

# **Sri Lanka Institute of Information Technology**

B.Sc. (Hons) Information Technology-

Cyber security



Y2 S1

Systems and Network Programming – IE 2012

Assignment

**M. A. AMANTHA**

**IT 23 1843 12**

## **Introduction**

This assignment aims to provide in-depth knowledge about system and network programming through hands-on assignments based on Linux. It is presumed that students, while doing these assignments, will develop the necessary practical skills in the configuration of core system components and basic services such as DHCP, DNS, and NTP. The students will also be introduced to shell scripting and security practices. Specifically, this will entail activities that will enable the students to establish skills in configuring Linux-based systems, user management, system information gathering, and ensuring security in network administration. This assignment also focuses on enhancing problem-solving skills in system automation, firewall configuration, and implementation of best security practices for effective learning.

## **Declaration**

I hereby declare that the work presented here is entirely my original work. I, myself, have carried out the practical work in the setup of the virtual environment, configuration of Linux services, and scripting of automation solutions. All contents and configurations documented are of my personal engagement in the said assignment tasks, and whatever resources utilized have appropriately been acknowledged. This report is hereby submitted in partial fulfillment of my academic requirements in the course, and I hereby attest that it is performed in compliance with the guidelines provided.

## Table of Contents

1. VM installation steps .....	4
2. Basic navigation commands and file manipulation commands .....	15
3. 15 basic commands with brief description .....	18
4. Configuration steps of DHCP, DNS, NTP services .....	23
a. DHCP installation and configuration .....	23
b. DNS installation and configuration .....	34
c. NTP installation and configuration .....	39
5. Shell Scripting and Security .....	47
a. Shell Scripting .....	46
b. SSH .....	55
6. Iptables and ACLs .....	59
7. Best Practices .....	72

## 1. VM installation steps

### Virtual Machine Setup

#### Step 01: Download VMware Workstation Pro (Emulator).

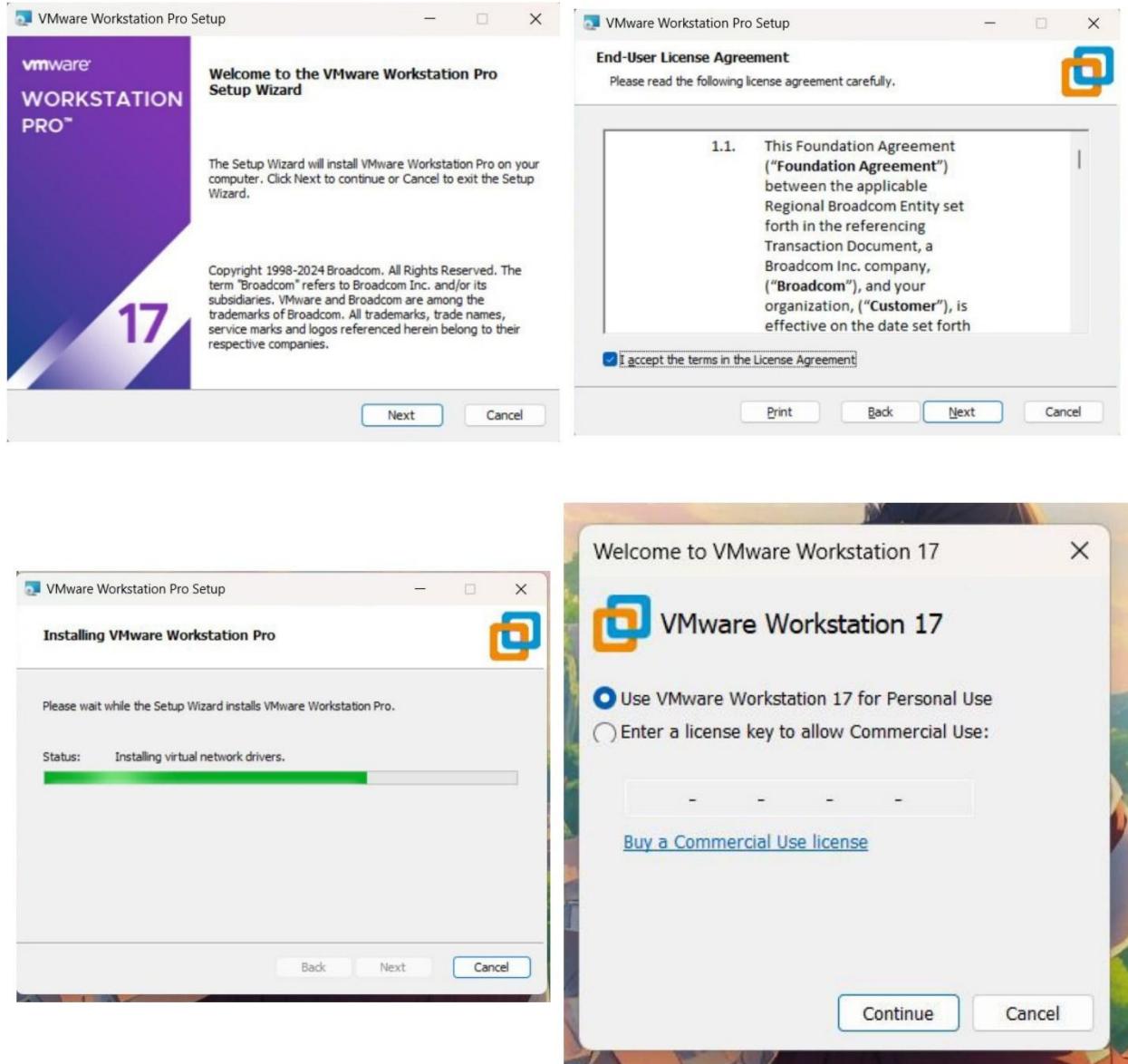
1. Visit VMware website.
  - Go to <https://blogs.vmware.com>
2. Download VMware Workstation Pro.
  - Choose the appropriate version based on your operating system.

The screenshot shows the product page for VMware Workstation 17.6.0. At the top, there's a navigation bar with tabs: OVERVIEW (selected), FAQ, CERTIFIED (with a checkmark), WHAT'S NEW, and SIMILARS (with a count of 5). Below the navigation, the main title is "VMware Workstation 17.6.0" with the subtitle "Software for developers and system administrators for software development, testing and deployment." To the left, there's a brief description: "Run Windows, Linux and BSD virtual machines on a Windows or Linux desktop with VMware Workstation Pro." To the right, there's another section with the text: "Fast servers and clean downloads. Serving tech enthusiasts for over 25 years. Tested on TechSpot Labs." Below this, there's a large blue "Download Now" button with a downward arrow icon. Underneath the button, it says "Download options:" followed by four dropdown menus: "Workstation Windows", "VMware Player Windows", "Workstation Linux", and "VMware Player Linux". At the bottom left, there's a file download summary: "VMware-workstation-full-17.6.0-24238078" (file icon), "9/18/2024 8:19 PM" (modified date), "Application" (type), and "458,724 KB" (size).

- Downloaded file.

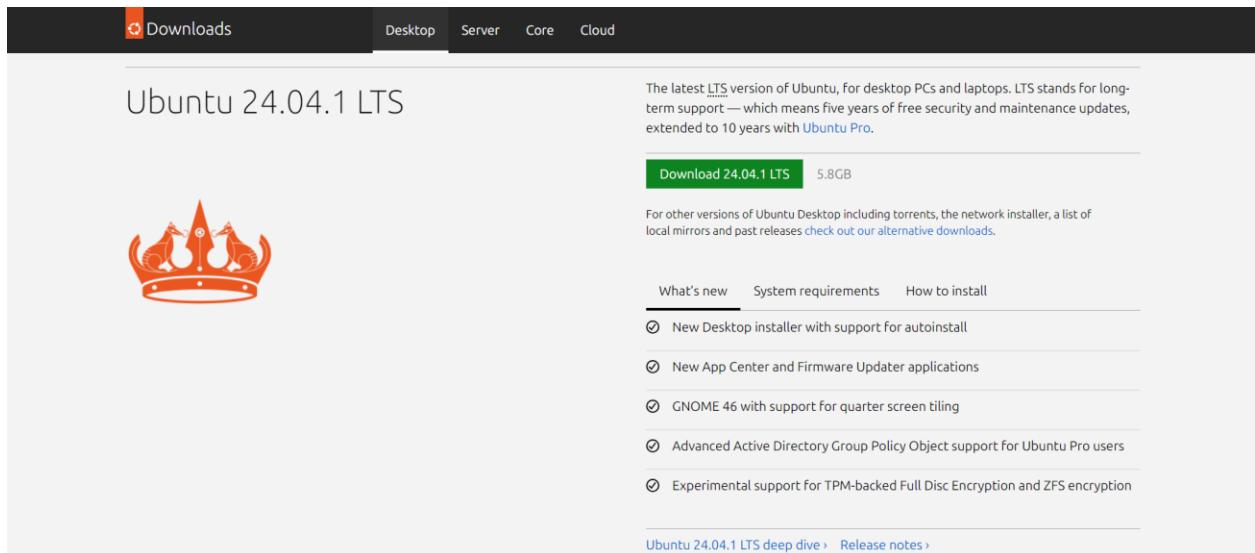
3. Install Vmware Workstation Pro.

- Once the download is complete, Open the installer file.
- Install the software accepting the terms and conditions.



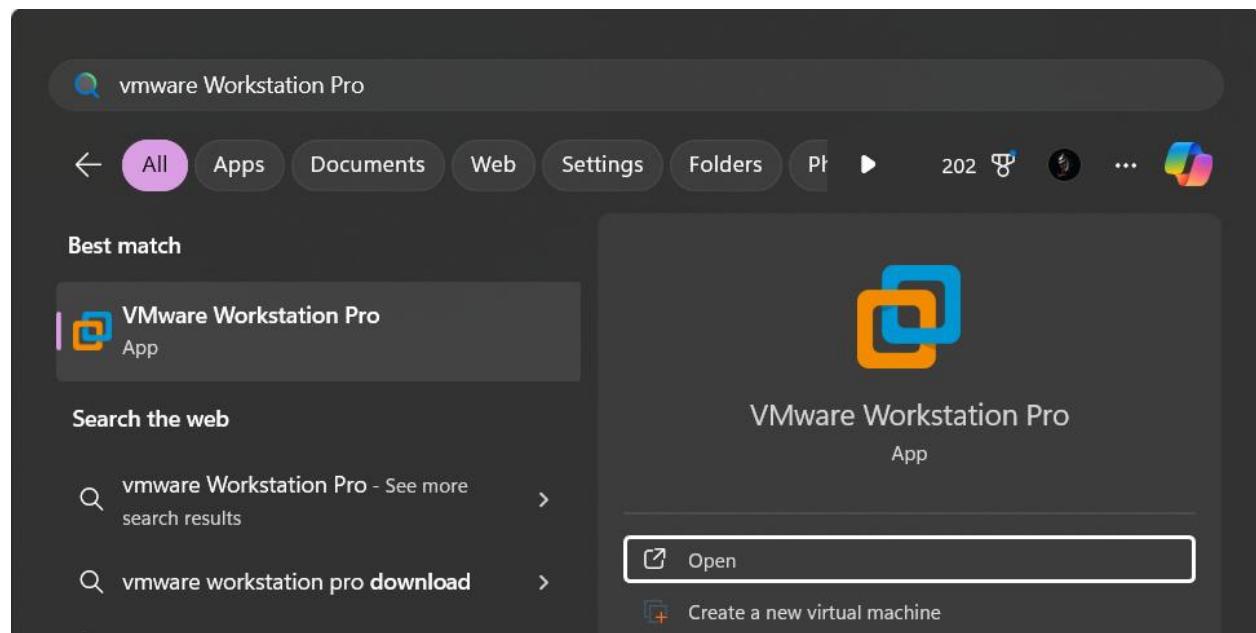
## Step 02: Download Ubuntu (Linux Distribution).

1. Visit Ubuntu Downloads page.
  - Go to <https://ubuntu.com/download/desktop>
2. Download Ubuntu ISO.
  - Choose the latest LTS (Long Term Support) version and click the download button.



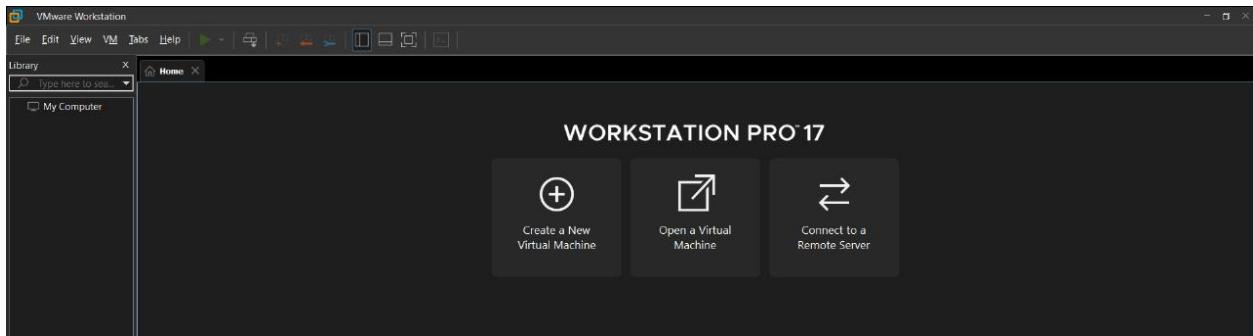
## Step 03: Create a New Virtual machine in VMware Workstation pro.

1. Open VMware Workstation Pro.
  - Launch VMware Workstation Pro from your desktop or start menu.

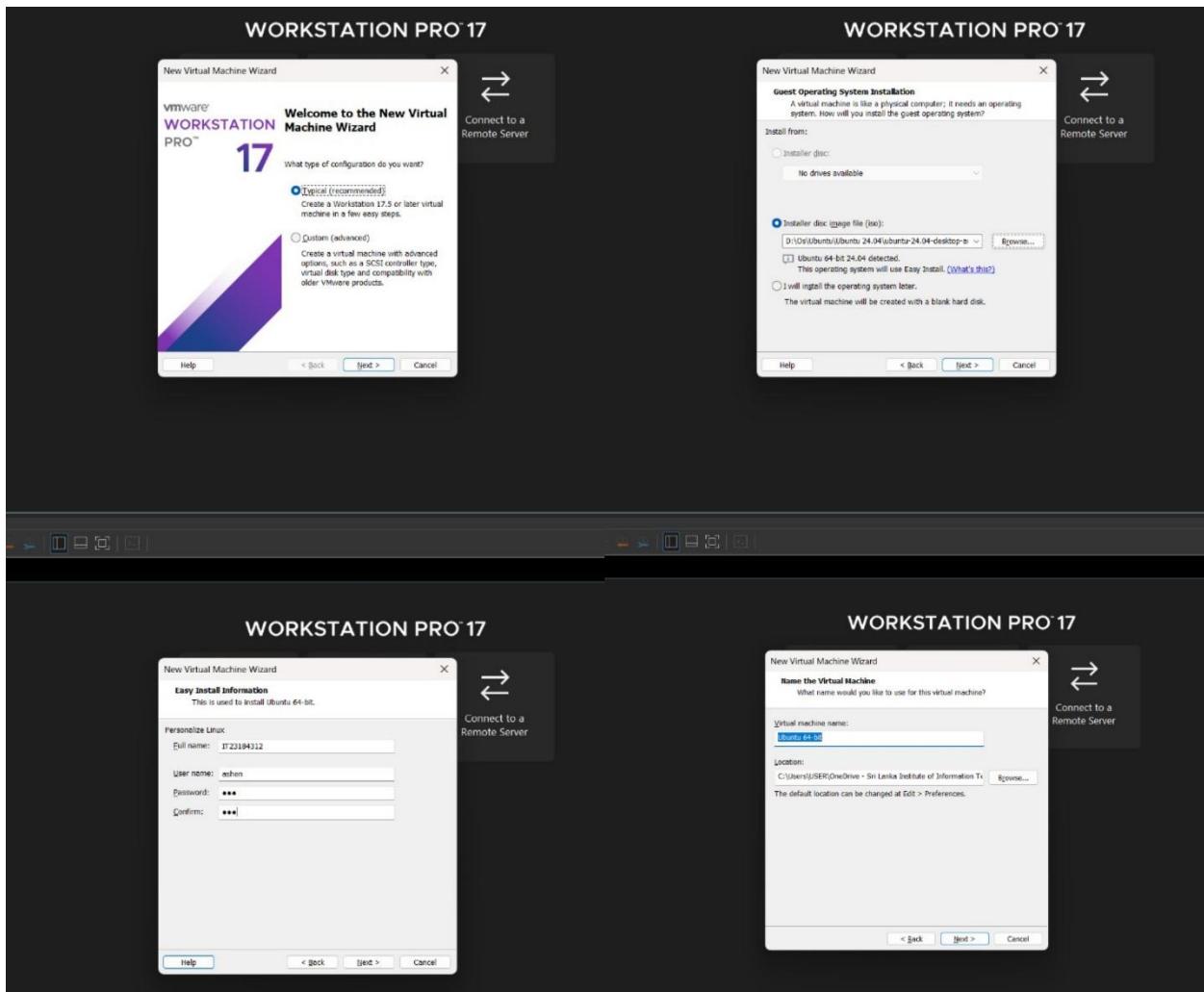


## 2. Create a new VM.

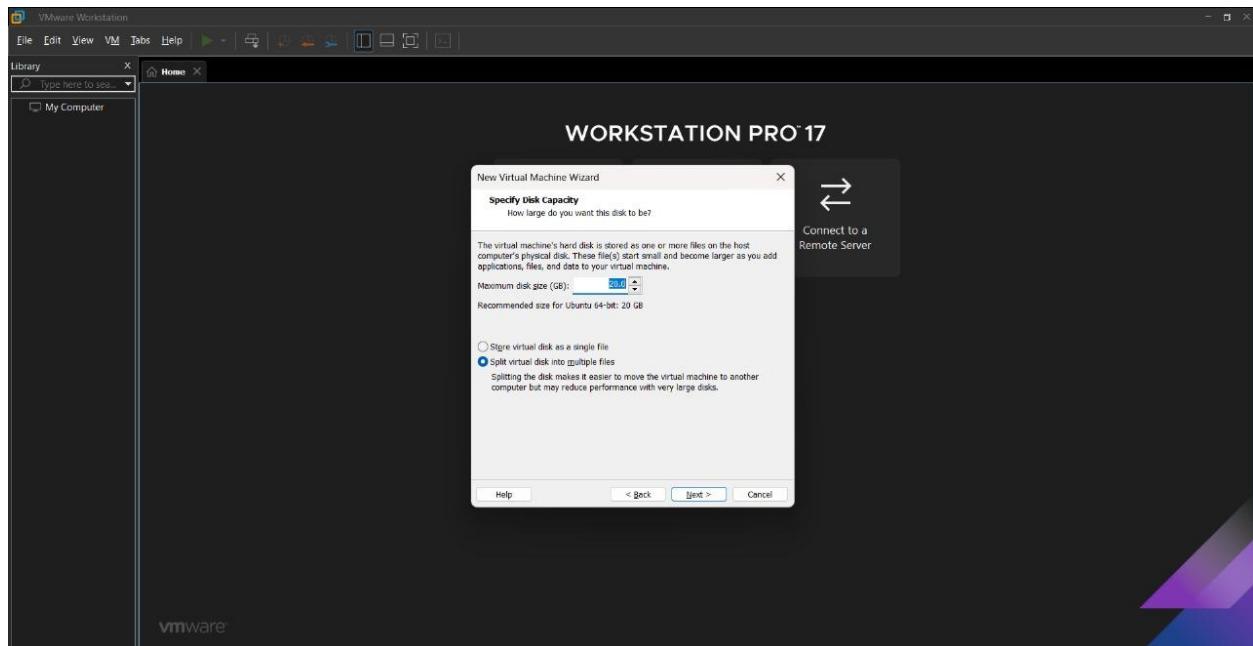
- Click on ‘Create a New Virtual Machine’.



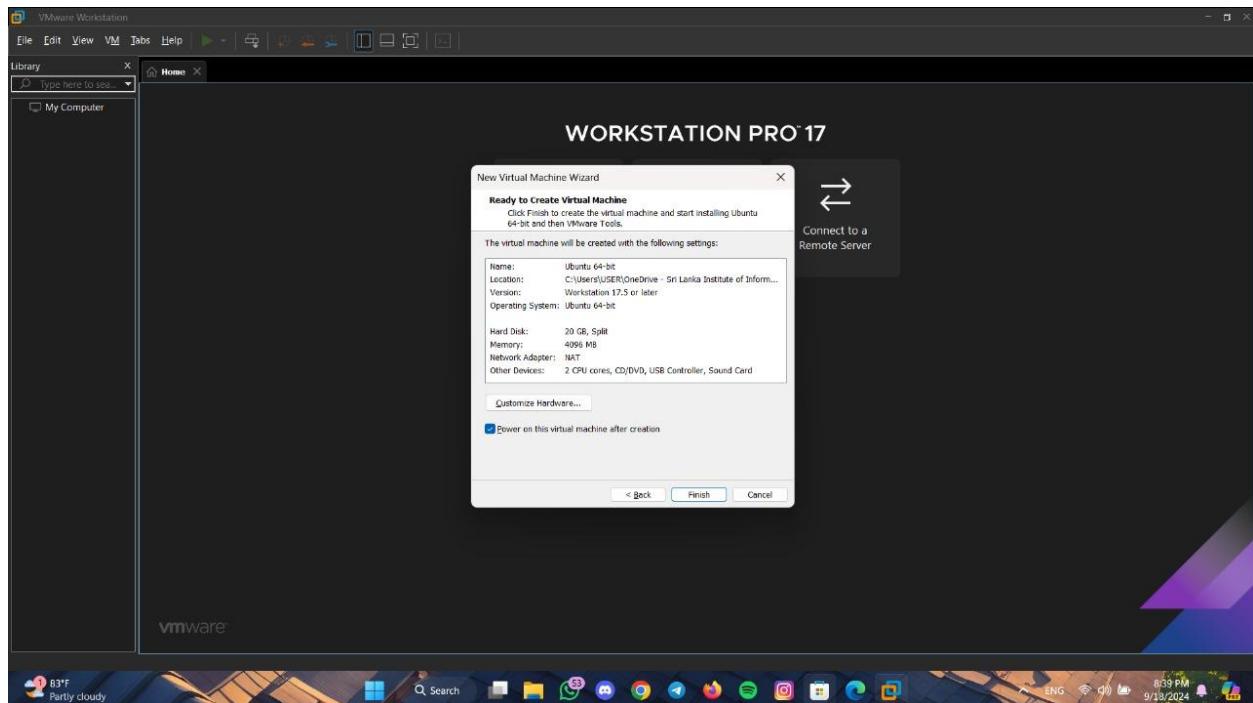
- Select ‘Typical (recommended)’ and click ‘Next’.
- Browse the ISO file.
- Give a name and a password.
- Name the Virtual machine (Set it to "Ubuntu (64-bit)" (or choose the correct version based on the ISO file downloaded).) and click next.



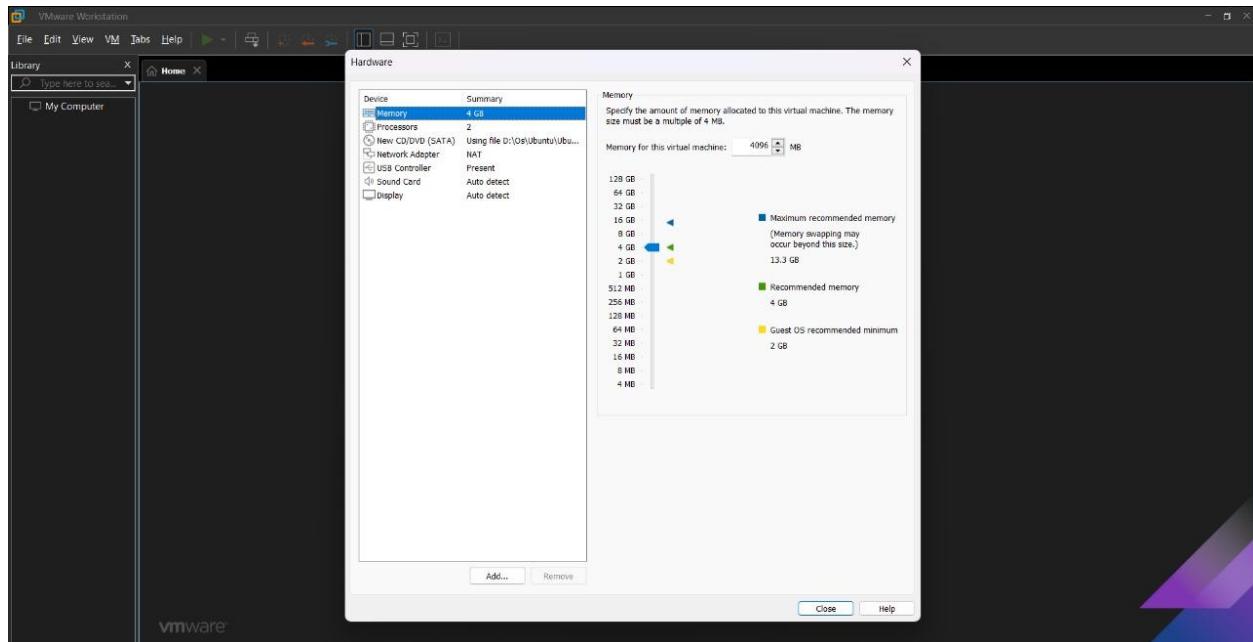
- Allocate storage.



- Allocate memory and set finish.

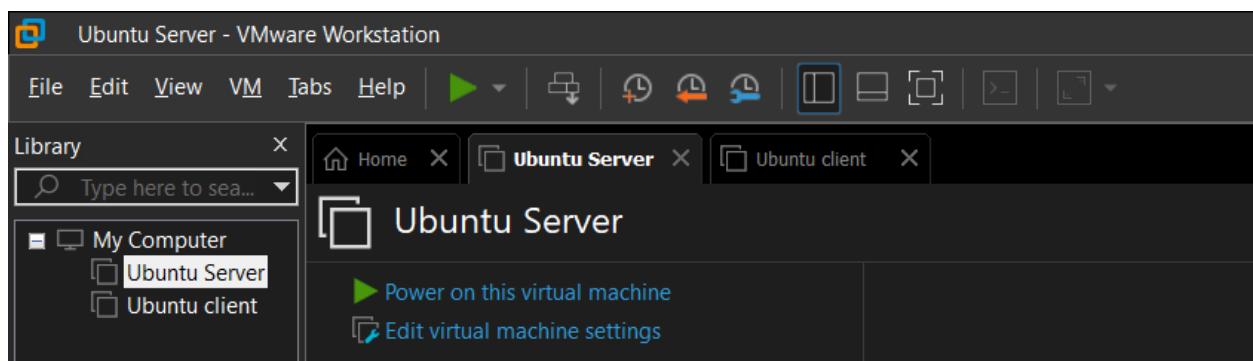


- We can change the settings from the settings tab.
  - Memory settings
  - Processors allocating
  - Network settings, etc.



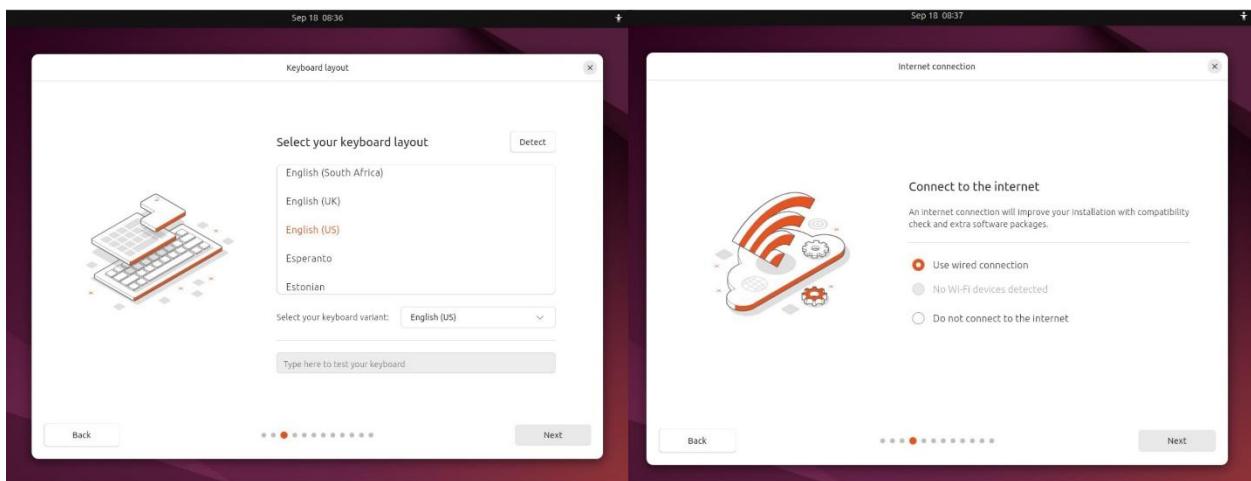
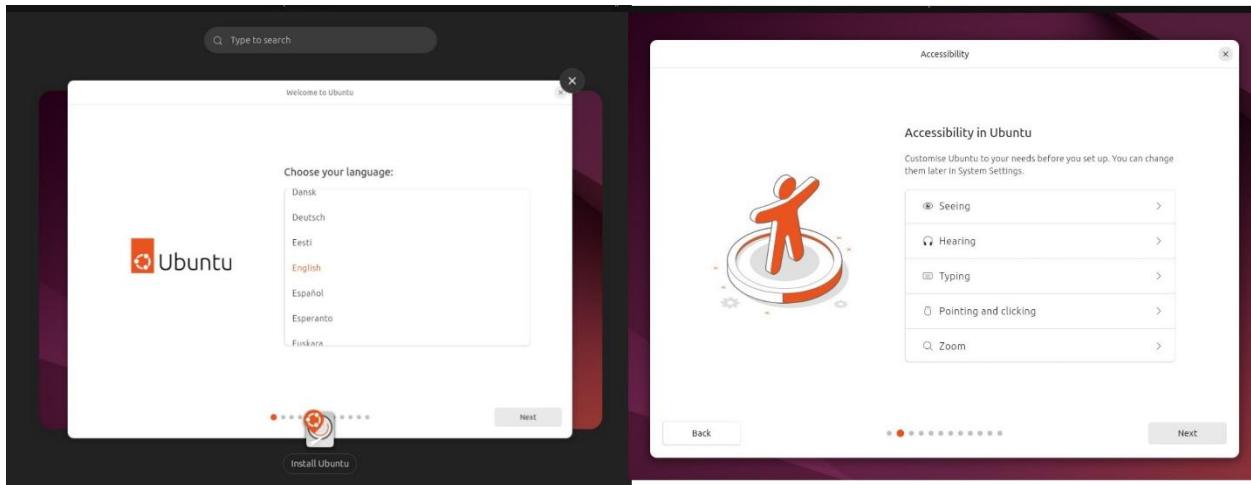
#### Step 04: Install Ubuntu on the virtual machine.

1. After creating the virtual machine, select it from the library tab and click ‘Power on this virtual machine’.



2. The VM will boot from the Ubuntu ISO. Follow the on-screen prompts to install Ubuntu:

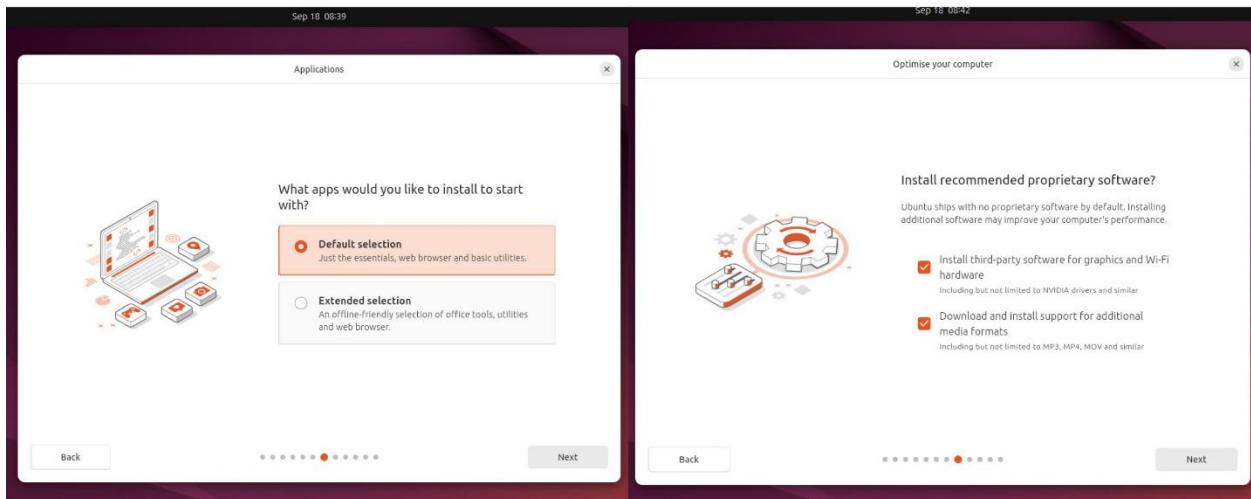
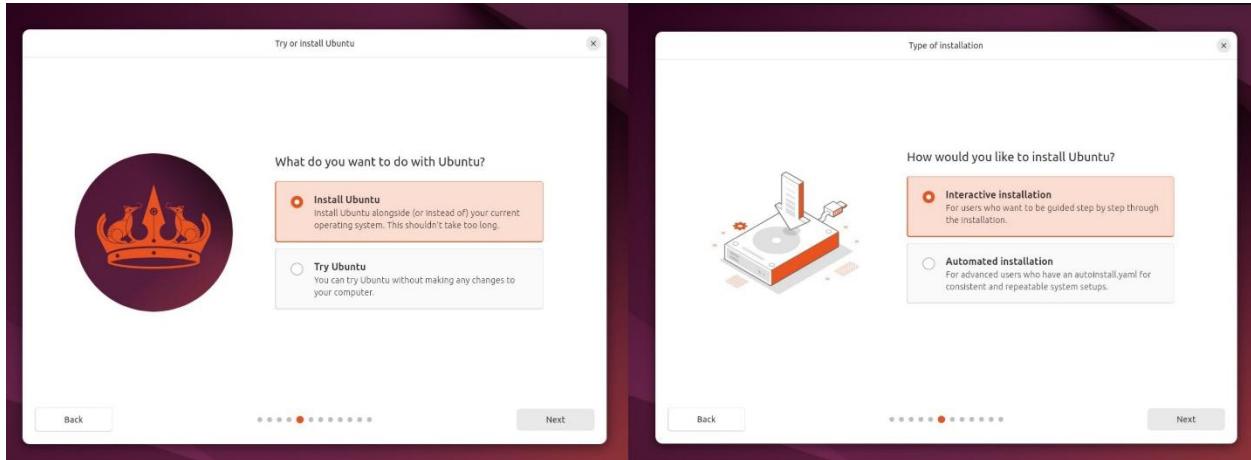
- **Language Selection:** Choose your language and click "Continue."
- **Keyboard Layout:** Select the appropriate layout and click "Continue."



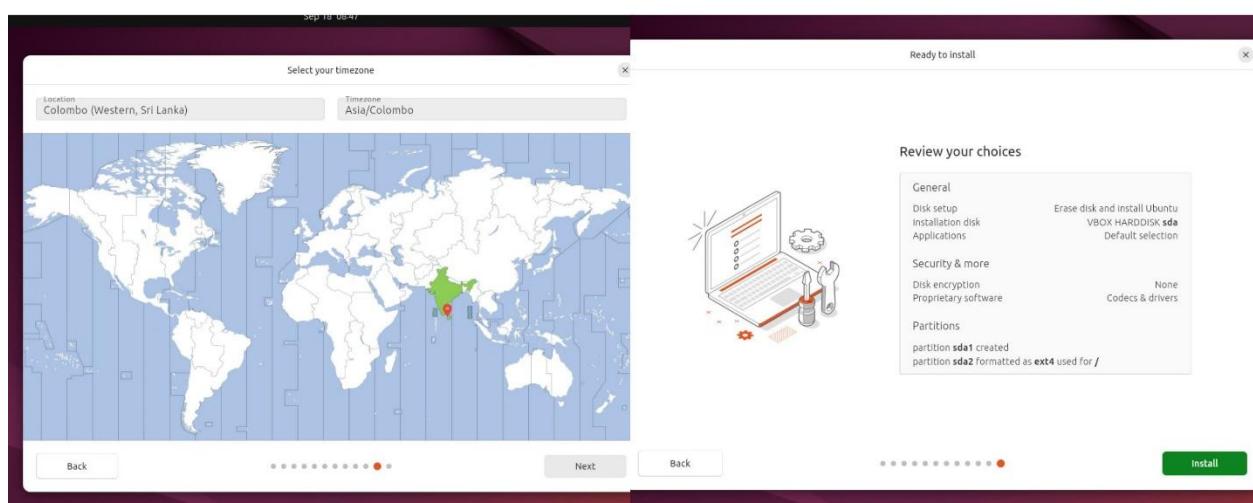
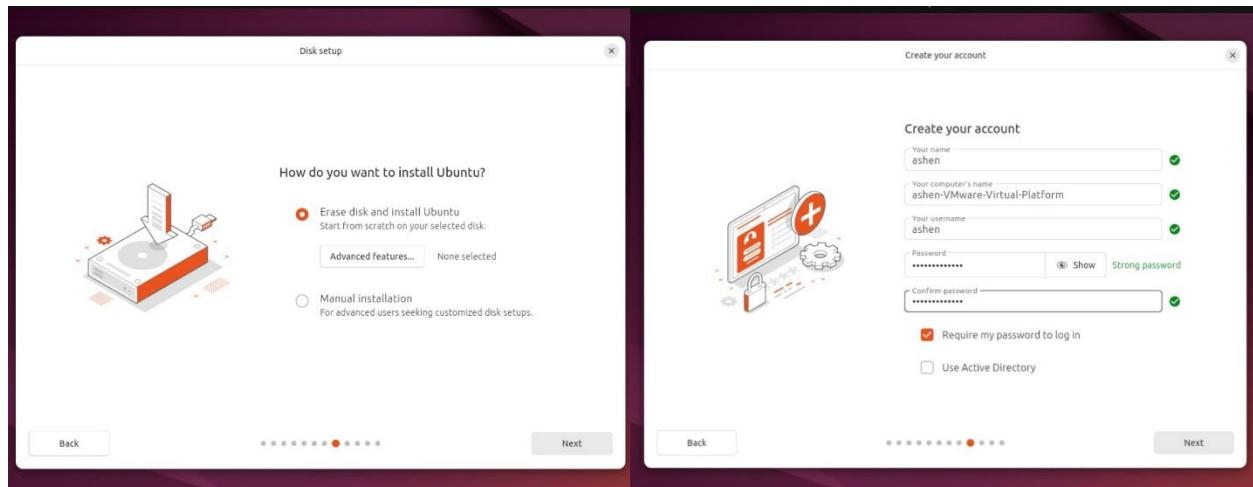
**- Install Ubuntu :** Select Install Ubuntu and 'Next'.

**- Updates and Other Software:** Choose your preference (select "Interactive installation" for a full desktop setup) and click "Next".

-Default Selection and click 'Next'.

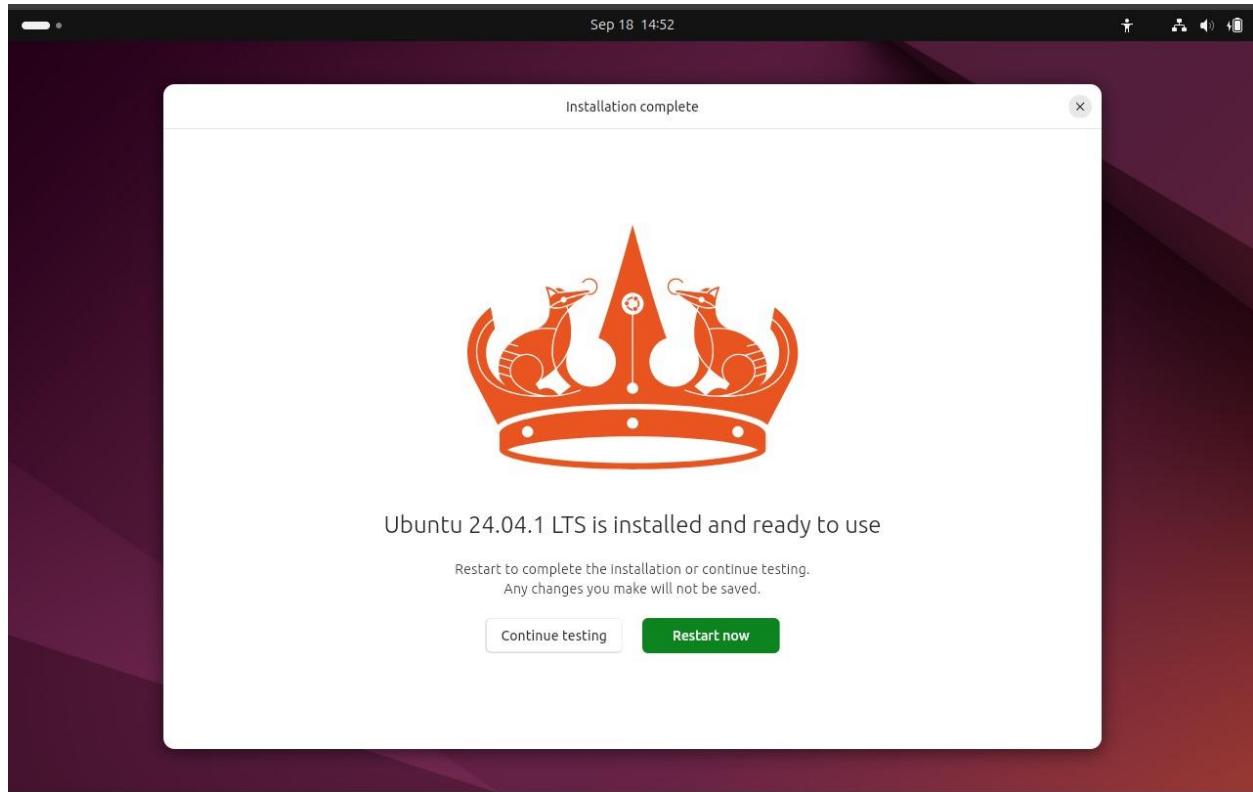


- **Installation Type:** Choose "Erase disk and install Ubuntu" (this applies to the VM, not your host system). Click "Install Now."
- **Time Zone:** Choose your time zone and click "Next."
- **User Details:** Set up your username, computer name, and password. Click "Next".



### 3. Complete Installation:

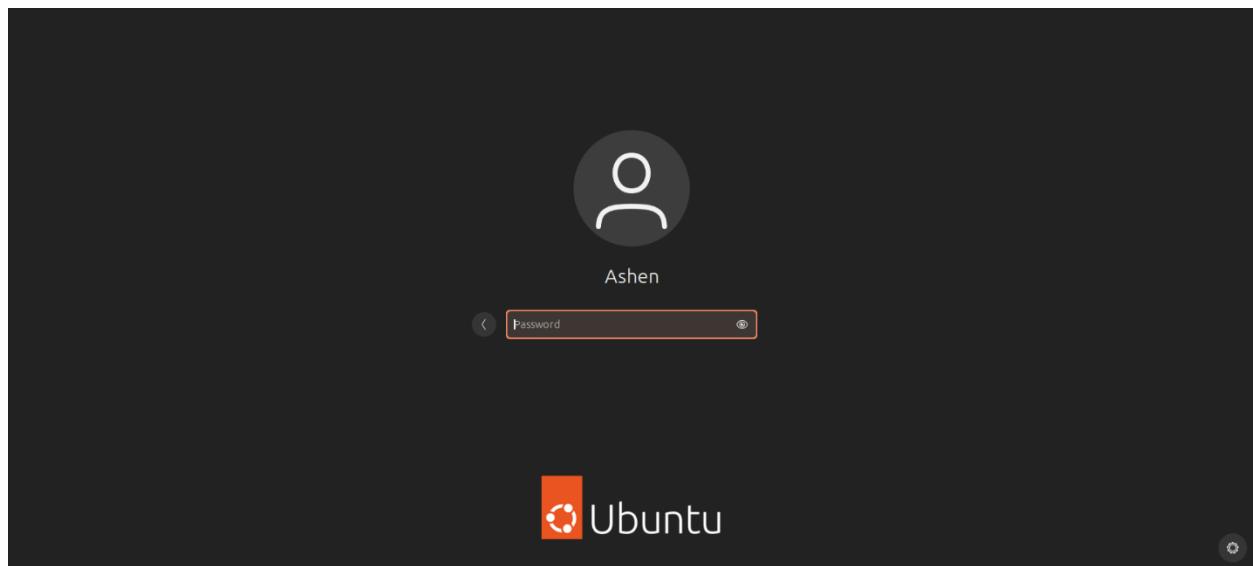
- Once the installation is complete, you'll be prompted to restart the VM. Click "Restart Now"



### Step 04: Post-Installation Configuration.

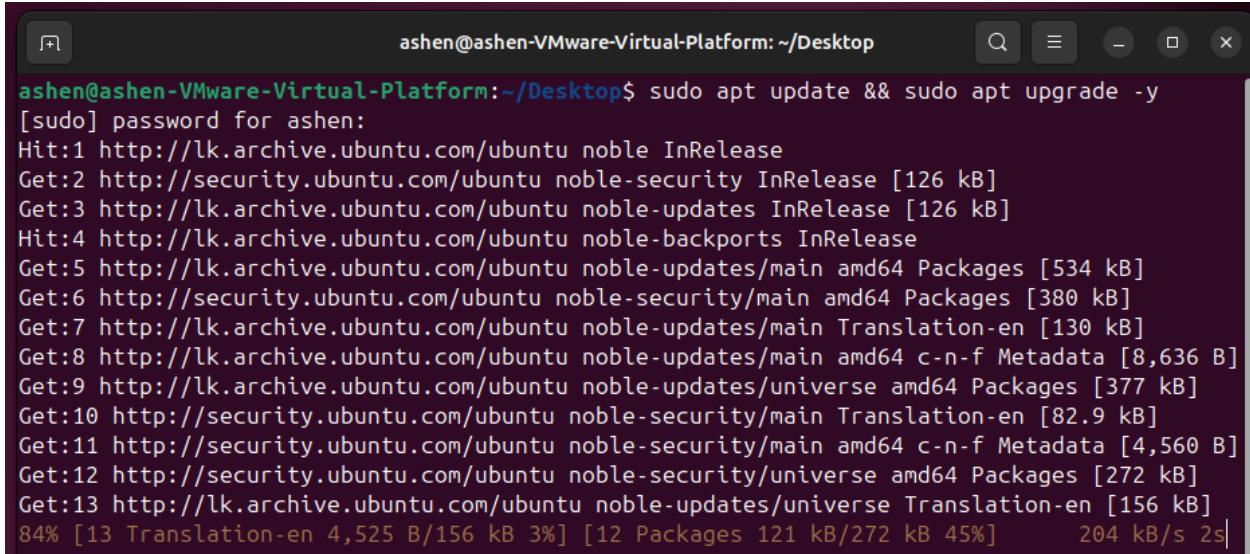
#### 1. First Boot:

- log in with the username and password you set up during installation.



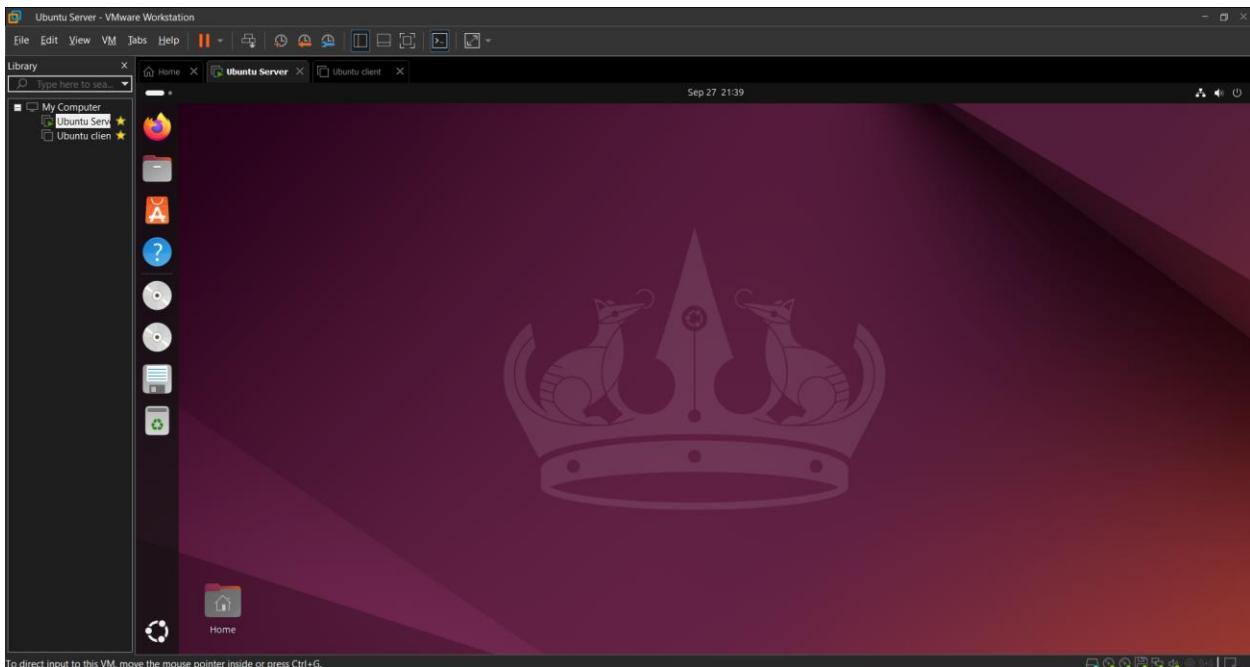
## 2. Update Ubuntu.

- sudo apt update && sudo apt upgrade -y
- Enter the password.



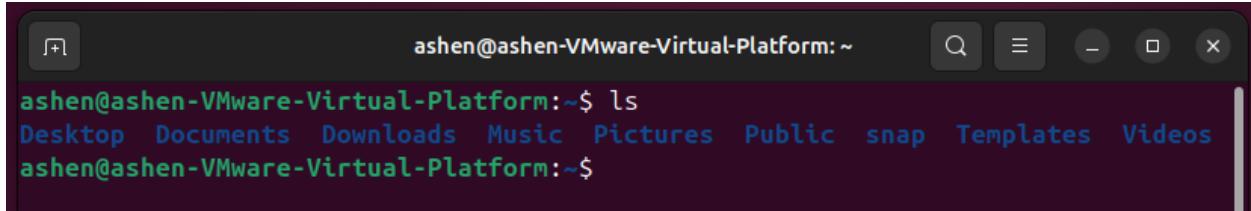
```
ashen@ashen-Virtual-Platform:~/Desktop$ sudo apt update && sudo apt upgrade -y
[sudo] password for ashen:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [534 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380 kB]
Get:7 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [130 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8,636 B]
Get:9 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [377 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [82.9 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4,560 B]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [272 kB]
Get:13 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [156 kB]
84% [13 Translation-en 4,525 B/156 kB 3%] [12 Packages 121 kB/272 kB 45%]      204 kB/s 2s
```

Installation successful.



## 2. Basic Navigation commands and File manipulation commands

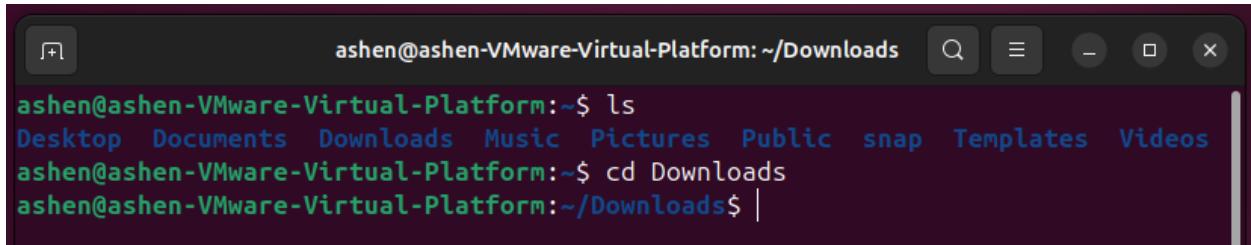
1. **ls** : This command is used to display the contents of a directory.



```
ashen@ashen-VMware-Virtual-Platform:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
ashen@ashen-VMware-Virtual-Platform:~$
```

A screenshot of a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~". The window shows the command "ls" being run, which lists several directories: Desktop, Documents, Downloads, Music, Pictures, Public, snap, Templates, and Videos. The prompt "ashen@ashen-VMware-Virtual-Platform: ~\$" appears at the bottom.

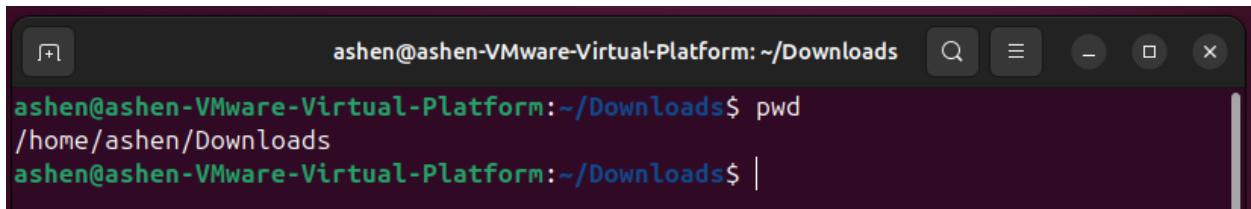
2. **cd** : This command is used to navigate between directories in the filesystem.



```
ashen@ashen-VMware-Virtual-Platform:~/Downloads$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
ashen@ashen-VMware-Virtual-Platform:~/Downloads$ cd Downloads
ashen@ashen-VMware-Virtual-Platform:~/Downloads$ |
```

A screenshot of a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Downloads". The window shows the command "ls" being run, listing the same set of directories as the previous screenshot. Then, the command "cd Downloads" is run, changing the current directory to "Downloads". The prompt "ashen@ashen-VMware-Virtual-Platform: ~/Downloads\$ |" appears at the bottom.

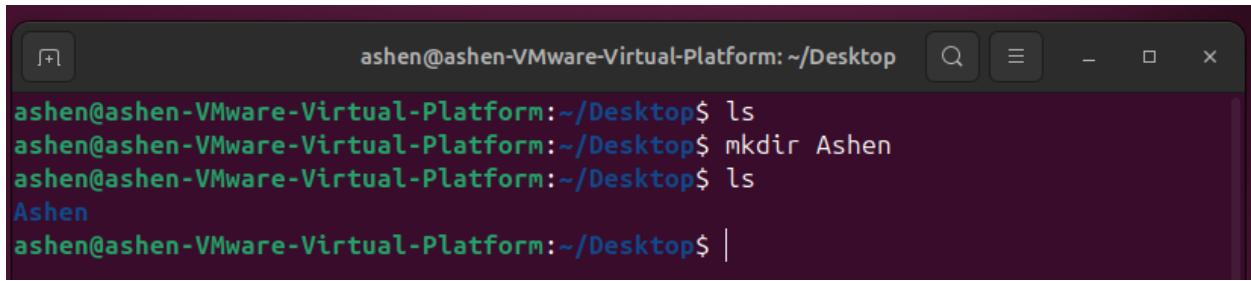
3. **pwd** : This command is used to display the full path of the current directory in which you are working.



```
ashen@ashen-VMware-Virtual-Platform:~/Downloads$ pwd
/home/ashen/Downloads
ashen@ashen-VMware-Virtual-Platform:~/Downloads$ |
```

A screenshot of a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Downloads". The window shows the command "pwd" being run, which outputs the full path "/home/ashen/Downloads". The prompt "ashen@ashen-VMware-Virtual-Platform: ~/Downloads\$ |" appears at the bottom.

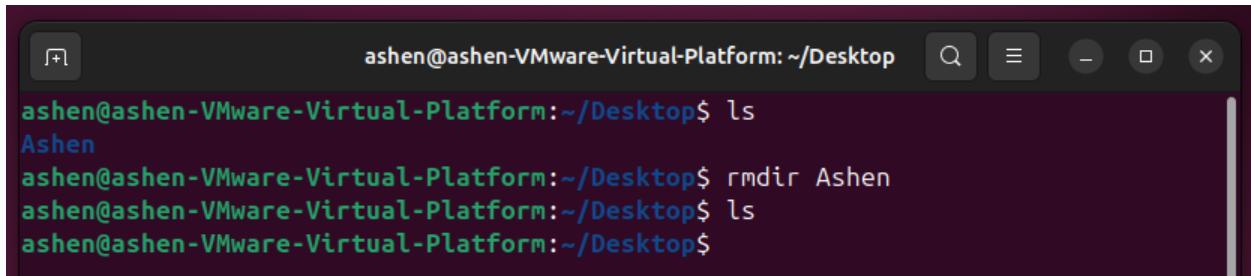
4. **mkdir** : This command is used to create a new directory(folder) in the file system. For example, if you want to create a directory named "Ashen" you have to type: **mkdir Ashen**.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ mkdir Ashen
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
Ashen
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

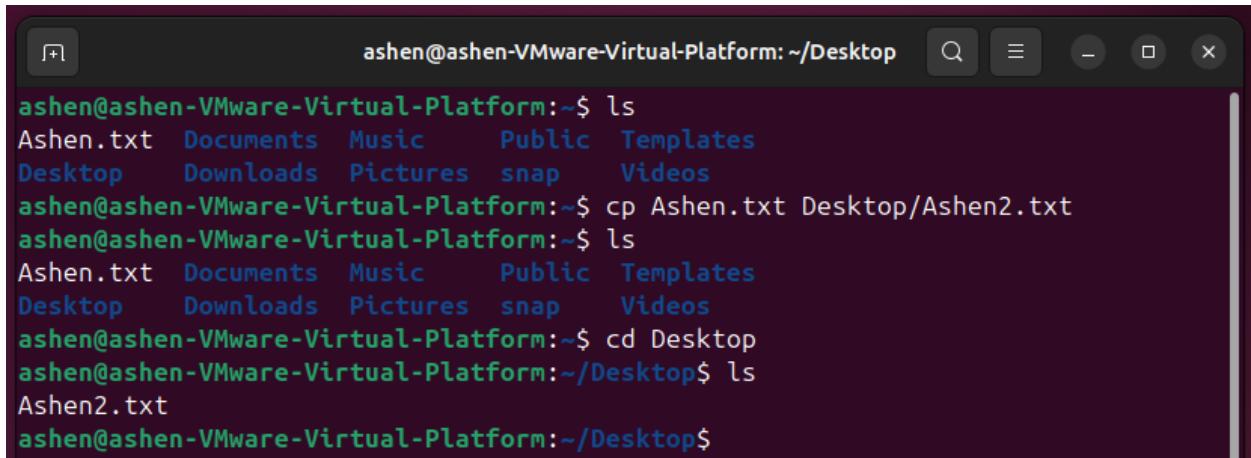
A screenshot of a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The window shows the command "ls" being run, followed by "mkdir Ashen" to create a new directory "Ashen", and then "ls" again to show the directory exists. The prompt "ashen@ashen-VMware-Virtual-Platform: ~/Desktop\$ |" appears at the bottom.

5. **rmdir** : This command is used to remove or delete an empty directory from the file system. For example, if you want to delete a directory named "Ashen" you have to type: **rmdir Ashen**.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
Ashen
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ rmdir Ashen
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

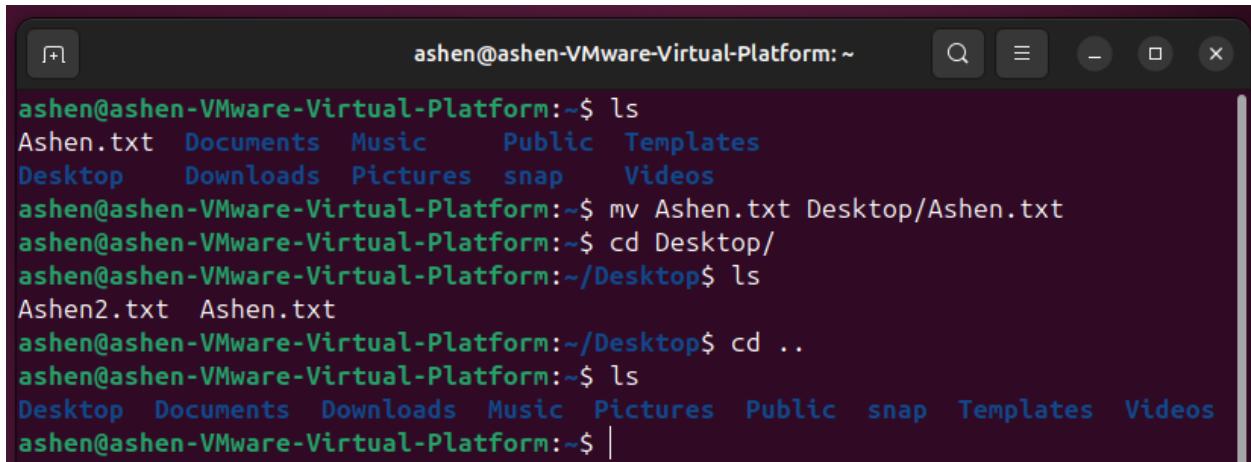
6. **cp** : This command is used for copying and rename files or directories to a different location. For example **cp source\_file destination\_file**



```
ashen@ashen-VMware-Virtual-Platform:~$ ls
Ashen.txt  Documents  Music  Public  Templates
Desktop   Downloads  Pictures  snap    Videos
ashen@ashen-VMware-Virtual-Platform:~$ cp Ashen.txt Desktop/Ashen2.txt
ashen@ashen-VMware-Virtual-Platform:~$ ls
Ashen.txt  Documents  Music  Public  Templates
Desktop   Downloads  Pictures  snap    Videos
ashen@ashen-VMware-Virtual-Platform:~$ cd Desktop
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
Ashen2.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

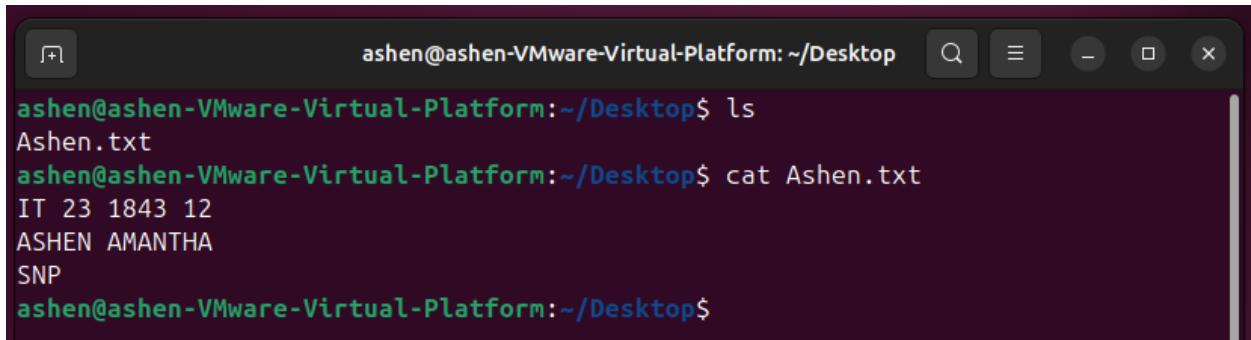
7. **mv** : This command is used to move the files or directories to another location. It also allows you to rename files or subdirectories by operating via the same directory.

- Simple syntax is **mv source\_file destination\_file** to move a file.



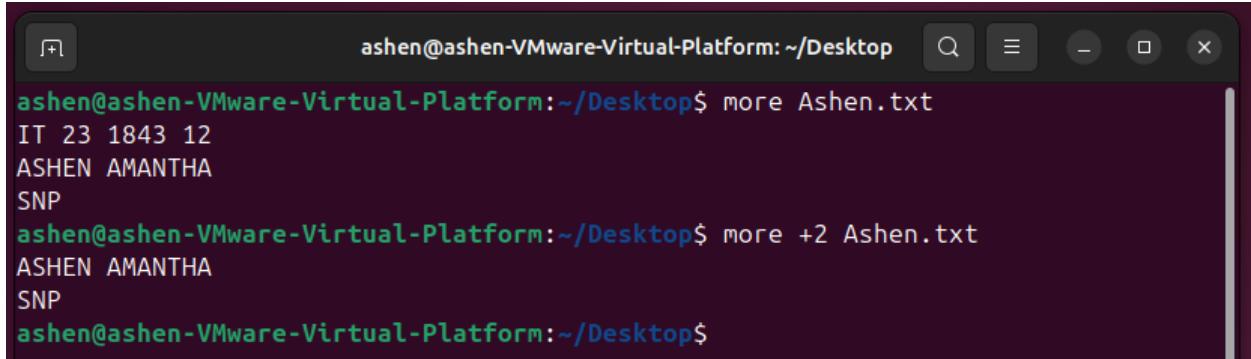
```
ashen@ashen-VMware-Virtual-Platform:~$ ls
Ashen.txt  Documents  Music  Public  Templates
Desktop   Downloads  Pictures  snap    Videos
ashen@ashen-VMware-Virtual-Platform:~$ mv Ashen.txt Desktop/Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~$ cd Desktop/
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
Ashen2.txt  Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ cd ..
ashen@ashen-VMware-Virtual-Platform:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
ashen@ashen-VMware-Virtual-Platform:~$ |
```

8. **cat** : (concatenate) This command is used to display the contents of a file, most commonly used in text files.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls
Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ cat Ashen.txt
IT 23 1843 12
ASHEN AMANTHA
SNP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

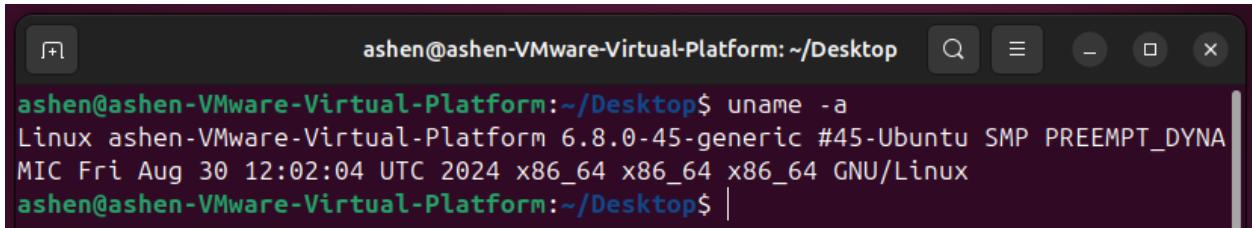
9. **more** : This command is used to view the contents of a text file one screen at a time(but not to edit) It's useful for viewing large files in a terminal window because it allows you to navigate through the file page by page, rather than displaying the entire content at once.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ more Ashen.txt
IT 23 1843 12
ASHEN AMANTHA
SNP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ more +2 Ashen.txt
ASHEN AMANTHA
SNP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

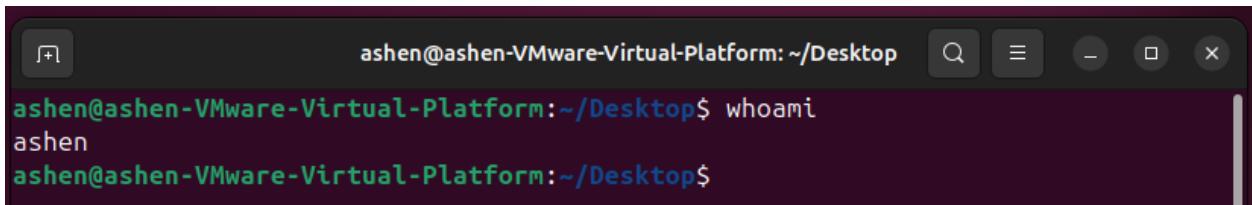
### 3. 15 Basic commands with brief Description

1. **uname -a** : This command shows system details. Will give out details about the operating system like the kernel version, machine hardware name and the operating system name.



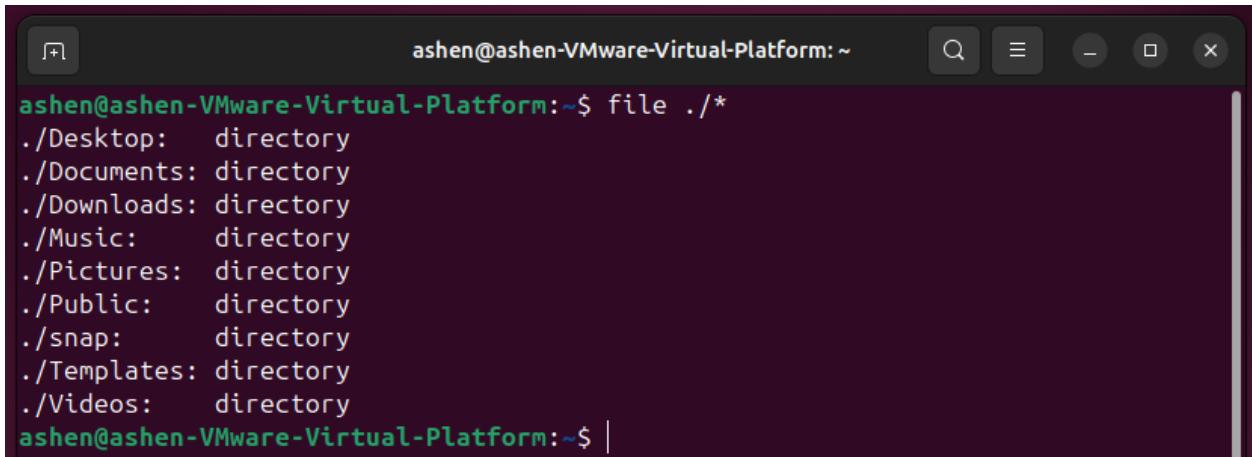
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ uname -a
Linux ashens-VMware-Virtual-Platform 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC
MIC Fri Aug 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

2. **whoami** : This command will print the name of the currently logged in user.



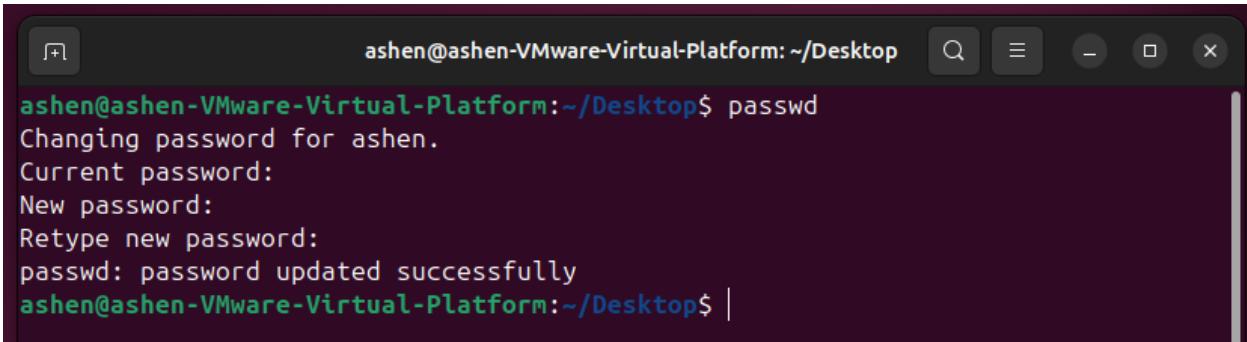
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ whoami
ashen
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

3. **file ./\*** : this command determine the type of each file and directory in the current directory.



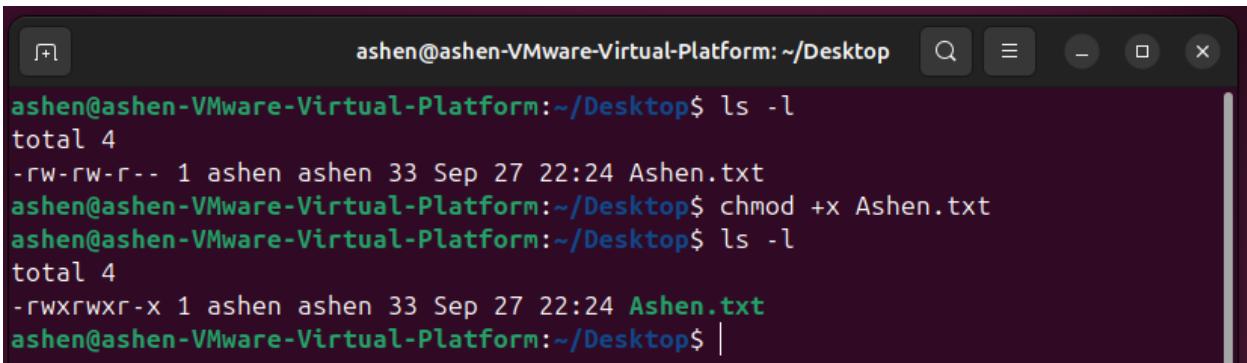
```
ashen@ashen-VMware-Virtual-Platform:~$ file ./*
./Desktop: directory
./Documents: directory
./Downloads: directory
./Music: directory
./Pictures: directory
./Public: directory
./snap: directory
./Templates: directory
./Videos: directory
ashen@ashen-VMware-Virtual-Platform:~$ |
```

4. **passwd** : This command is used to change the password of the already logged in account.



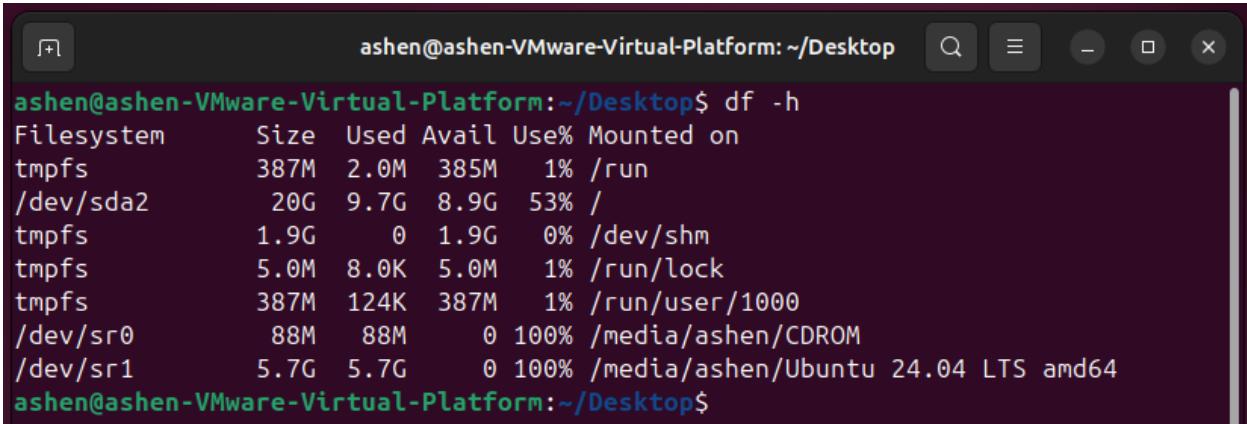
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ passwd
Changing password for ashen.
Current password:
New password:
Retype new password:
passwd: password updated successfully
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

5. **chmod** : This command is used to change file or directory permissions.



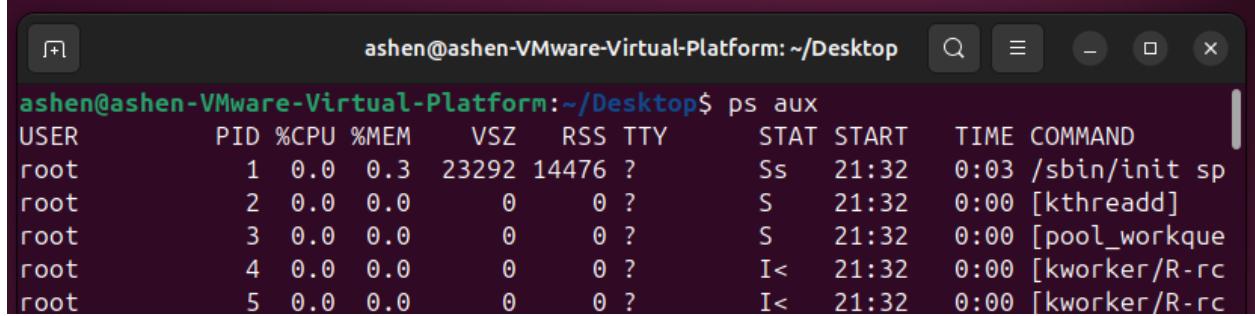
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 ashen ashen 33 Sep 27 22:24 Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ chmod +x Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ls -l
total 4
-rwxrwxr-x 1 ashen ashen 33 Sep 27 22:24 Ashen.txt
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

6. **df -h** : This command shows the disk space usage in a human-readable format.



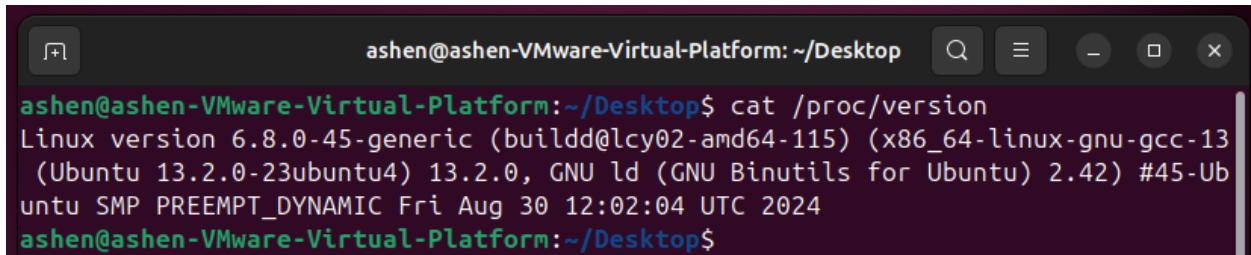
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs          387M   2.0M  385M   1% /run
/dev/sda2        20G   9.7G  8.9G  53% /
tmpfs          1.9G     0  1.9G   0% /dev/shm
tmpfs          5.0M   8.0K  5.0M   1% /run/lock
tmpfs          387M  124K  387M   1% /run/user/1000
/dev/sr0         88M   88M     0 100% /media/ashen/CDROM
/dev/sr1        5.7G  5.7G     0 100% /media/ashen/Ubuntu 24.04 LTS amd64
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

7. **ps aux** :This command lists currently running processes on the system .



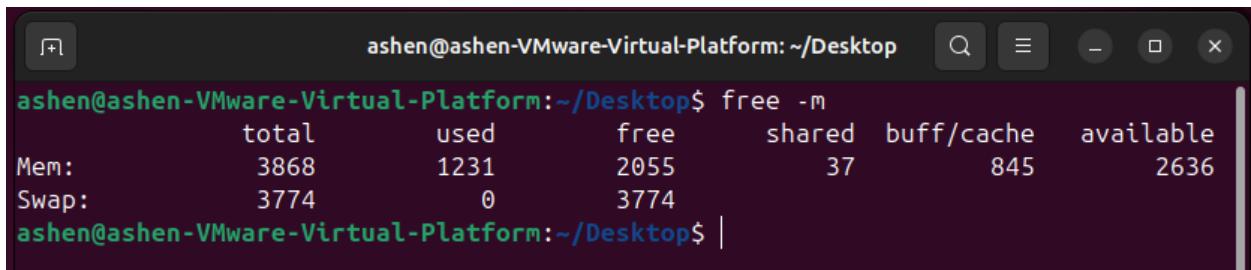
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3  23292 14476 ?        Ss   21:32  0:03 /sbin/init sp
root         2  0.0  0.0      0     0 ?        S    21:32  0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    21:32  0:00 [pool_workque
root         4  0.0  0.0      0     0 ?        I<   21:32  0:00 [kworker/R-rc
root         5  0.0  0.0      0     0 ?        I<   21:32  0:00 [kworker/R-rc
```

8. **cat /proc/version** : This command displays the version information of the Linux kernel and related details about the system. The **/proc/version** file contains the kernel version, the compiler used to build the kernel etc.



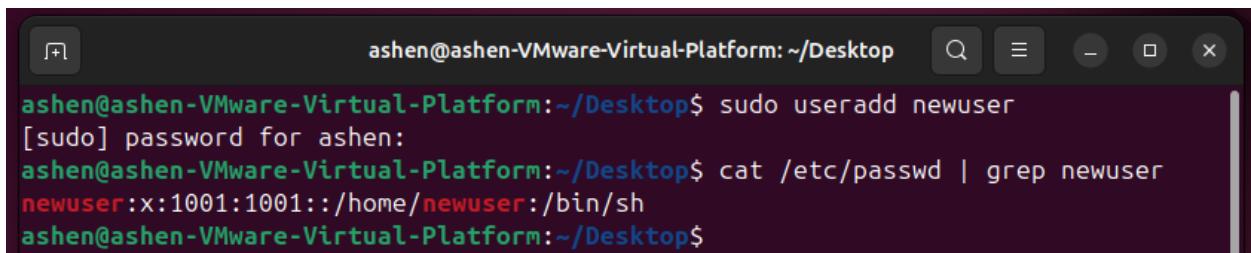
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ cat /proc/version
Linux version 6.8.0-45-generic (buildd@lcy02-amd64-115) (x86_64-linux-gnu-gcc-13
(Ubuntu 13.2.0-23ubuntu4) 13.2.0, GNU ld (GNU Binutils for Ubuntu) 2.42) #45-Ub
untu SMP PREEMPT_DYNAMIC Fri Aug 30 12:02:04 UTC 2024
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

9. **free -m** : This command in Linux displays information about the system's memory usage, both RAM and swap space, in megabytes



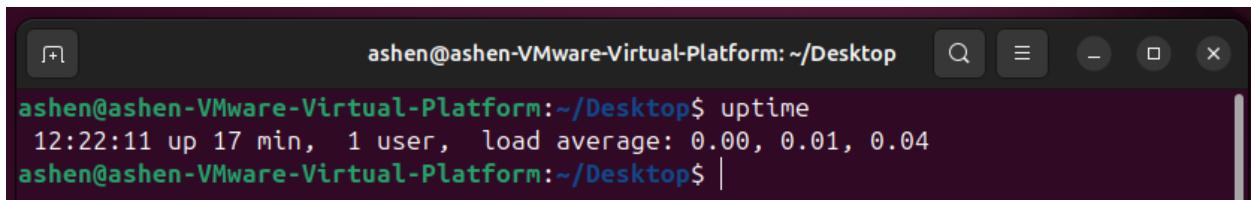
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ free -m
              total        used        free      shared  buff/cache   available
Mem:          3868       1231       2055         37       845       2636
Swap:         3774          0       3774
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

10. **useradd** : This command in Linux is used to create a new user account on the system.



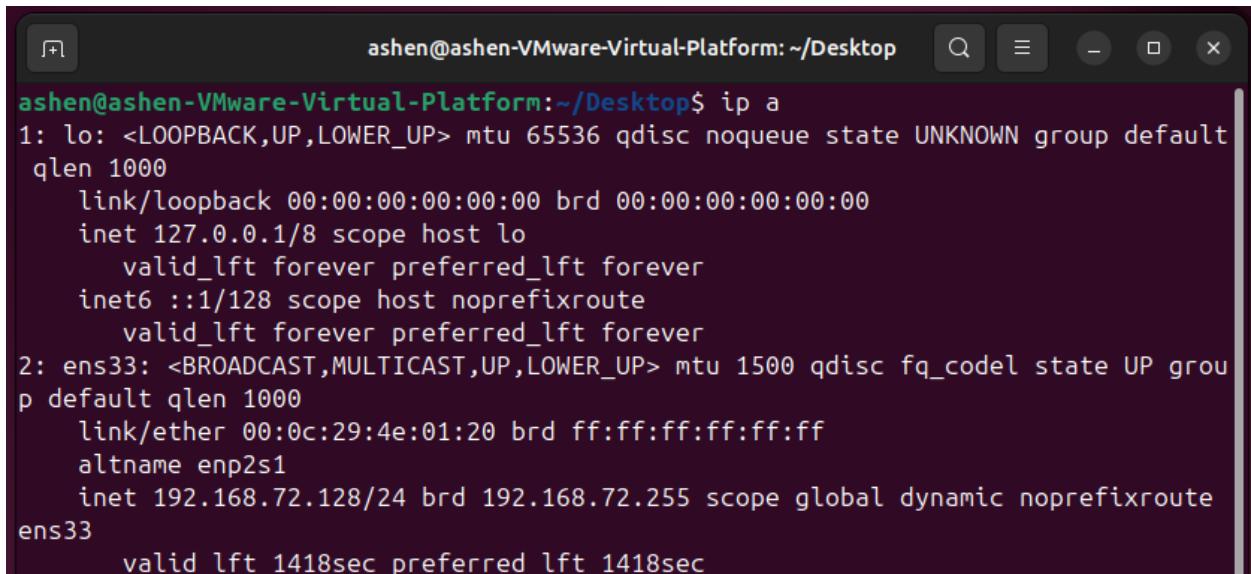
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo useradd newuser
[sudo] password for asheng:
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ cat /etc/passwd | grep newuser
newuser:x:1001:1001::/home/newuser:/bin/sh
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

11. **uptime** : This command shows how long the system has been running, along with the number of users and load averages.



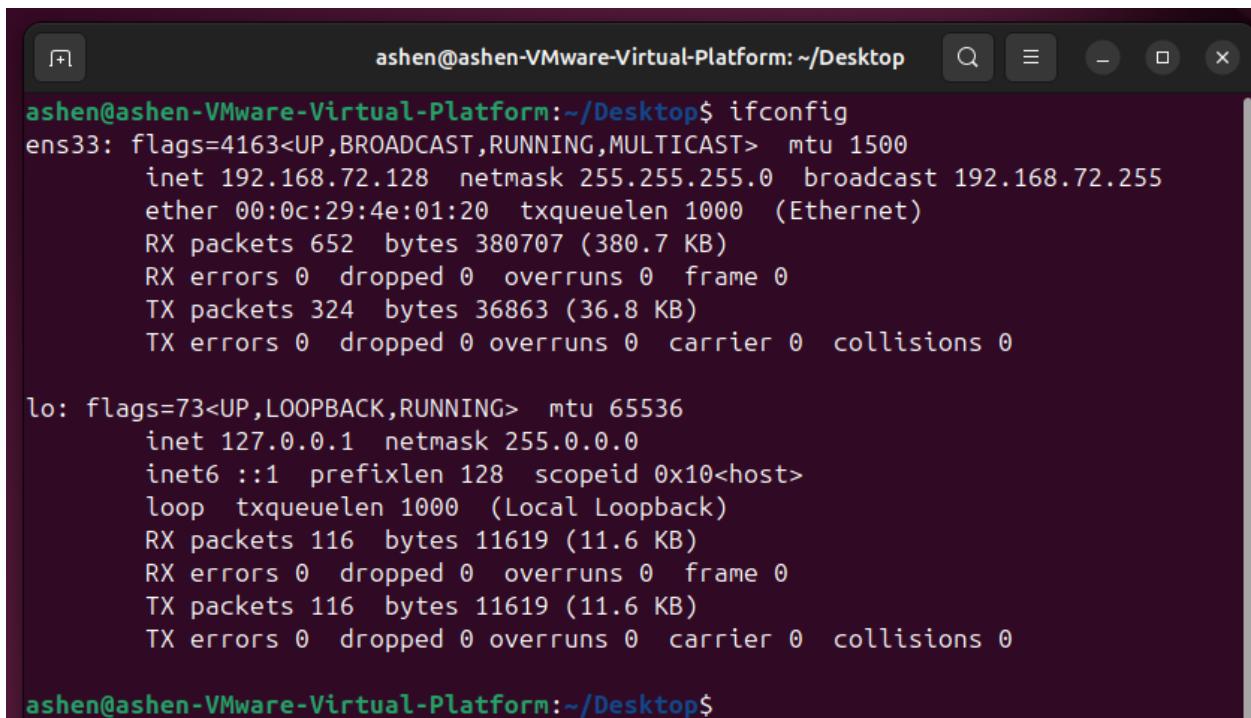
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ uptime
12:22:11 up 17 min, 1 user, load average: 0.00, 0.01, 0.04
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

12. **ip a** : This command used to display all network interfaces and their IP addresses.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
        link/ether 00:0c:29:4e:01:20 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.72.128/24 brd 192.168.72.255 scope global dynamic noprefixroute
            ens33
            valid_lft 1418sec preferred_lft 1418sec
```

13. **ifconfig** : This command used to display network interface configurations

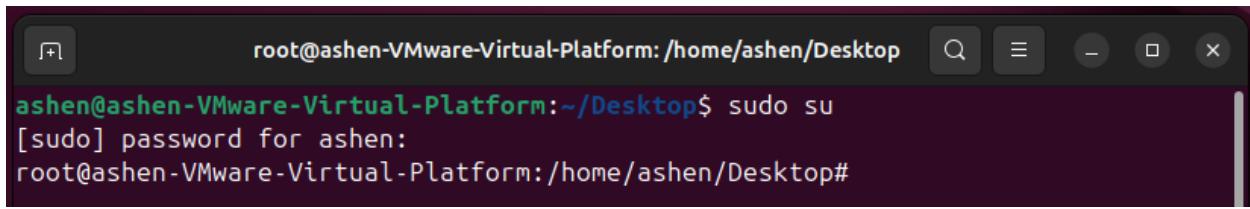


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.72.128 netmask 255.255.255.0 broadcast 192.168.72.255
        ether 00:0c:29:4e:01:20 txqueuelen 1000 (Ethernet)
        RX packets 652 bytes 380707 (380.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 324 bytes 36863 (36.8 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 116 bytes 11619 (11.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 116 bytes 11619 (11.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

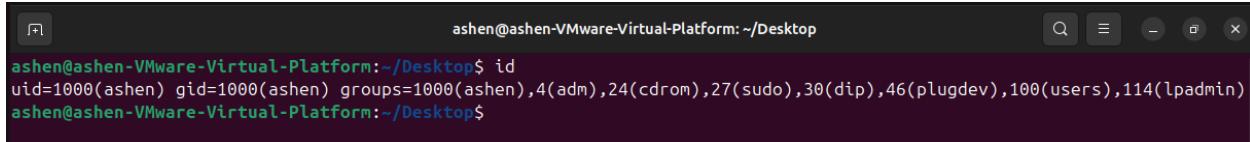
14. **sudo su** : This command is used to switch to Root User



A screenshot of a terminal window titled "root@ashen-VMware-Virtual-Platform: /home/ashen/Desktop". The command "sudo su" is entered, followed by a password prompt "[sudo] password for ashén:" and finally a root prompt "#".

```
root@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
[sudo] password for ashén:
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop#
```

15. **id** : This command is useful for quickly checking user and group IDs, which can help in managing permissions and understanding user roles in a Linux system.



A screenshot of a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The command "id" is entered, displaying the user's ID (uid=1000), group ID (gid=1000), and groups (groups=1000(ashen),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114(lpadmin)).

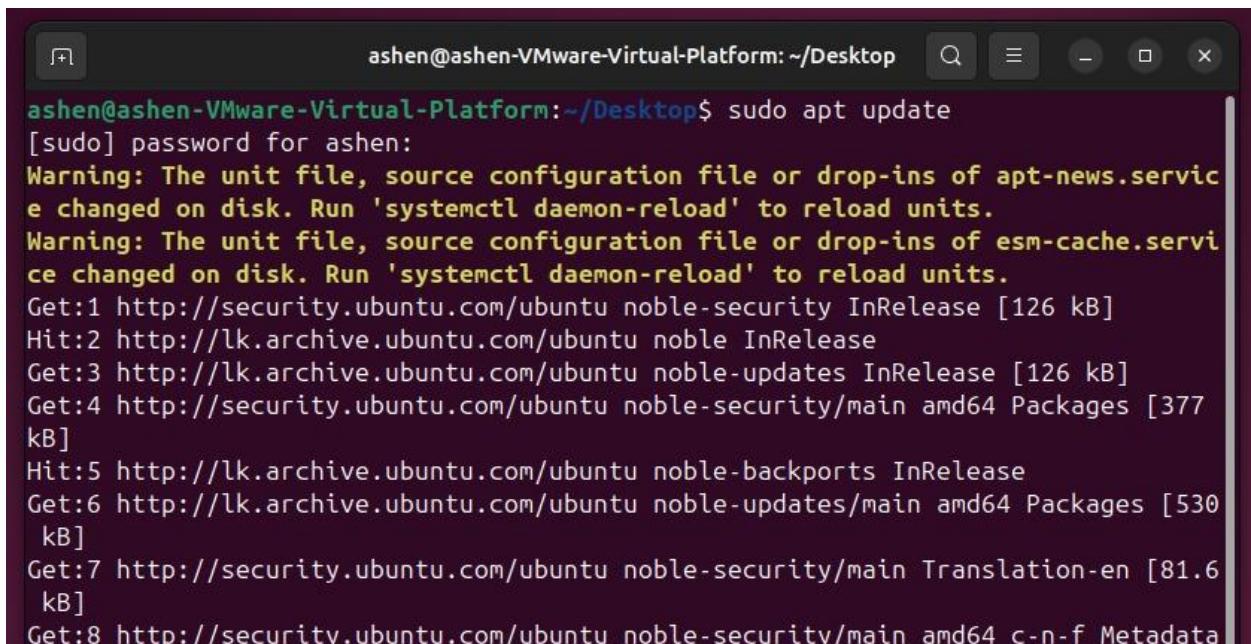
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ id
uid=1000(ashen) gid=1000(ashen) groups=1000(ashen),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114(lpadmin)
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

## 4.Configuration steps for DHCP, DNS and NTP Services

### DHCP(Dynamic Host Configuration Protocol) Installation and Configuration

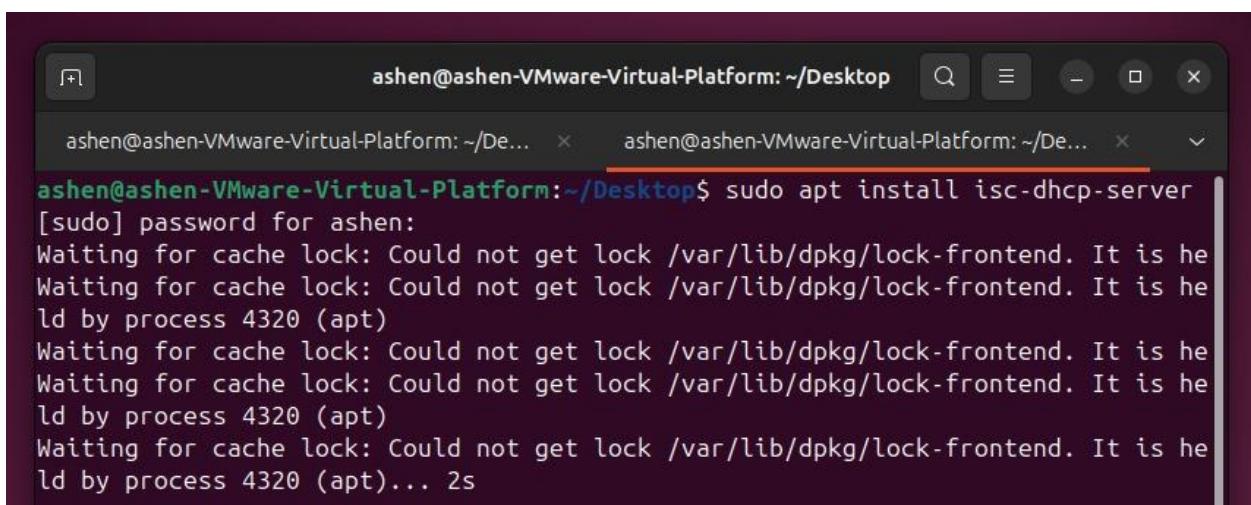
#### ➤ *DHCP Server Configuration*

1. Update the package list.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo apt update
[sudo] password for ashén:
Warning: The unit file, source configuration file or drop-ins of apt-news.service changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of esm-cache.service changed on disk. Run 'systemctl daemon-reload' to reload units.
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 [377 kB]
Hit:5 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [530 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.6 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata
```

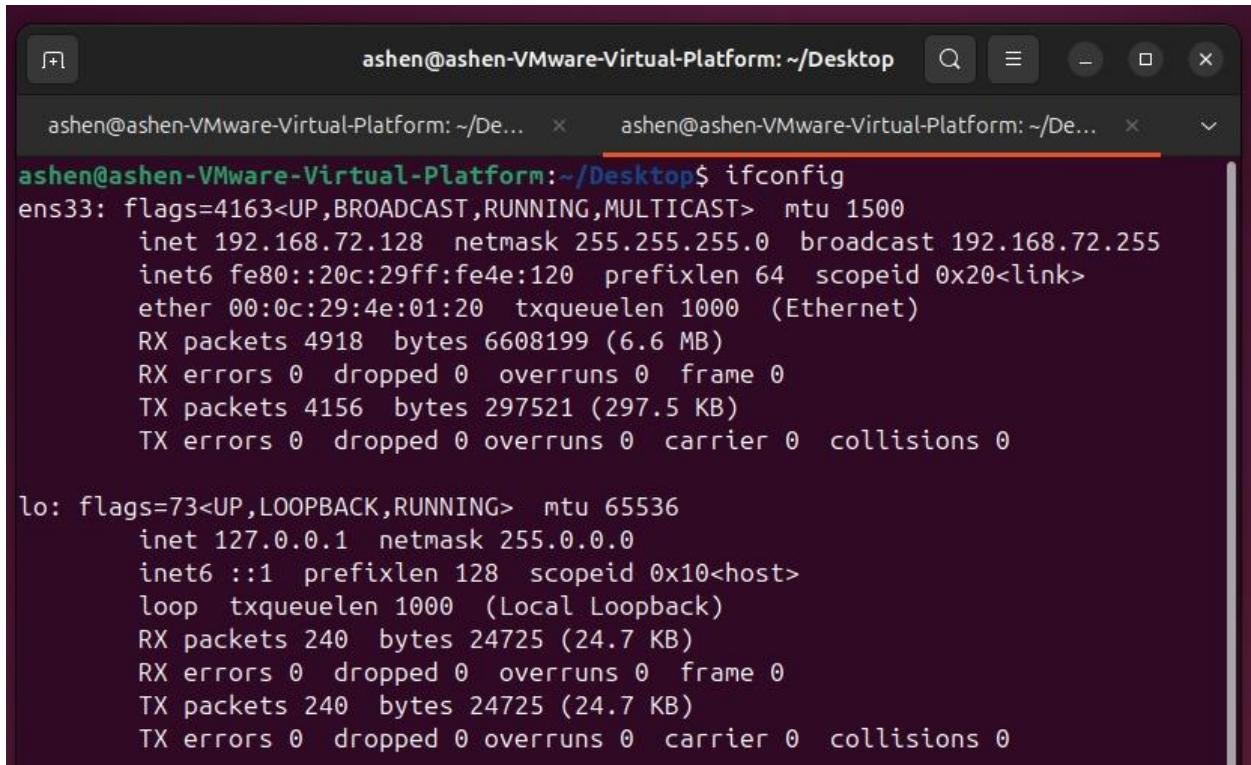
2. Install the **isc-dhcp-server** package



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo apt install isc-dhcp-server
[sudo] password for ashén:
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 4320 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 4320 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 4320 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 4320 (apt)... 2s
```

3. Use **ifconfig** command to view the network interfaces and record the NIC.

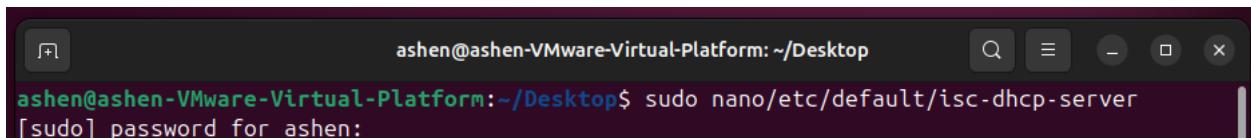
(if command not found install in with **sudo apt install net-tools**)



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.72.128 netmask 255.255.255.0 broadcast 192.168.72.255
              inet6 fe80::20c:29ff:fe4e:120 prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:4e:01:20 txqueuelen 1000 (Ethernet)
                  RX packets 4918 bytes 6608199 (6.6 MB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 4156 bytes 297521 (297.5 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 240 bytes 24725 (24.7 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 240 bytes 24725 (24.7 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. Open the configuration file for the ISC DHCP server using the nano text editor.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo nano/etc/default/isc-dhcp-server
[sudo] password for ash:
```

5. Modify the details for INTERFACESv4 inside the configuration file

- Here we have to specify which network interfaces the DHCP server should listen on to provide IP addresses to clients.
- By setting INTERFACESv4="ens33" → the DHCP server listens for DHCP requests on the ens33 network interface.
- By keeping INTERFACESv6="" variable empty → this implies that the DHCP server will not handle IPv6 DHCP requests.

The screenshot shows a terminal window with two tabs, both titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The active tab displays the contents of the file "/etc/default/isc-dhcp-server". The file contains configuration options for the DHCP server, including paths to configuration files, PID files, additional options, and interfaces. The bottom of the screen shows the nano editor's command-line interface with various keyboard shortcuts.

```
GNU nano 7.2          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDV4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpcd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

[ Read 18 lines ]

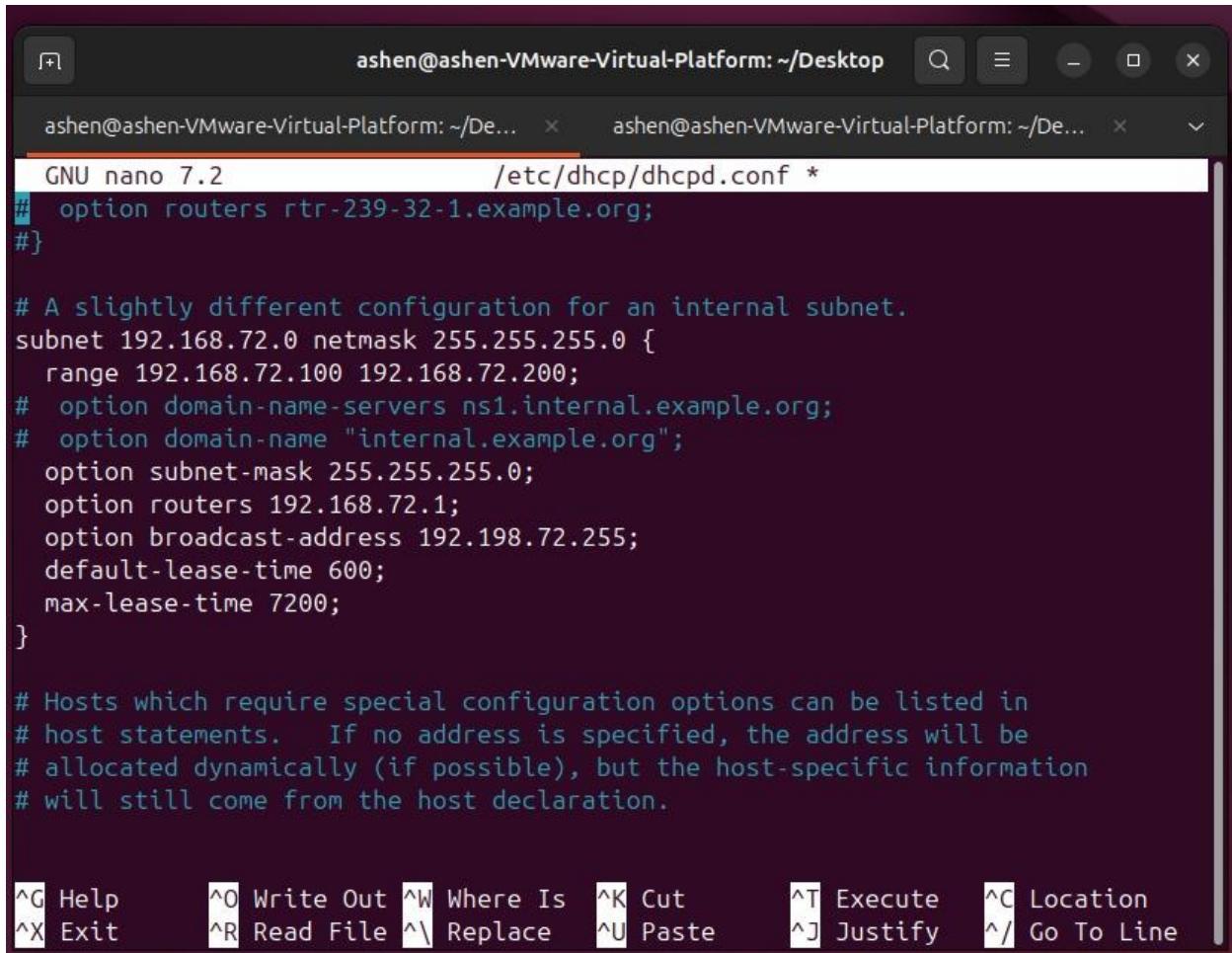
^C Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

6. Now open the main configuration file of DHCP.

The screenshot shows a terminal window with the title bar "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The command "sudo nano /etc/dhcp/dhcpcd.conf" is entered, followed by a password prompt "[sudo] password for ashlen: [REDACTED]".

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/dhcp/dhcpcd.conf
[sudo] password for ashlen: [REDACTED]
```

7. Modify and save the details inside the main configuration file according to our NIC to complete the DHCP configuration.



The screenshot shows a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The command "nano /etc/dhcp/dhcpd.conf" is running. The file contains configuration for a subnet and host statements. At the bottom, there is a menu bar with various keyboard shortcuts for nano editor.

```
GNU nano 7.2          /etc/dhcp/dhcpd.conf *
option routers rtr-239-32-1.example.org;
}

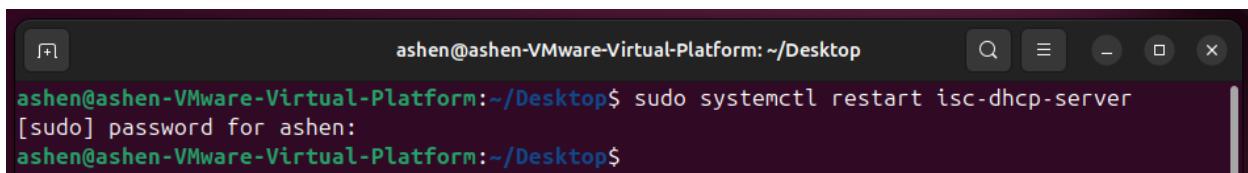
# A slightly different configuration for an internal subnet.
subnet 192.168.72.0 netmask 255.255.255.0 {
    range 192.168.72.100 192.168.72.200;
#    option domain-name-servers ns1.internal.example.org;
#    option domain-name "internal.example.org";
    option subnet-mask 255.255.255.0;
    option routers 192.168.72.1;
    option broadcast-address 192.198.72.255;
    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
# will still come from the host declaration.

^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
```

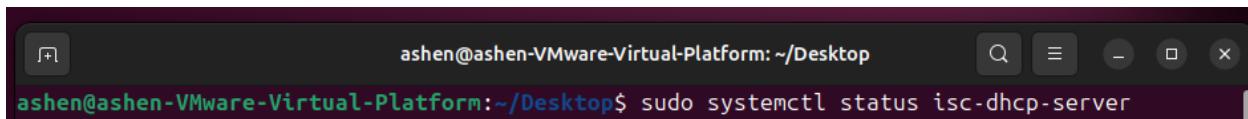
8. Restart the DHCP server.

-      sudo systemctl restart isc-dhcp-server



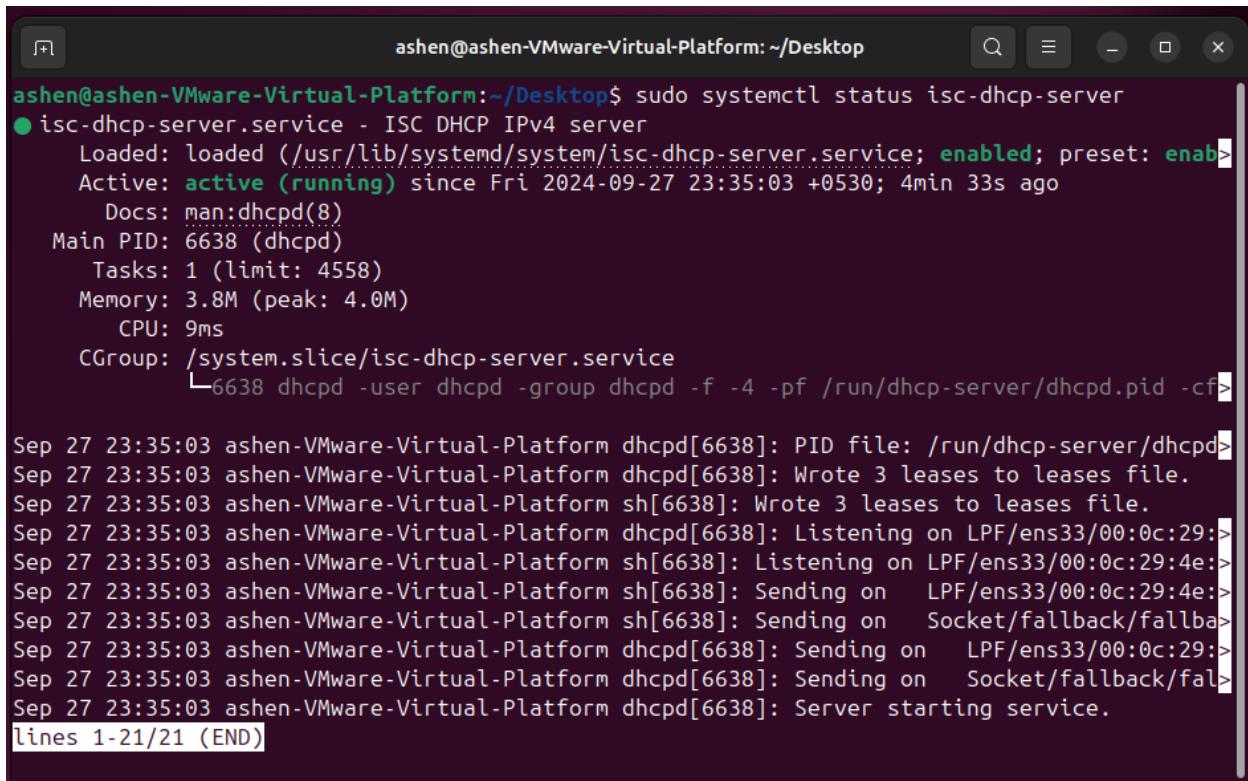
The screenshot shows a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop\$". The command "sudo systemctl restart isc-dhcp-server" is being run. A password prompt "[sudo] password for ashen:" appears before the command is executed.

9. To verify the configuration check the status of the DHCP server.



The screenshot shows a terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop\$". The command "sudo systemctl status isc-dhcp-server" is being run to check the status of the DHCP service.

10. If the configuration is successful, it is indicated with a status: active

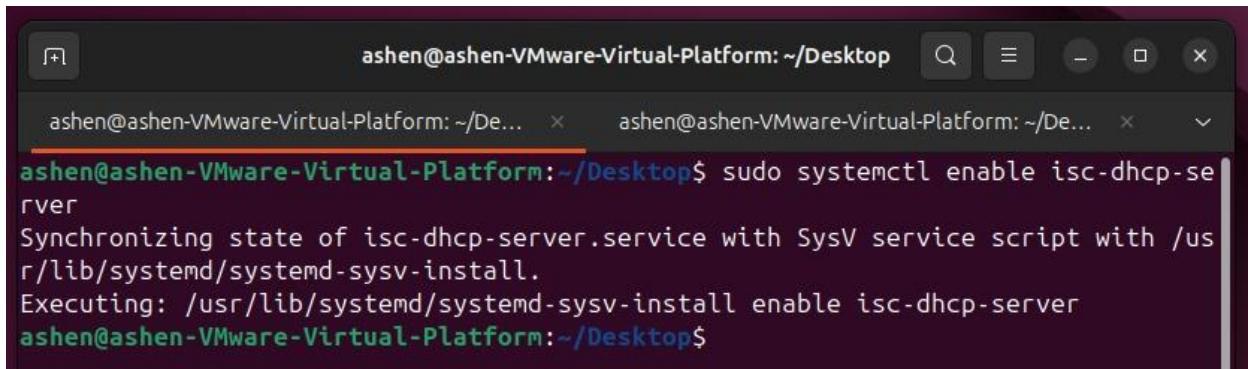


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
  Active: active (running) since Fri 2024-09-27 23:35:03 +0530; 4min 33s ago
    Docs: man:dhcpcd(8)
   Main PID: 6638 (dhcpcd)
      Tasks: 1 (limit: 4558)
     Memory: 3.8M (peak: 4.0M)
        CPU: 9ms
       CGroup: /system.slice/isc-dhcp-server.service
               └─6638 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcpcd.pid -cf /etc/dhcpcd.conf -lf /var/lib/dhcp

Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: PID file: /run/dhcp-server/dhcpcd.pid
Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: Wrote 3 leases to leases file.
Sep 27 23:35:03 ashen-VMware-Virtual-Platform sh[6638]: Wrote 3 leases to leases file.
Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: Listening on LPF/ens33/00:0c:29:4e:00:0c%ens33
Sep 27 23:35:03 ashen-VMware-Virtual-Platform sh[6638]: Listening on LPF/ens33/00:0c:29:4e%ens33
Sep 27 23:35:03 ashen-VMware-Virtual-Platform sh[6638]: Sending on   LPF/ens33/00:0c:29:4e%ens33
Sep 27 23:35:03 ashen-VMware-Virtual-Platform sh[6638]: Sending on   Socket/fallback/fallback-wait(0)
Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: Sending on   LPF/ens33/00:0c:29:4e%ens33
Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: Sending on   Socket/fallback/fallback-wait(0)
Sep 27 23:35:03 ashen-VMware-Virtual-Platform dhcpcd[6638]: Server starting service.
lines 1-21/21 (END)
```

11. Enable the service for the boot time (ensure that the DHCP server (isc-dhcp-server) starts automatically whenever the system is booted)

- sudo systemctl enable isc-dhcp-server

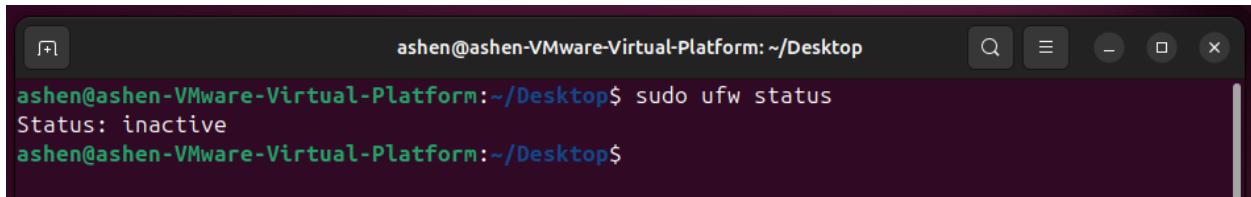


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable isc-dhcp-server
Synchronizing state of isc-dhcp-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable isc-dhcp-server
ashen@ashen-VMware-Virtual-Platform:~/Desktop$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

12. Check the current status of the firewall.

-        sudo ufw status

If the firewall status is inactive, the server will be able to communicate with clients without any restrictions.



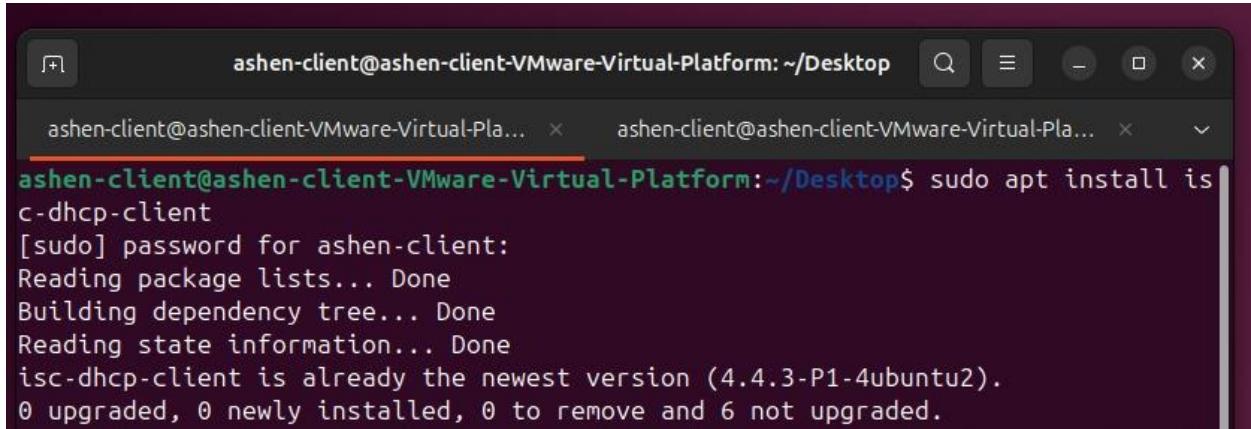
The screenshot shows a terminal window with a dark background and light-colored text. At the top, it displays the user's name, host, and current directory: "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". Below this, the command "sudo ufw status" is run, followed by its output: "Status: inactive". The prompt "ashen@ashen-VMware-Virtual-Platform:~/Desktop\$" appears again at the bottom. The window has standard operating system window controls (minimize, maximize, close) at the top right.

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo ufw status
Status: inactive
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

## ➤ **DHCP Client Configuration**

1. Install the DHCP client on another separate virtual machine (Linux distribution)

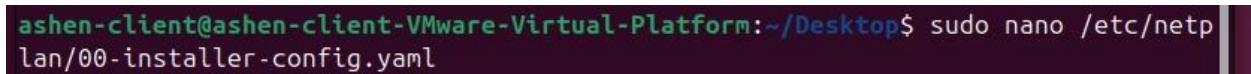
- sudo apt install isc-dhcp-client



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo apt install isc-dhcp-client
[sudo] password for ashen-client:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
isc-dhcp-client is already the newest version (4.4.3-P1-4ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
```

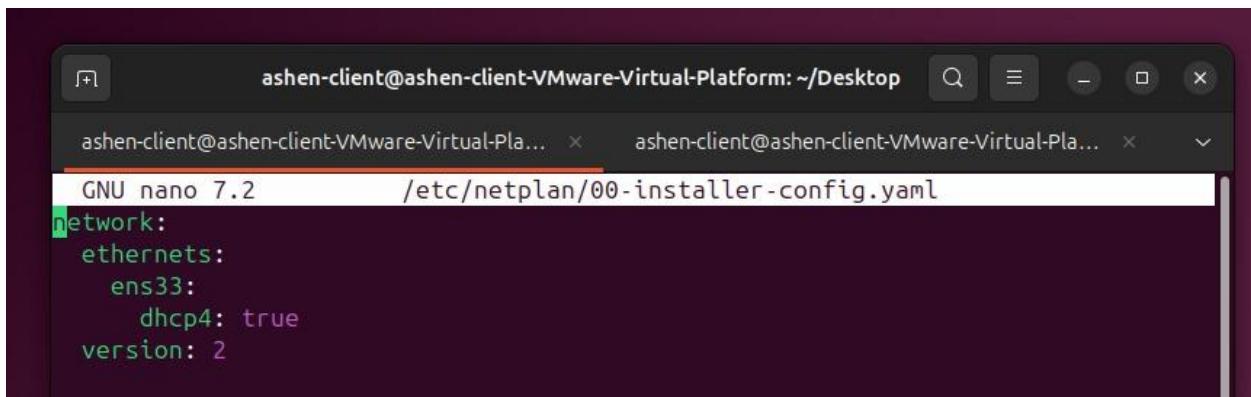
2. Configure the client to obtain an IP Address via DHCP

- Open the configuration file on the client.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/netplan/00-installer-config.yaml
```

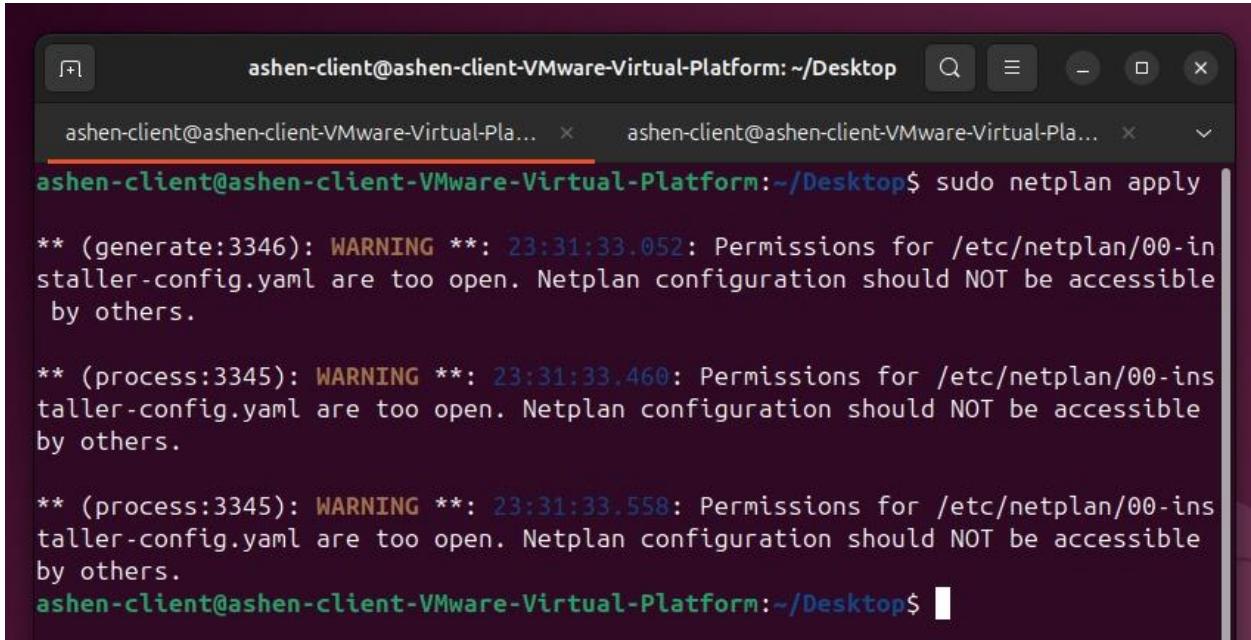
- Modify the configuration file.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ 
GNU nano 7.2          /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    ens33:
      dhcp4: true
      version: 2
```

### 3. Apply the changes .

-      sudo netplan apply



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo netplan apply

** (generate:3346): WARNING **: 23:31:33.052: Permissions for /etc/netplan/00-installer-config.yaml are too open. Netplan configuration should NOT be accessible by others.

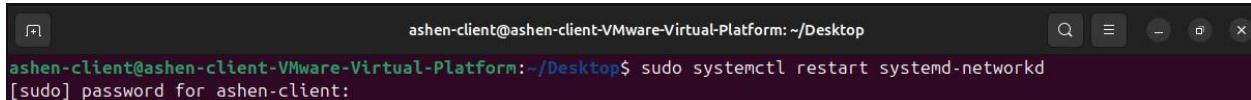
** (process:3345): WARNING **: 23:31:33.460: Permissions for /etc/netplan/00-installer-config.yaml are too open. Netplan configuration should NOT be accessible by others.

** (process:3345): WARNING **: 23:31:33.558: Permissions for /etc/netplan/00-installer-config.yaml are too open. Netplan configuration should NOT be accessible by others.

ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

### 4. Restart the service to apply the changes.

-      sudo systemctl restart systemd-networkd



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart systemd-networkd
[sudo] password for ashén-client:
```

### 5. To verify the configuration check the status.

-      status : active



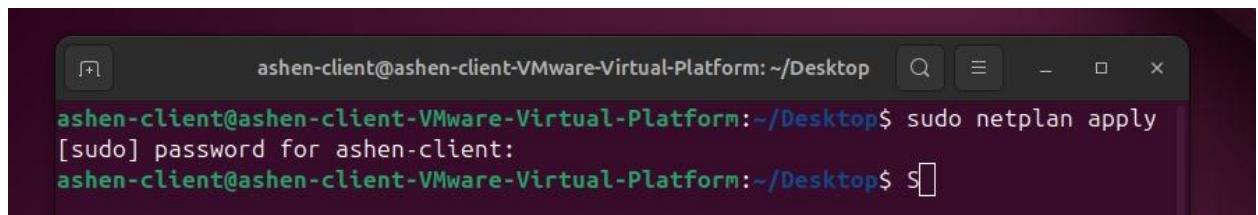
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl status systemd-networkd
● systemd-networkd.service - Network Configuration
  Loaded: loaded (/usr/lib/systemd/system/systemd-networkd.service)
  Active: active (running) since Wed 2024-09-25 23:42:16 +0530; 1min 1s ago
    TriggeredBy: ● systemd-networkd.socket
    Docs: man:systemd-networkd.service(8)
           man:org.freedesktop.network1(5)
   Main PID: 5465 (systemd-network)
      Status: "Processing requests..."
        Tasks: 1 (limit: 4558)
       FD Store: 0 (limit: 512)
      Memory: 3.1M (peak: 3.4M)
         CPU: 29ms
      CGroup: /system.slice/systemd-networkd.service
              └─5465 /usr/lib/systemd/systemd-networkd
```

## 6. Enable the service for the boot time.

- sudo systemctl enable system-networkd

```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable systemd-networkd
Created symlink /etc/systemd/system/dbus-org.freedesktop.network1.service → /usr/lib/systemd/system/systemd-networkd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/systemd-networkd.service → /usr/lib/systemd/system/systemd-networkd.service.
Created symlink /etc/systemd/system/sockets.target.wants/systemd-networkd.socket → /usr/lib/systemd/system/systemd-networkd.socket.
Created symlink /etc/systemd/system/sysinit.target.wants/systemd-network-generator.service → /usr/lib/systemd/system/systemd-network-generator.service.
Created symlink /etc/systemd/system/network-online.target.wants/systemd-networkd-wait-online.service → /usr/lib/systemd/system/systemd-networkd-wait-online.service.
```

## 7. Reapply the netplan.

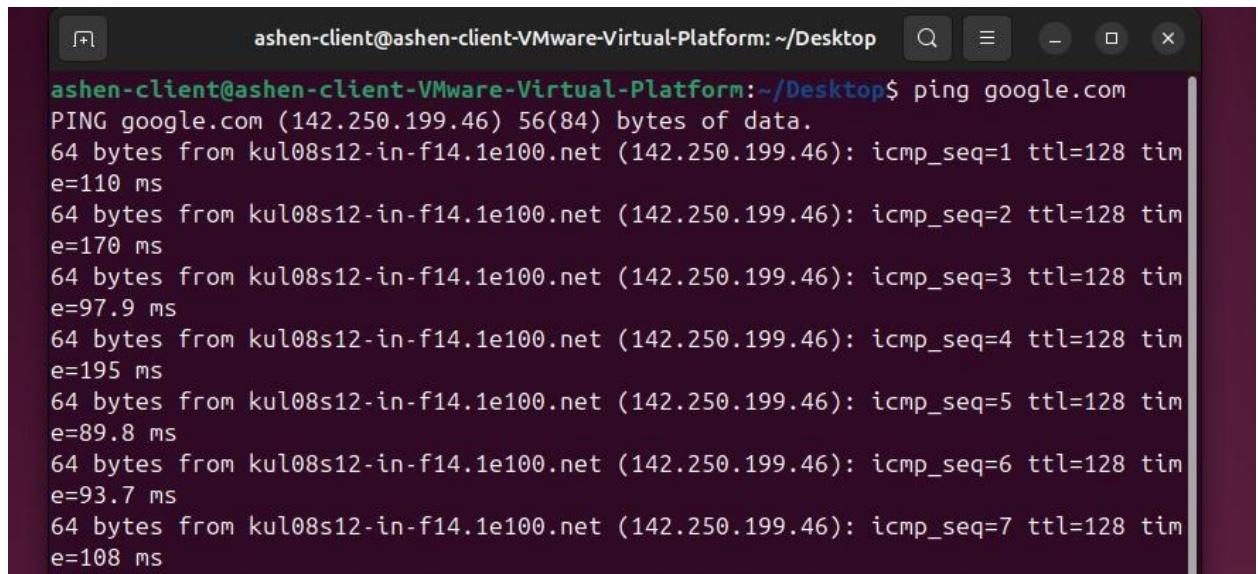


```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo netplan apply
[sudo] password for ashen-client:
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## Verification

### Check Network Connectivity

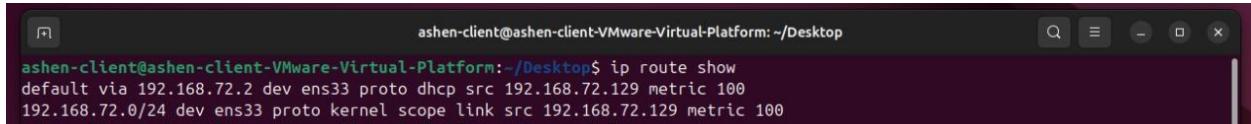
Try to check your internet or network connectivity by pinging an external website or the gateway provided by the DHCP server.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ping google.com
PING google.com (142.250.199.46) 56(84) bytes of data.
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=1 ttl=128 time=110 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=2 ttl=128 time=170 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=3 ttl=128 time=97.9 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=4 ttl=128 time=195 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=5 ttl=128 time=89.8 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=6 ttl=128 time=93.7 ms
64 bytes from kul08s12-in-f14.1e100.net (142.250.199.46): icmp_seq=7 ttl=128 time=108 ms
```

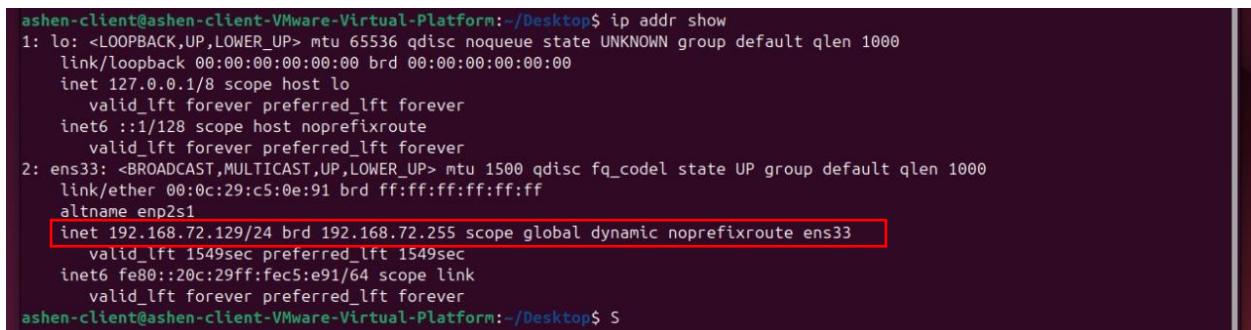
(The ping google.com command's output verifies that your Ubuntu client, configured as a DHCP client has effectively acquired network connectivity and can thus interact with outside networks).

## To check the default gateway



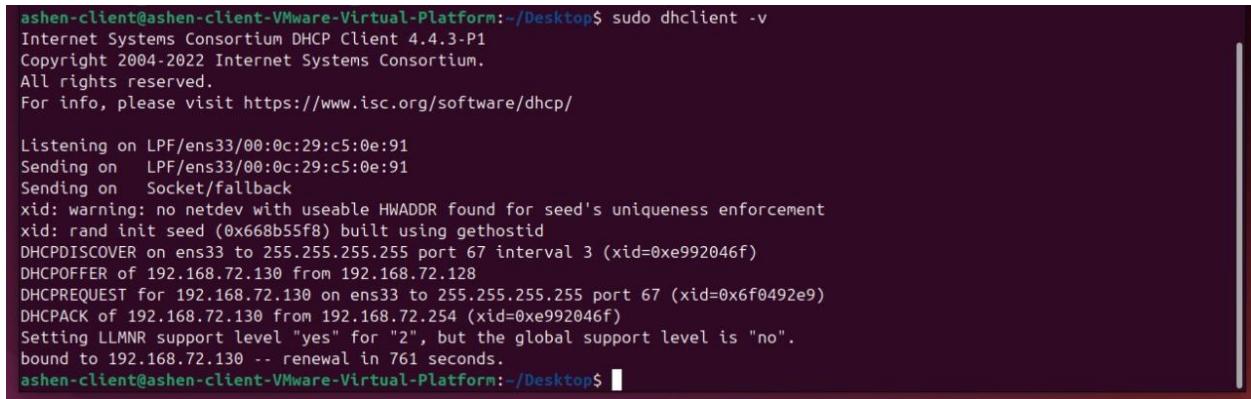
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ip route show
default via 192.168.72.2 dev ens33 proto dhcp src 192.168.72.129 metric 100
192.168.72.0/24 dev ens33 proto kernel scope link src 192.168.72.129 metric 100
```

## Check the status of your network interfaces and whether they've obtained IP addresses



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ip addr show
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c5:0e:91 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.72.129/24 brd 192.168.72.255 scope global dynamic noprefixroute ens33
        valid_lft 1549sec preferred_lft 1549sec
        inet6 fe80::20c:29ff:fe91:64 scope link
            valid_lft forever preferred_lft forever
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

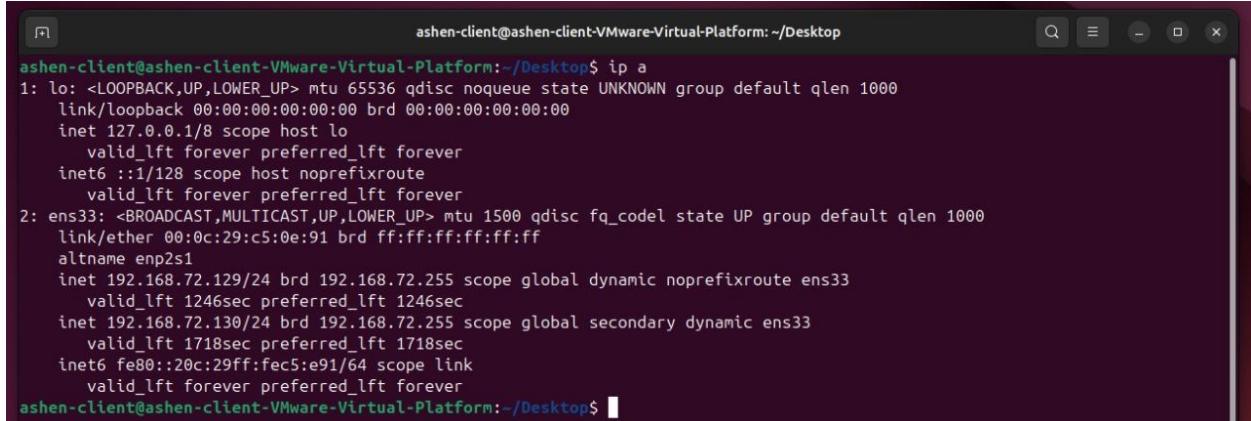
## Check if the DHCP Client Obtained an IP Address.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

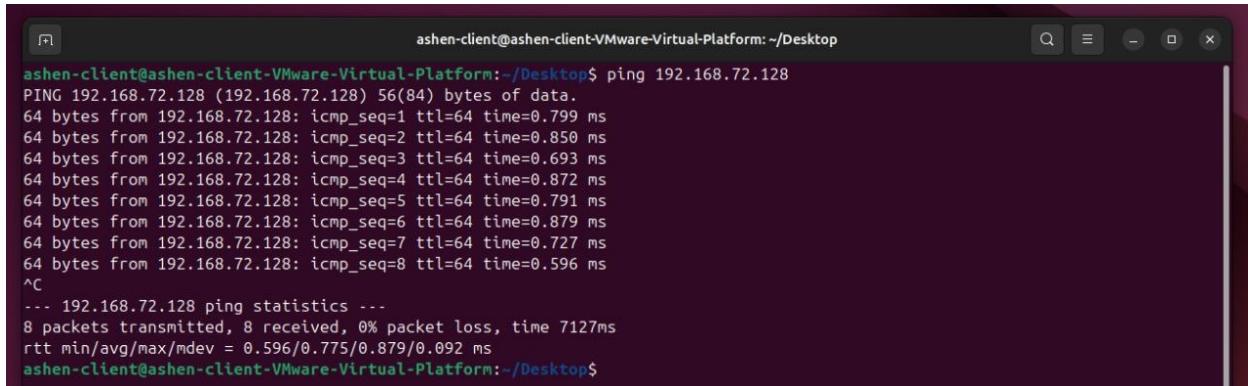
Listening on LPF/ens33/00:0c:29:c5:0e:91
Sending on  LPF/ens33/00:0c:29:c5:0e:91
Sending on  Socket/fallback
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement
xid: rand init seed (0x668b5f8) built using gethostid
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 3 (xid=0xe992046f)
DHCPOFFER of 192.168.72.130 from 192.168.72.128
DHCPREQUEST for 192.168.72.130 on ens33 to 255.255.255.255 port 67 (xid=0x6f0492e9)
DHCPACK of 192.168.72.130 from 192.168.72.254 (xid=0xe992046f)
Setting LLMNR support level "yes" for "2", but the global support level is "no".
bound to 192.168.72.130 -- renewal in 761 seconds.
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## Verify the DHCP client setup



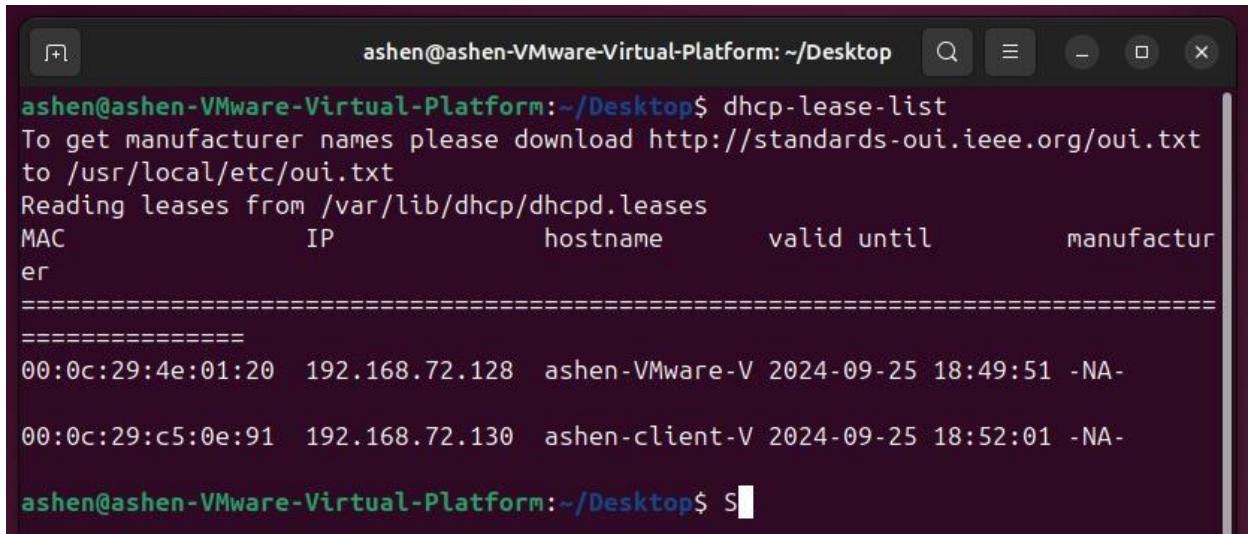
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c5:0e:91 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.72.129/24 brd 192.168.72.255 scope global dynamic noprefixroute ens33
        valid_lft 1246sec preferred_lft 1246sec
        inet 192.168.72.130/24 brd 192.168.72.255 scope global secondary dynamic ens33
            valid_lft 1718sec preferred_lft 1718sec
        inet6 fe80::20c:29ff:fe91:64 scope link
            valid_lft forever preferred_lft forever
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## Get the dhcp server ip address and ping it in the dhcp client



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ping 192.168.72.128
PING 192.168.72.128 (192.168.72.128) 56(84) bytes of data.
64 bytes from 192.168.72.128: icmp_seq=1 ttl=64 time=0.799 ms
64 bytes from 192.168.72.128: icmp_seq=2 ttl=64 time=0.850 ms
64 bytes from 192.168.72.128: icmp_seq=3 ttl=64 time=0.693 ms
64 bytes from 192.168.72.128: icmp_seq=4 ttl=64 time=0.872 ms
64 bytes from 192.168.72.128: icmp_seq=5 ttl=64 time=0.791 ms
64 bytes from 192.168.72.128: icmp_seq=6 ttl=64 time=0.879 ms
64 bytes from 192.168.72.128: icmp_seq=7 ttl=64 time=0.727 ms
64 bytes from 192.168.72.128: icmp_seq=8 ttl=64 time=0.596 ms
^C
--- 192.168.72.128 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7127ms
rtt min/avg/max/mdev = 0.596/0.775/0.879/0.092 ms
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

Finally, in the dhcp server/ubuntu server get a list of the clients that are connected to the server.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ dhclient-lease-list
To get manufacturer names please download http://standards-oui.ieee.org/oui.txt
to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC           IP           hostname      valid until      manufacturer
=====
00:0c:29:4e:01:20  192.168.72.128  ashen-VMware-V  2024-09-25 18:49:51 -NA-
00:0c:29:c5:0e:91  192.168.72.130  ashen-client-V  2024-09-25 18:52:01 -NA-
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ S
```

# DNS(Domain Name System Protocol) Installation and Configuration

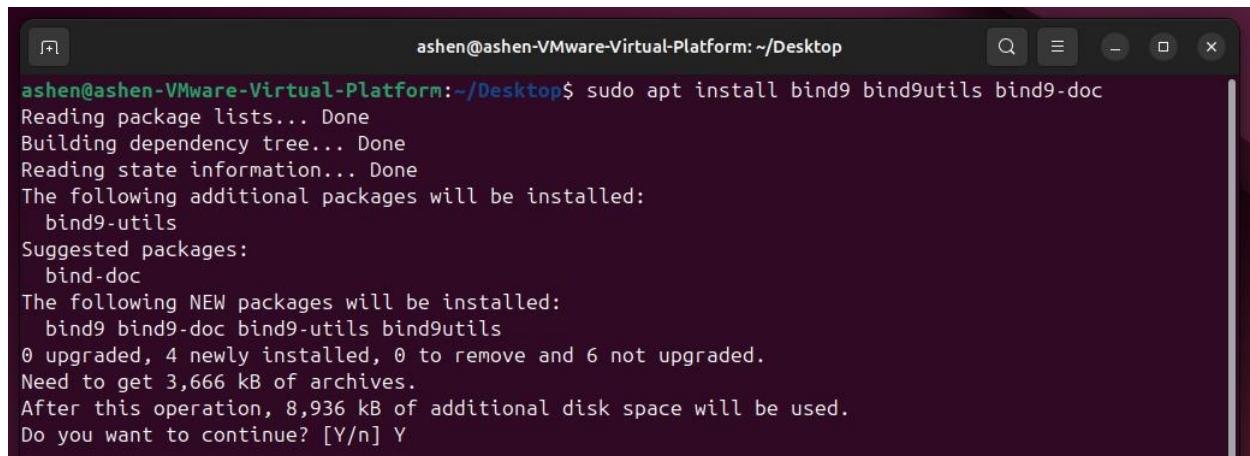
## ➤ DNS Sever Configuration

1. Update the package list

- sudo apt update

2. Install BIND9 (BIND9 DNS server and related utilities on a Debian-based system like Ubuntu)

- sudo apt install bind9 bind9utils bind9-doc



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ 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 6 not upgraded.
Need to get 3,666 kB of archives.
After this operation, 8,936 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

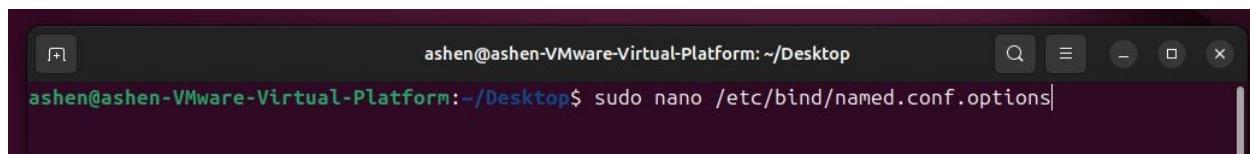
3. Configure DNS forwarders

- When your DNS server receives a query it cannot resolve locally, it will forward the query to another DNS server.

- If your DNS server also needs to resolve external domain names DNS forwarders is necessary.

a) Open the configuration file.

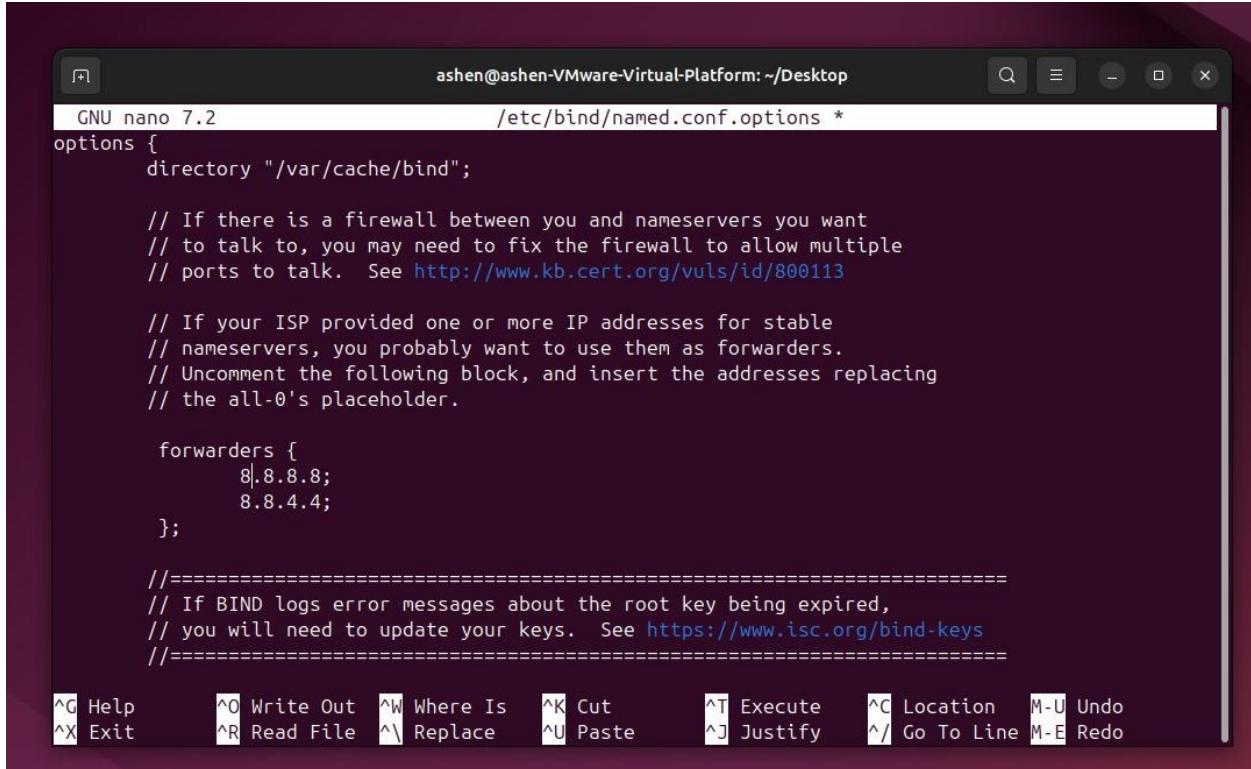
- sudo nano /etc/bind/named.conf.options



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/bind/named.conf.options
```

b) Modify the forwarders section

- we can add Google's public DNS servers or Cloudflare's public DNS servers.
- here I have added Google's public and Secondary DNS servers



```
ashen@ashen-VMware-Virtual-Platform: ~/Desktop
GNU nano 7.2          /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

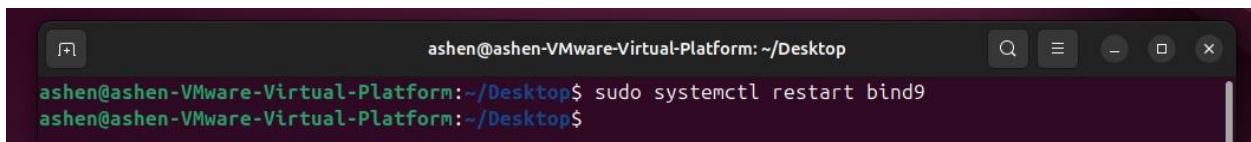
    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====

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

c) Save and Exit.

d) Restart the service to apply changes.

- sudo systemctl restart bind9



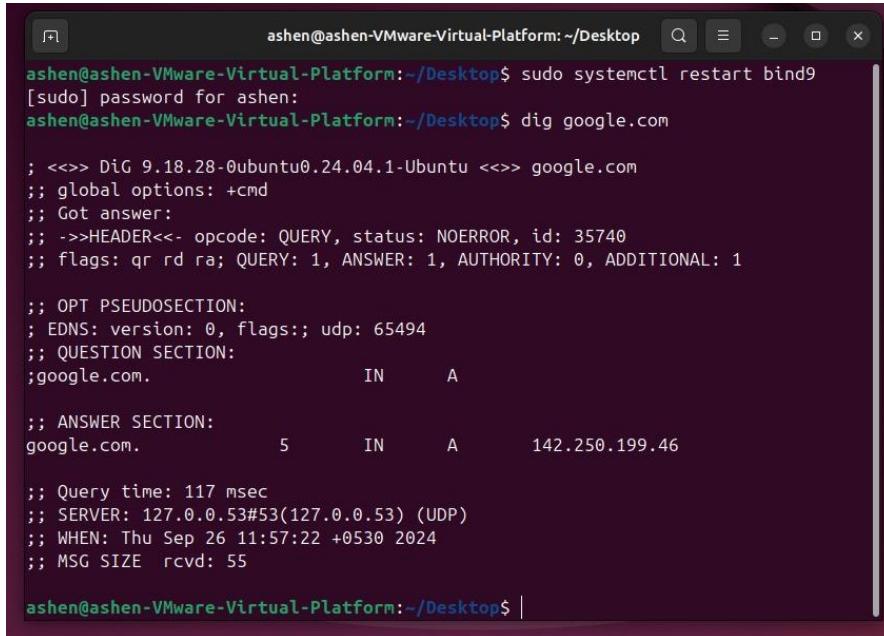
```
ashen@ashen-VMware-Virtual-Platform: ~/Desktop
ashen@ashen-VMware-Virtual-Platform: ~/Desktop$ sudo systemctl restart bind9
ashen@ashen-VMware-Virtual-Platform: ~/Desktop$
```

## Verification of Forwarders

The **dig** tool is one of the most popular DNS troubleshooting tools. It allows you to query DNS servers and see how they respond.

- dig google.com

if this returns IP address of google.com , the forwarders are working correctly.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart bind9
[sudo] password for ashén:
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ dig google.com

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35740
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

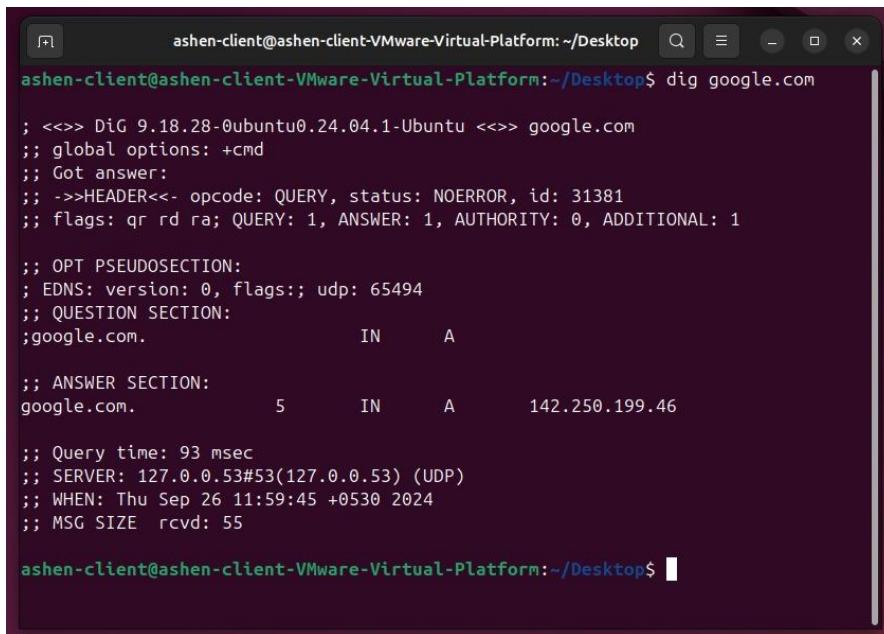
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.          5       IN      A      142.250.199.46

;; Query time: 117 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Sep 26 11:57:22 +0530 2024
;; MSG SIZE  rcvd: 55

ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

Server



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ dig google.com

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31381
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.          5       IN      A      142.250.199.46

;; Query time: 93 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Sep 26 11:59:45 +0530 2024
;; MSG SIZE  rcvd: 55

ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ |
```

Client

## ➤ DNS Client Configuration

### 1. Install the DNS Client

#### 1. Update the package list.

```
- sudo apt update
```

#### 2. Install resolvconf if necessary.

```
- sudo apt install resolvconf
```

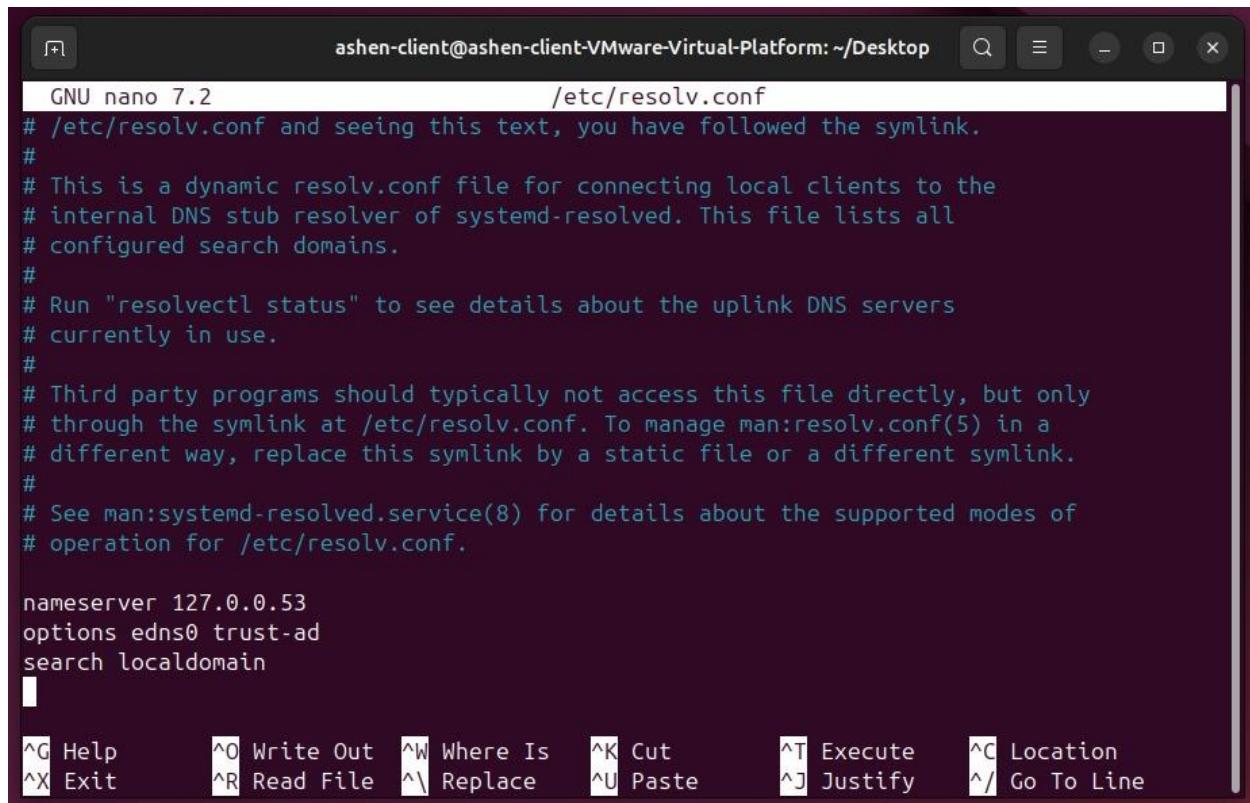
### 2. Configure the DNS client settings

#### 1. Open server VM conf file and note down the ip address of DNS server.

```
- cat /etc/resolv.conf
```

#### 2. Set the DNS server as the nameserver of the client VM .

```
- sudo nano /etc/resolv.conf
```



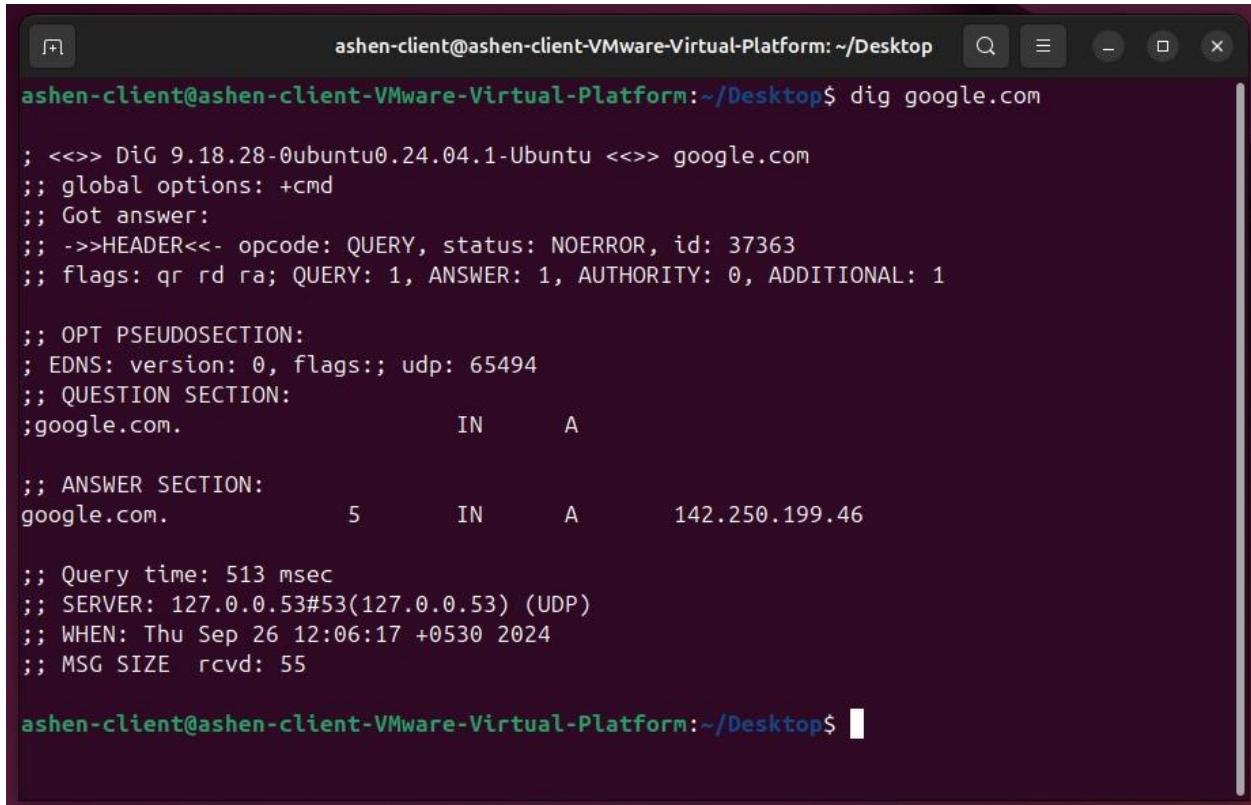
```
GNU nano 7.2          /etc/resolv.conf
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
```

The screenshot shows a terminal window titled "ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop". The window displays the contents of the /etc/resolv.conf file. The file is a dynamic resolv.conf file managed by systemd-resolved, containing comments about its purpose and how to use it. It includes a nameserver entry for 127.0.0.53 and options for edns0 and trust-ad. The bottom of the window shows the nano editor's command bar with various keyboard shortcuts for file operations like Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, and Go To Line.

### 3. Test DNS Resolution

- To test DNS resolution on your system, you can use tools like nslookup, dig, and ping.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ dig google.com

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37363
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.          5       IN      A      142.250.199.46

;; Query time: 513 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Sep 26 12:06:17 +0530 2024
;; MSG SIZE  rcvd: 55

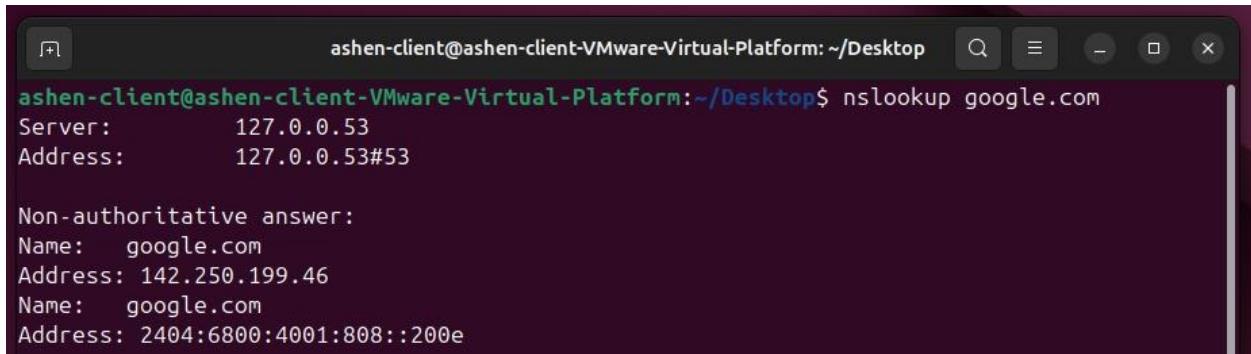
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

**ANSWER SECTION :** This shows the resolved IP address for the domain

**SERVER :** Indicates which DNS server was used for the query

- **nslookup**

- **Address :** This shows the resolved IP address for the domain
- **Server :** Indicates which DNS server was used for the query



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ nslookup google.com
Server:      127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name:  google.com
Address: 142.250.199.46
Name:  google.com
Address: 2404:6800:4001:808::200e
```

## NTP(Network Time Protocol) Installation and Configuration

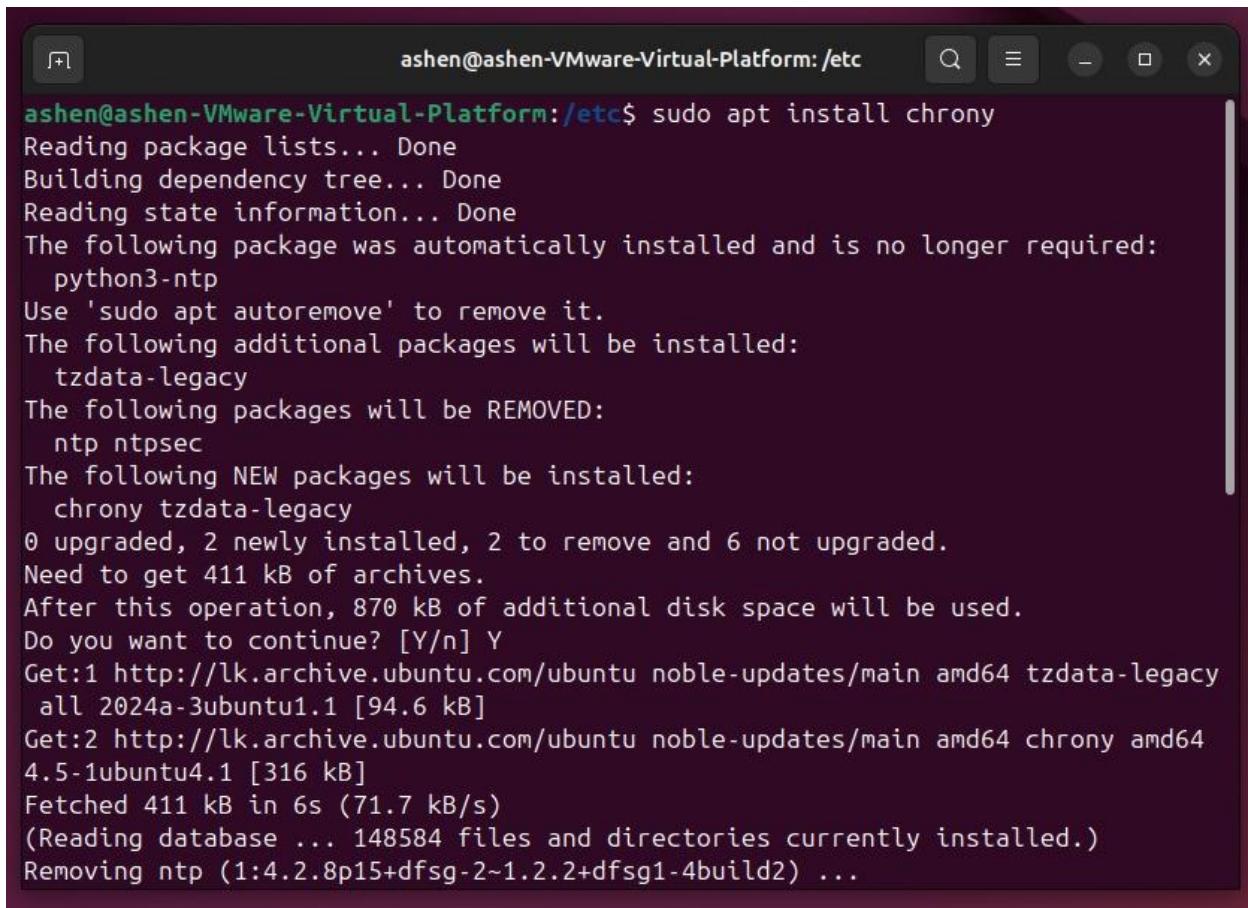
### ➤ NTP Server Configuration

1. update the package list

- sudo apt update

2. install chrony in the Server machine (chrony - Network Time Protocol (NTP) used to synchronize the system clock with NTP servers.)

- sudo apt install chrony



```
ashen@ashen-Virtual-Platform:/etc$ sudo apt install chrony
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-ntp
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  tzdata-legacy
The following packages will be REMOVED:
  ntp ntpsec
The following NEW packages will be installed:
  chrony tzdata-legacy
0 upgraded, 2 newly installed, 2 to remove and 6 not upgraded.
Need to get 411 kB of archives.
After this operation, 870 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 tzdata-legacy
  all 2024a-3ubuntu1.1 [94.6 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 chrony amd64
  4.5-1ubuntu4.1 [316 kB]
Fetched 411 kB in 6s (71.7 kB/s)
(Reading database ... 148584 files and directories currently installed.)
Removing ntp (1:4.2.8p15+dfsg-2~1.2.2+dfsg1-4build2) ...
```

3. Open and modify the configuration file using nano/vi text editor.

- sudo nano /etc/chrony/chrony.conf
- remove existing server entries by commenting out
- Add relevant external NTP servers
- Add the local network that is allows to use this server.(add the server ip address )

```
GNU nano 7.2                               /etc/chrony/chrony.conf *
# About using servers from the NTP Pool Project in general see (LP: #104525).
# Approved by Ubuntu Technical Board on 2011-02-08.
# See http://www.pool.ntp.org/join.html for more information.
#pool ntp.ubuntu.com          iburst maxsources 4
#pool 0.ubuntu.pool.ntp.org iburst maxsources 1
#pool 1.ubuntu.pool.ntp.org iburst maxsources 1
#pool 2.ubuntu.pool.ntp.org iburst maxsources 2

server 0.asia.pool.ntp.org
server 1.asia.pool.ntp.org
server 2.asia.pool.ntp.org
server 3.asia.pool.ntp.org

# Use time sources from DHCP.
sourcedir /run/chrony-dhcp

# Use NTP sources found in /etc/chrony/sources.d.
sourcedir /etc/chrony/sources.d

# This directive specify the location of the file containing ID/key pairs for
```

```
GNU nano 7.2                               /etc/chrony/chrony.conf
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0

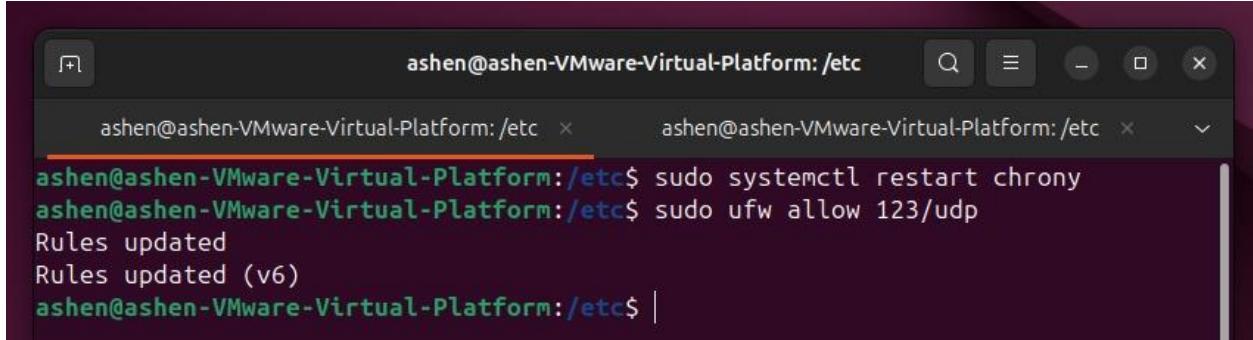
# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcfile' directive.
# rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
leapsectz right/UTC
allow 192.168.72.0/24
```

4. Restart the service to apply changes and allow NTP service through firewall (Allow incoming UDP traffic on port 123 which typically used by NTP, This is an essential step if you want your server to receive time synchronization requests from NTP clients.)

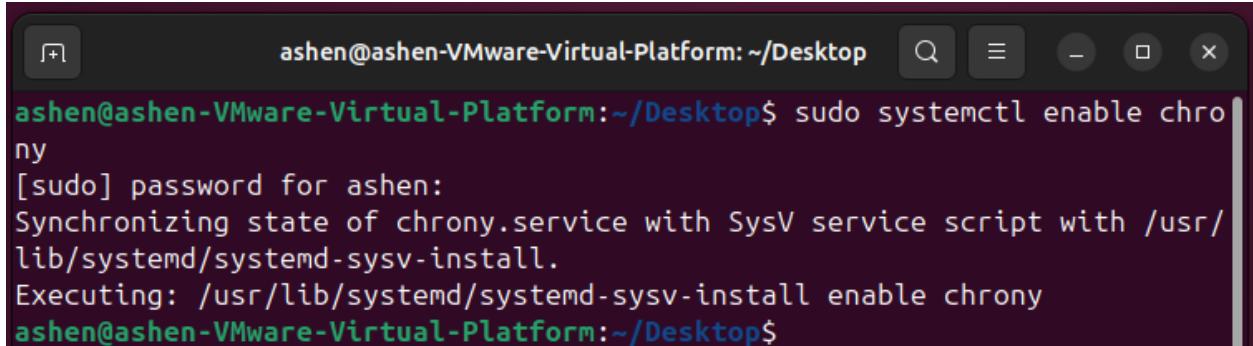
- sudo systemctl restart chrony



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart chrony
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo ufw allow 123/udp
Rules updated
Rules updated (v6)
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

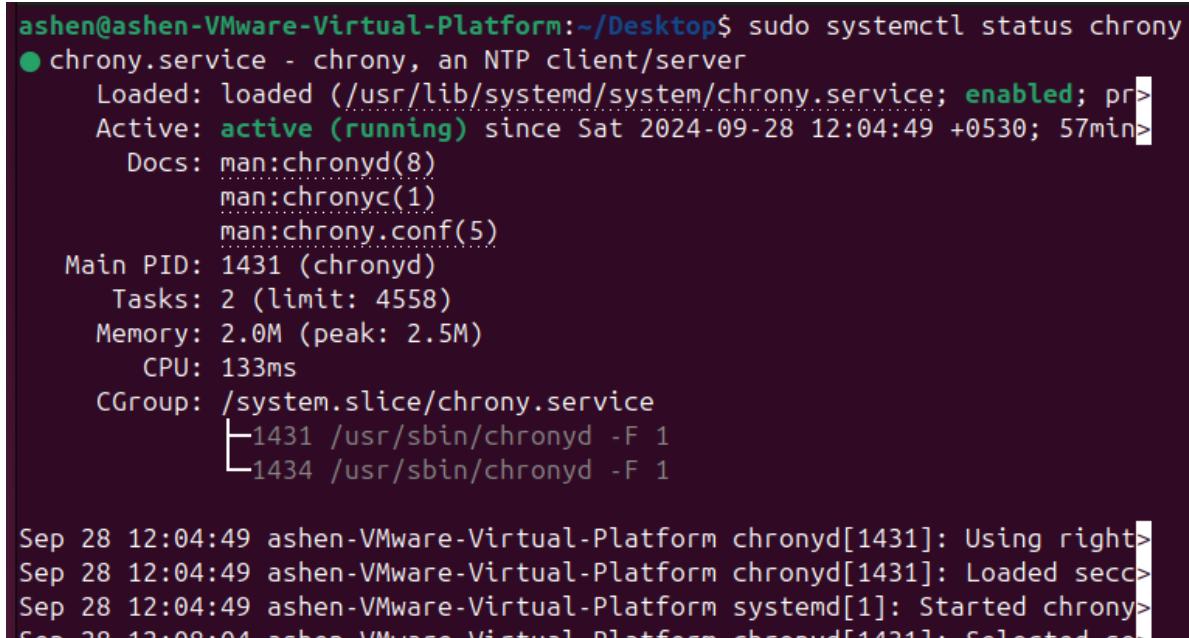
5. Enable chrony on boot time.

- sudo systemctl enable chrony



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable chrony
[sudo] password for asheng:
Synchronizing state of chrony.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable chrony
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

6. Check the status whether active or not



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl status chrony
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled; prior)
   Active: active (running) since Sat 2024-09-28 12:04:49 +0530; 57min ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
   Main PID: 1431 (chronyd)
      Tasks: 2 (limit: 4558)
     Memory: 2.0M (peak: 2.5M)
        CPU: 133ms
      CGroup: /system.slice/chrony.service
              └─1431 /usr/sbin/chronyd -F 1
                  ├─1434 /usr/sbin/chronyd -F 1

Sep 28 12:04:49 asheng-VMware-Virtual-Platform chronyd[1431]: Using right>
Sep 28 12:04:49 asheng-VMware-Virtual-Platform chronyd[1431]: Loaded secc>
Sep 28 12:04:49 asheng-VMware-Virtual-Platform systemd[1]: Started chrony>
Sep 28 12:04:49 asheng-VMware-Virtual-Platform chrony[1431]: Selected co|
```

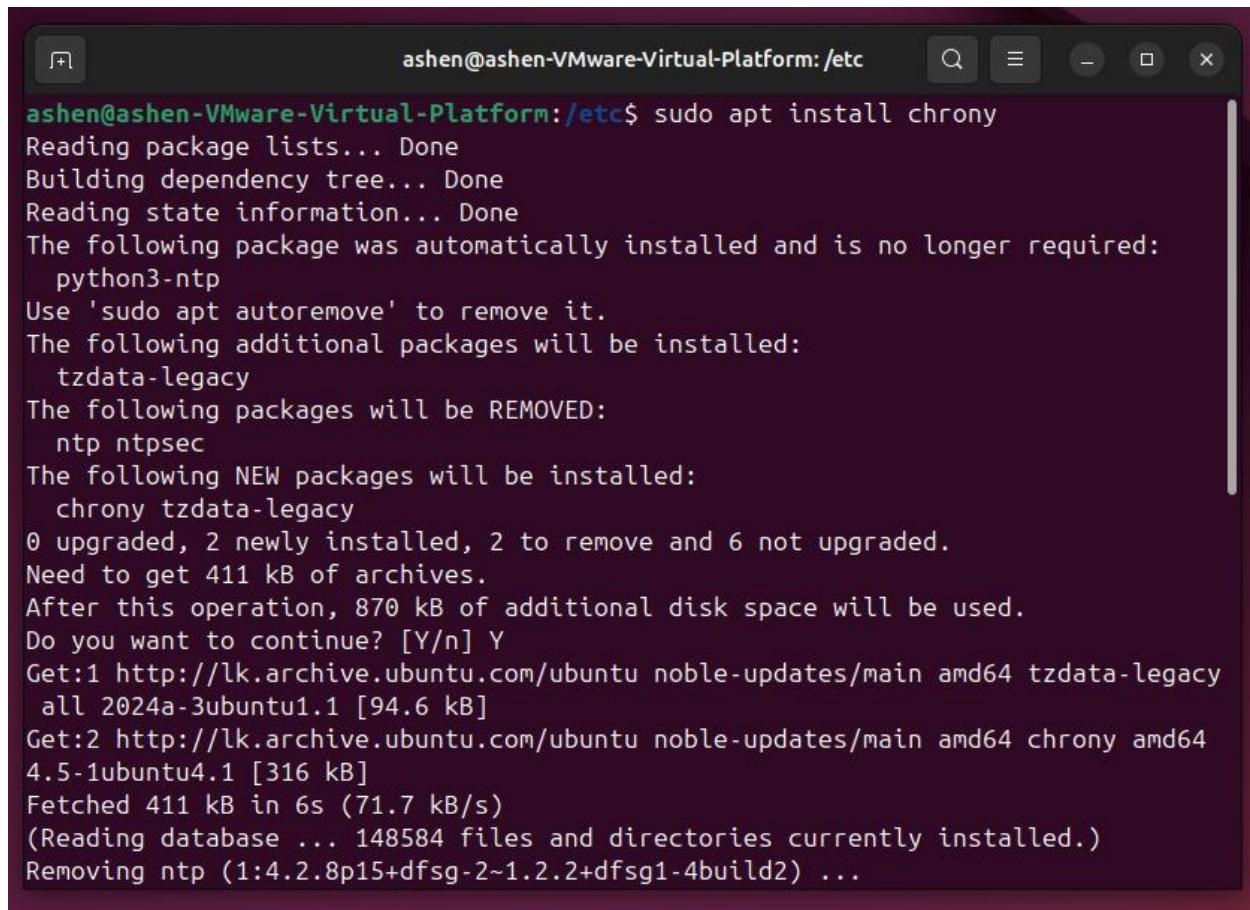
## ➤ NTP Client Configuration

1. update the package list

- sudo apt update

2. Install chrony in the Client machine

- sudo apt install chrony



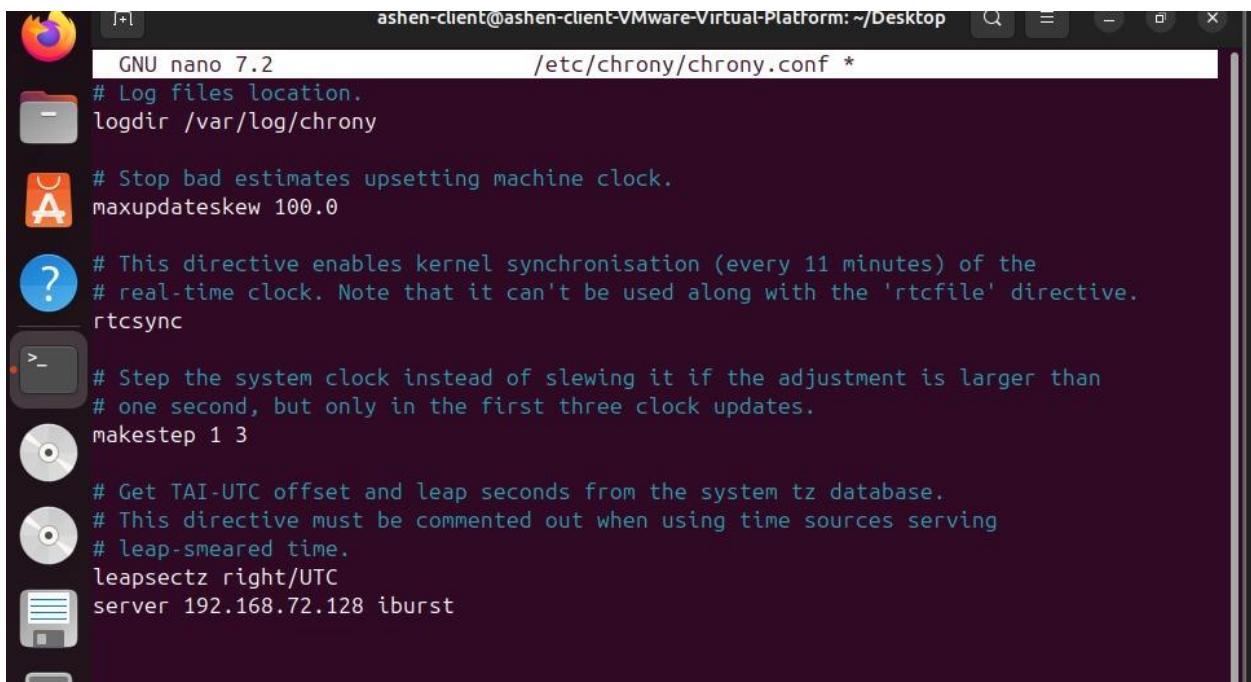
```
ashen@ashen-Virtual-Platform:/etc$ sudo apt install chrony
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-ntp
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  tzdata-legacy
The following packages will be REMOVED:
  ntp ntpsec
The following NEW packages will be installed:
  chrony tzdata-legacy
0 upgraded, 2 newly installed, 2 to remove and 6 not upgraded.
Need to get 411 kB of archives.
After this operation, 870 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 tzdata-legacy
  all 2024a-3ubuntu1.1 [94.6 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 chrony amd64
  4.5-1ubuntu4.1 [316 kB]
Fetched 411 kB in 6s (71.7 kB/s)
(Reading database ... 148584 files and directories currently installed.)
Removing ntp (1:4.2.8p15+dfsg-2~1.2.2+dfsg1-4build2) ...
```

3. Open and modify the configuration file using nano/vi text editor.

-sudo nano /etc/chrony/chrony.conf

-remove existing server entries by commenting out

-Add the IP address of your NTP server



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop
GNU nano 7.2
/etc/chrony/chrony.conf *
# Log files location.
logdir /var/log/chrony

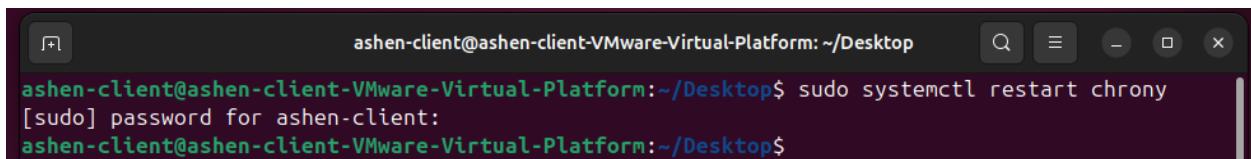
# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcffile' directive.
rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3

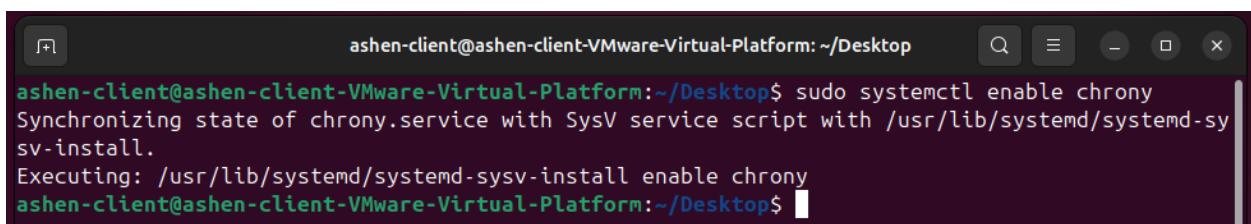
# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
leapsez right/UTC
server 192.168.72.128 iburst
```

4. Restart chrony service



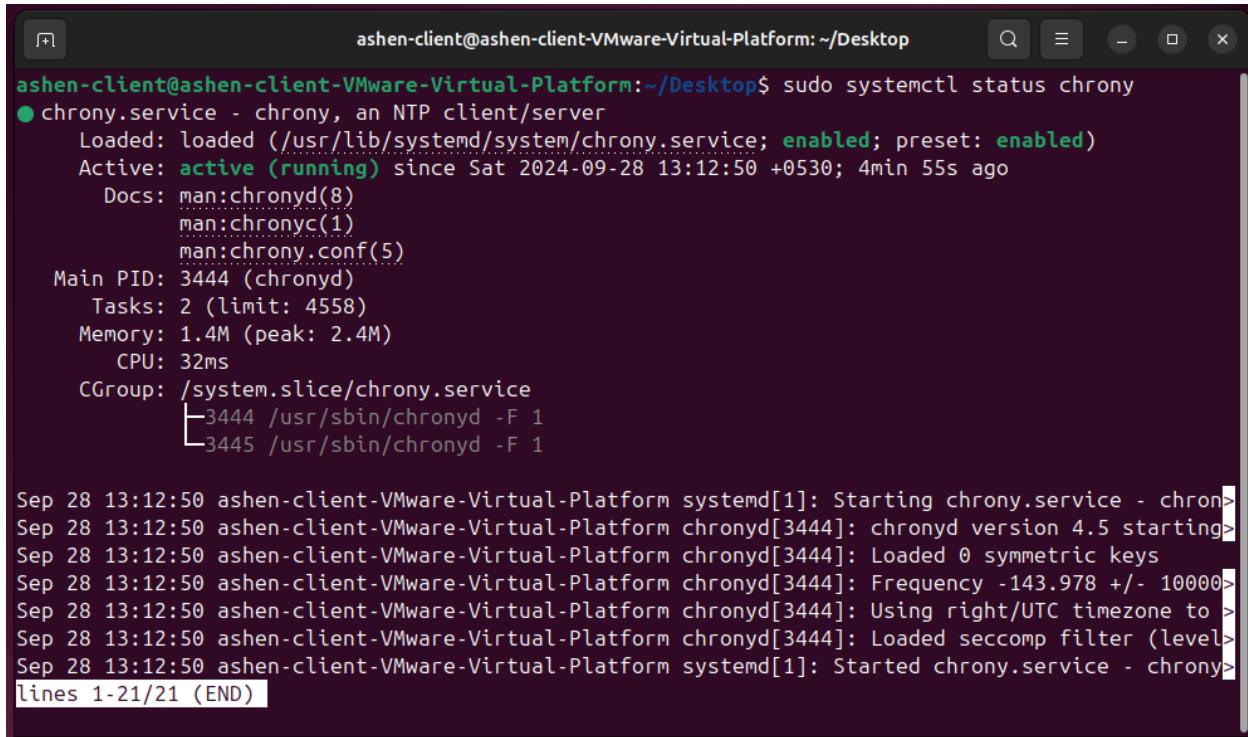
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart chrony
[sudo] password for ashen-client:
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

5. Enable chrony to start on boot



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable chrony
Synchronizing state of chrony.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable chrony
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## 6. check the status of the chrony client.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo systemctl status chrony
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-09-28 13:12:50 +0530; 4min 55s ago
     Docs: man:chrony(8)
           man:chronyc(1)
           man:chrony.conf(5)
   Main PID: 3444 (chronyd)
      Tasks: 2 (limit: 4558)
     Memory: 1.4M (peak: 2.4M)
        CPU: 32ms
      CGroup: /system.slice/chrony.service
              └─3444 /usr/sbin/chronyd -F 1
            ├─3445 /usr/sbin/chronyd -F 1

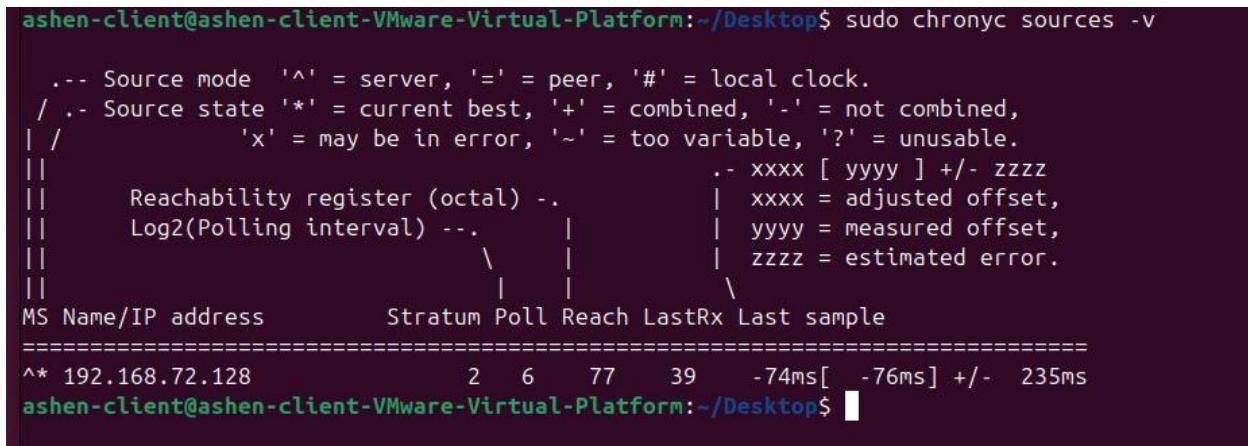
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform systemd[1]: Starting chrony.service - chrony...
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform chronyd[3444]: chronyd version 4.5 starting...
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform chronyd[3444]: Loaded 0 symmetric keys
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform chronyd[3444]: Frequency -143.978 +/- 10000
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform chronyd[3444]: Using right/UTC timezone to >
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform chronyd[3444]: Loaded seccomp filter (level=0)
Sep 28 13:12:50 ashen-client-VMware-Virtual-Platform systemd[1]: Started chrony.service - chrony...
lines 1-21/21 (END)
```

## Verification

### Client-Side verification

#### **sudo chronyc sources -v**

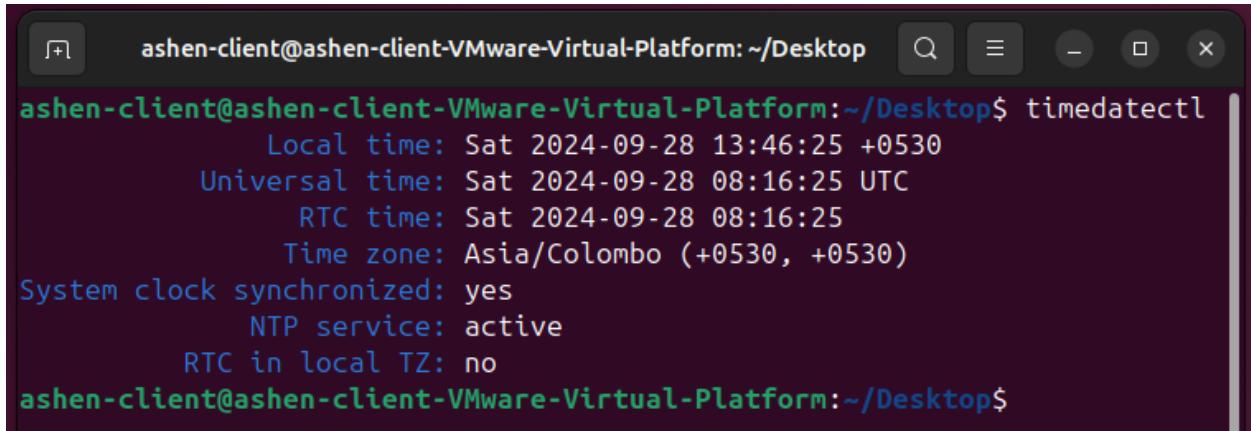
- Command is used to display detailed information about the NTP sources that the Chrony NTP client is using for synchronization.



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo chronyc sources -v
... Source mode '^' = server, '=' = peer, '#' = local clock.
/ .. Source state '*' = current best, '+' = combined, '-' = not combined,
| /          'x' = may be in error, '~' = too variable, '?' = unusable.
||          Reachability register (octal) ...
||          Log2(Polling interval) ...
||          \
||          MS Name/IP address       Stratum Poll  Reach LastRx Last sample
=====
^* 192.168.72.128             2      6    77    39    -74ms[-76ms] +/- 235ms
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## **timedatectl**

- Helps to verify the system's time is synchronized with the NTP server.

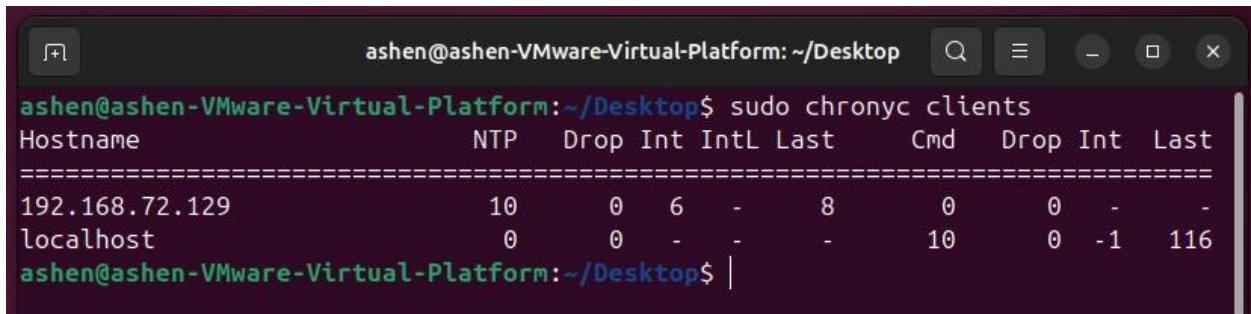


```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ timedatectl
    Local time: Sat 2024-09-28 13:46:25 +0530
    Universal time: Sat 2024-09-28 08:16:25 UTC
          RTC time: Sat 2024-09-28 08:16:25
        Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
      NTP service: active
    RTC in local TZ: no
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

## Server-Side verification

### **sudo chronyc clients**

- Command is used to display information about the clients that are currently connected to the chrony NTP server.

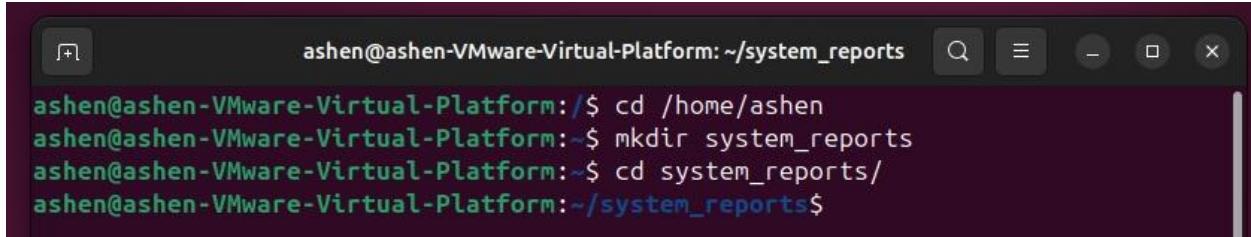


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo chronyc clients
      Hostname          NTP   Drop Int IntL Last      Cmd   Drop Int  Last
=====
192.168.72.129           10     0   6   -     8     0     0   -   -
localhost                 0     0   -   -     -     10     0   -1   116
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

## 4. Shell Scripting and Security

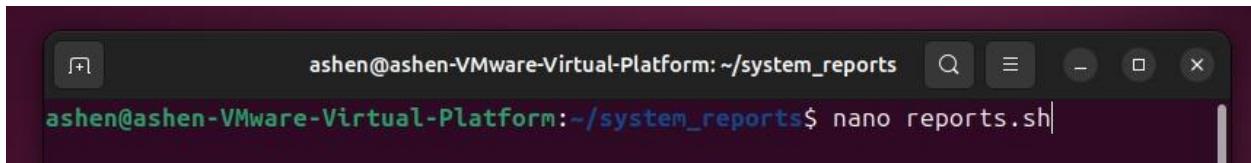
**Q1→ Write a script to automate a report that captures key system details every day.**

1. Create a new directory in the home directory.



```
ashen@ashen-VMware-Virtual-Platform:~/system_reports
ashen@ashen-VMware-Virtual-Platform:~$ cd /home/ashen
ashen@ashen-VMware-Virtual-Platform:~$ mkdir system_reports
ashen@ashen-VMware-Virtual-Platform:~$ cd system_reports/
ashen@ashen-VMware-Virtual-Platform:~/system_reports$
```

2. Create a new shell script in the home directory inside the directory created above.



```
ashen@ashen-VMware-Virtual-Platform:~/system_reports
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ nano reports.sh
```

3. Write the below shell script inside the report.sh file using the text editor.

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

# Set the directory for storing reports
REPORT_DIR="/home/ashen/system_reports"

# Ensure the directory exists, creating it if necessary
mkdir -p "$REPORT_DIR"

# Capture the current date and time
DATE=$(date "+%Y-%m-%d %H:%M:%S")

# Gather system stats like uptime, available memory, and disk usage
UPTIME=$(uptime -p) # Shows system running time
FREE_MEMORY=$(free -h | grep Mem | awk '{print $4}') # Available RAM in human-readable format
DISK_USAGE=$(df -h / | grep / | awk '{print $5}') # Root directory disk usage percentage

# Define the report file name with a timestamp
SYSTEM_REPORT="$REPORT_DIR/system_report_${DATE}.txt"

# Output system details to the report file
echo "System Report - $DATE" > "$SYSTEM_REPORT"
echo "-----" >> "$SYSTEM_REPORT"
echo "Date : $DATE" >> "$SYSTEM_REPORT"
echo "Uptime: $UPTIME" >> "$SYSTEM_REPORT"
echo "Free Memory: $FREE_MEMORY" >> "$SYSTEM_REPORT"
echo "Disk Usage: $DISK_USAGE" >> "$SYSTEM_REPORT"
echo "-----" >> "$SYSTEM_REPORT"

# Notify the user where the report was saved
echo "System report saved to: $SYSTEM_REPORT"
```

## **Script**

```
#!/bin/bash

# Set the directory for storing reports
REPORT_DIR="/home/ashen/system_reports"

# Ensure the directory exists, creating it if necessary
mkdir -p "$REPORT_DIR"

# Capture the current date and time
DATE=$(date "+%Y-%m-%d %H:%M:%S")

# Gather system stats like uptime, available memory, and disk usage
UPTIME=$(uptime -p) # Shows system running time
FREE_MEMORY=$(free -h | grep Mem | awk '{print $4}') # Available RAM in human-readable
format
DISK_USAGE=$(df -h / | grep / | awk '{print $5}') # Root directory disk usage percentage

# Define the report file name with a timestamp
SYSTEM_REPORT="$REPORT_DIR/system_report_$(date "+%Y-%m-
%d_%H:%M:%S").txt"

# Output system details to the report file
echo "System Report - $DATE" > "$SYSTEM_REPORT"
echo "-----" >> "$SYSTEM_REPORT"
echo "Date : $DATE" >> "$SYSTEM_REPORT"
echo "Uptime: $UPTIME" >> "$SYSTEM_REPORT"
echo "Free Memory: $FREE_MEMORY" >> "$SYSTEM_REPORT"
echo "Disk Usage: $DISK_USAGE" >> "$SYSTEM_REPORT"
echo "-----" >> "$SYSTEM_REPORT"

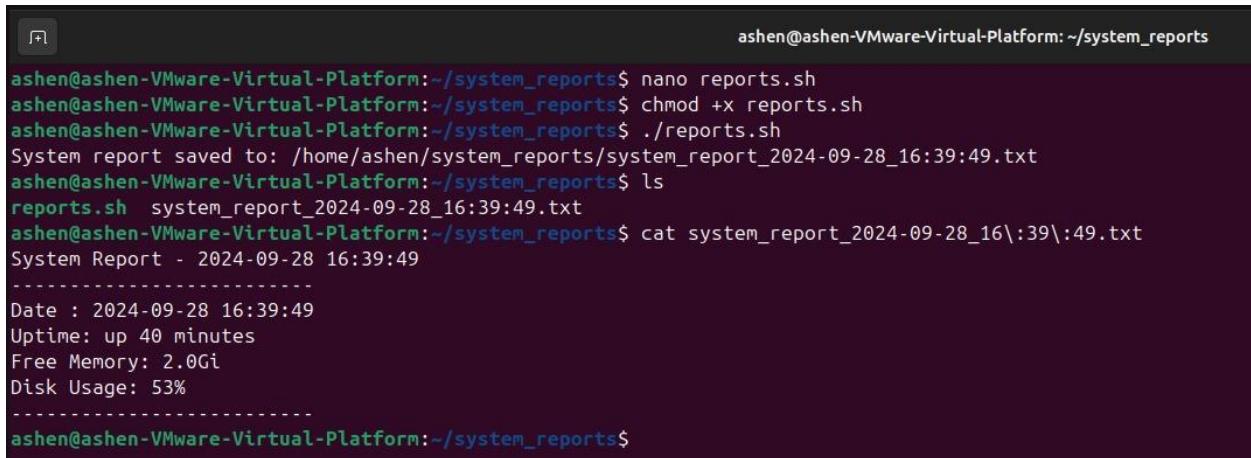
# Notify the user where the report was saved
echo "System report saved to: $SYSTEM_REPORT"
```

4. Change the permissions of the script file to make it executable.

- chmod +x report.sh

5. Execute the script.

- ./report.sh

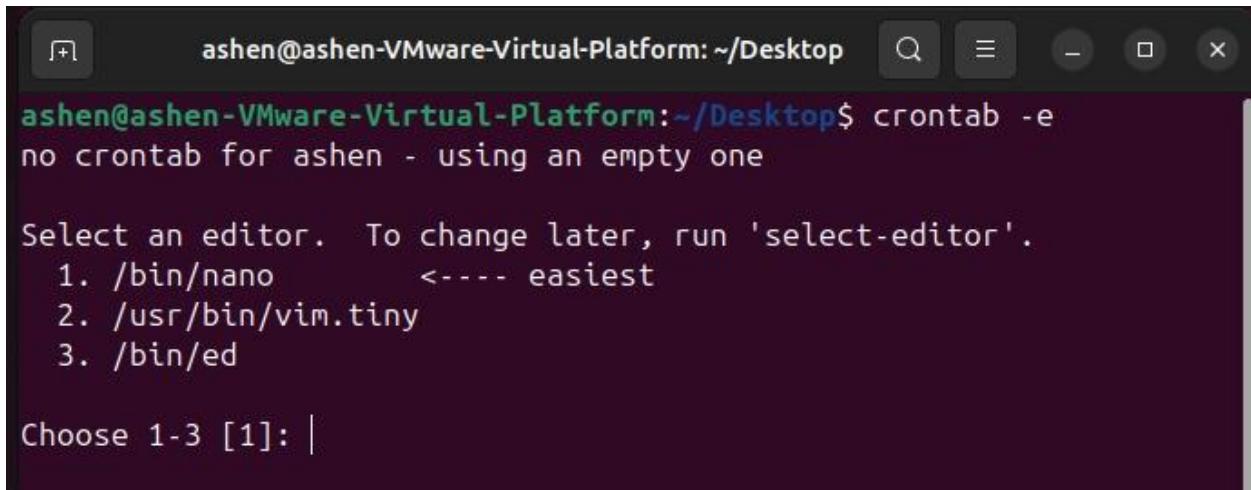


```
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ nano reports.sh
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ chmod +x reports.sh
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ ./reports.sh
System report saved to: /home/ashen/system_reports/system_report_2024-09-28_16:39:49.txt
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ ls
reports.sh  system_report_2024-09-28_16:39:49.txt
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ cat system_report_2024-09-28_16\:39\:49.txt
System Report - 2024-09-28 16:39:49
-----
Date : 2024-09-28 16:39:49
Uptime: up 40 minutes
Free Memory: 2.0Gi
Disk Usage: 53%
-----
ashen@ashen-VMware-Virtual-Platform:~/system_reports$
```

If a system report is created, it means that the script works.

6. Schedule the script to run automatically using cron.

- crontab -e
- select the preferred text editor (select 1)



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ crontab -e
no crontab for ashen - 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]: |
```

7. Add the below command to run the script everyday at 8 AM

- 0 8 \* \* \* /home/ashen/report.sh

The screenshot shows a terminal window titled "ashen@ashen-Virtual-Platform: ~/Desktop". The window contains the crontab file with the following content:

```
GNU nano 7.2          /tmp/crontab.wqvEb7/crontab *
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 8 * * * /home/ashen/report.sh
```

The bottom of the terminal shows the nano key bindings:

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

8. Save and Exit .

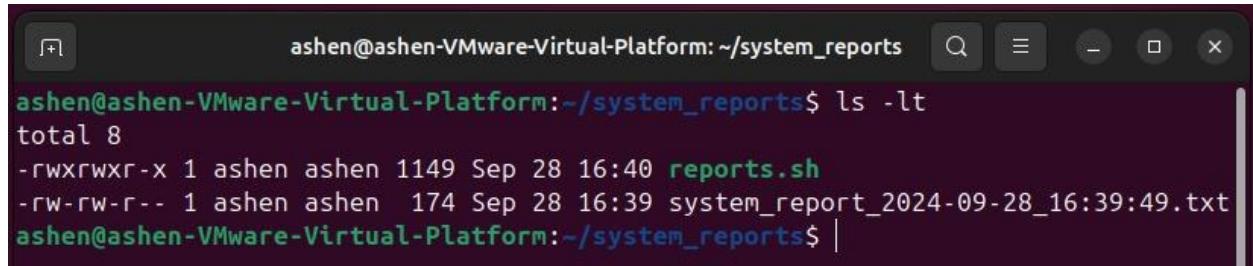
9. Check the status of the cron service.

The screenshot shows a terminal window titled "ashen@ashen-Virtual-Platform: ~/Desktop\$". The command "systemctl status cron" is run, and the output is as follows:

```
ashen@ashen-Virtual-Platform:~/Desktop$ systemctl status cron
● cron.service - Regular background program processing daemon
  Loaded: loaded (/usr/lib/systemd/system/cron.service; enabled; preset: enabled)
  Active: active (running) since Sat 2024-09-28 15:59:48 +0530; 47min ago
    Docs: man:cron(8)
   Main PID: 1037 (cron)
      Tasks: 1 (limit: 4558)
     Memory: 472.0K (peak: 2.1M)
        CPU: 66ms
       CGroup: /system.slice/cron.service
               └─1037 /usr/sbin/cron -f -P

Sep 28 16:25:01 ashen-Virtual-Platform CRON[3711]: pam_unix(cron:session>
Sep 28 16:30:01 ashen-Virtual-Platform CRON[3739]: pam_unix(cron:session>
Sep 28 16:30:01 ashen-Virtual-Platform CRON[3740]: (root) CMD ([ -x /etc>
Sep 28 16:30:01 ashen-Virtual-Platform CRON[3739]: pam_unix(cron:session>
Sep 28 16:35:01 ashen-Virtual-Platform CRON[3798]: pam_unix(cron:session>
Sep 28 16:35:01 ashen-Virtual-Platform CRON[3799]: (root) CMD (command ->
Sep 28 16:35:01 ashen-Virtual-Platform CRON[3798]: pam_unix(cron:session>
```

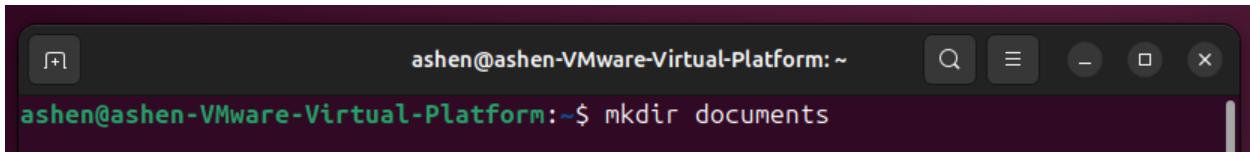
10. Verify the Generated Reports Files.
11. If our script creates report files in /home/ashen/system\_reports, can check the directory to see if new files are being generated every day at 8:00 AM.



```
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ ls -lt
total 8
-rwxrwxr-x 1 ashen ashen 1149 Sep 28 16:40 reports.sh
-rw-rw-r-- 1 ashen ashen   174 Sep 28 16:39 system_report_2024-09-28_16:39:49.txt
ashen@ashen-VMware-Virtual-Platform:~/system_reports$ |
```

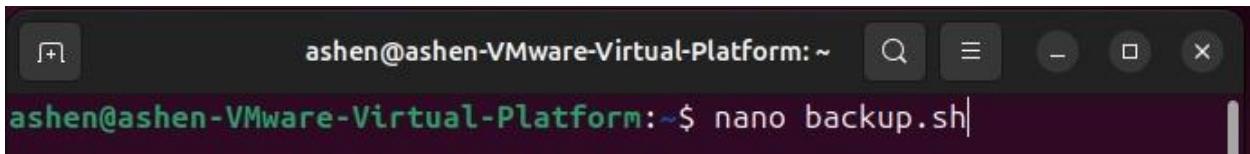
**Q2→ Write a script to automate the backup of a critical directory containing important files.**

1. Create a new Directory which needs to be backup.



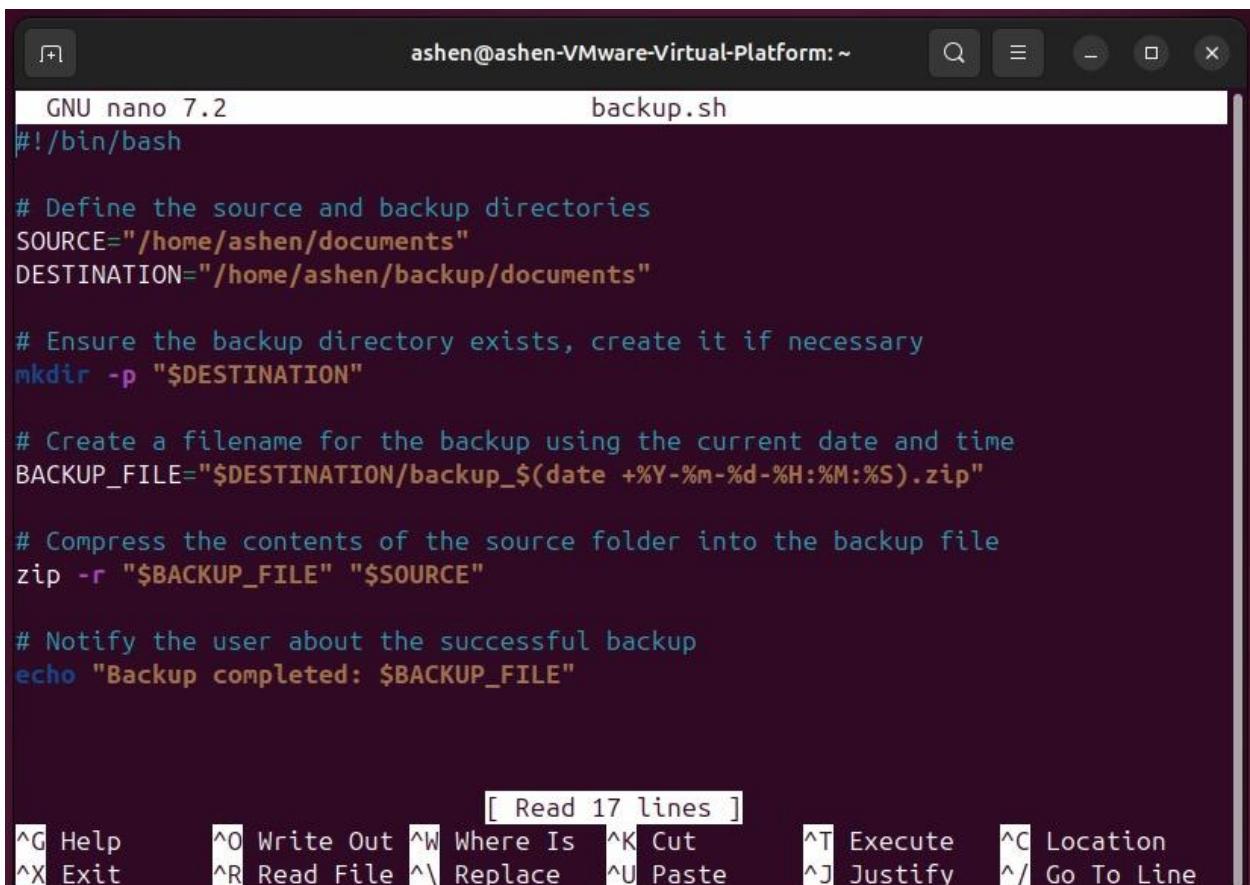
```
ashen@ashen-VMware-Virtual-Platform:~$ mkdir documents
```

2. Create a new script file .



```
ashen@ashen-VMware-Virtual-Platform:~$ nano backup.sh
```

3. Write the below shell script inside the opened script file.



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

# Define the source and backup directories
SOURCE="/home/ashen/documents"
DESTINATION="/home/ashen/backup/documents"

# Ensure the backup directory exists, create it if necessary
mkdir -p "$DESTINATION"

# Create a filename for the backup using the current date and time
BACKUP_FILE="$DESTINATION/backup_$(date +%Y-%m-%d-%H:%M:%S).zip"

# Compress the contents of the source folder into the backup file
zip -r "$BACKUP_FILE" "$SOURCE"

# Notify the user about the successful backup
echo "Backup completed: $BACKUP_FILE"

[ Read 17 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify   ^/ Go To Line
```

## Script

```
#!/bin/bash

# Define the source and backup directories
SOURCE="/home/ashen/documents"
DESTINATION="/home/ashen/backup/documents"

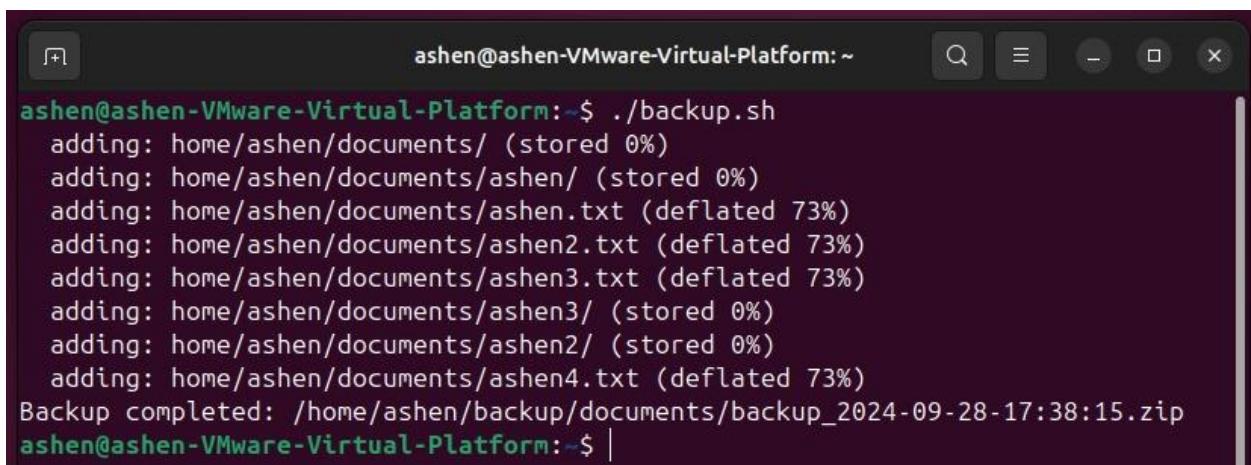
# Ensure the backup directory exists, create it if necessary
mkdir -p "$DESTINATION"

# Create a filename for the backup using the current date and time
BACKUP_FILE="$DESTINATION/backup_$(date +\%Y-\%m-\%d-\%H:\%M:\%S).zip"

# Compress the contents of the source folder into the backup file
zip -r "$BACKUP_FILE" "$SOURCE"

# Notify the user about the successful backup
echo "Backup completed: $BACKUP_FILE"
```

4. Execute the script to check that it works.



The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "ashen@ashen-VMware-Virtual-Platform: ~". The command entered is ". ./backup.sh". The terminal then displays the output of the zip command, showing the compression of various files and folders from the source directory into the backup file. The final line of output is "Backup completed: /home/ashen/backup/documents/backup\_2024-09-28-17:38:15.zip".

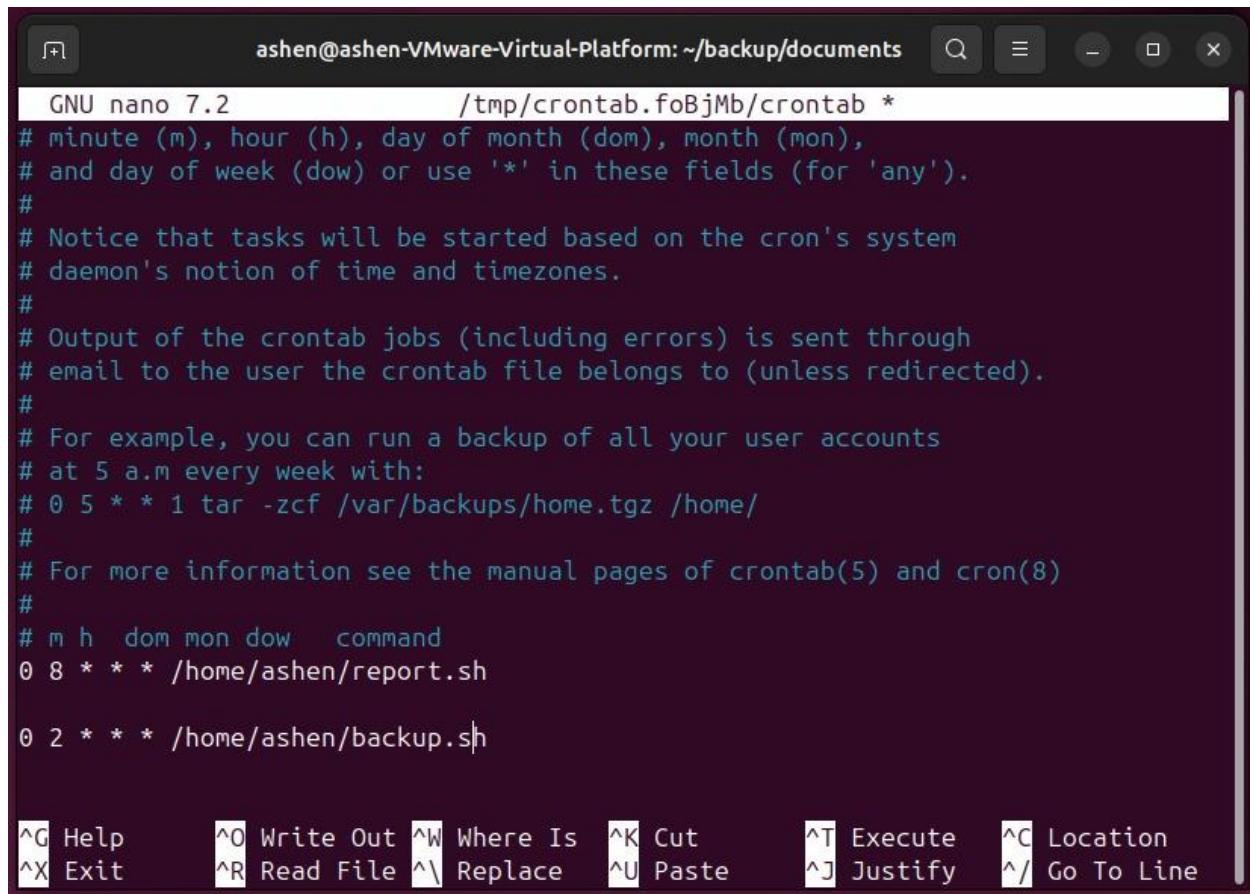
```
ashen@ashen-VMware-Virtual-Platform:~$ ./backup.sh
adding: home/ashen/documents/ (stored 0%)
adding: home/ashen/documents/ashen/ (stored 0%)
adding: home/ashen/documents/ashen.txt (deflated 73%)
adding: home/ashen/documents/ashen2.txt (deflated 73%)
adding: home/ashen/documents/ashen3.txt (deflated 73%)
adding: home/ashen/documents/ashen3/ (stored 0%)
adding: home/ashen/documents/ashen2/ (stored 0%)
adding: home/ashen/documents/ashen4.txt (deflated 73%)
Backup completed: /home/ashen/backup/documents/backup_2024-09-28-17:38:15.zip
ashen@ashen-VMware-Virtual-Platform:~$ |
```

5. Verify that a new backup file with current date and time had been created in the given directory.

```
ashen@ashen-VMware-Virtual-Platform:~$ cd backup/documents/
ashen@ashen-VMware-Virtual-Platform:~/backup/documents$ ls
backup_2024-09-28-17:34:56.zip  backup_2024-09-28-17:38:15.zip
ashen@ashen-VMware-Virtual-Platform:~/backup/documents$ |
```

6. Schedule the script to run automatically using cron.

- Open the configuration file
  - crontab -e
  - add the below line to schedule the backup script to run daily at 2.00 am.
    - 0 2 \* \* \* /home/ashen/backup.sh



The screenshot shows a terminal window with the title "ashen@ashen-VMware-Virtual-Platform: ~/backup/documents". The window contains the crontab configuration file. The file starts with a header explaining the syntax of cron jobs. It includes a comment about tasks being based on the system's notion of time and timezones. A section for a weekly backup job is shown, followed by a comment about more information in the manual pages. Finally, two specific cron entries are listed: one for a daily report at 08:00 and another for a daily backup at 02:00. The bottom of the window shows the nano editor's command bar with various keyboard shortcuts.

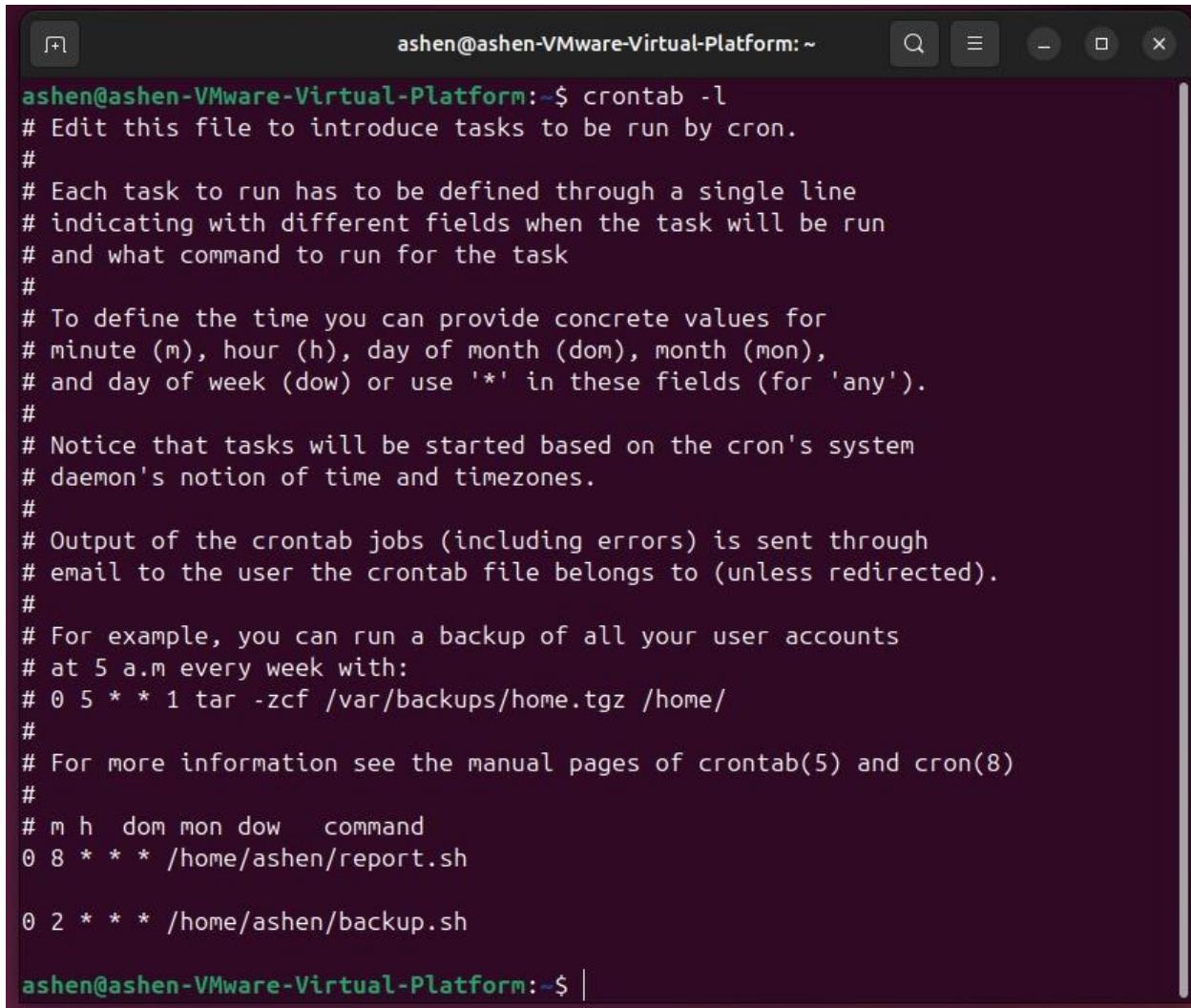
```
GNU nano 7.2          /tmp/crontab.foBjMb/crontab *
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 8 * * * /home/ashen/report.sh

0 2 * * * /home/ashen/backup.sh
```

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

Save and exit.

7. To ensure the cron job is set up correctly, list the cron jobs for the current user. The output should display the scheduled command.



```
ashen@ashen-VMware-Virtual-Platform:~$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 8 * * * /home/ashen/report.sh

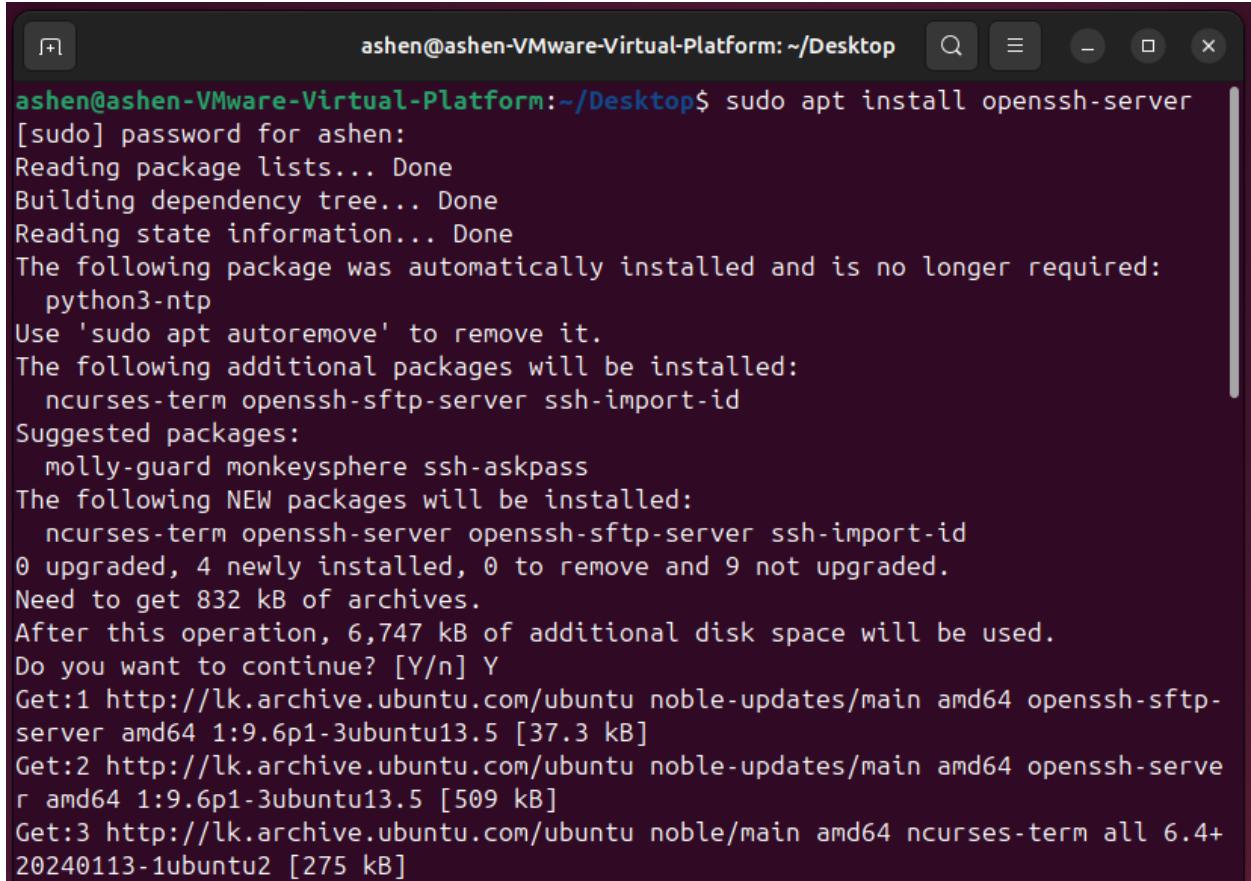
0 2 * * * /home/ashen/backup.sh

ashen@ashen-VMware-Virtual-Platform:~$ |
```

After all, above configurations the script will run automatically everyday 2.00am and generate a backup zip file in /home/user/backup/documents.

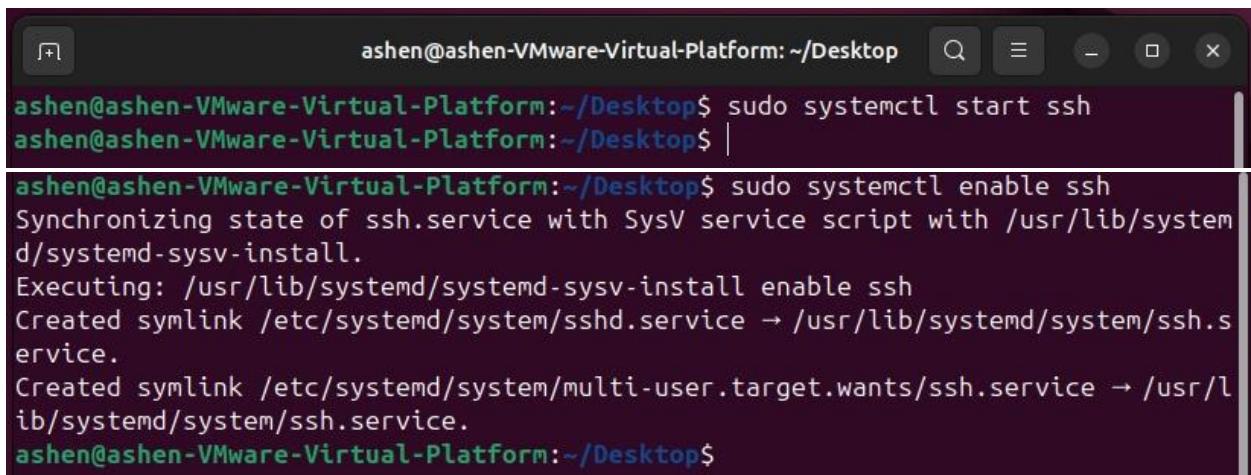
## SSH (Secure Shell)

1. Install the OpenSSH Server.



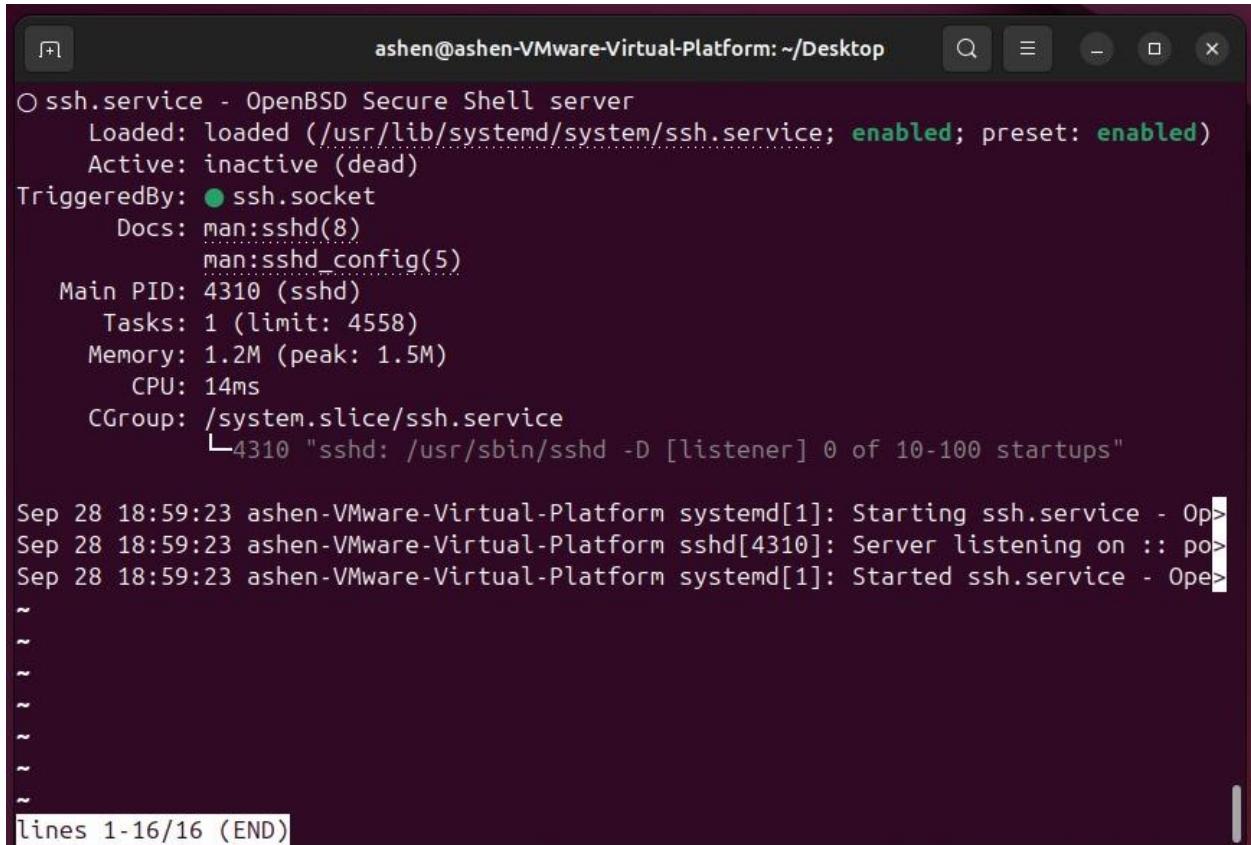
```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo apt install openssh-server
[sudo] password for ashén:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-ntp
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 9 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,747 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.5 [37.3 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.5 [509 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
```

2. Start and enable the ssh service.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl start ssh
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

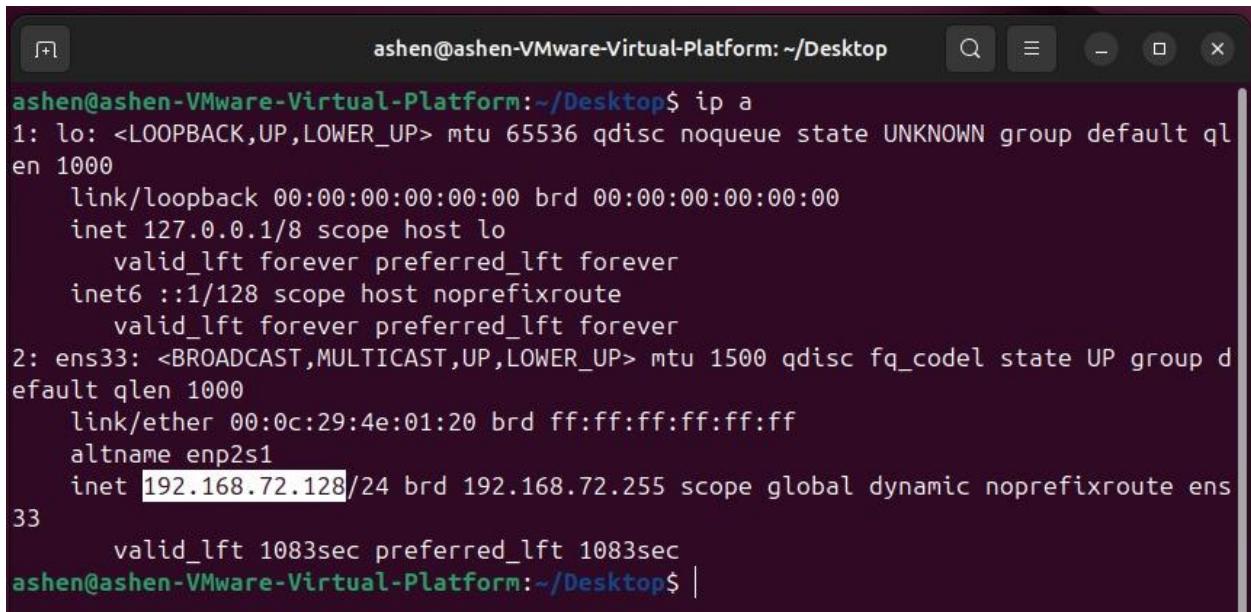
3. Verify the SSH Server is Running.



```
ashen@ashen-VMware-Virtual-Platform: ~/Desktop
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: inactive (dead)
     TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
          man:sshd_config(5)
     Main PID: 4310 (sshd)
        Tasks: 1 (limit: 4558)
       Memory: 1.2M (peak: 1.5M)
          CPU: 14ms
        CGroup: /system.slice/ssh.service
                  └─4310 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 28 18:59:23 ashen-VMware-Virtual-Platform systemd[1]: Starting ssh.service - Op>
Sep 28 18:59:23 ashen-VMware-Virtual-Platform sshd[4310]: Server listening on :: po>
Sep 28 18:59:23 ashen-VMware-Virtual-Platform systemd[1]: Started ssh.service - Ope>
~
~
~
~
~
~
~
~
lines 1-16/16 (END)
```

4. Check and note down the IP address of the ubuntu server.



```
ashen@ashen-VMware-Virtual-Platform: ~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4e:01:20 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.72.128/24 brd 192.168.72.255 scope global dynamic noprefixroute ens33
        valid_lft 1083sec preferred_lft 1083sec
ashen@ashen-VMware-Virtual-Platform: ~/Desktop$ |
```

5. Establish an SSH Connection.

- To connect to the remote server, use the ssh command. Be sure to substitute username with the actual user account name on the server and server-ip with the server's IP address.
- **ssh username@server-ip**
- **Confirm the Connection:** If you're connecting for the first time, you'll see a prompt asking you to verify the server's fingerprint. Type yes to proceed.
- **Input Credentials:** After confirming, you'll be asked to provide the password for the specified user account on the server. Enter the password to successfully log in.

The screenshot shows a terminal window titled "ashen@ashen-VMware-Virtua". The session starts with a Microsoft Windows login screen. Then, the user runs the command "ssh ashen@192.168.72.128". The terminal displays the authenticity of the host being established, showing a SHA256 key fingerprint. The user types "yes" to continue. A warning message indicates the host is added to the list of known hosts. The user then enters their password. Finally, they are logged into an Ubuntu 24.04.1 LTS system with version 6.8.0-45-generic x86\_64. The terminal shows standard Ubuntu welcome messages, including documentation links and update information. The session ends with the user's name and the virtual platform name.

```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>ssh ashen@192.168.72.128
The authenticity of host '192.168.72.128 (192.168.72.128)' can't be established.
ED25519 key fingerprint is SHA256:X+6nv4Ewvv5huw0RNA3HXezNB1RWo+GCDFd6+jww708.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.72.128' (ED25519) to the list of known hosts.
ashen@192.168.72.128's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

2 updates can be applied immediately.
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

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

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

ashen@ashen-VMware-Virtual-Platform:~$ |
```

## 4. iptables and ACLs

- i. **Web Server Security:** Allow incoming traffic only on port 80 (HTTP) and port 443 (HTTPS) for your web server. Block all other incoming traffic by default.

Step 01

Check any existing iptables rules.

- sudo iptables -L -n -v
- (Optional) Flush existing iptables rules
  - sudo iptables -F

```
root@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# 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 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# |
```

Step 02

Block all incoming traffic by default and allow all outgoing traffic.

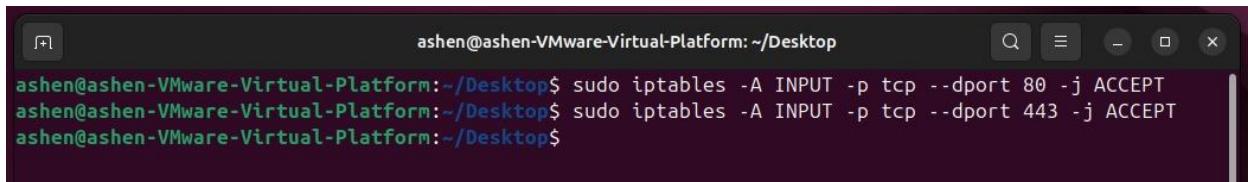
- sudo iptables -P INPUT DROP
- sudo iptables -P FORWARD DROP
- sudo iptables -P OUTPUT ACCEPT

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -P INPUT DROP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -P FORWARD DROP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -P OUTPUT ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

### Step 03

Allow incoming traffic only on ports 80 (HTTP) and 443 (HTTPS).

- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

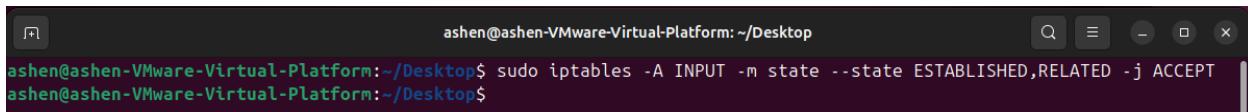


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

### Step 04

Allow established and related Connections.

- sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

### Step 05

Save the rules.

- To save the rules first you need super user privileges.
  - sudo su
- Save the rules.
  - sudo iptables-save > /etc/iptables/rules.v4

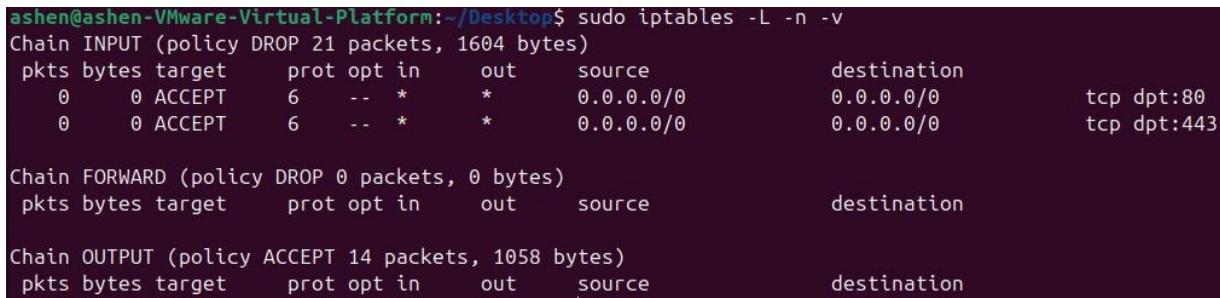


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# sudo iptables-save > /etc/iptables/rules.v4
```

### Step 06

Verify the iptables configurations

- sudo iptables -L -n -v



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -L -n -v
Chain INPUT (policy DROP 21 packets, 1604 bytes)
pkts bytes target     prot opt in     out     source               destination
  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

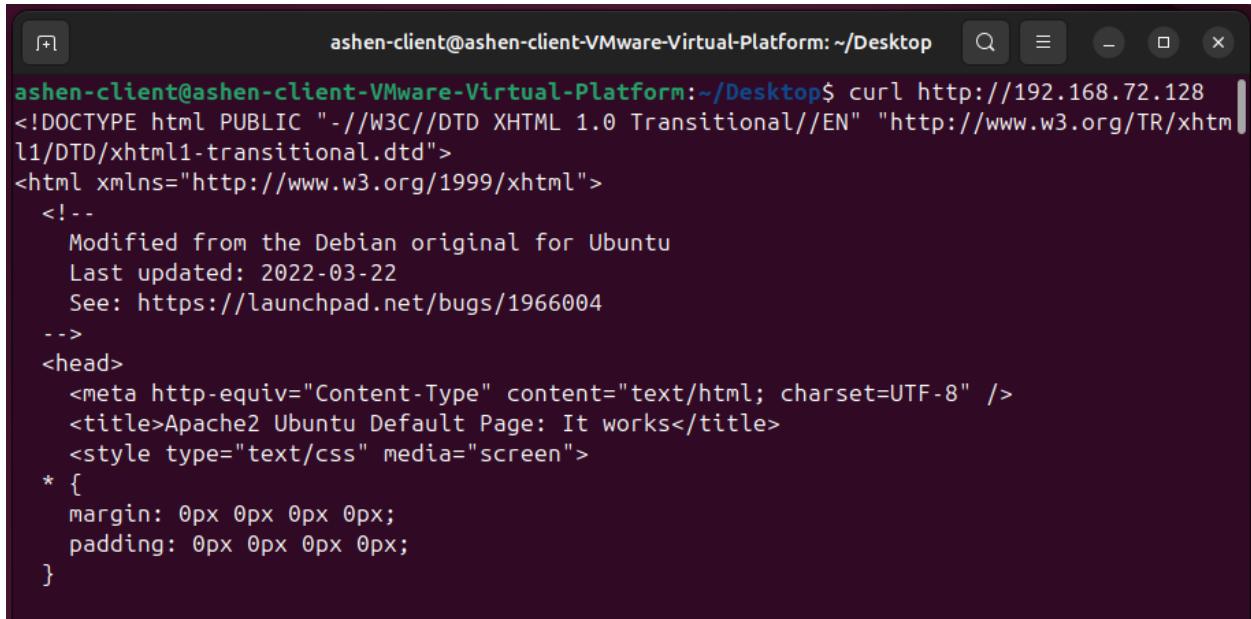
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 14 packets, 1058 bytes)
pkts bytes target     prot opt in     out     source               destination
```

## Step 07

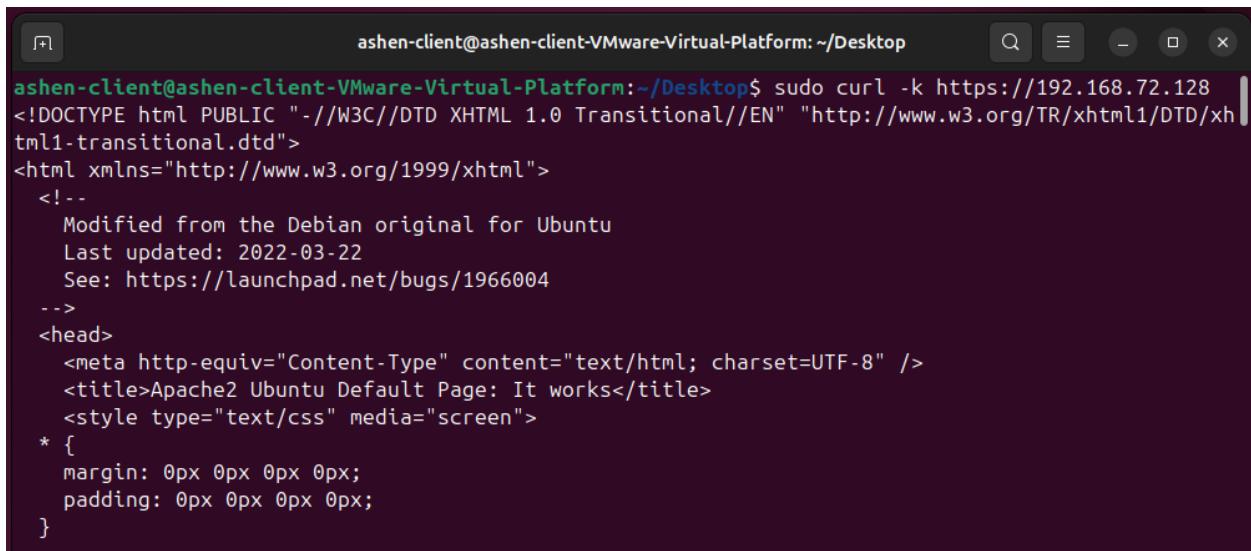
Test the configurations (allowed ports).

- Test HTTP .
  - curl http://192.168.72.128



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ curl http://192.168.72.128
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }
    </style>
  </head>
  <body>
    <h1>It works</h1>
    <p>This is the default web page for this server.<br/>
    The page you requested may have been removed,<br/>
    had its name changed, or is暂无此页.<br/>
    If you followed a link here, please check back later.</p>
  </body>
</html>
```

- Test HTTPS
  - sudo curl -k https://192.168.72.128
  - curl -k :- ignores SSL certificate validation

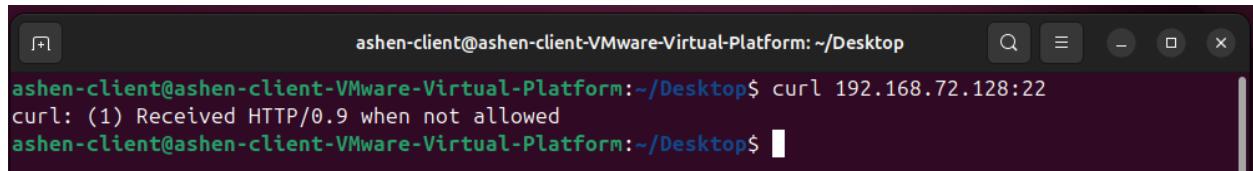


```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ sudo curl -k https://192.168.72.128
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }
    </style>
  </head>
  <body>
    <h1>It works</h1>
    <p>This is the default web page for this server.<br/>
    The page you requested may have been removed,<br/>
    had its name changed, or is暂无此页.<br/>
    If you followed a link here, please check back later.</p>
  </body>
</html>
```

As above we could get the html content of the server if the configuration is success.

Test the configurations (blocked ports).

- Test port 22
  - curl 192.168.72.128:22



A screenshot of a terminal window titled "ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop". The window shows the command "curl 192.168.72.128:22" being run. The output is: "curl: (1) Received HTTP/0.9 when not allowed". The terminal has a dark background with light-colored text.

```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ curl 192.168.72.128:22
curl: (1) Received HTTP/0.9 when not allowed
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

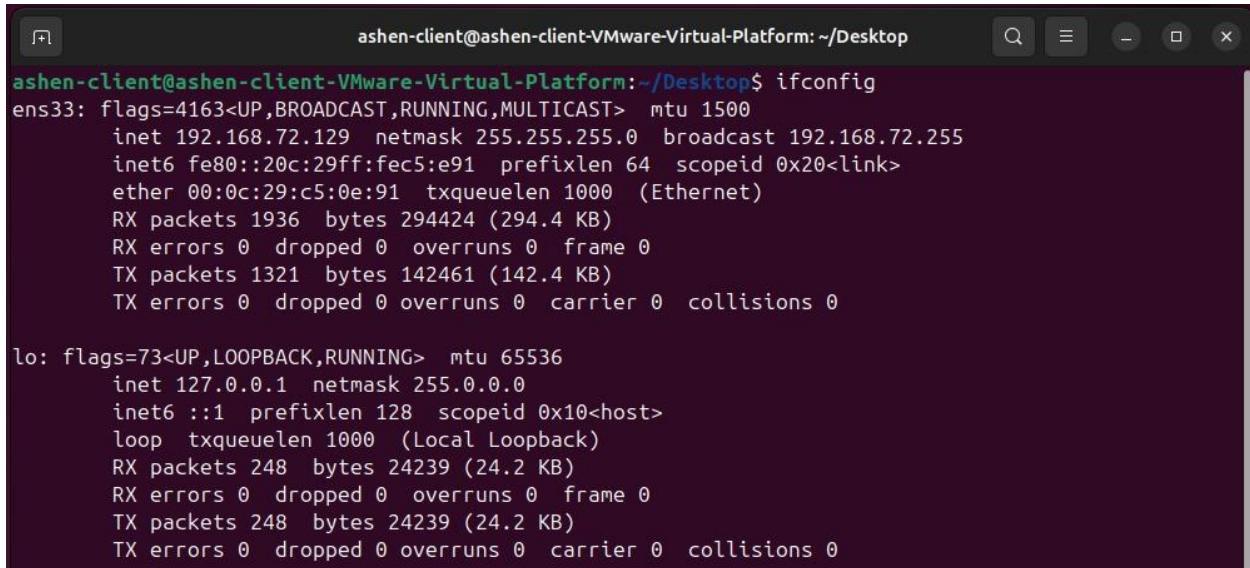
You should receive an error message as above if the ports are blocked.

- ii. **Remote Administration Access: Allow SSH access (port 22) only from specific IP addresses of your trusted machines used for administration. This restricts remote access attempts to authorized source.**

### Step 01

Identify the trusted IP addresses.

- I have chosen my ubuntu client VM.



A terminal window titled "ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop". The command "ifconfig" is run, displaying network interface information. The output shows two interfaces: ens33 (Ethernet) and lo (Loopback). The ens33 interface has an IP of 192.168.72.129 and a broadcast address of 192.168.72.255. The lo interface has an IP of 127.0.0.1.

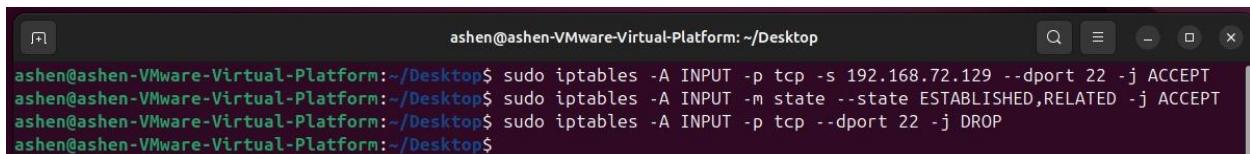
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.72.129 netmask 255.255.255.0 broadcast 192.168.72.255
              inet6 fe80::20c:29ff:fe5:e91 prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:c5:0e:91 txqueuelen 1000 (Ethernet)
                  RX packets 1936 bytes 294424 (294.4 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 1321 bytes 142461 (142.4 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 248 bytes 24239 (24.2 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 248 bytes 24239 (24.2 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Step 02

Allow SSH from Trusted IPs and drop all other incoming SSH connections.

- sudo iptables -A INPUT -p tcp -s 192.168.72.129 --dport 22 -j ACCEPT
- sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 22 -j DROP

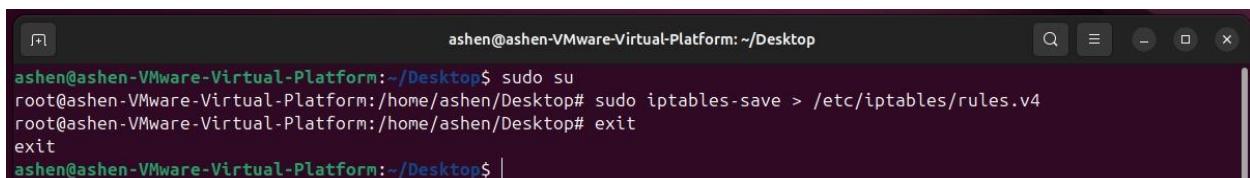


A terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The user runs three commands to set up the iptables rules: accepting traffic from 192.168.72.129 on port 22, accepting established and related connections, and dropping all other incoming SSH traffic.

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp -s 192.168.72.129 --dport 22 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

### Step 03

Save the rules.



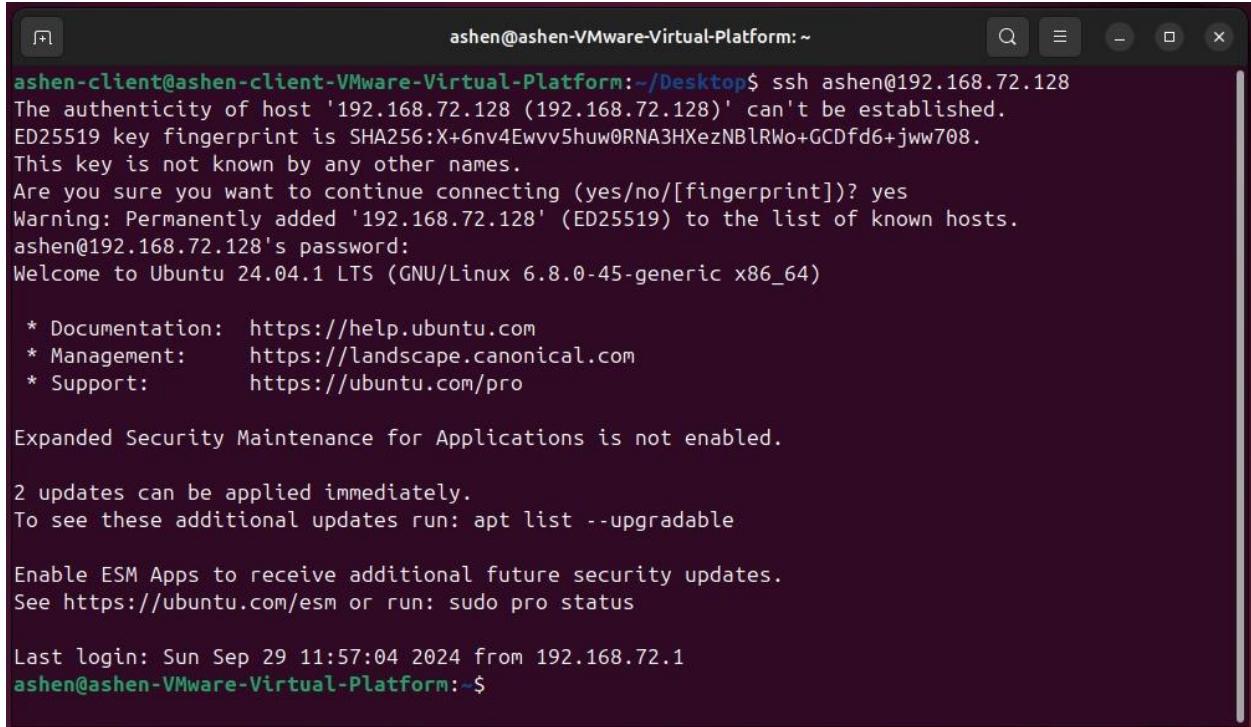
A terminal window titled "ashen@ashen-VMware-Virtual-Platform: ~/Desktop". The user runs "sudo su" to become root, then runs "sudo iptables-save > /etc/iptables/rules.v4" to save the current iptables rules to a file. Finally, they exit the root shell.

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# sudo iptables-save > /etc/iptables/rules.v4
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# exit
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

## Step 04

Testing the SSH access.

(From the allowed IP)



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ssh asheng@192.168.72.128
The authenticity of host '192.168.72.128 (192.168.72.128)' can't be established.
ED25519 key fingerprint is SHA256:X+6nv4Ewvv5huw0RNA3HXezNB1RWo+GCDfd6+jww708.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.72.128' (ED25519) to the list of known hosts.
ashen@192.168.72.128's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

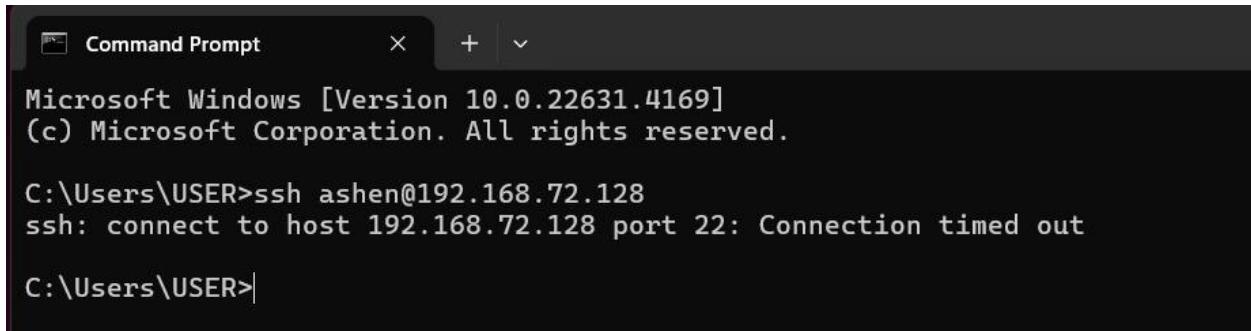
2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Last login: Sun Sep 29 11:57:04 2024 from 192.168.72.1
ashen@ashen-VMware-Virtual-Platform:~$
```

(From a blocked IP)

You should get a error message as below.



```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>ssh asheng@192.168.72.128
ssh: connect to host 192.168.72.128 port 22: Connection timed out

C:\Users\USER>
```

- iii. Allow Specific Applications: If you know the port numbers used by specific applications you want to allow (like a video conferencing app using port 443), you can create an ACL rule to permit traffic only for those ports**

#### Step 01

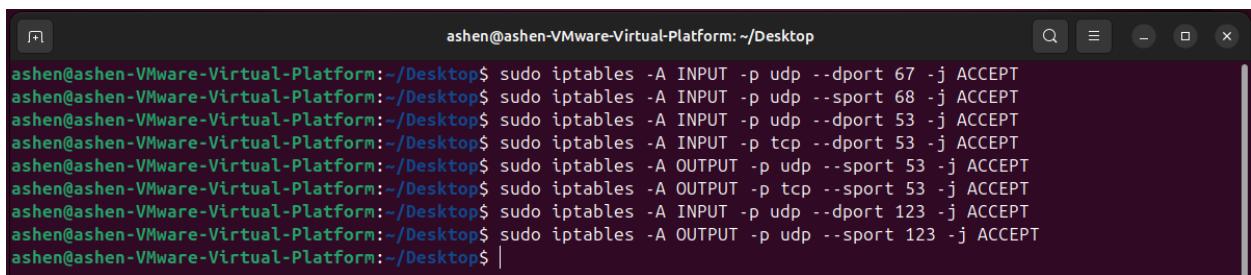
Identify the ports and application services want to allow.

- a. DHCP
  - a. port 67 - requests to the server
  - b. port 68 – responses from the server
- b. DNS
  - a. port 53
- c. NTP
  - a. port 123

#### Step 02

Allow the identified services.

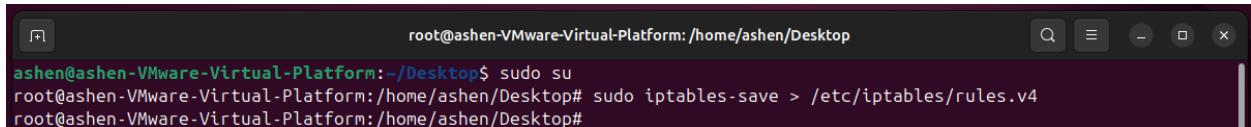
- sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT (Allow DHCP requests to the server)
- sudo iptables -A INPUT -p udp --sport 68 -j ACCEPT (Allow DHCP responses from the server)
- sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT (Allow incoming DNS requests)
- sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT (Allow DNS zone transfers or large queries)
- sudo iptables -A OUTPUT -p udp --sport 53 -j ACCEPT (Allow DNS responses)
- sudo iptables -A OUTPUT -p tcp --sport 53 -j ACCEPT
- sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT (Allow incoming NTP requests)
- sudo iptables -A OUTPUT -p udp --sport 123 -j ACCEPT (Allow NTP responses)



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p udp --sport 68 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A OUTPUT -p udp --sport 53 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A OUTPUT -p tcp --sport 53 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A OUTPUT -p udp --sport 123 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

## Step 03

Save the rules.

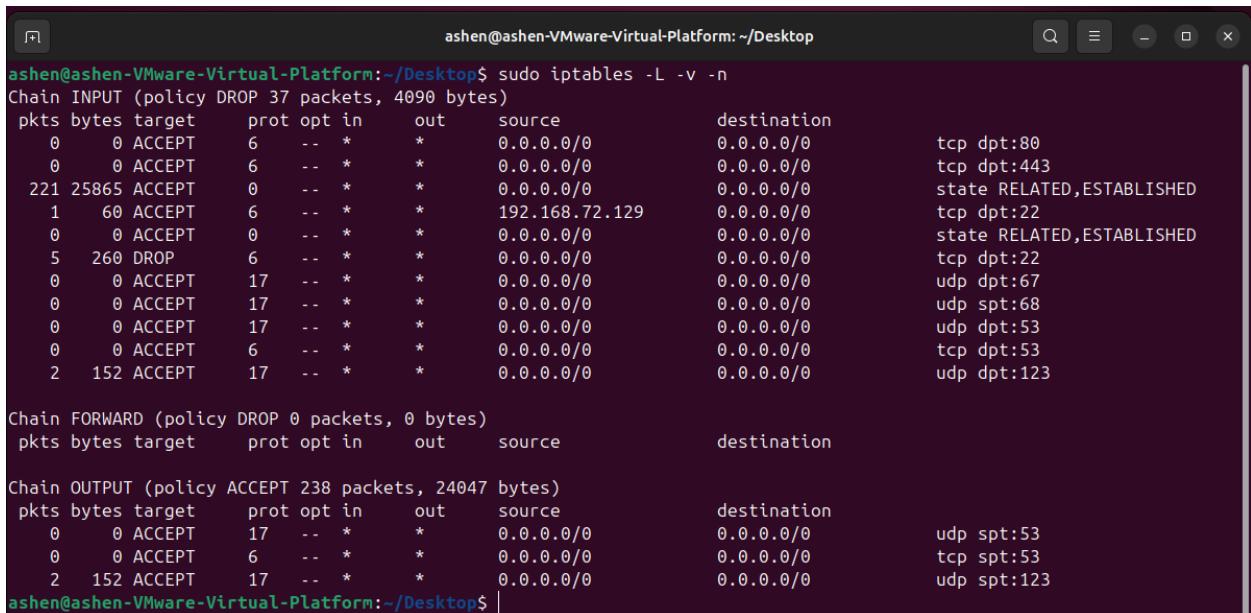


```
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# sudo iptables-save > /etc/iptables/rules.v4
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop#
```

## Step 04

Check the rules whether they are applied.

- sudo iptables -L -v -n



```
ashen@ashen-VMware-Virtual-Platform:/Desktop$ sudo iptables -L -v -n
Chain INPUT (policy DROP 37 packets, 4090 bytes)
pkts bytes target prot opt in     out    source          destination
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp  dpt:80
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp  dpt:443
 221 25865 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        state RELATED,ESTABLISHED
  1   60 ACCEPT  all  --  *      *      192.168.72.129  0.0.0.0/0        tcp  dpt:22
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        state RELATED,ESTABLISHED
  5   260 DROP   all  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp  dpt:22
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  dpt:67
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  spt:68
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  dpt:53
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp  dpt:53
  2   152 ACCEPT all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  dpt:123

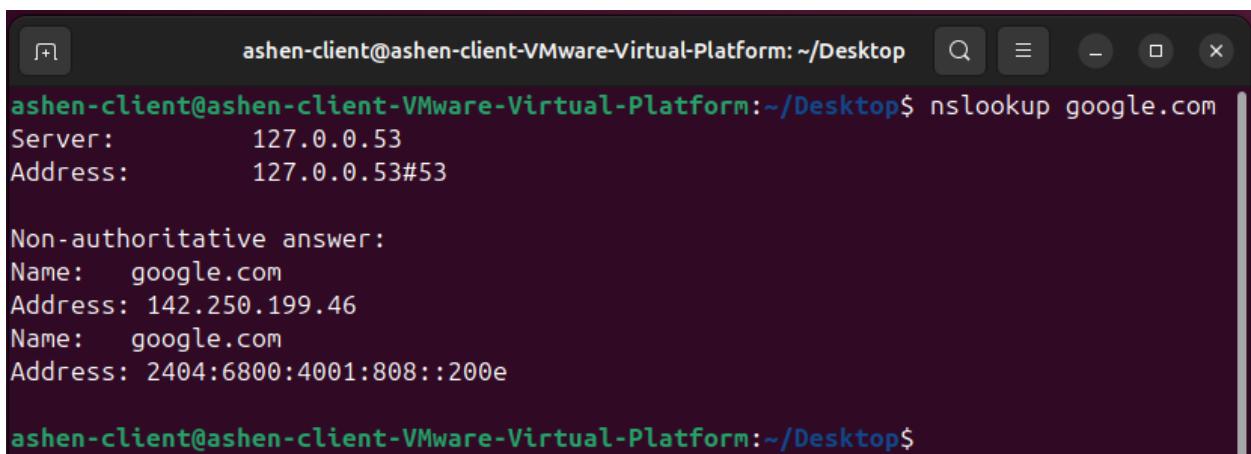
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in     out    source          destination

Chain OUTPUT (policy ACCEPT 238 packets, 24047 bytes)
pkts bytes target prot opt in     out    source          destination
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  spt:53
  0   0 ACCEPT  all  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp  spt:53
  2   152 ACCEPT all  --  *      *      0.0.0.0/0        0.0.0.0/0        udp  spt:123
ashen@ashen-VMware-Virtual-Platform:/Desktop$ |
```

## Step 05

Verification

- Checking the DNS

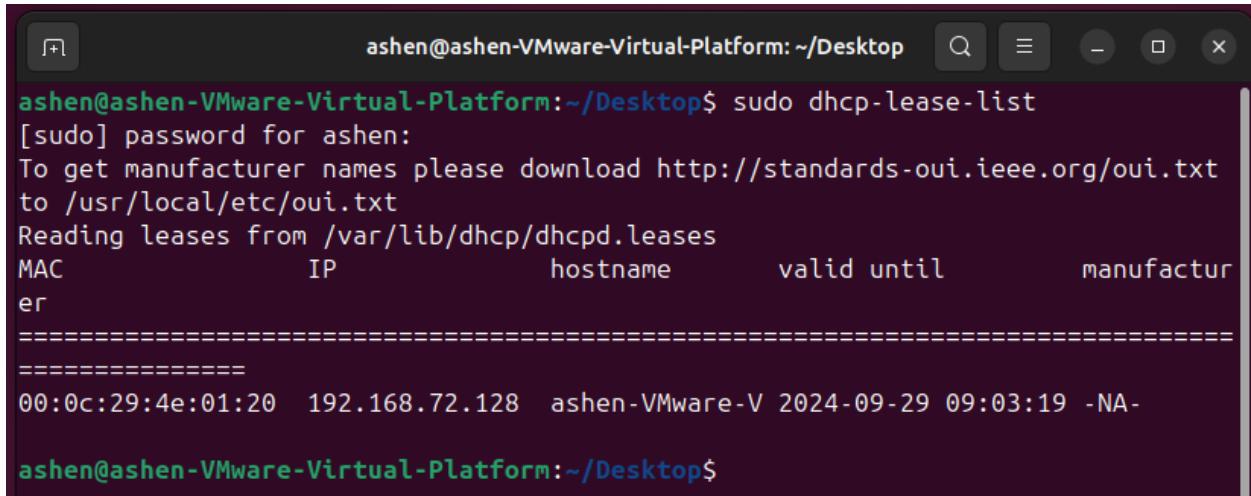


```
ashen-client@ashen-client-VMware-Virtual-Platform:/Desktop$ nslookup google.com
Server:      127.0.0.53
Address:      127.0.0.53#53

Non-authoritative answer:
Name:      google.com
Address:   142.250.199.46
Name:      google.com
Address:   2404:6800:4001:808::200e

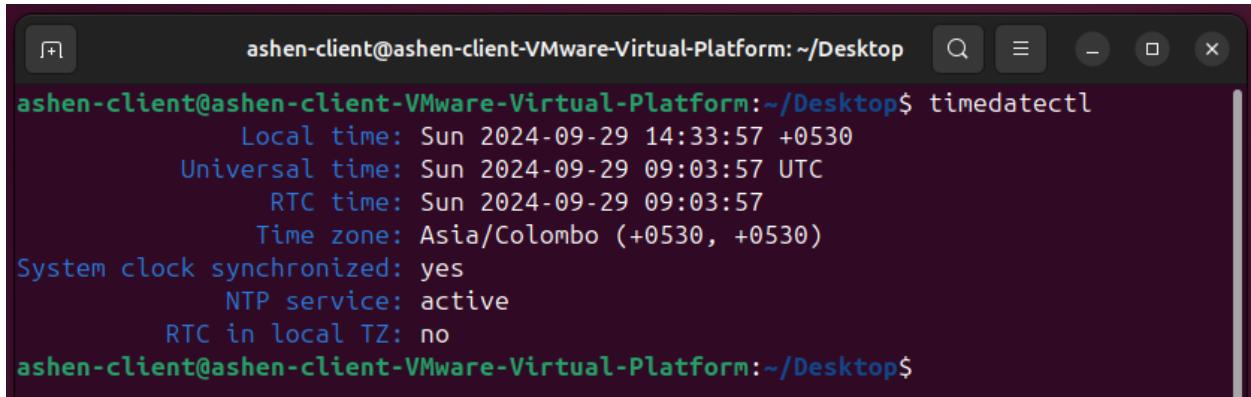
ashen-client@ashen-client-VMware-Virtual-Platform:/Desktop$
```

- Checking DHCP



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo dhcp-lease-list
[sudo] password for ashén:
To get manufacturer names please download http://standards-oui.ieee.org/oui.txt
to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC           IP           hostname      valid until      manufacturer
=====
00:0c:29:4e:01:20  192.168.72.128  ashén-VMware-V  2024-09-29 09:03:19 -NA-
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

- Checking NTP



```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ timedatectl
          Local time: Sun 2024-09-29 14:33:57 +0530
          Universal time: Sun 2024-09-29 09:03:57 UTC
                RTC time: Sun 2024-09-29 09:03:57
                  Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$
```

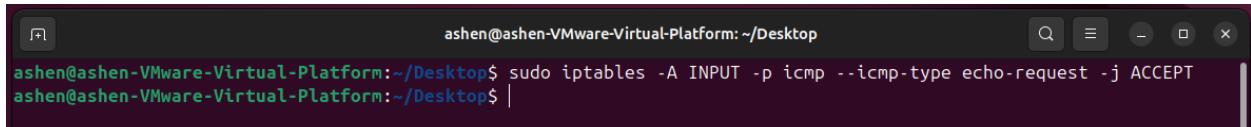
As you can see you will get the output as above if the configurations are successful.

- iv. **Allow Pings (ICMP Echo Request):** This basic rule allows ping requests (ICMP Echo Request) to your machine, which can be helpful for troubleshooting network connectivity

### Step 01

Add the rule to allow ICMP Echo Requests that used for pinging.

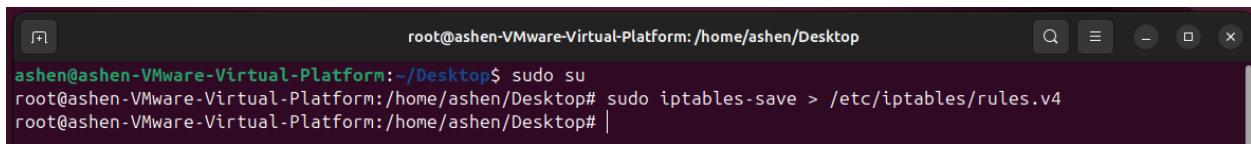
- sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

### Step 02

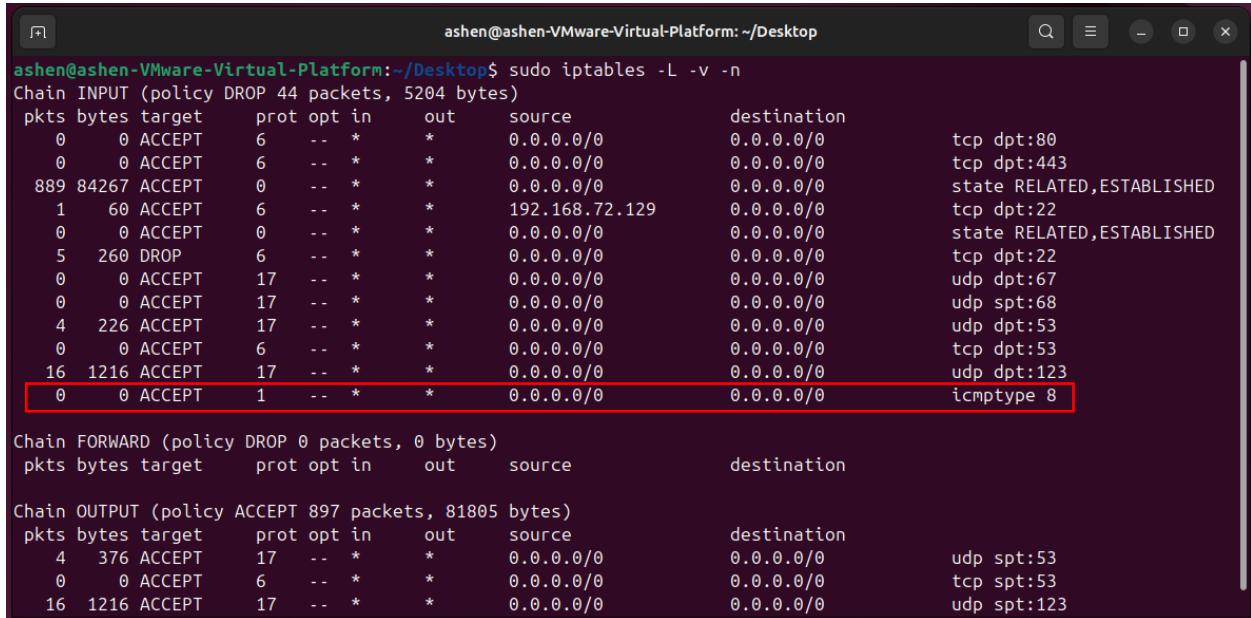
Save the rules.



```
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# sudo iptables-save > /etc/iptables/rules.v4
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# |
```

### Step 03

Verify the rules whether applied.



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -L -v -n
Chain INPUT (policy DROP 44 packets, 5204 bytes)
pkts bytes target     prot opt in     out    source          destination
  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
 889 84267 ACCEPT     0  --  *      *      0.0.0.0/0        0.0.0.0/0        state RELATED,ESTABLISHED
  1   60 ACCEPT      6  --  *      *      192.168.72.129  0.0.0.0/0        tcp dpt:22
  0   0 ACCEPT      0  --  *      *      0.0.0.0/0        0.0.0.0/0        state RELATED,ESTABLISHED
  5   260 DROP       6  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:22
  0   0 ACCEPT      17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:67
  0   0 ACCEPT      17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:68
  4   226 ACCEPT     17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:53
  0   0 ACCEPT      6  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:53
 16  1216 ACCEPT     17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:123
  0   0 ACCEPT      1  --  *      *      0.0.0.0/0        0.0.0.0/0        icmptype 8

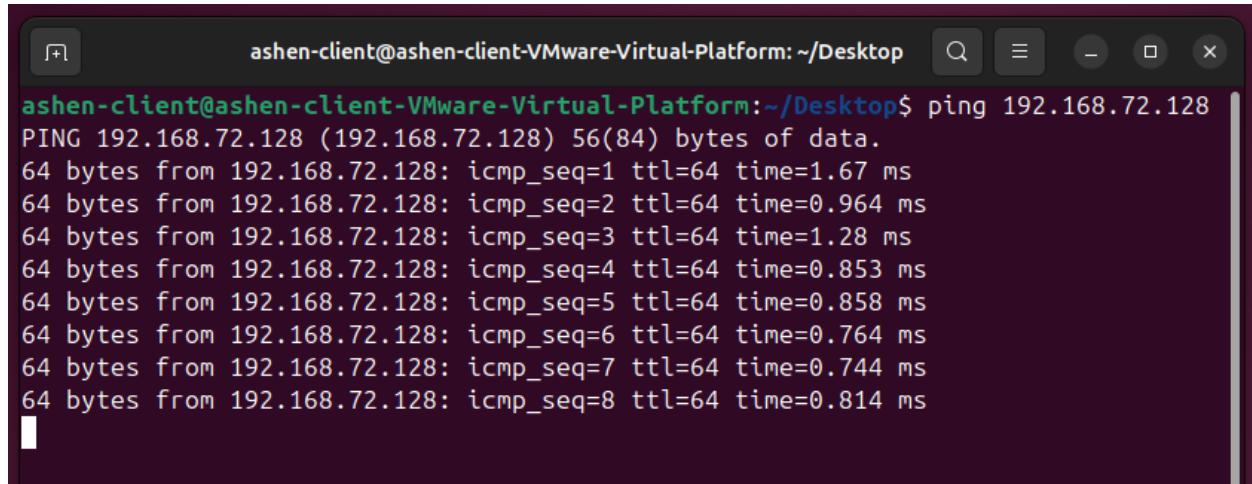
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination

Chain OUTPUT (policy ACCEPT 897 packets, 81805 bytes)
pkts bytes target     prot opt in     out    source          destination
  4   376 ACCEPT      17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:53
  0   0 ACCEPT      6  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:53
 16  1216 ACCEPT     17 --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:123
```

## Step 04

### Testing the configurations

- ping 198.168.72.128



A screenshot of a terminal window titled "ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop". The window contains the following text:

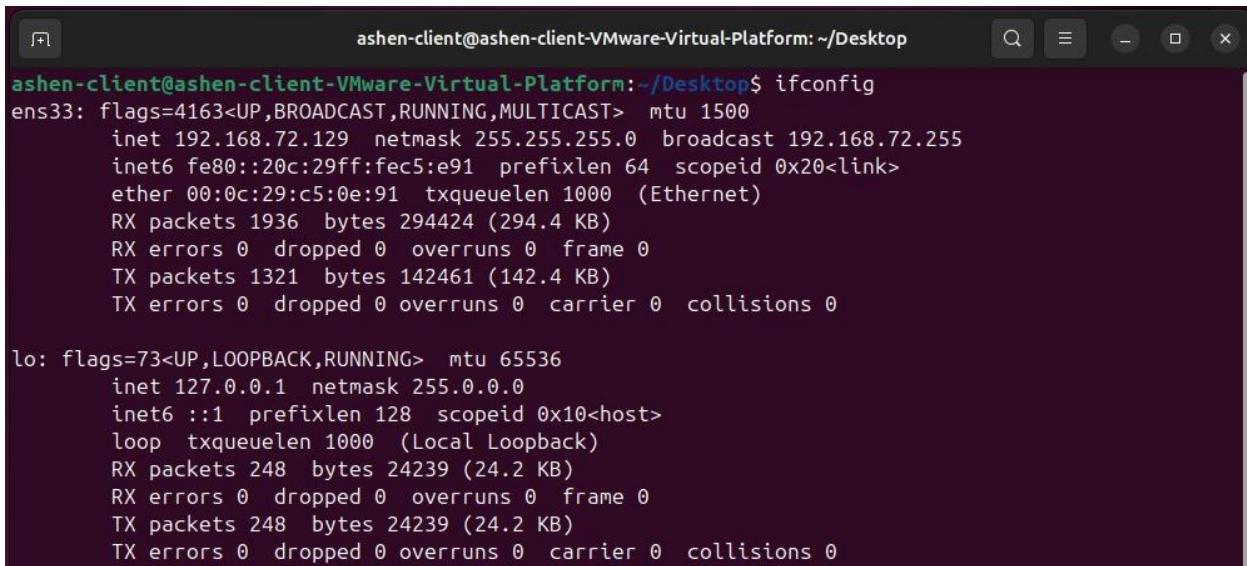
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ping 192.168.72.128
PING 192.168.72.128 (192.168.72.128) 56(84) bytes of data.
64 bytes from 192.168.72.128: icmp_seq=1 ttl=64 time=1.67 ms
64 bytes from 192.168.72.128: icmp_seq=2 ttl=64 time=0.964 ms
64 bytes from 192.168.72.128: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 192.168.72.128: icmp_seq=4 ttl=64 time=0.853 ms
64 bytes from 192.168.72.128: icmp_seq=5 ttl=64 time=0.858 ms
64 bytes from 192.168.72.128: icmp_seq=6 ttl=64 time=0.764 ms
64 bytes from 192.168.72.128: icmp_seq=7 ttl=64 time=0.744 ms
64 bytes from 192.168.72.128: icmp_seq=8 ttl=64 time=0.814 ms
```

- v. **Printer Server Access: For a printer server, allow printing traffic (port 9100) only from specific IP addresses within your local network. Block all external access to the printer server to prevent unauthorized printing.**

### Step 01

Identify the trusted IP addresses.

- I have chosen my ubuntu client VM.



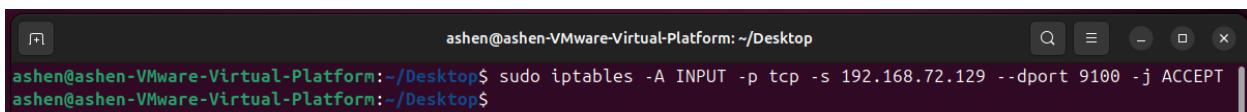
```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.72.129 netmask 255.255.255.0 broadcast 192.168.72.255
        inet6 fe80::20c:29ff:fe91:txqueuelen 1000 (Ethernet)
          ether 00:0c:29:c5:0e:91 txqueuelen 1000 (Ethernet)
          RX packets 1936 bytes 294424 (294.4 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 1321 bytes 142461 (142.4 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 248 bytes 24239 (24.2 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 248 bytes 24239 (24.2 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Step 02

Allow printing traffic from trusted IPs

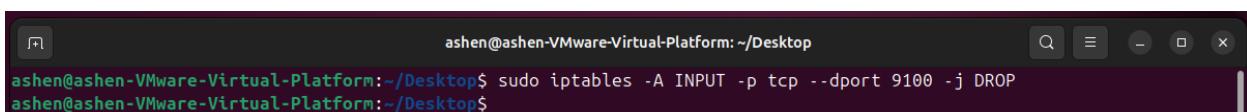
- sudo iptables -A INPUT -p tcp -s 192.168.72.129 --dport 9100 -j ACCEPT



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp -s 192.168.72.129 --dport 9100 -j ACCEPT
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

### Step 03

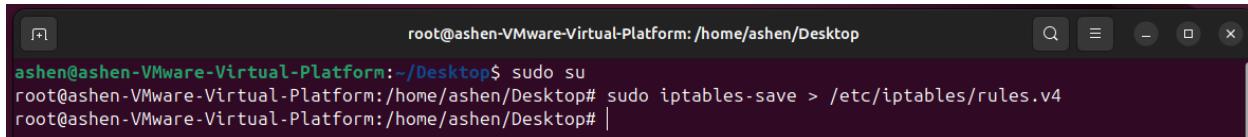
Drop all the other incoming traffic from port 9100



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -A INPUT -p tcp --dport 9100 -j DROP
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

## Step 04

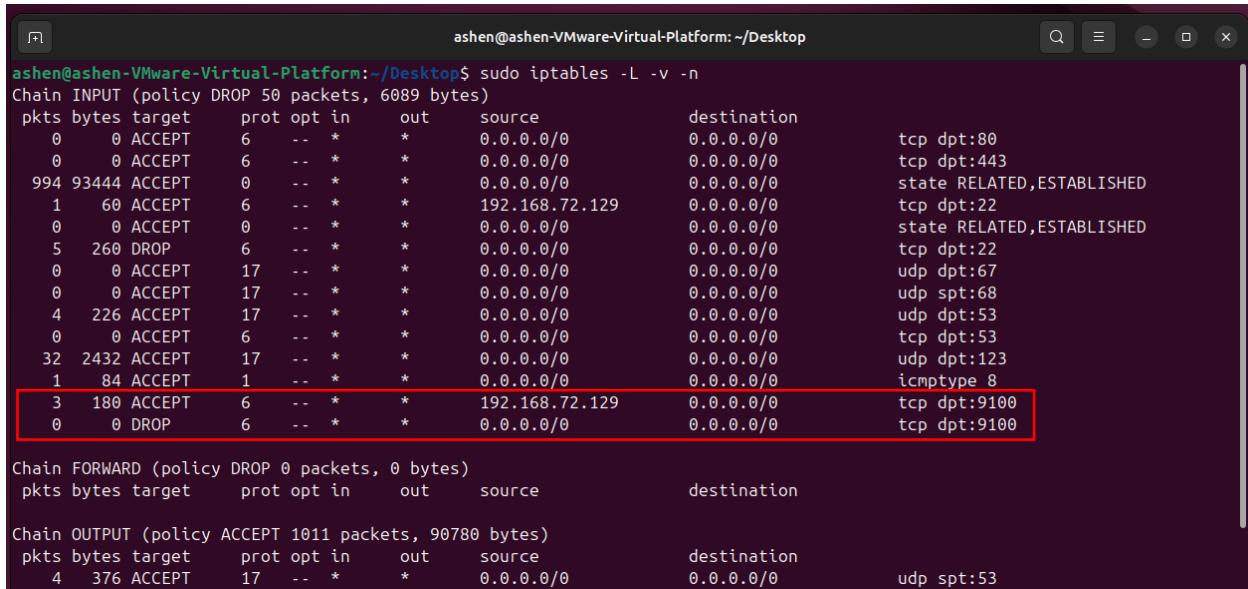
Save the rules.



```
root@ashen-VMware-Virtual-Platform:~/Desktop$ sudo su
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# sudo iptables-save > /etc/iptables/rules.v4
root@ashen-VMware-Virtual-Platform:/home/ashen/Desktop# |
```

## Step 05

Verify .



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo iptables -L -v -n
Chain INPUT (policy DROP 50 packets, 6089 bytes)
pkts bytes target     prot opt in     out      source          destination
  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
994 93444 ACCEPT     0  --  *      *      0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED
  1   60 ACCEPT     6  --  *      *      192.168.72.129  0.0.0.0/0          tcp dpt:22
  0   0 ACCEPT      6  --  *      *      0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED
  5   260 DROP       6  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:22
  0   0 ACCEPT     17  --  *      *      0.0.0.0/0        0.0.0.0/0          udp dpt:67
  0   0 ACCEPT     17  --  *      *      0.0.0.0/0        0.0.0.0/0          udp spt:68
  4   226 ACCEPT     17  --  *      *      0.0.0.0/0        0.0.0.0/0          udp dpt:53
  0   0 ACCEPT      6  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:53
32  2432 ACCEPT     17  --  *      *      0.0.0.0/0        0.0.0.0/0          udp dpt:123
  1   84 ACCEPT      1  --  *      *      0.0.0.0/0        0.0.0.0/0          icmp type 8
  3  180 ACCEPT      6  --  *      *      192.168.72.129  0.0.0.0/0          tcp dpt:9100
  0   0 DROP        6  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:9100

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out      source          destination

Chain OUTPUT (policy ACCEPT 1011 packets, 90780 bytes)
pkts bytes target     prot opt in     out      source          destination
  4   376 ACCEPT      17  --  *      *      0.0.0.0/0        0.0.0.0/0          udp spt:53
```

## Step 06

Testing the configurations

- Since I'm working with two Ubuntu VMs and don't have a physical printer, we can simulate access to a "printer server" by testing connectivity on port 9100.

Run the command in server VM.

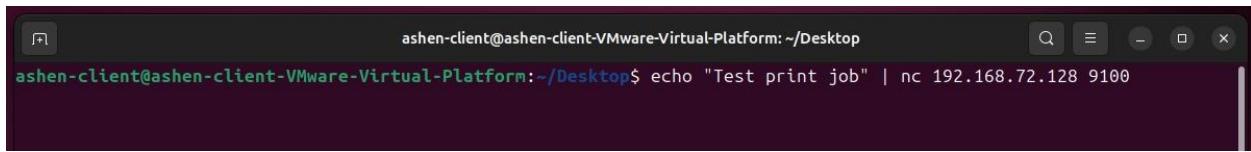
- `sudo nc -l -p 9100`
  - This command listens for any incoming connection on port 9100, which mimics a printer service.

Run the command in trusted machine.

- `echo "Test print job" | nc 192.168.72.128 9100`

if the connection works we can see "Test print job" in server machine.

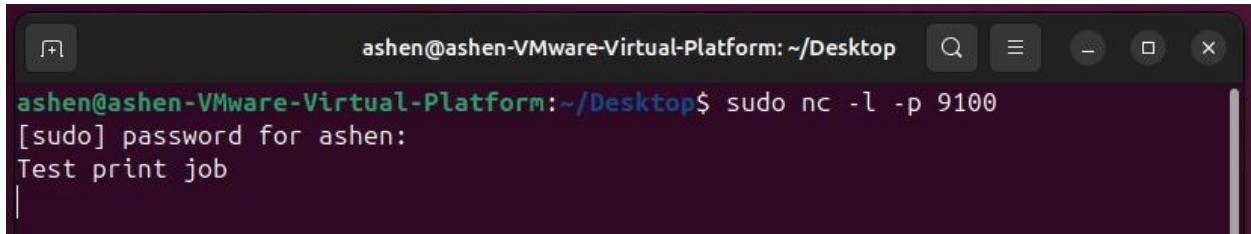
Client side



```
ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ echo "Test print job" | nc 192.168.72.128 9100
```

A terminal window titled 'ashen-client@ashen-client-VMware-Virtual-Platform: ~/Desktop'. The command 'echo "Test print job" | nc 192.168.72.128 9100' is entered and executed.

Server side



```
ashen@ashen-VMware-Virtual-Platform: ~/Desktop
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo nc -l -p 9100
[sudo] password for ash: 
Test print job
```

A terminal window titled 'ashen@ashen-VMware-Virtual-Platform: ~/Desktop'. The command 'sudo nc -l -p 9100' is entered and executed. A password is prompted, followed by the received message 'Test print job'.

If you get the sent “Test print job” in the server side , it means that the service works properly.

## 5. Best Practices

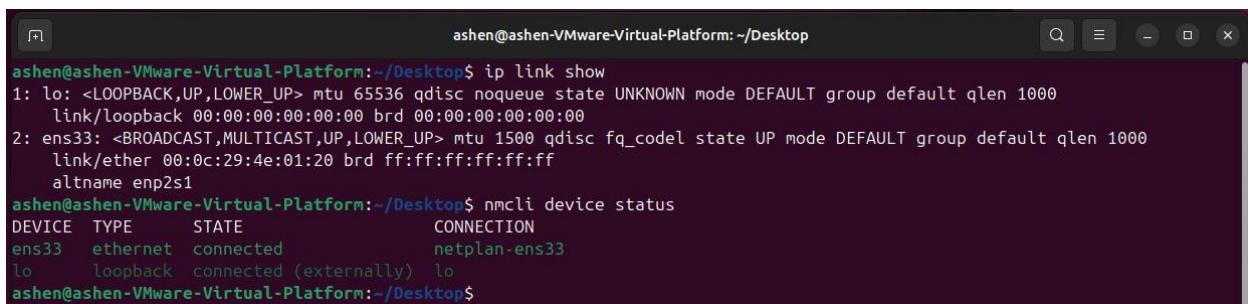
### 1. Disable Unused Network Interfaces.

- unused network interfaces can be potential attack vector, so disabling them reduce the attack surface.

Step 01

Check all network interfaces.

- ip link show
- nmcli device status



A terminal window titled 'ashen@ashen-VMware-Virtual-Platform: ~/Desktop\$' showing the output of two commands: 'ip link show' and 'nmcli device status'. The 'ip link show' command lists network interfaces lo and ens33 with their respective MTU, queueing discipline (qdisc), state, and link layer information. The 'nmcli device status' command shows that ens33 is an ethernet device connected via netplan-ens33, while lo is a loopback device connected externally.

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:4e:01:20 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ nmcli device status
DEVICE      TYPE      STATE      CONNECTION
ens33       ethernet  connected  netplan-ens33
lo          loopback  connected (externally)  lo
ashen@ashen-VMware-Virtual-Platform:~/Desktop$
```

state up – active

state down – inactive or unused

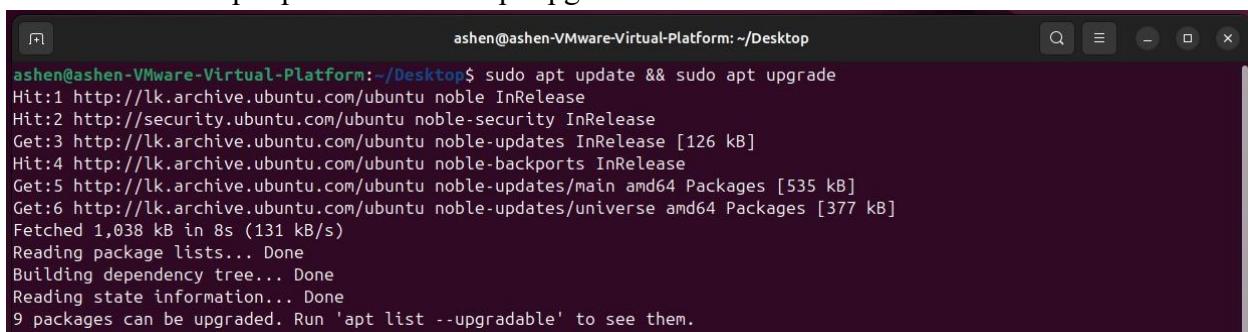
Step 02

Check for any state down network interfaces and disable them.(In here I don't have any state down Network interfaces)

- sudo ip link set <interface> down
  - o ex:- sudo ip link set ens33 down

### 2. Keep the system Updated

- Frequent updates help to ensure that patches are fixed, therefore lower the chance of exploitation.
- sudo apt update && sudo apt upgrade



A terminal window titled 'ashen@ashen-VMware-Virtual-Platform: ~/Desktop\$' showing the output of the 'sudo apt update && sudo apt upgrade' command. The output shows the process of fetching packages from the Ubuntu archive, reading package lists, building dependency trees, and upgrading 9 packages.

```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo apt update && sudo apt upgrade
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]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [535 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [377 kB]
Fetched 1,038 kB in 8s (131 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
9 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

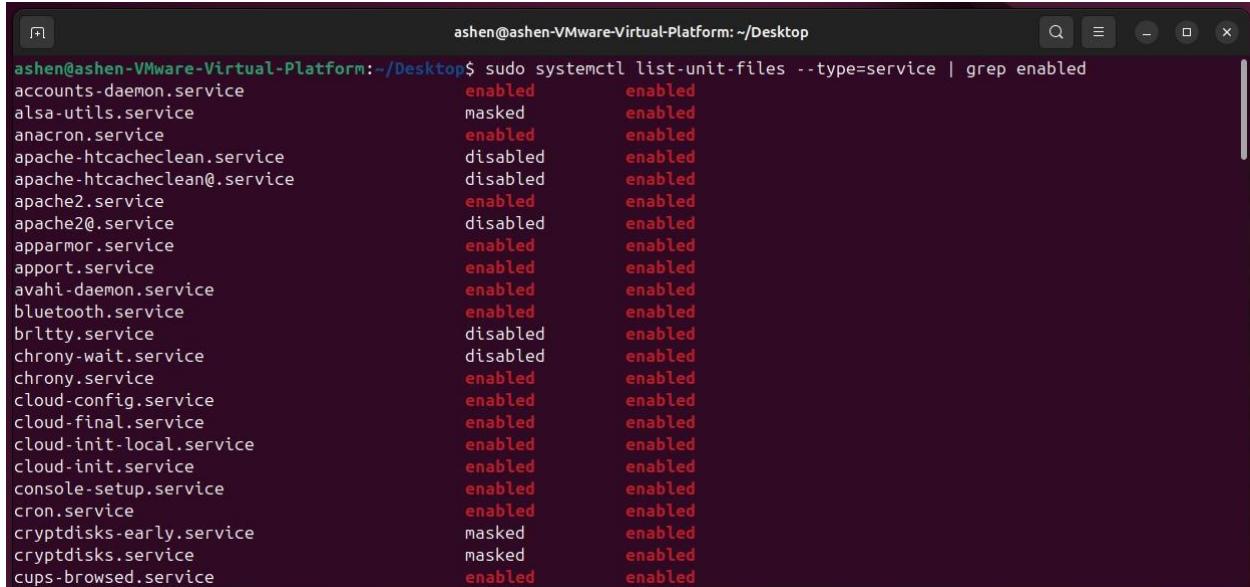
### 3. Limit unused Network Services.

- Disable or remove any unnecessary network services that are not required, reducing the attack surface.

#### Step 01

List the enabled services.

- `sudo systemctl list-unit-files --type=service | grep enabled`

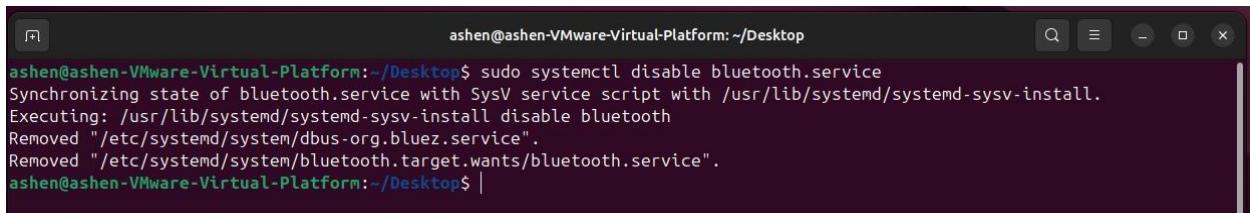


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl list-unit-files --type=service | grep enabled
accounts-daemon.service          enabled    enabled
alsa-utils.service                masked     enabled
anacron.service                  enabled    enabled
apache-htcacheclean.service      disabled   enabled
apache-htcacheclean@.service     disabled   enabled
apache2.service                  enabled    enabled
apache2@.service                 disabled   enabled
apparmor.service                 enabled    enabled
apport.service                   enabled    enabled
avahi-daemon.service            enabled    enabled
bluetooth.service                enabled    enabled
brltty.service                   disabled   enabled
chrony-wait.service              disabled   enabled
chrony.service                   enabled    enabled
cloud-config.service             enabled    enabled
cloud-final.service              enabled    enabled
cloud-init-local.service         enabled    enabled
cloud-init.service               enabled    enabled
console-setup.service            enabled    enabled
cron.service                     enabled    enabled
cryptdisks-early.service        masked     enabled
cryptdisks.service               masked     enabled
cups-browsed.service             enabled    enabled
```

#### Step 02

Disable unnecessary services.

- `sudo systemctl disable bluetooth.service` (Disable if your machine doesn't use Bluetooth, as it reduces the attack surface.)



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl disable bluetooth.service
Synchronizing state of bluetooth.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable bluetooth
Removed "/etc/systemd/system/dbus-org.bluez.service".
Removed "/etc/systemd/system/bluetooth.target.wants/bluetooth.service".
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

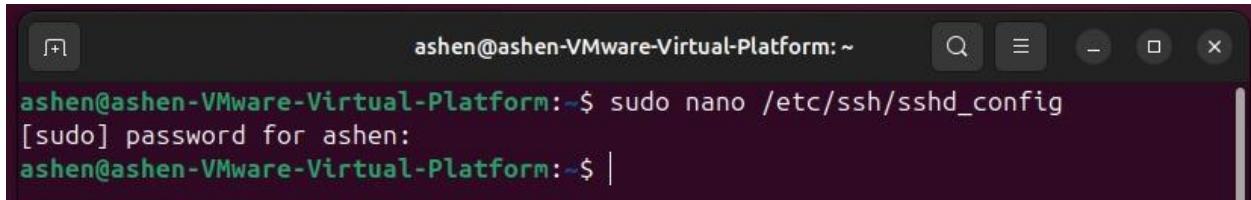
#### 4. Disable root login via ssh

- As we know the root access is highly privileged , the root account has complete control over the system , so it is important to limit root access to reduce the risk of exploitation.

Step 01

Open SSH configuration file.

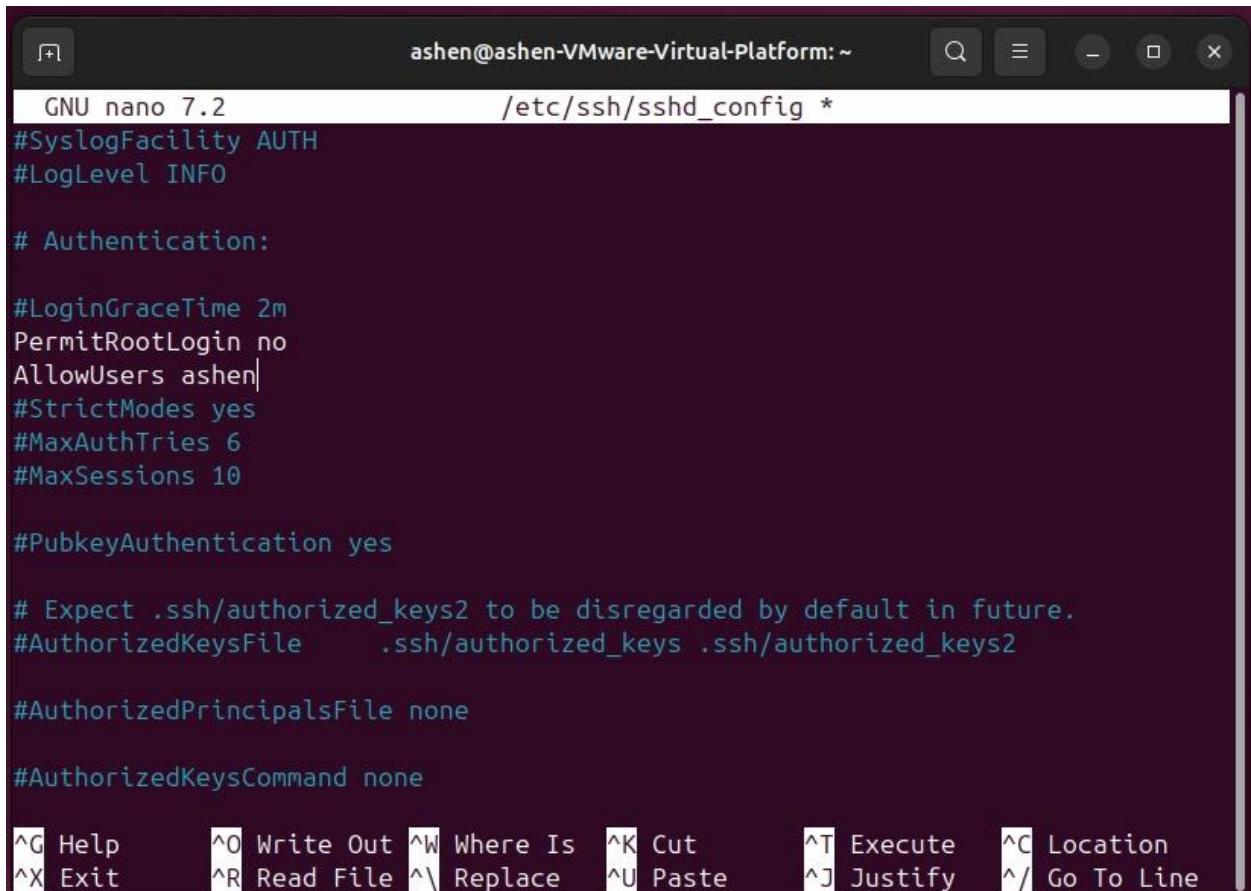
- sudo nano /etc/ssh/sshd\_config



```
ashen@ashen-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for asheng:
```

Step 02

Update or Add PermitRootLogin and the AllowUser Directive.



```
GNU nano 7.2                               /etc/ssh/sshd_config *
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers asheng|
#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

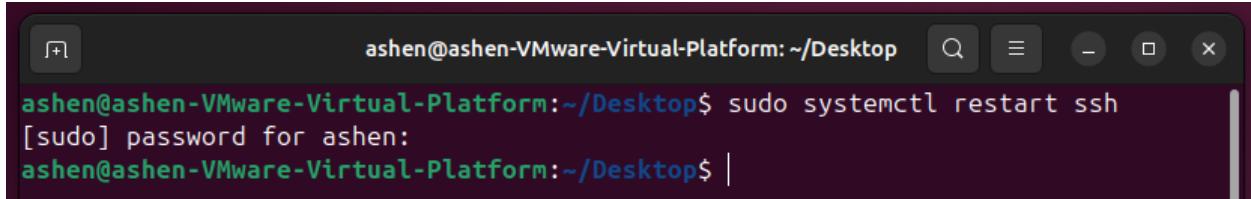
^G Help          ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit         ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

Save and Exit.

### Step 03

Restart the ssh service to apply changes.

- sudo systemctl restart ssh

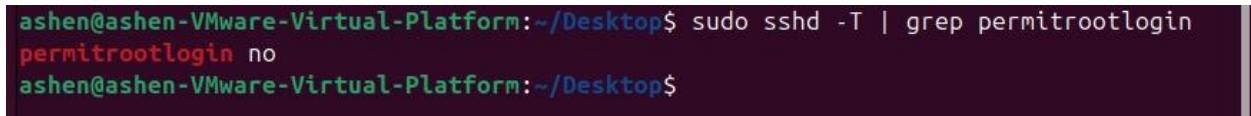


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart ssh
[sudo] password for ash: [REDACTED]
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

### Step 04

Verify the configuration

- sudo sshd -T | grep permitrootlogin

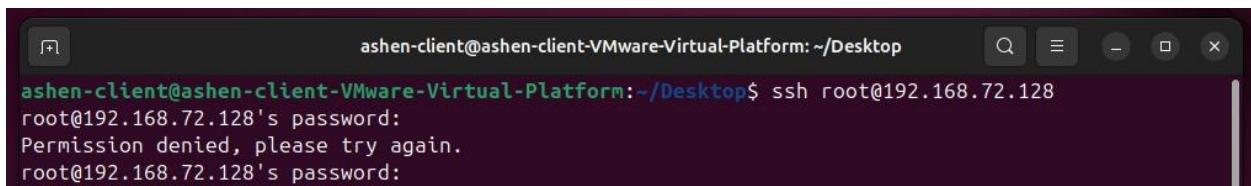


```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo sshd -T | grep permitrootlogin
permitrootlogin no
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ |
```

### Step 05

Test root login using a client machine.

- ssh root@192.168.72.128

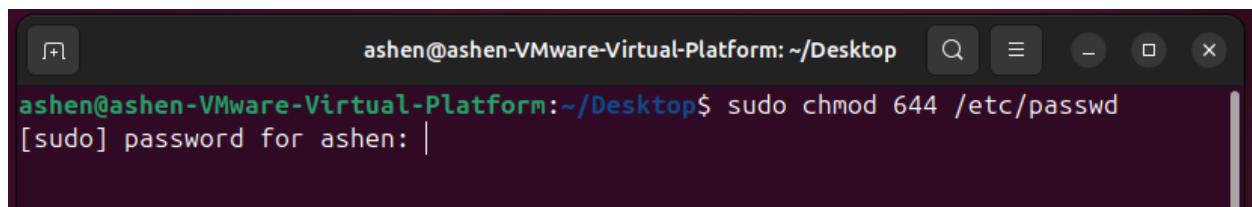


```
ashen-client@ashen-client-VMware-Virtual-Platform:~/Desktop$ ssh root@192.168.72.128
root@192.168.72.128's password:
Permission denied, please try again.
root@192.168.72.128's password:
```

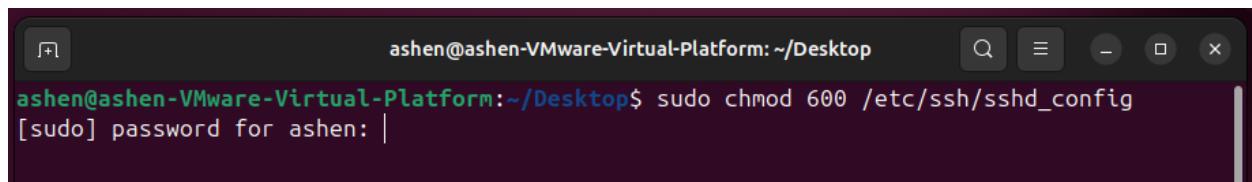
If the configuration is successful, you will get an error message as above.

## 5. Use secure file permissions.

- Securing configuration files that contain sensitive information. Ensures that script and configuration files are owned by the root.
  - /etc/passwd
    - Contains user account information.
      - sudo chmod 644 /etc/passwd  
(Readable by all users, but only writable by the root user.)
    - /etc/ssh/sshd\_config
      - ssh server configuration file
      - sudo chmod 600 /etc/ssh/sshd\_config



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo chmod 644 /etc/passwd
[sudo] password for ash: |
```



```
ashen@ashen-VMware-Virtual-Platform:~/Desktop$ sudo chmod 600 /etc/ssh/sshd_config
[sudo] password for ash: |
```

Not only these, using iptables rules for only to allow trusted parties to use services is also a best practice considering security.