$


ruvindi@ruvindi:~/Desktop$ strings data.txt
@_RT\
ruvindi@ruvindi:~/Desktop$ hexdump -C data.txt
00000000 0e 03 1c 52 01 40 5f 52 54 5c |...R.@_RT\|
0000000a
ruvindi@ruvindi:~/Desktop$