



Qualification national code and title	AE780 Transition to Cyber Security Skillset
Unit/s national code/s and title/s	VU23214: Configure and secure networked end points

**Assessment type (☑):**

- ☐ Questioning (Oral/Written)  
☐ Practical Demonstration  
☐ 3<sup>rd</sup> Party Report  
☒ Other – Project/**Portfolio** (Part of assessment task 1)

**Assessment Resources:**

- PC
- Google
- Computer components PowerPoint
- Linux Virtual Machine

**Assessment Instructions:**
Instructions to the assessor:

This lab is a part of Assessment Task 2 portfolio, it is a practical lab based on the performance criteria requirements of the unit. Each student should be given a copy of this lab to complete either in class or out of class. As the student completes each section of this lab you should verify, check off and sign off the section (Use this document as the observation checklist). Use the assessor section at the bottom to provide feedback to the student if required. See the instructions to the student section for the remainder of the instructions.

Instructions to the student:

This lab consists of activities that you perform on the hardware and software nominated concerning preventative maintenance and base level troubleshooting procedures. There are several short answer questions where you will be asked to research and answer questions relating to these topics. You are encouraged to use the documentation in the resource section to help you work on the requirements.

Time:

Nominally 120 mins

Due date:

This lab is part of assessment 1 and inherits its due date.

Submission instructions:

When the lab is complete, submit the assessment via Blackboard.

Reasonable adjustment:

Should there be difficulty with reading technical manuals relating to disability of language and literacy levels you are encouraged to use online video tutorials similar to the following:

- [https://www.youtube.com/watch?v=HBP8\\_LqBj44](https://www.youtube.com/watch?v=HBP8_LqBj44)

Your Student ID: 20145454	Your Name: Rajib Hossain Khan
------------------------------	-------------------------------



Qualification national code and title	AE780 Transition to Cyber Security Skillset
Unit/s national code/s and title/s	VU23214: Configure and secure networked end points

# Lab: Linux System Administration and Security Fundamentals

## Objective

In this lab, students will perform essential Linux system administration tasks, including managing processes, installing packages, handling user accounts, setting file permissions, managing services, and using networking commands.

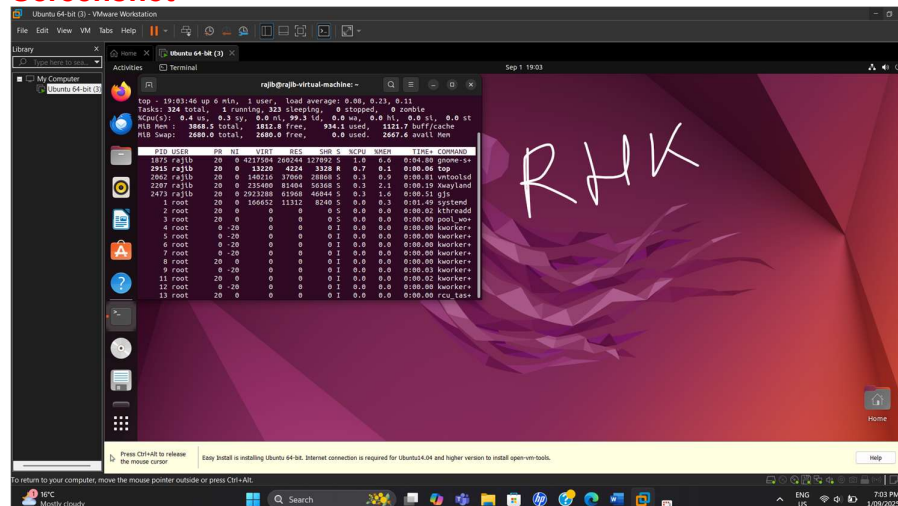
## Instructions for Students

### Step 1: Managing Processes

1. Open a terminal and use the 'top' command to view running processes.
  - Observe CPU and memory usage.
  - Identify the process ID (PID) of a high-resource-consuming process.
  - Take a screenshot of your top output.

*top*

### Screenshot

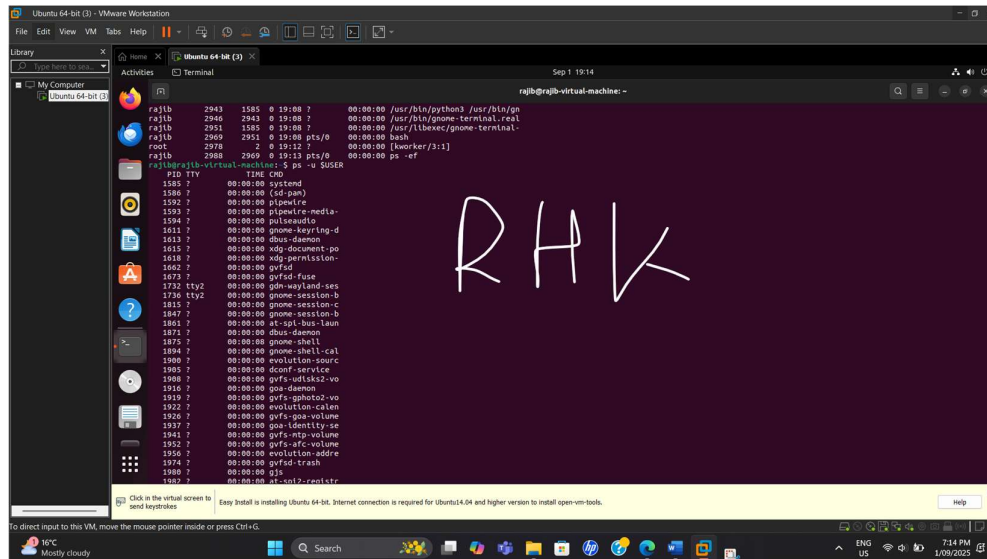


2. Use the ps command to list active processes.
  - Run ps aux and ps -ef to explore different output formats.
  - Identify your current user processes using ps -u \$USER.

### Screenshot



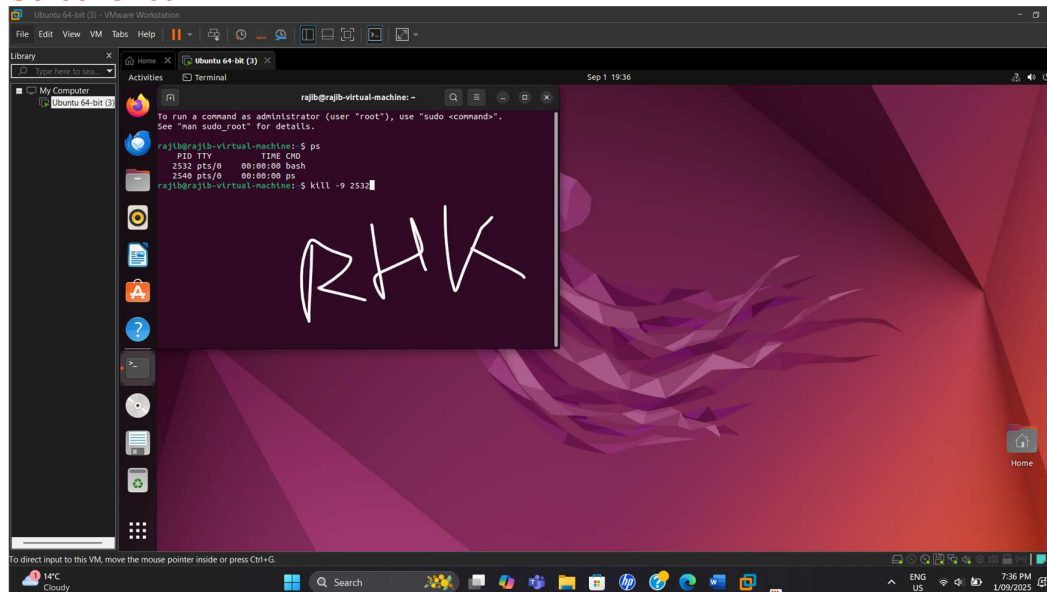
Qualification national code and title	AE780 Transition to Cyber Security Skillset
Unit/s national code/s and title/s	VU23214: Configure and secure networked end points



### 3. Kill a process using the kill command:

- Use kill <PID> to terminate a process.
- Use kill -9 <PID> if a process does not terminate with the default signal.
- Take a screenshot of the output.

### Screenshot



## Step 2: Installing Packages

- ```
sudo apt update
```

The screenshot displays a Windows 10 desktop environment. In the foreground, a VMware Workstation window is open, showing a virtual machine named 'Ubuntu 64-bit (3)'. The terminal window within the VM is active, displaying the command 'sudo apt update' and its output. The output lists various Ubuntu repositories and their security updates, including 'http://security.ubuntu.com/ubuntu jammy-security InRelease' and 'http://au.archive.ubuntu.com/ubuntu jammy-security InRelease'. The desktop background is a purple and blue abstract design. The taskbar at the bottom shows various application icons, including the Start button, Search, and several open applications like File Explorer, Edge, and the VMware Workstation interface.

- ## Screenshot



|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

```

rajib@rajib-virtual-machine: ~
$ sudo apt install htop -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  in-sensors
The following NEW packages will be installed:
  htop
0 to upgrade, 1 to newly install, 0 to remove and 288 not to upgrade.
Need to get 128 kB of archives.
After this operation, 342 kB of additional disk space will be used.
Get:1 http://au.archive.ubuntu.com/ubuntu jammy/main amd64 htop amd64 3.0.5-7build2
Err:1 http://au.archive.ubuntu.com/ubuntu jammy/main amd64 htop amd64 3.0.5-7build2
Temporary failure resolving 'au.archive.ubuntu.com'
Err:2 http://au.archive.ubuntu.com/ubuntu jammy/main amd64 htop amd64 3.0.5-7build2
Temporary failure resolving 'au.archive.ubuntu.com'
$ sudo apt-get update || true
$ sudo apt-get install htop -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  in-sensors
The following NEW packages will be installed:
  htop
0 to upgrade, 1 to newly install, 0 to remove and 288 not to upgrade.
Need to get 128 kB of archives.
After this operation, 342 kB of additional disk space will be used.
Get:1 http://au.archive.ubuntu.com/ubuntu jammy/main amd64 htop amd64 3.0.5-7build2 [128 kB]
Fetched 128 kB (1.3 MB/s)
Selecting previously unselected package htop.
(Reading database ... 263777 files and directories currently installed.)
Preparing to unpack .../htop_3.0.5-7build2_amd64.deb ...
Unpacking htop (3.0.5-7build2) ...
Setting up htop (3.0.5-7build2) ...
Processing triggers for maltrail (1.7bmmuubuntu3) ...
Processing triggers for desktop-file-utils (0.26-ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.8-1ubuntu3) ...
Processing triggers for man-db (2.10.2-1) ...
rajib@rajib-virtual-machine: ~
$
  
```

3. Verify the package installation by running:

*htop*

- Take a screenshot of the htop interface.

## Screenshot

```

rajib@rajib-virtual-machine: ~
$ htop
Tasks: 135, 282 (lth): 1 running
Load average: 0.00 0.02 0.01
Uptime: 00:14:05
Mem: 383M / 786M [ 49%]
Swap: 0M / 2.0G [ 0%]

PID USER      PRI  NI  VIRT   RES   SHR  S  CPU% MEM%   TIME+  Command
1782 rajib    20    0 1418 5192 1664 S  0.7 1.3 0:01.29 /usr/libexec/gn
359  root     19    0 1400 1516 188 S  0.0 0.3 0:01.01 /sbin/init auto
385  root     20    0 1408 1292 1152 S  0.0 0.0 0:00.00 /lib/systemd/sy
386  root     20    0 1408 1292 1152 S  0.0 0.0 0:00.00 /lib/systemd/sy
387  root     20    0 1408 1292 1152 S  0.0 0.0 0:00.00 /lib/systemd/sy
454  root     20    0 1568 7552 660 S  0.0 0.2 0:00.54 /lib/systemd/sy
639  systemd- 20    0 14836 7784 6016 S  0.0 0.2 0:01.74 /lib/systemd/sy
640  systemd- 20    0 15648 15568 344 S  0.0 0.2 0:00.35 /lib/systemd/sy
646  systemd- 20    0 93388 7188 4400 S  0.0 0.2 0:00.21 /lib/systemd/sy
670  systemd- 20    0 93388 7188 4400 S  0.0 0.2 0:00.10 /lib/systemd/sy
675  root     20    0 13752 1432 984 S  0.0 0.3 0:00.00 /usr/bin/ncat
680  root     20    0 1376 1688 688 S  0.0 0.2 0:02.04 /usr/bin/vmtool
  
```

## Step 3: Creating and Managing Users and Groups

Take screenshots of each command output.

1. Create a new user named student1:

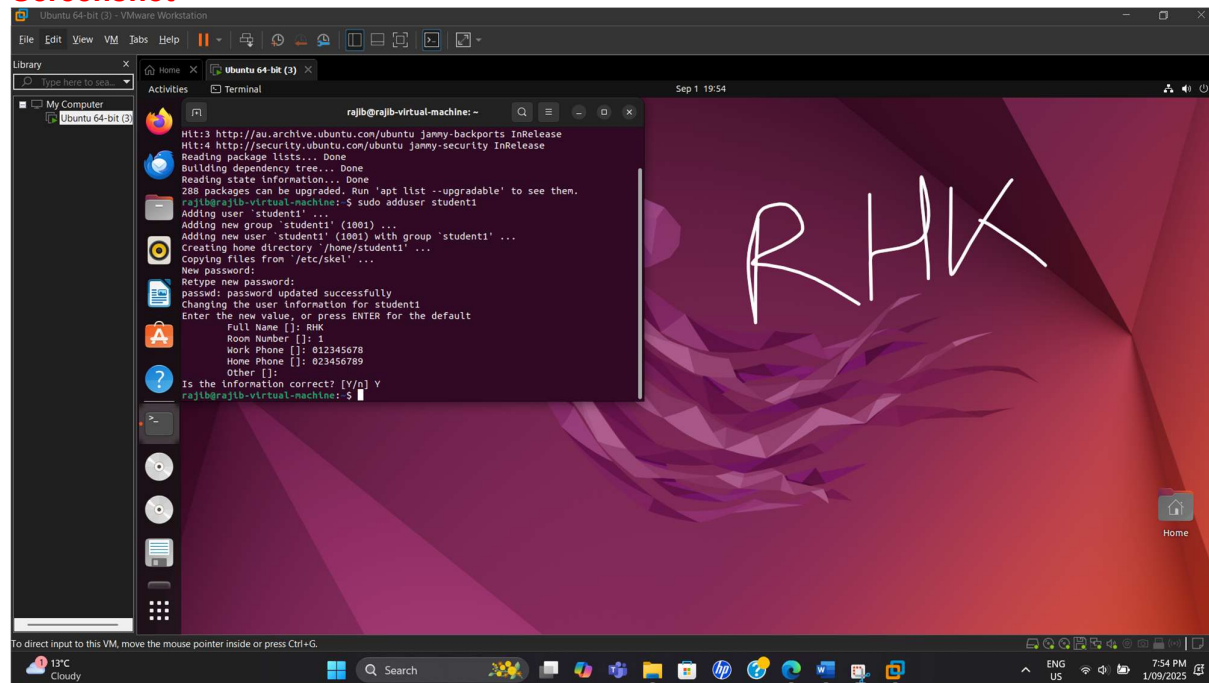
*sudo adduser student1*





|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

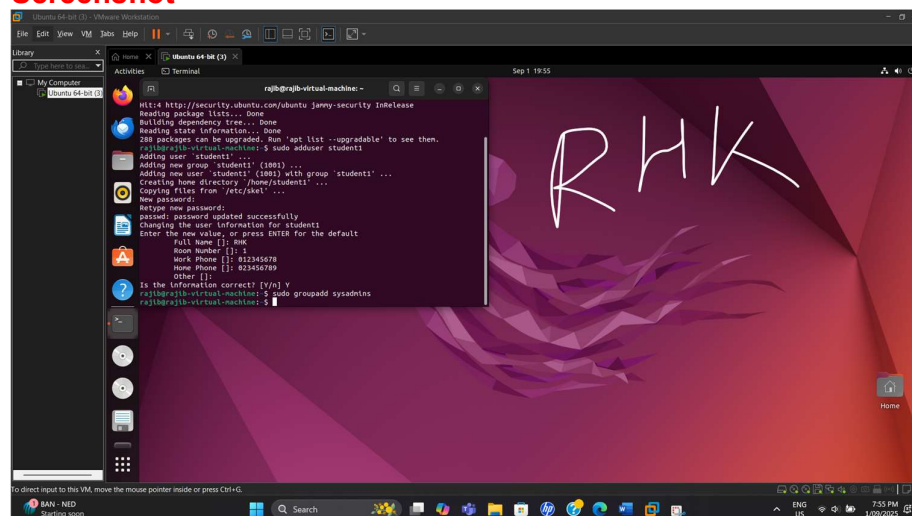
## Screenshot



2. Create a group called sysadmins:

```
sudo groupadd sysadmins
```

## Screenshot



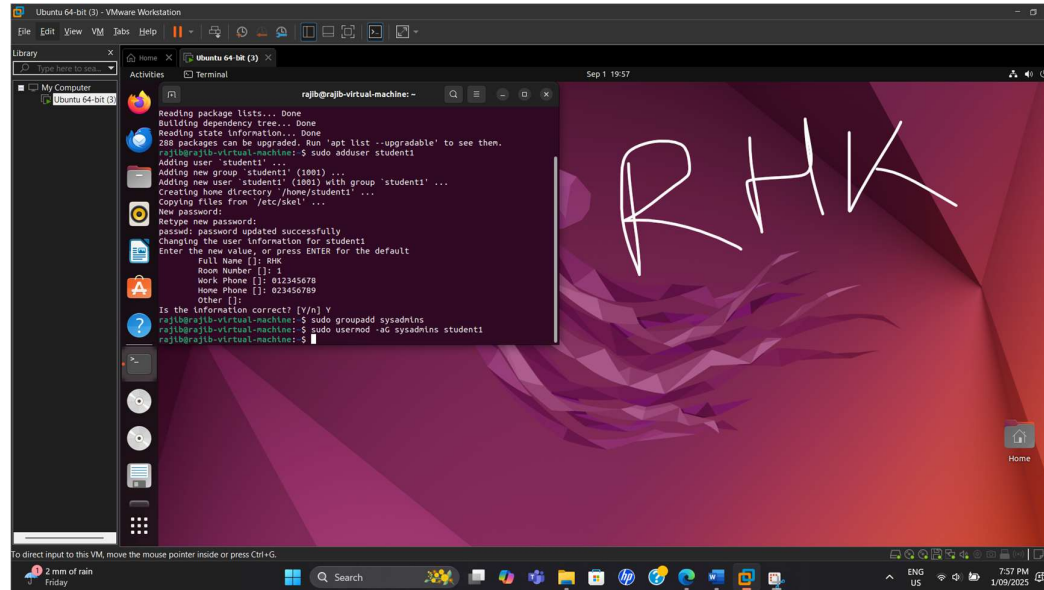
3. Add student1 to the sysadmins group:

```
sudo usermod -aG sysadmins student1
```



|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

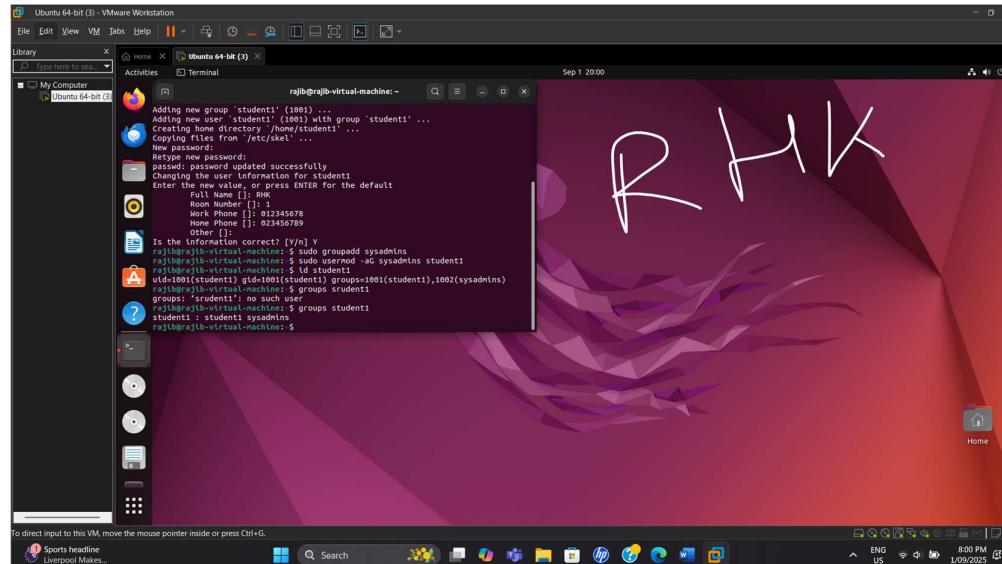
## Screenshot



4. Verify the user and group creation:

```
id student1
groups student1
```

## Screenshot

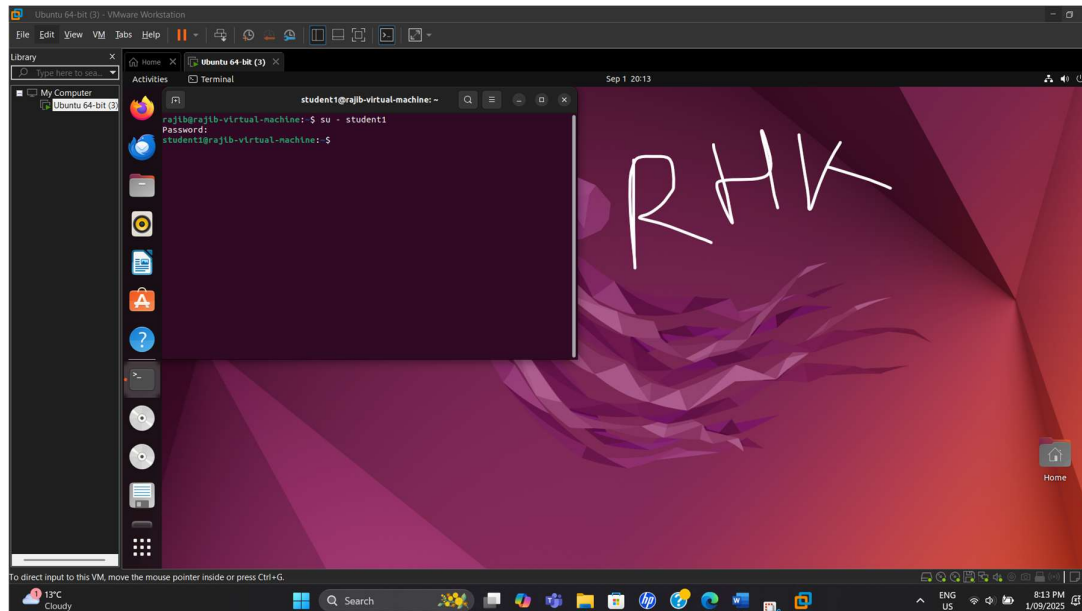


5. Switch to the new user and confirm permissions:

```
su - student1
```

## Screenshot

|                                              |                                                    |
|----------------------------------------------|----------------------------------------------------|
| <b>Qualification national code and title</b> | AE780 Transition to Cyber Security Skillset        |
| <b>Unit/s national code/s and title/s</b>    | VU23214: Configure and secure networked end points |



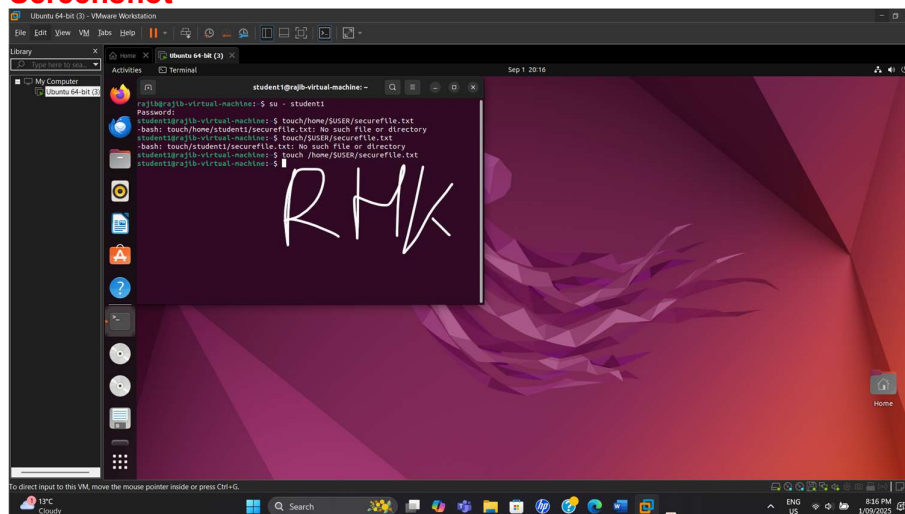
## Step 4: Inspecting and Setting File Permissions

Take screenshots of each command output

1. Create a new file and set custom permissions:

```
touch /home/$USER/securefile.txt
```

## Screenshot



- ## 2. Restrict access to only the owner:

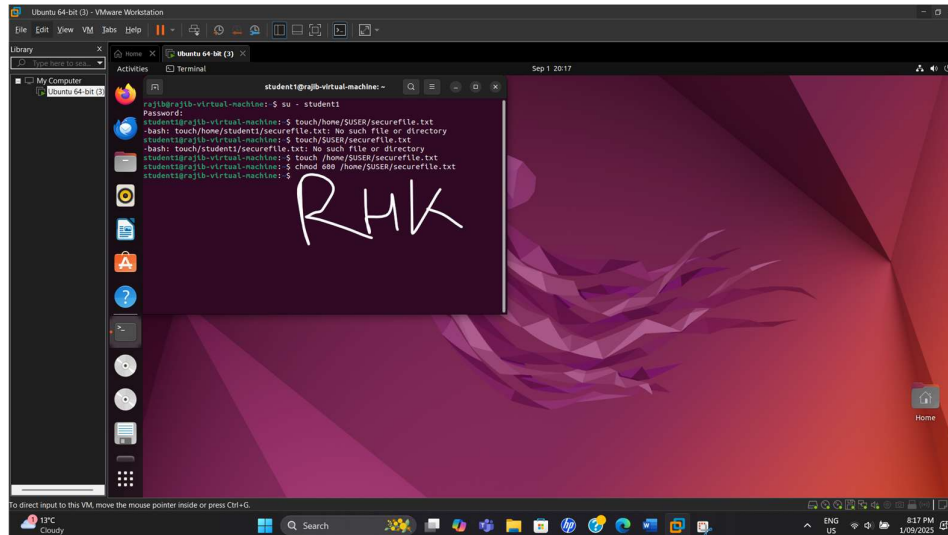
```
chmod 600 /home/$USER/securefile.txt
```





|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

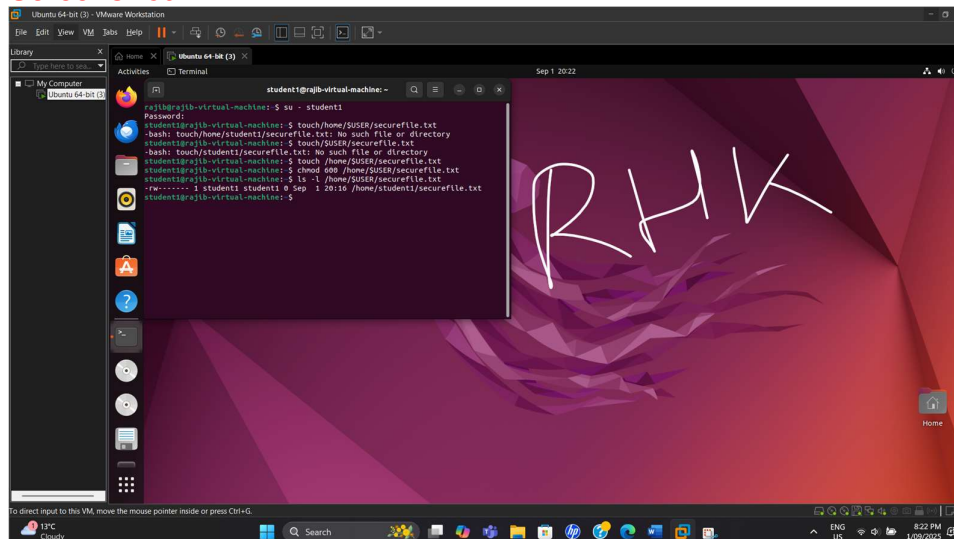
## Screenshot



### 3. Verify permissions:

*ls -l /home/\$USER/securefile.txt*

## Screenshot



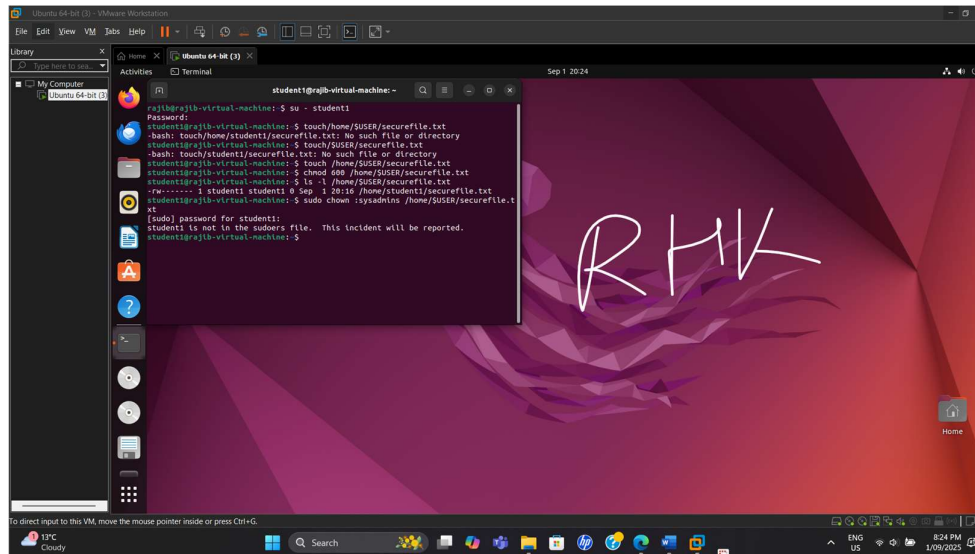
### 4. Change ownership of the file to the sysadmins group:

*sudo chown :sysadmins /home/\$USER/securefile.txt*

## Screenshot



|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |



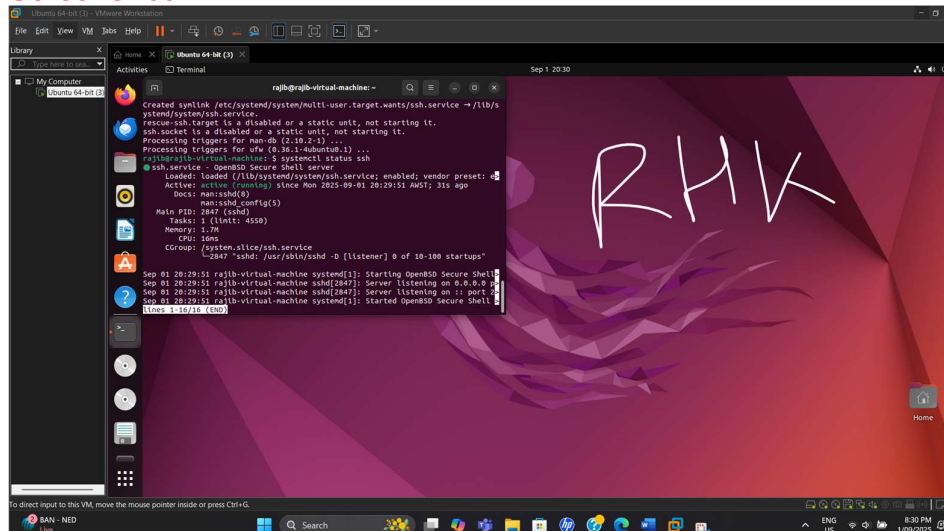
## Step 5: Managing and Monitoring Services

Take screenshots of each command output.

1. Check the status of a running service (e.g., SSH):

*systemctl status ssh*

### Screenshot



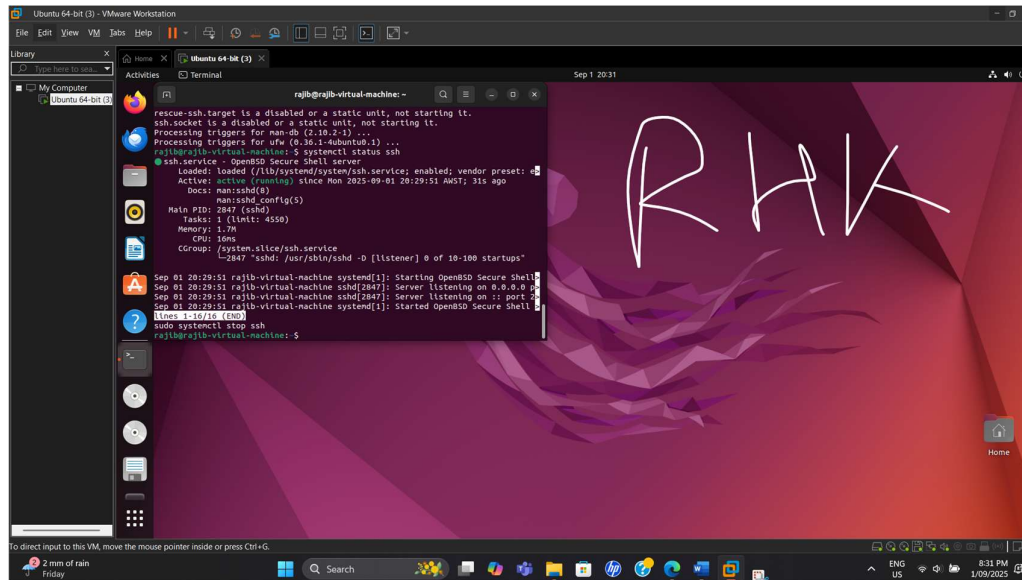
2. Stop the service:

*sudo systemctl stop ssh*

### Screenshot



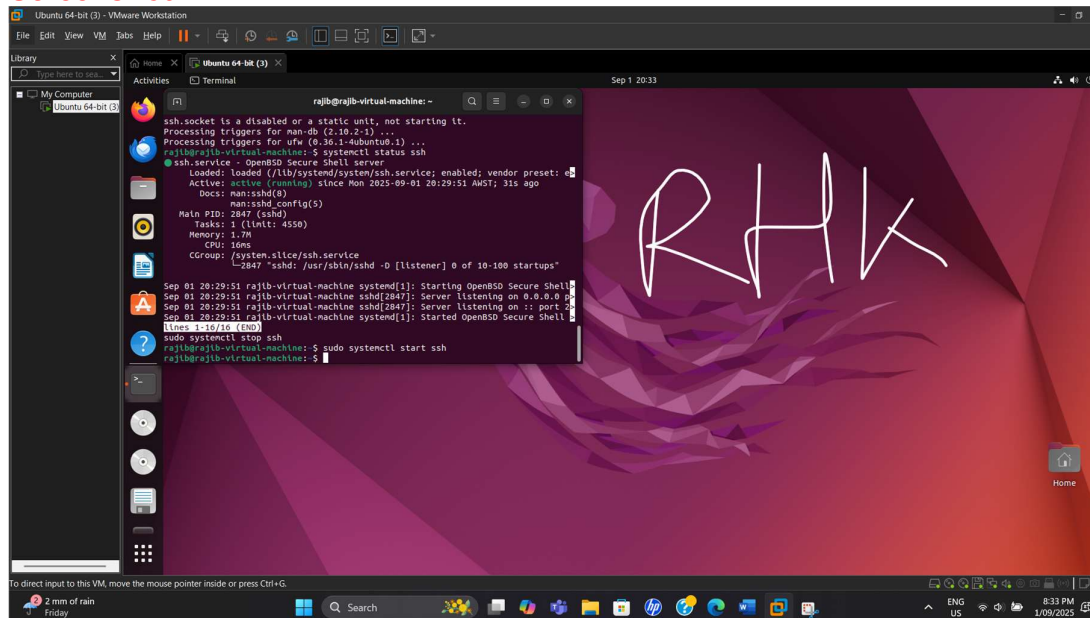
|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |



### 3. Restart the service:

*sudo systemctl start ssh*

### Screenshot



### 4. Disable an unnecessary service (e.g., cups for printers):

*sudo systemctl disable cups*



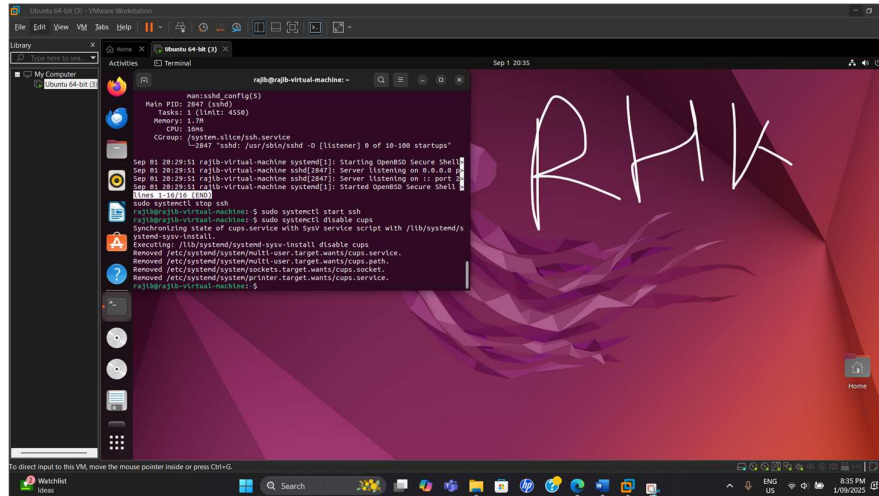
Qualification national code and title

AE780 Transition to Cyber Security Skillset

Unit/s national code/s and title/s

VU23214: Configure and secure networked end points

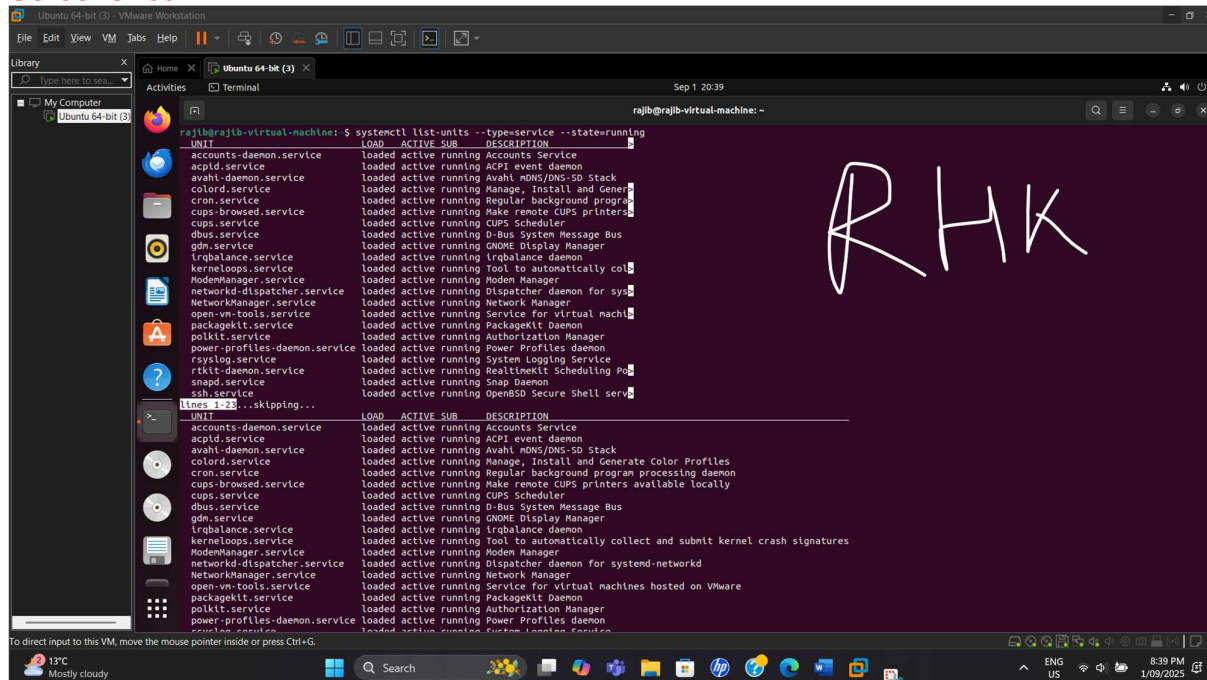
## Screenshot



5. Verify service management with:

*systemctl list-units --type=service --state=running*

## Screenshot



## Step 6: Basic Networking Commands

Take screenshots of each command output.

1. Check network configuration:

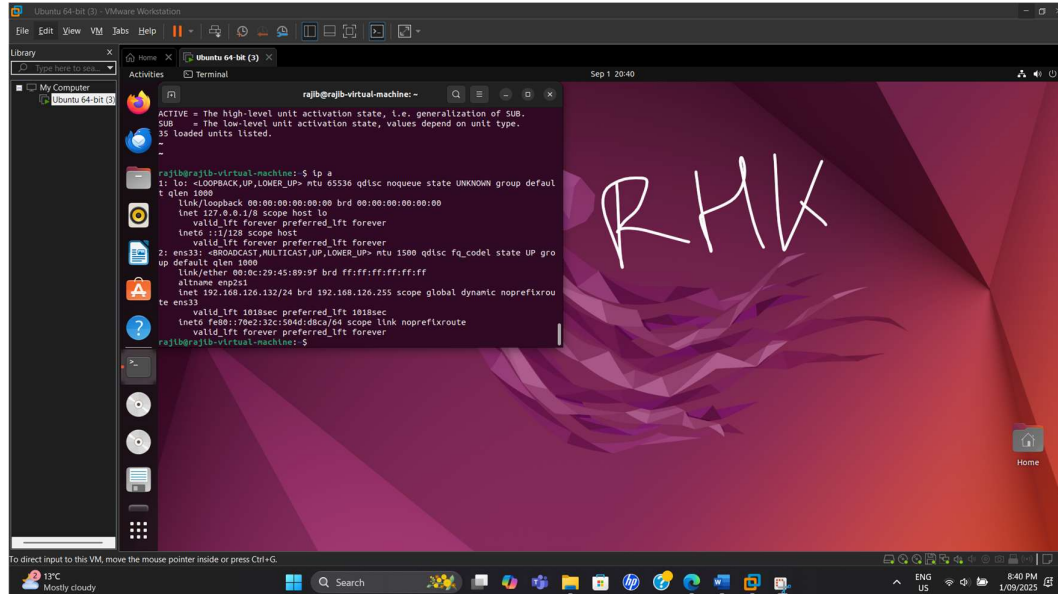




|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

*ip a*

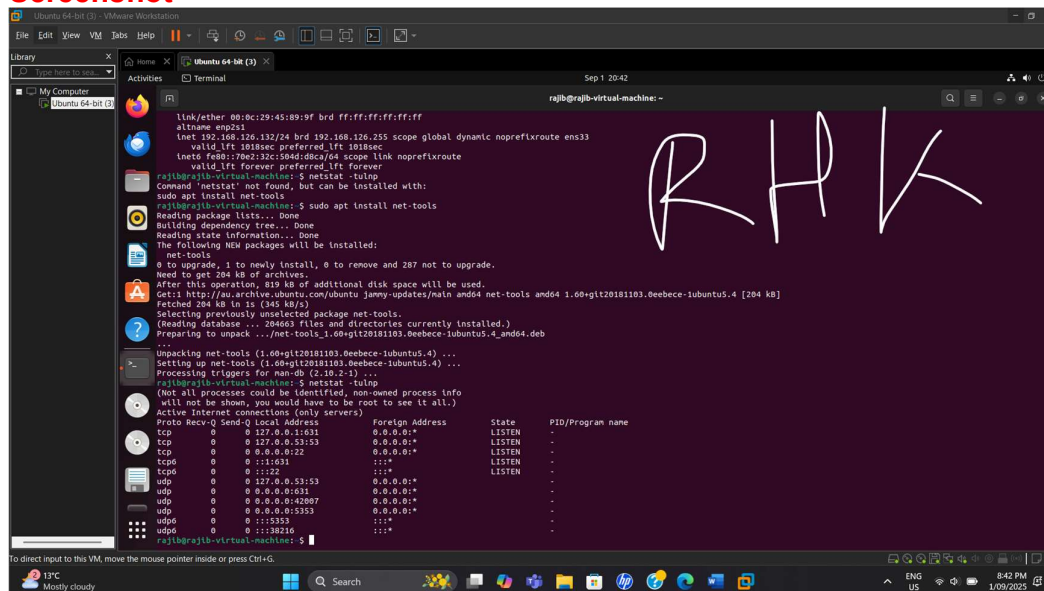
## Screenshot



2. Display active network connections:

*netstat -tulnp*

## Screenshot



3. Test connectivity to google.com:

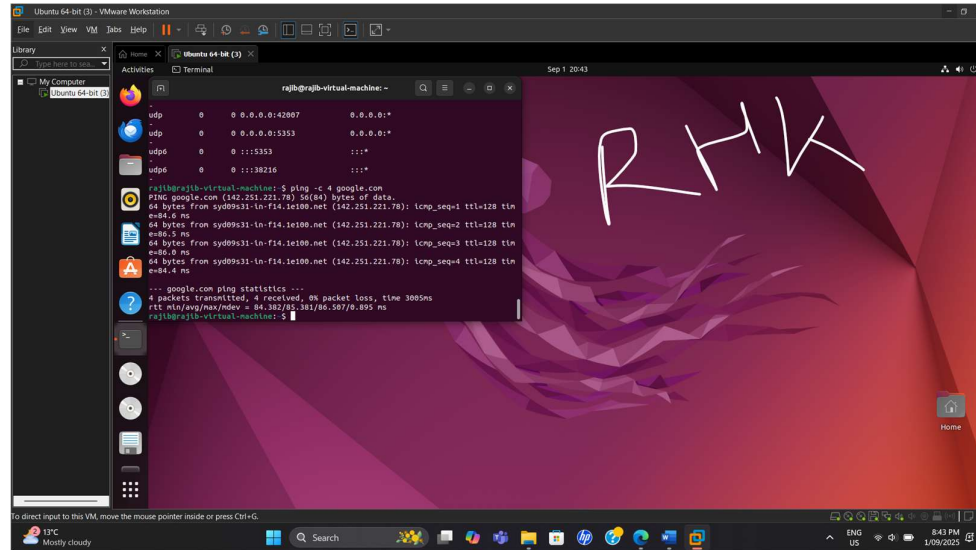
*ping -c 4 google.com*





|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

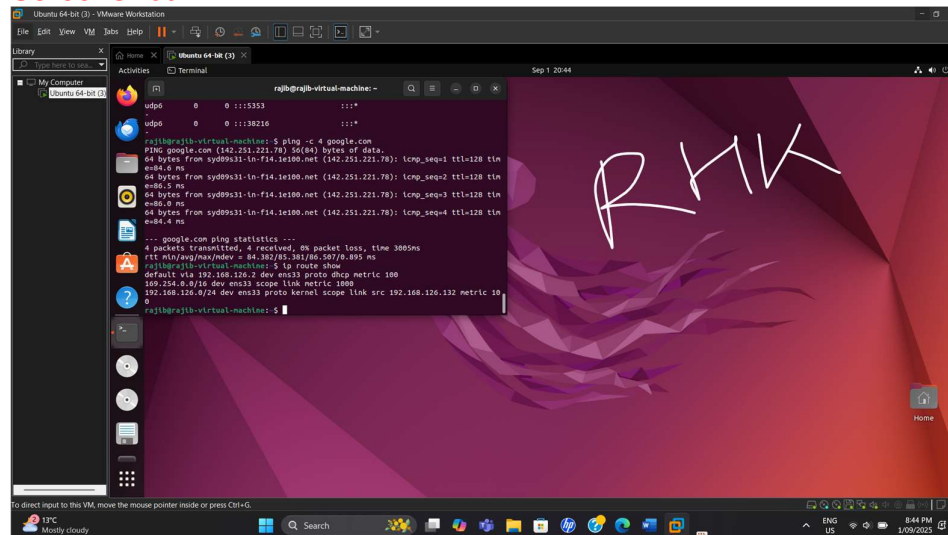
## Screenshot



### 4. Display routing table:

*ip route show*

## Screenshot



### 5. Find the IP address of a domain:

*nslookup google.com*

## Screenshot



|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| Qualification national code and title | AE780 Transition to Cyber Security Skillset        |
| Unit/s national code/s and title/s    | VU23214: Configure and secure networked end points |

