HW 05 – Linux

By :- Faraz Ahmed

Contents

1. Adding Firewall Rules

- To allow AdminNet to access pfSense Router webConfiguration GUI, we need to a new firewall rule in AdminNet as highlighted (or checked) in Figure 1 below. In Source, we have to enter “AdminNet Address” and in destination, we have to enter “Address of pfSense” and “HTTPS” should be the default port.

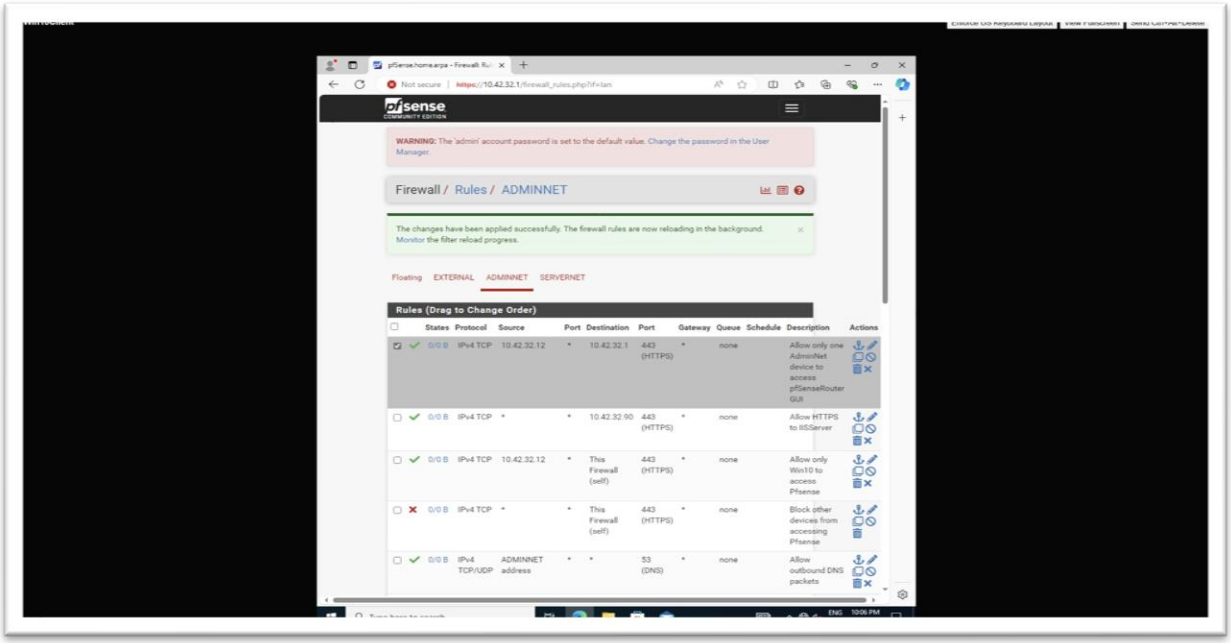

Figure 1: Screenshot of New “Highlighted” Firewall Rules in AdminNet.

- As we can see from figure 2, all new 6 firewall rules from which one is used to block “All Inbound Traffic from External devices to ServerNet” then another one is to allow “AdminNet to access ServerNet” and then rest is to allow “HTTP/HTTPS, DNS and ICMP(Ping) from ServerNet” as shown in highlighted (or checked) Figure 2.

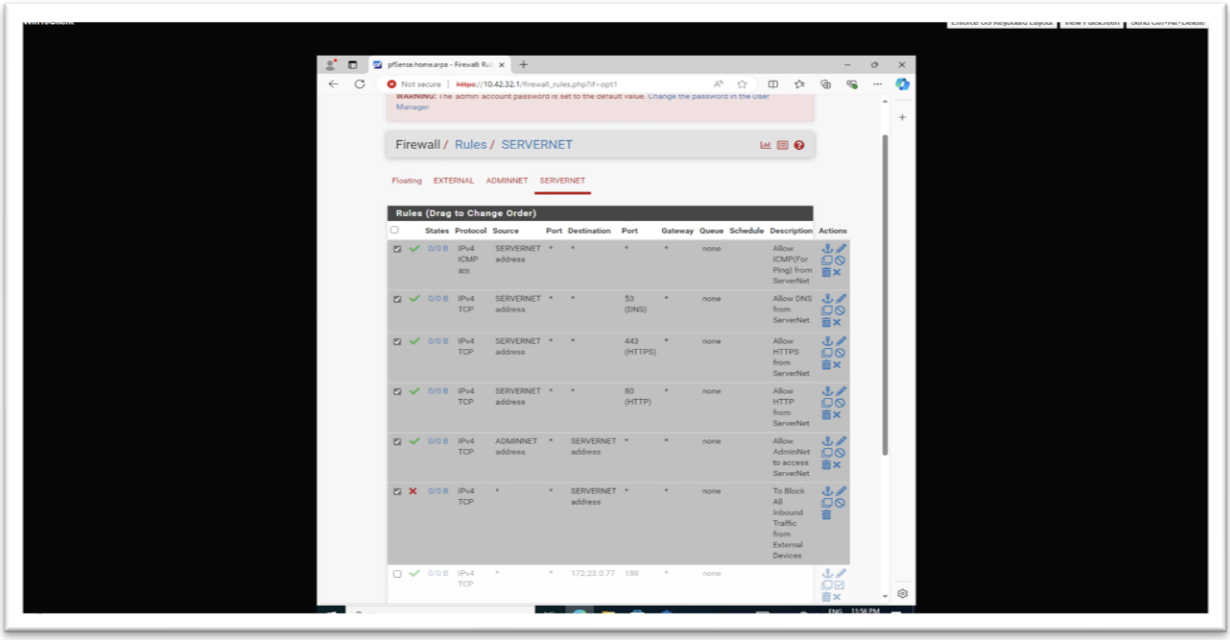

Figure 2: Screenshot of New “Highlighted” Firewall Rules in ServerNet.

2. Linux Server Setup

a. Install and configure the UbuntuWebServer VM

- As we can notice in Figure 3, we type “ip r” command to display connection properties of UbuntuWebServer VM as highlighted below.

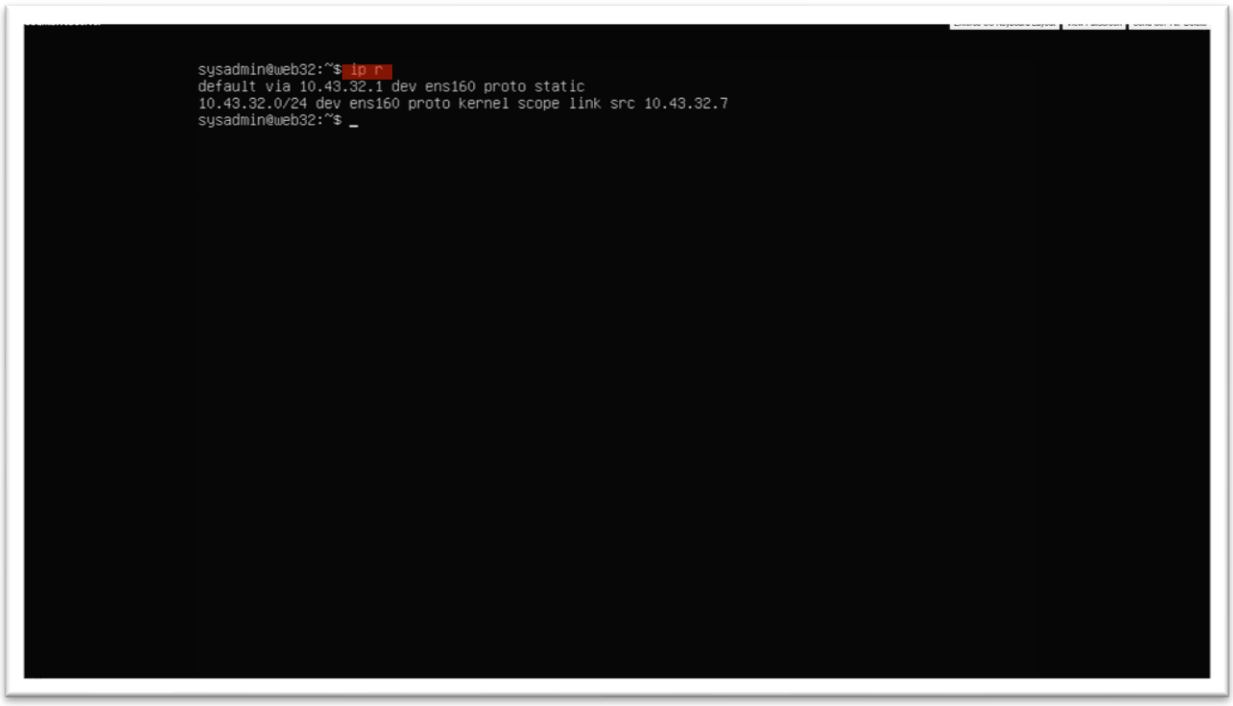

Figure 3: Screenshot of “ip r” command in UbuntuWebServer VM.

- Now to ping dns.google i.e. “ping 8.8.8.8” to check connection of device with DNS of Google as highlighted in Figure 4.

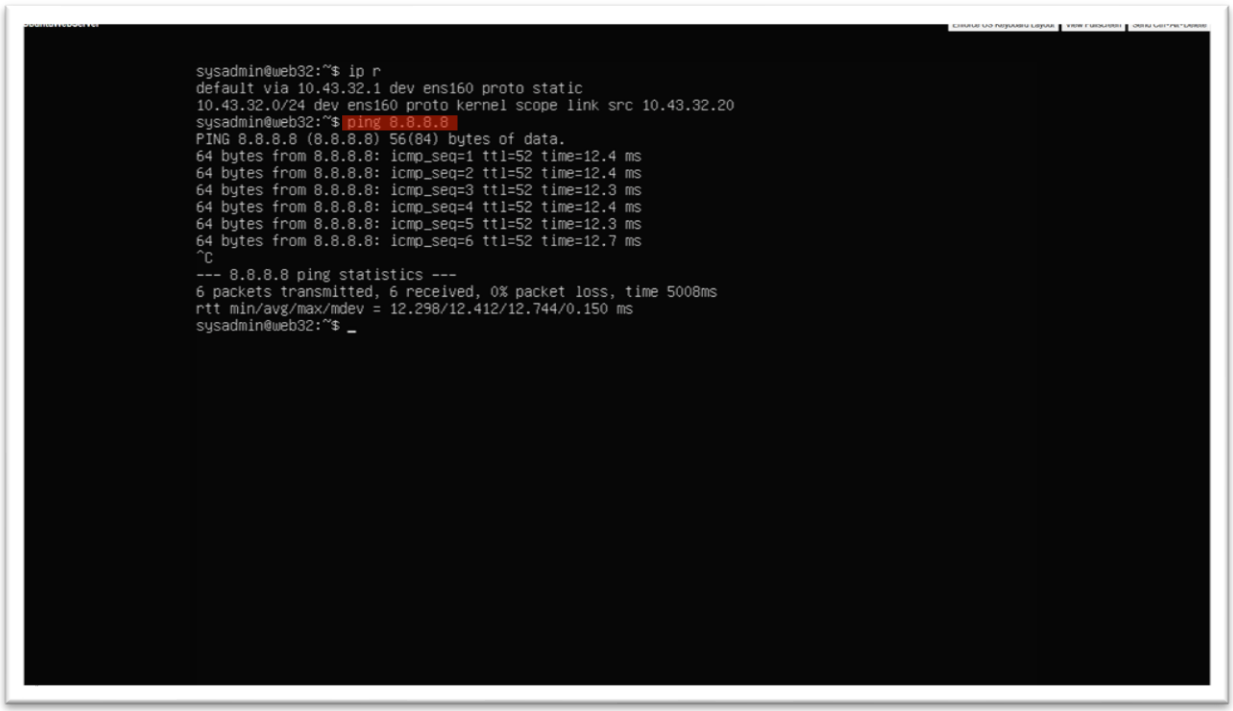

Figure 4: Screenshot of “ping 8.8.8.8” command in UbuntuWebServer.

➢ Now, we enter “sudo apt update” to update the operating system for this VM as highlighted in Figure 5.

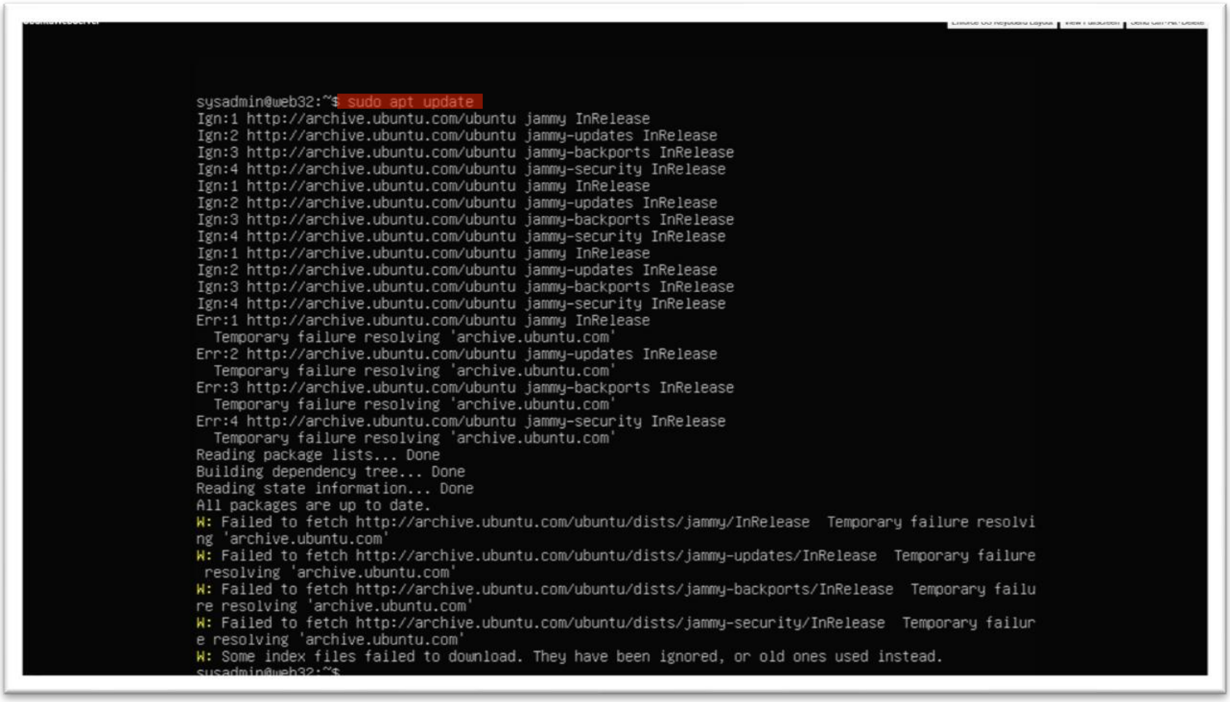

Figure 5: Screenshot of “sudo apt update” to update OS.

➢ After that, we enter “sudo apt open-vm-tools” to install VMWare tools in this VM as highlighted in Figure 6.

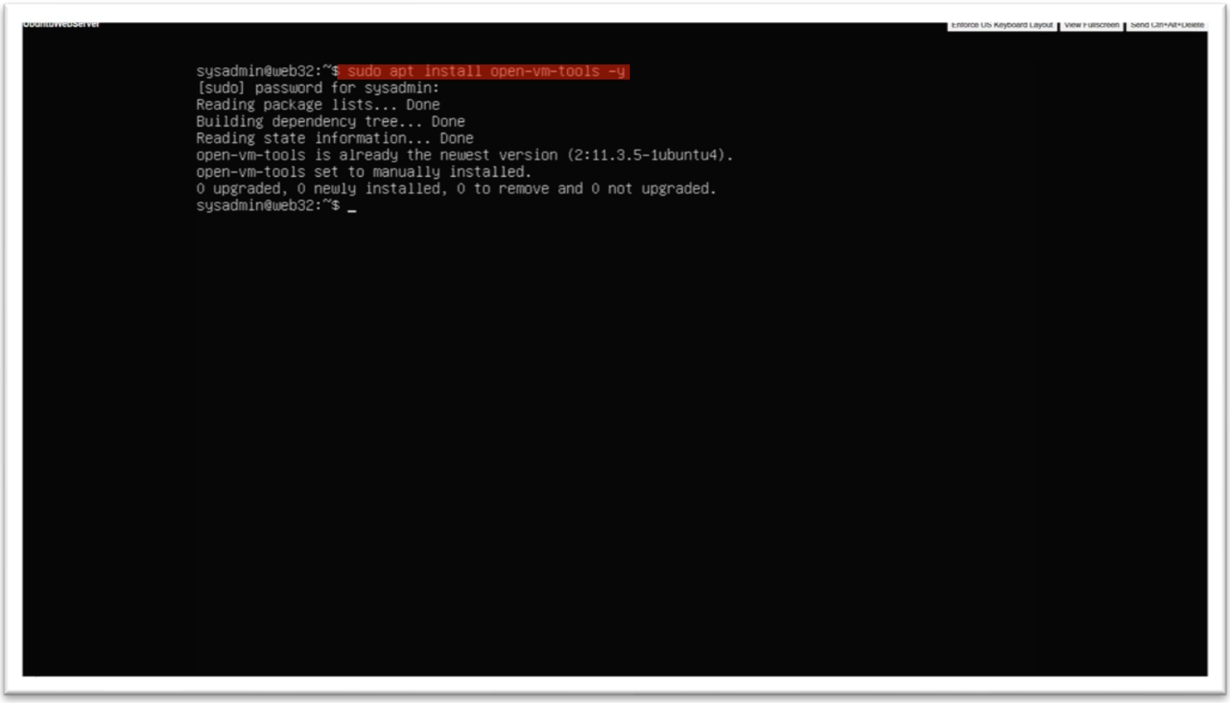

Figure 6: Screenshot of “sudo apt install open-vm-tools” to install VMWare Tools.

- Now we enter “sudo systemctl status open-vm-tools” to check the status of VMWare tools if its installed and working or not as highlighted in Figure 7.

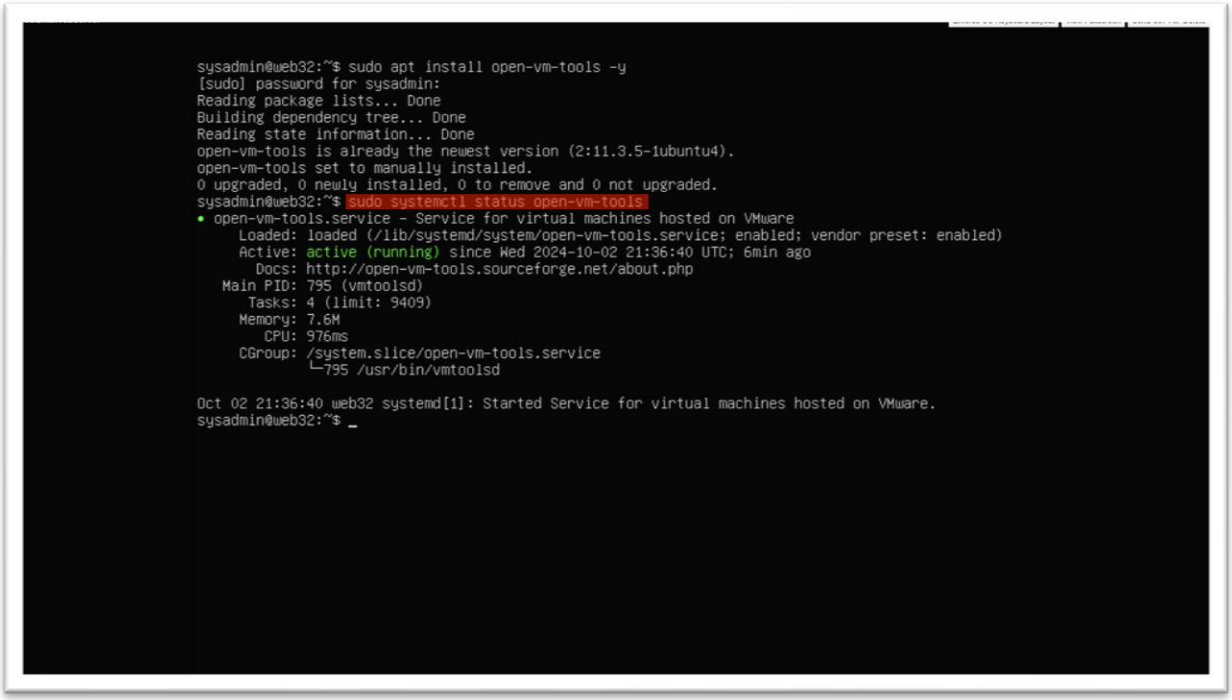

Figure 7: Screenshot of “sudo systemctl status open-vm-tools” to check status of VMWare tools.

- After that we enter “sudo apt install apache2 libapache2-mod-php php php-mysql php-xml php-mbstring php-apcu php-intl php-gd php-cli php-curl imagemagick inkscape git openssh-server” to install apache2 service. And we can observe the result in Figure 8 and Figure 9.

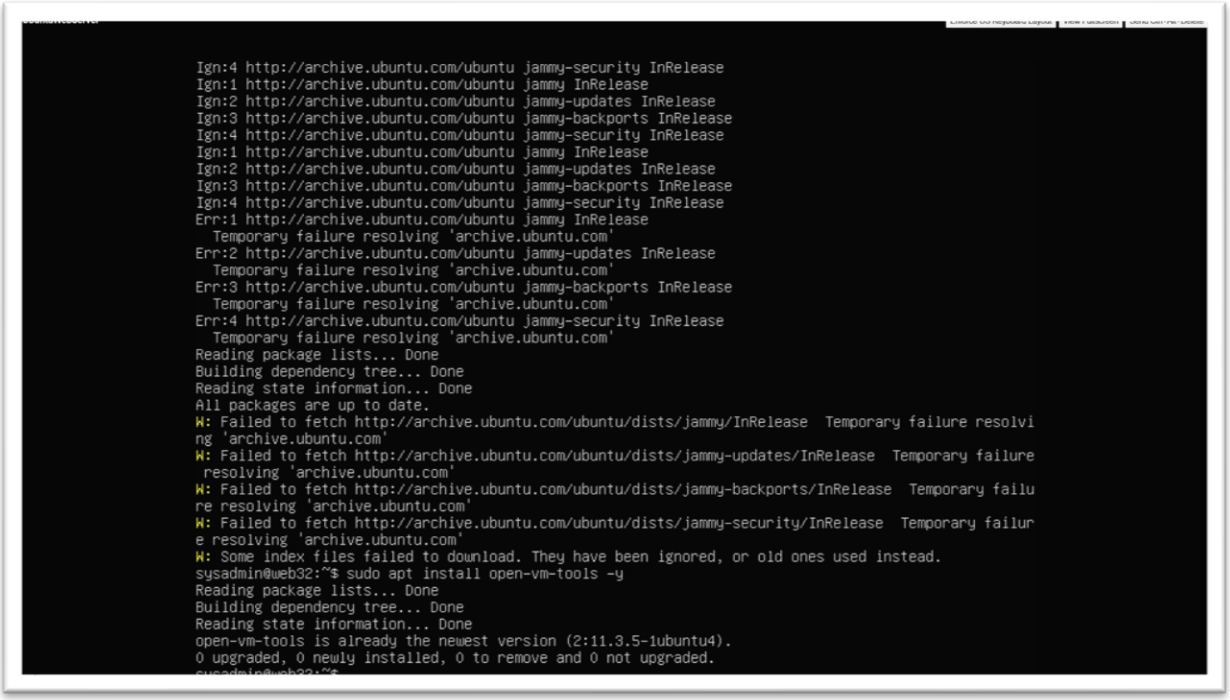

Figure 8: Screenshot of result of “sudo apt install apache2 libapache2-mod-php php php-mysql php-xml php-mbstring php-apcu php-intl php-gd php-cli php-curl imagemagick inkscape git openssh-server” in installation of apache2 service.

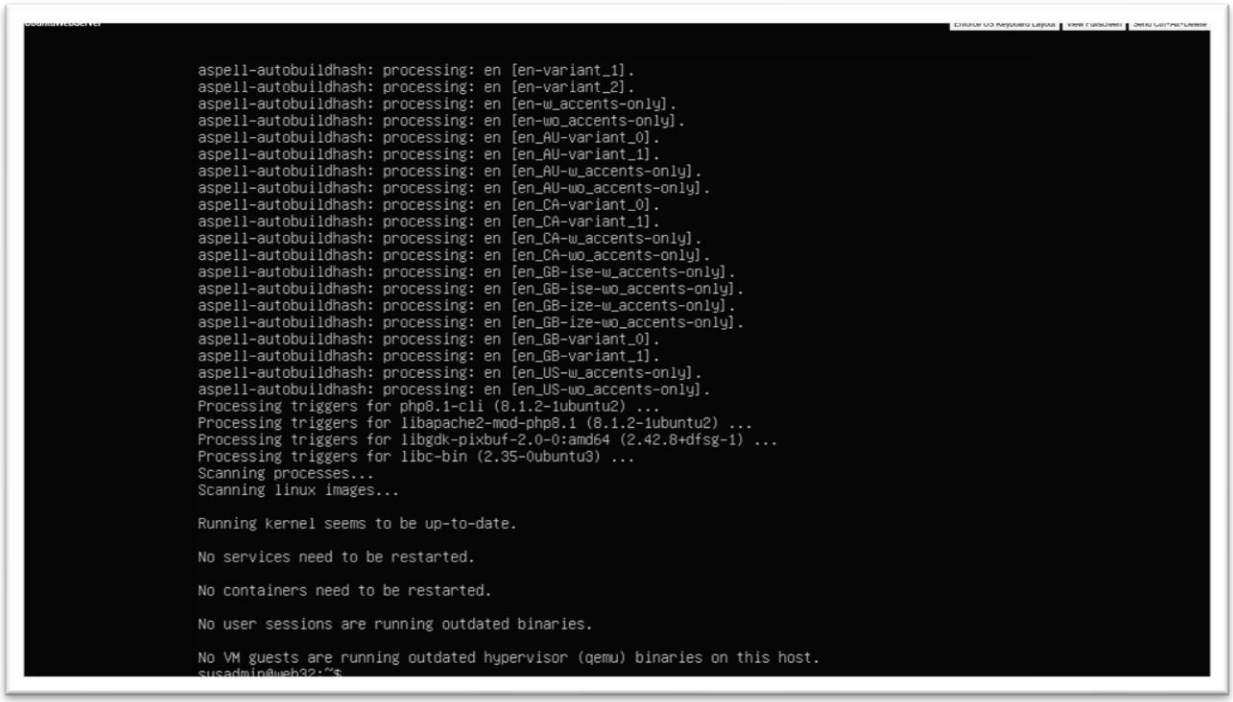

Figure 9: Screenshot of result of "sudo apt install apache2 libapache2-mod-php php php-mysql php-xml php-mbstring php-apcu php-intl php-gd php-cli php-curl imagemagick inkscape git openssh-server" in installation of apache2 service.

b. Install and Configure the RockyDBServer VM

- We enter "ip r" command to display connection properties of RockyDBServer as highlighted in Figure 10.

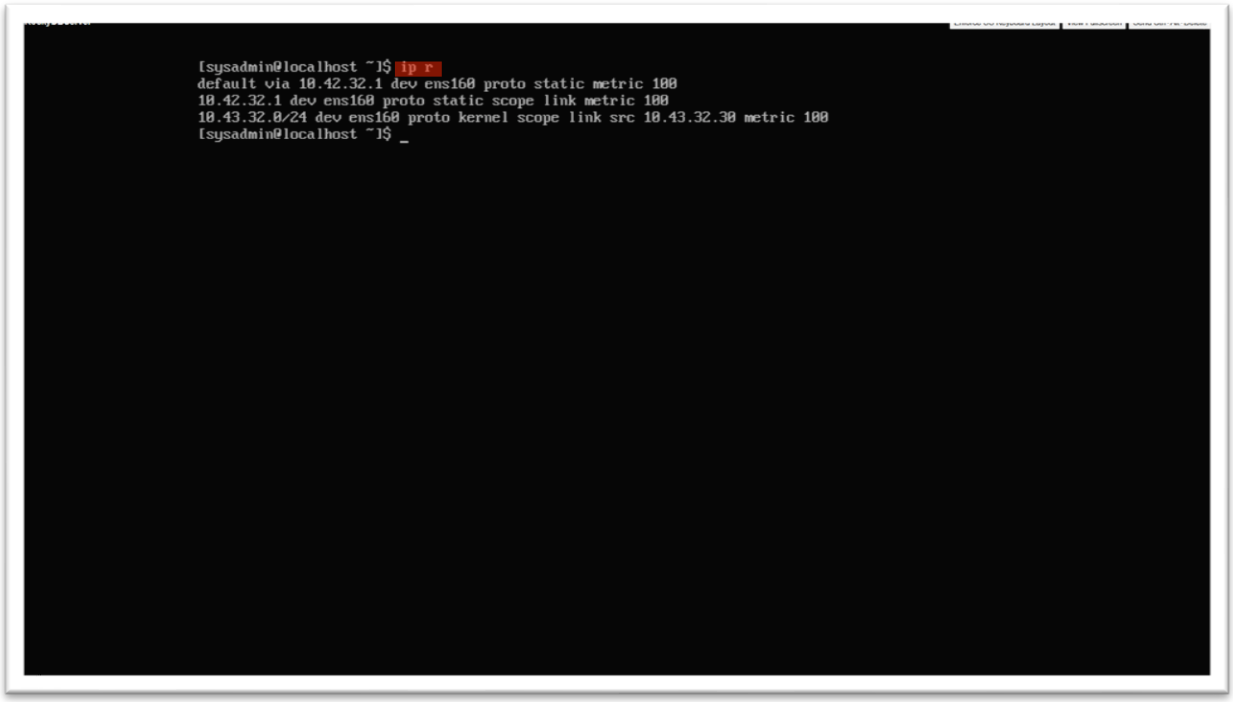

Figure 10: Screenshot of "ip r" command in RockyDBServer.

- After that, we enter “ping 8.8.8.8” to ping the DNS of Google to communicate with it as shown in Figure 11.

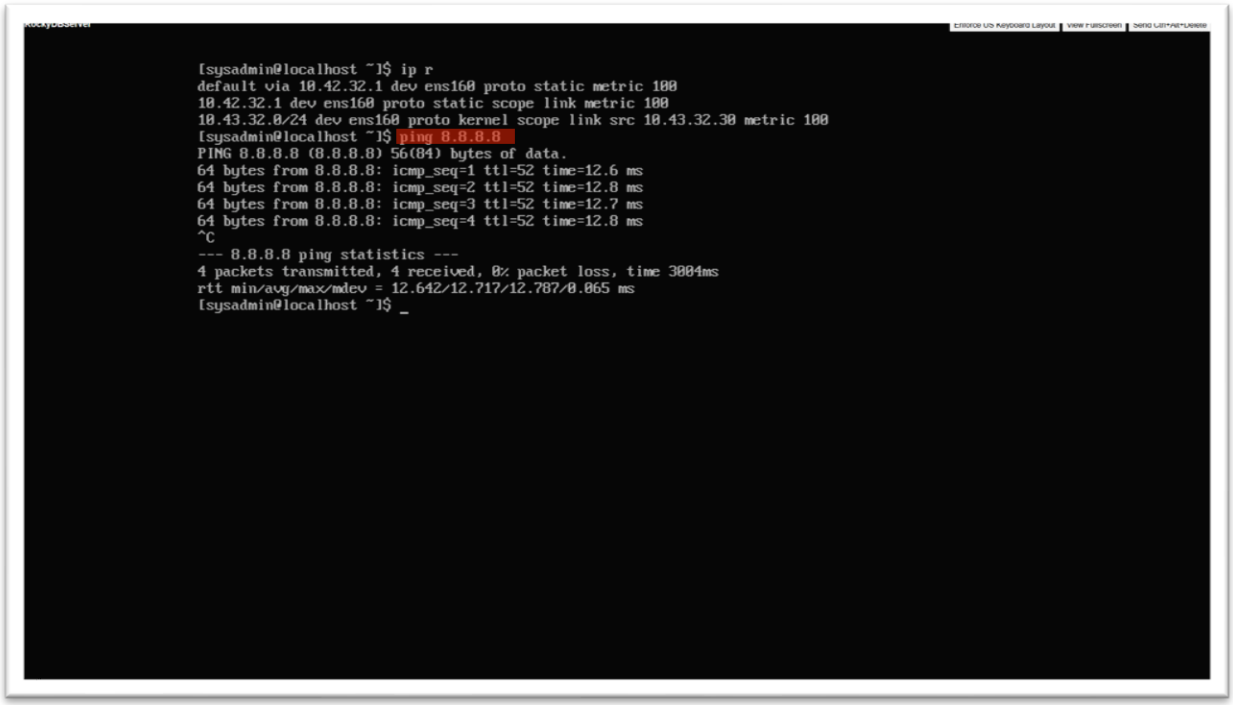

Figure 11: Screenshot of “ping 8.8.8.8” command in RockyDBServer.

- Now we enter “sudo yum update” to update the operating system of RockyBDServer. So we can see the result of that command in Figure 12 and 13.

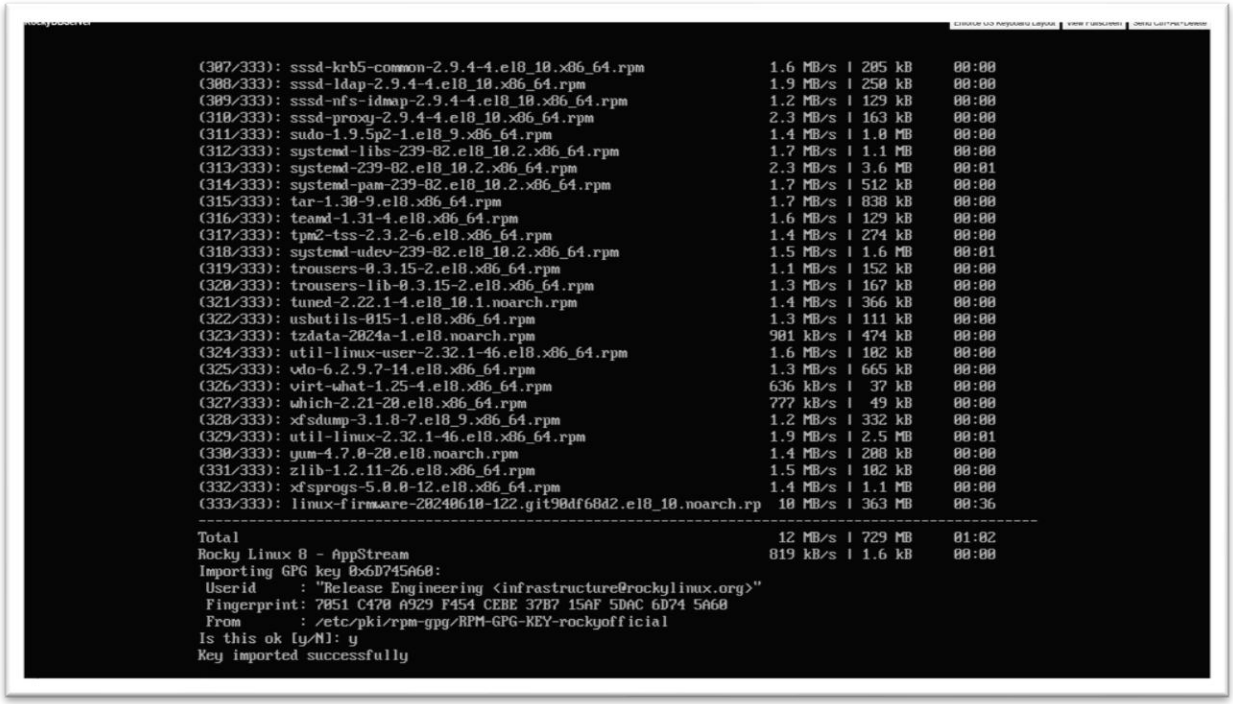

Figure 12: Screenshot of result for “sudo yum update” command in RockyBDServer.

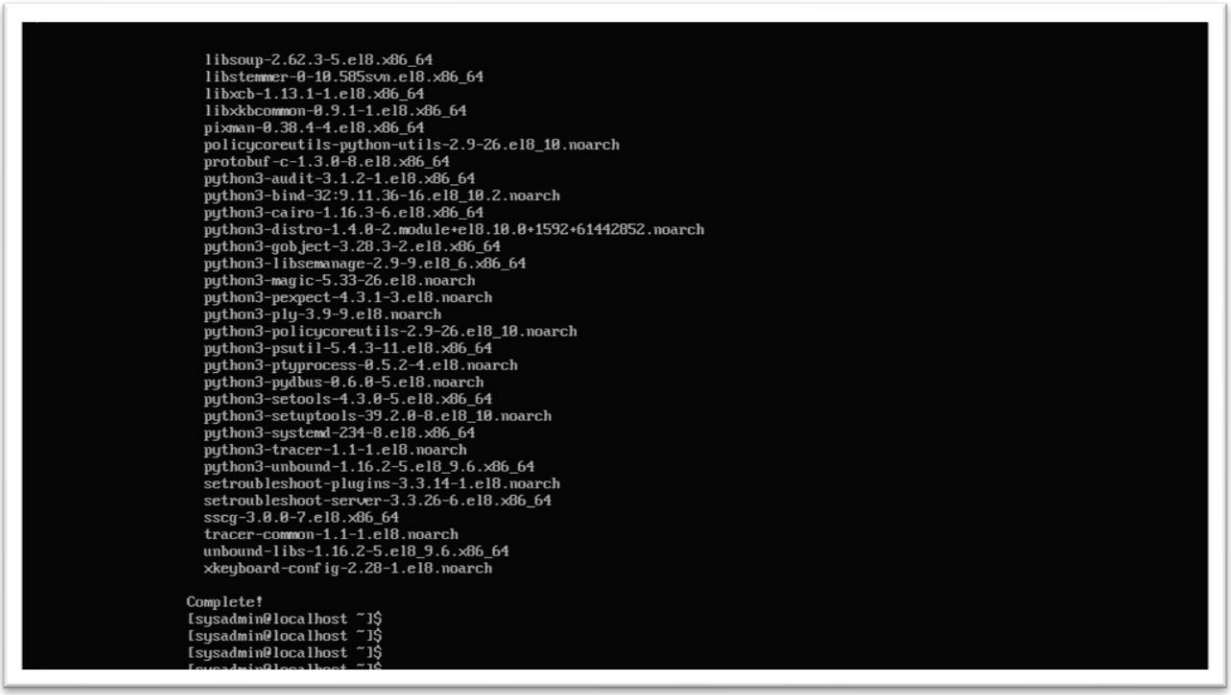

Figure 13: Screenshot of result for "sudo yum update" command in RockyBDServer.

- Now to enter "sudo yum install open-vm-tools" to install VMWare Tools in RockyBDServer and the result is in Figure 14.

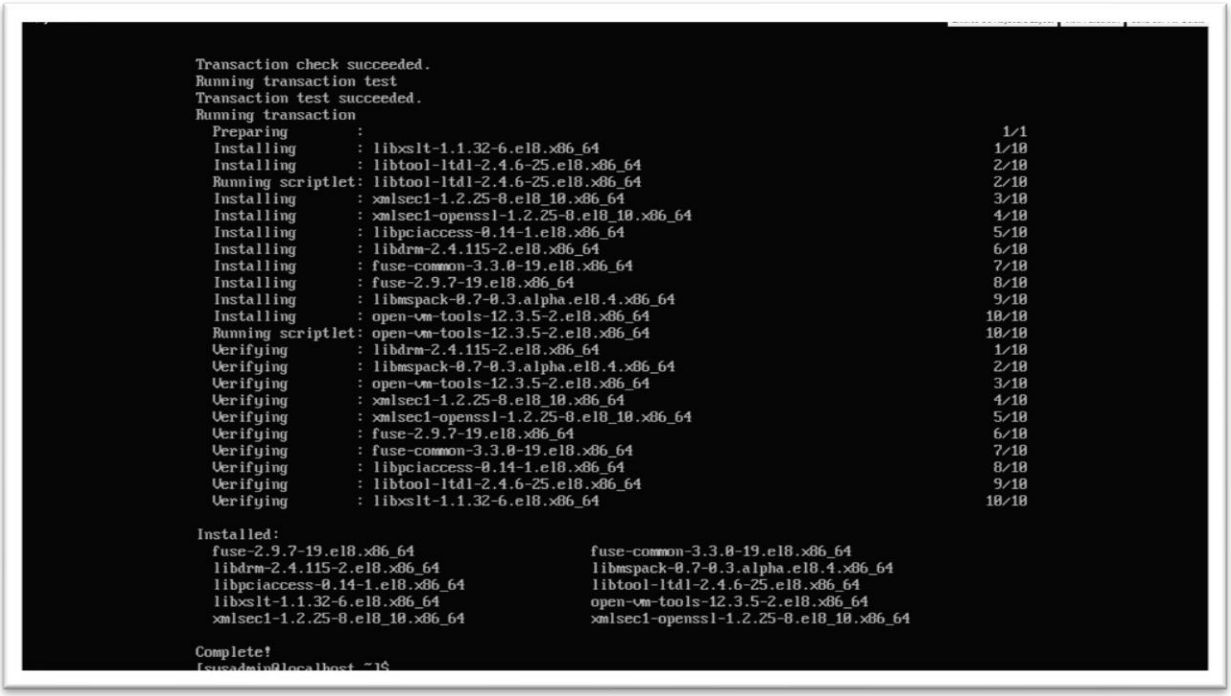

Figure 14: Screenshot of Result for "sudo yum install open-vm-tools" command in RockyBDServer.

- So to verify the installation of VMWare Tools, we use “sudo systemctl enable vmtoolsd” and “sudo systemctl start vmtoolsd” as highlighted and we can see the result as shown in Figure 15.

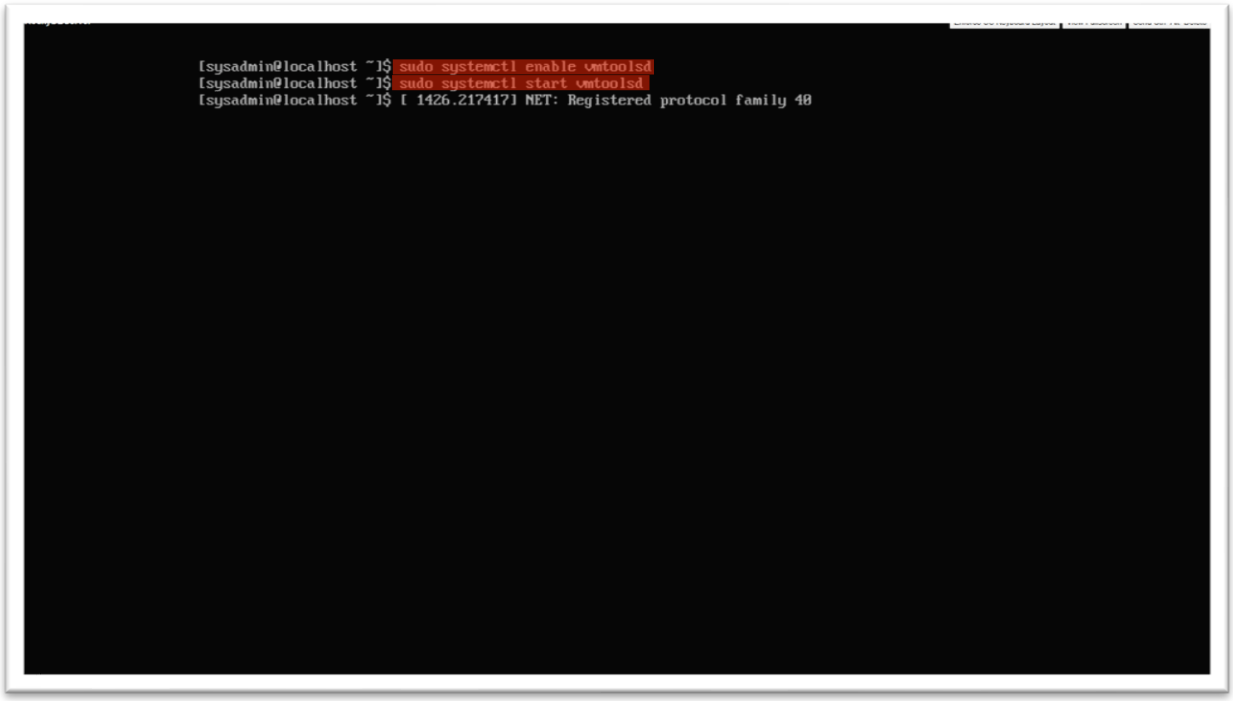

Figure 15: Screenshot of verify VMWare Tools by “sudo systemctl start vmtoolsd”.

- Finally, now we install additional software packages by putting “sudo yum install mariadb-server” and the result of that command is shown in Figure 16.

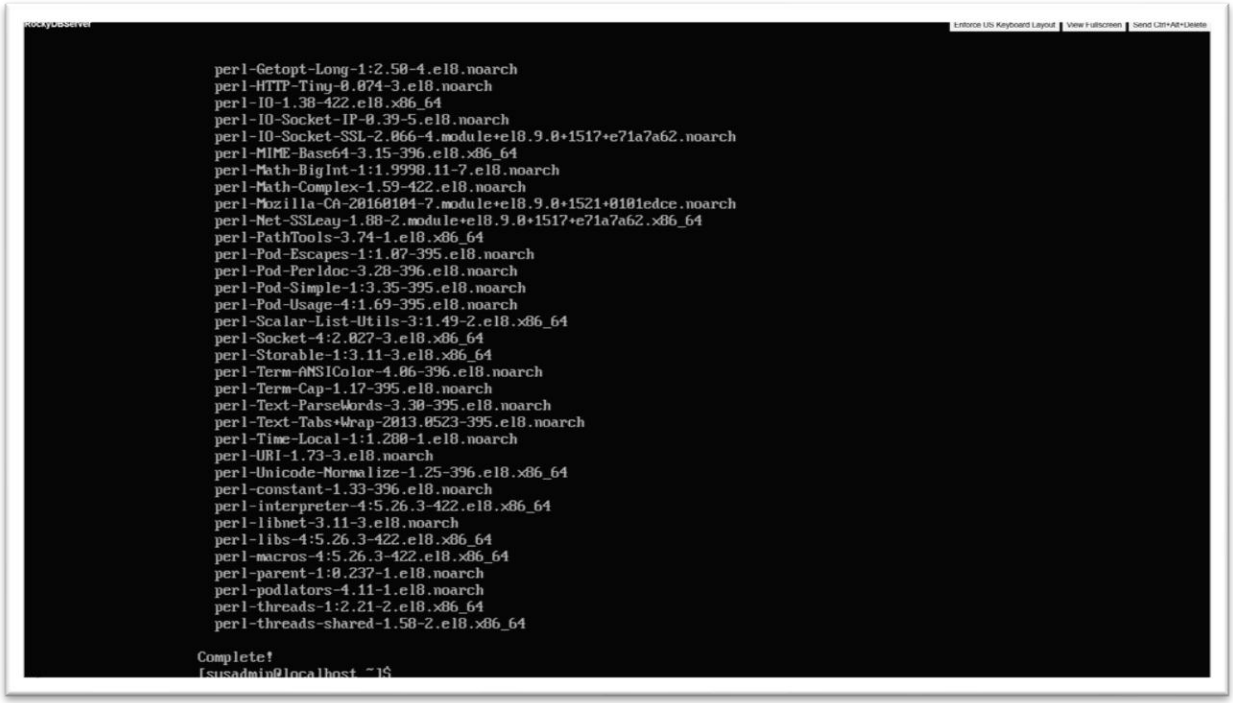

Figure 16: Screenshot of result of “sudo yum install mariadb-server” command in RockyBDServer.

3. User and Group Creation

- On “terminal”, we enter “sudo adduser fahmed29 (my UBITname) to add new user as highlighted in Figure 17. And enter the password as “Change.me!” and press “Enter” for rest of the information to get default values in that.

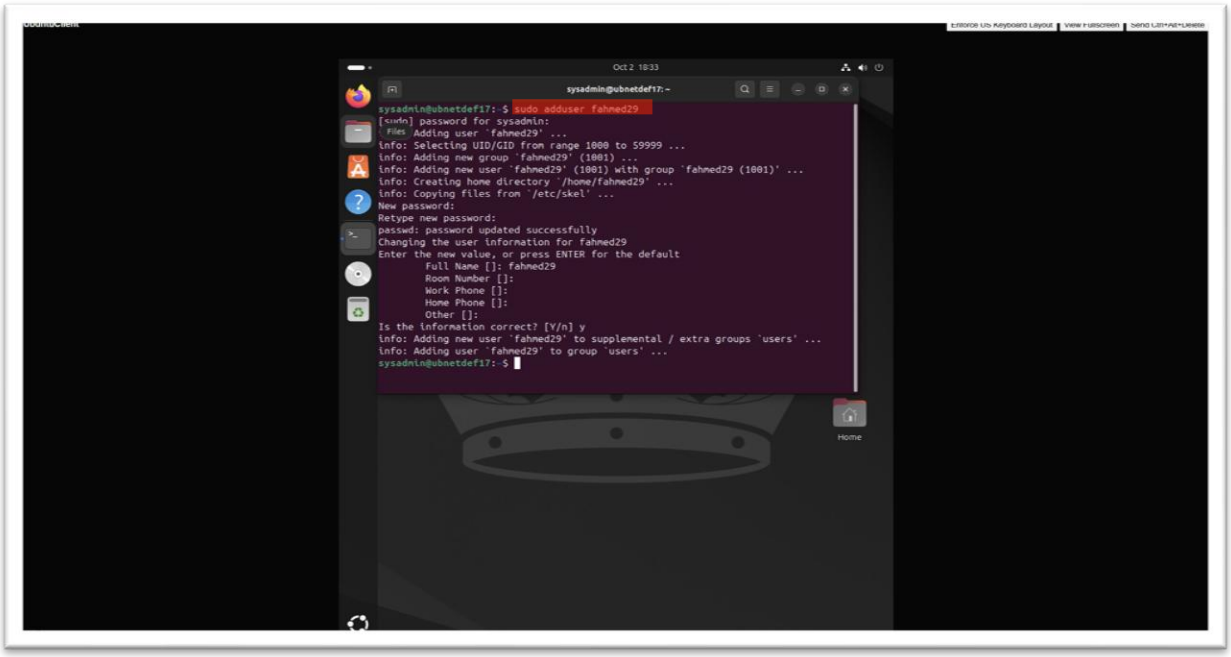

Figure 17: Screenshot of making new user using “sudo adduser fahmed29” command.

- Now we can also the new user using different commands- useradd command “sudo useradd -n -s /bin/bash kpcleary” where “-m” to create a home directory and “-s /bin/bash” to set the default shell to bash as shown in Figure 18. Also we can enter “sudo passwd kpcleary” to add password to that new user as highlighted in Figure 18.

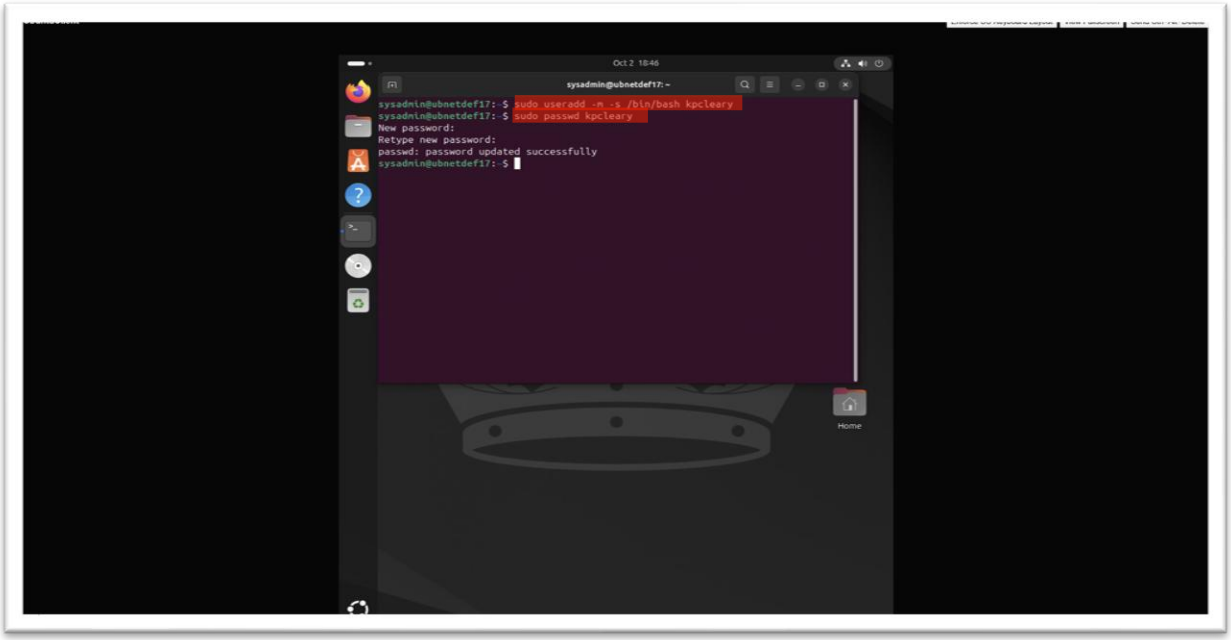

Figure 18: Screenshot of “sudo useradd -n -s /bin/bash kpcleary” command to add new user.

- Now to create a new group- UBNetDef using “sudo groupadd UBNetDef” as highlighted below and add new users vasudevb, ethanvia, pfox and kpcleary using command “sudo usermod -aG UBNetDef username” as highlighted in Figure 19.

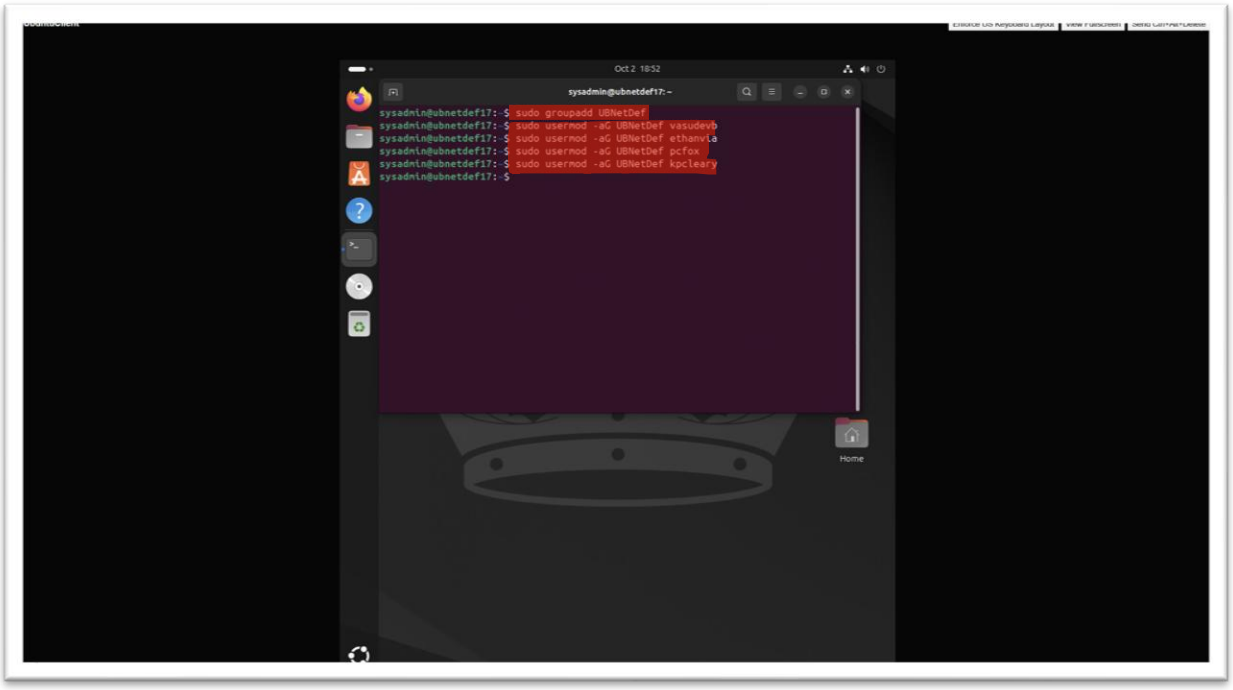

Figure 19: Screenshot of commands “sudo groupadd UBNetDef” to create new group and add users in that.

- After that, we create new group- BlackTeam using “sudo groupadd BlackTeam” as highlighted below and also add new users vasudevb, ethanvia and pcfox using command “sudo usermod -aG BlackTeam username” as highlighted in Figure 20.

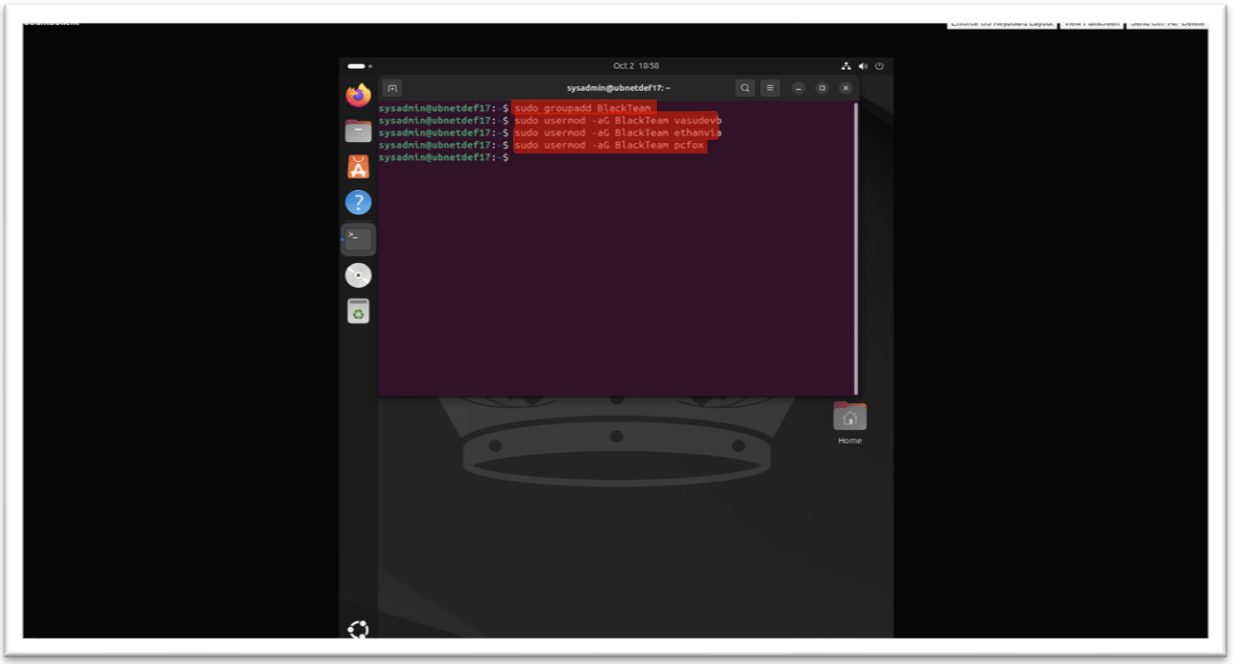

Figure 20: Screenshot of commands “sudo groupadd BlackTeam” to create new group and also add users to it.

- Now, we create new group “SysSec” using same commands and adding new user “fahmed29” by also using same adding command.

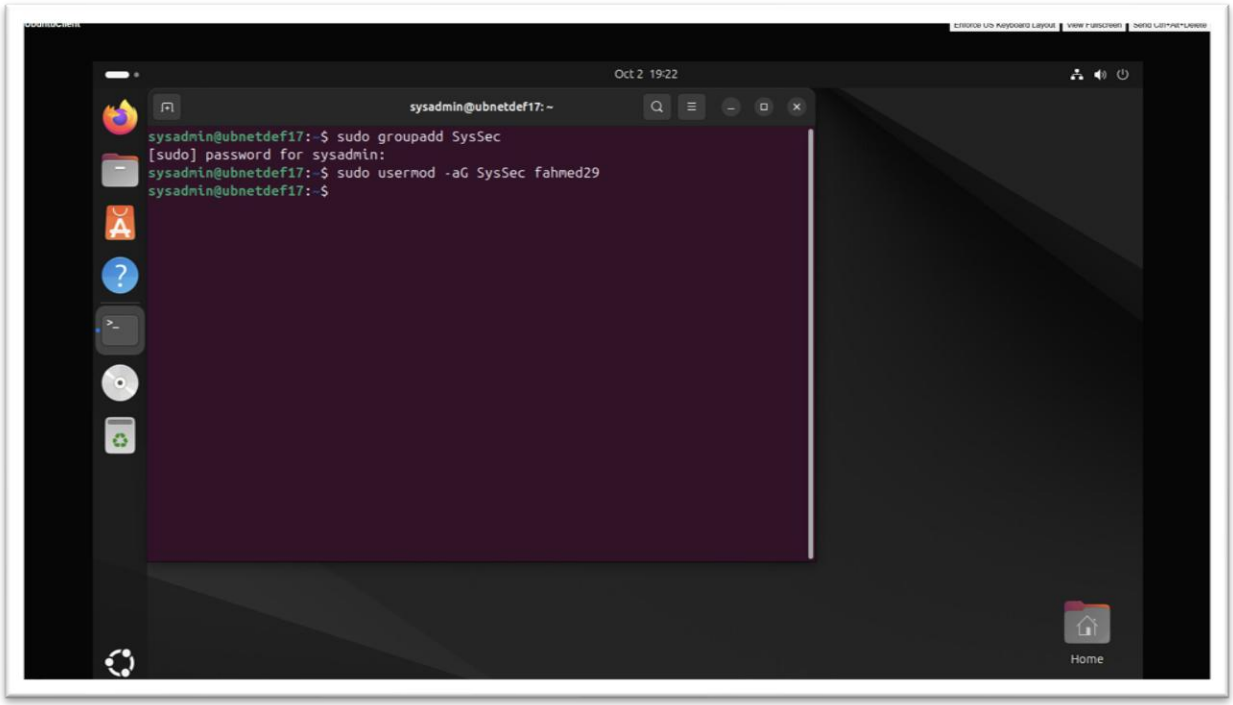

Figure 21: Screenshot of commands “sudo groupadd SysSec” to create new group and also add users to it.

- So now, we use “getent group BlackTeam” command to list and verify all members or users of that group.

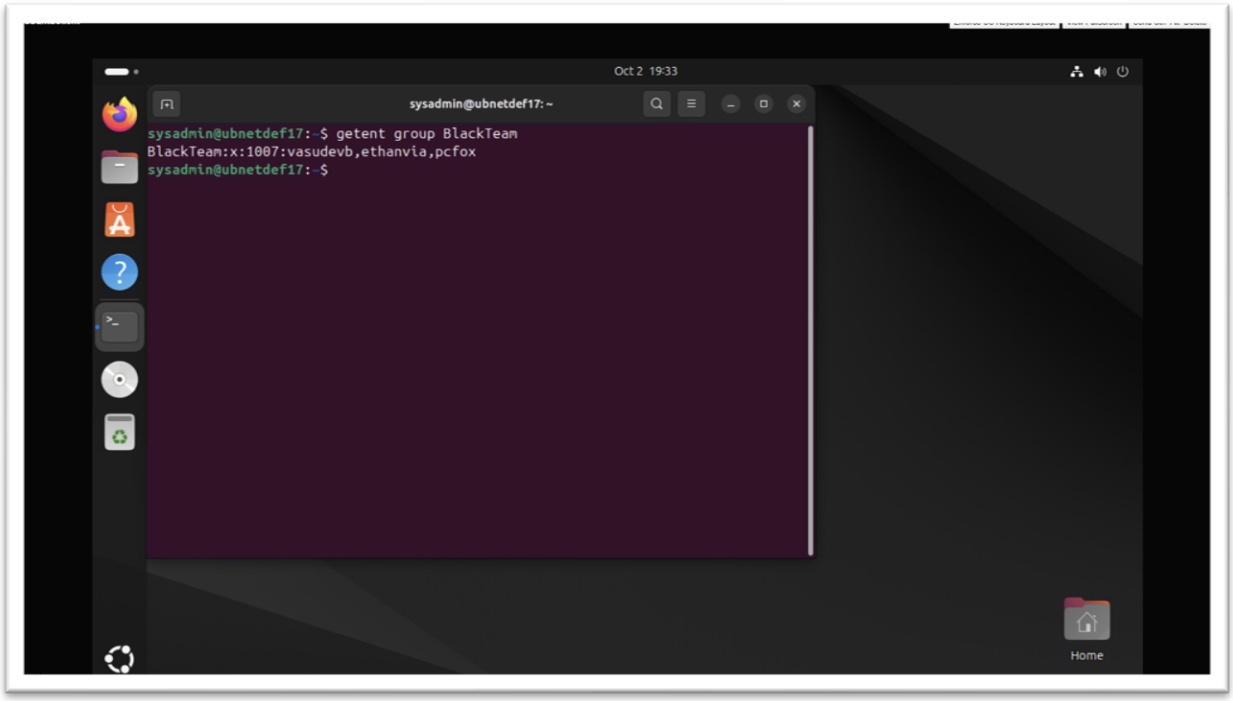

Figure 22: Screenshot of using command “getant group BlackTeam” to list all users.

4. Using Linux Hardening

- Now to edit the database of password in location "/etc/login.defs" so we enter "sudo nano /etc/login.defs" as highlighted in Figure 23.

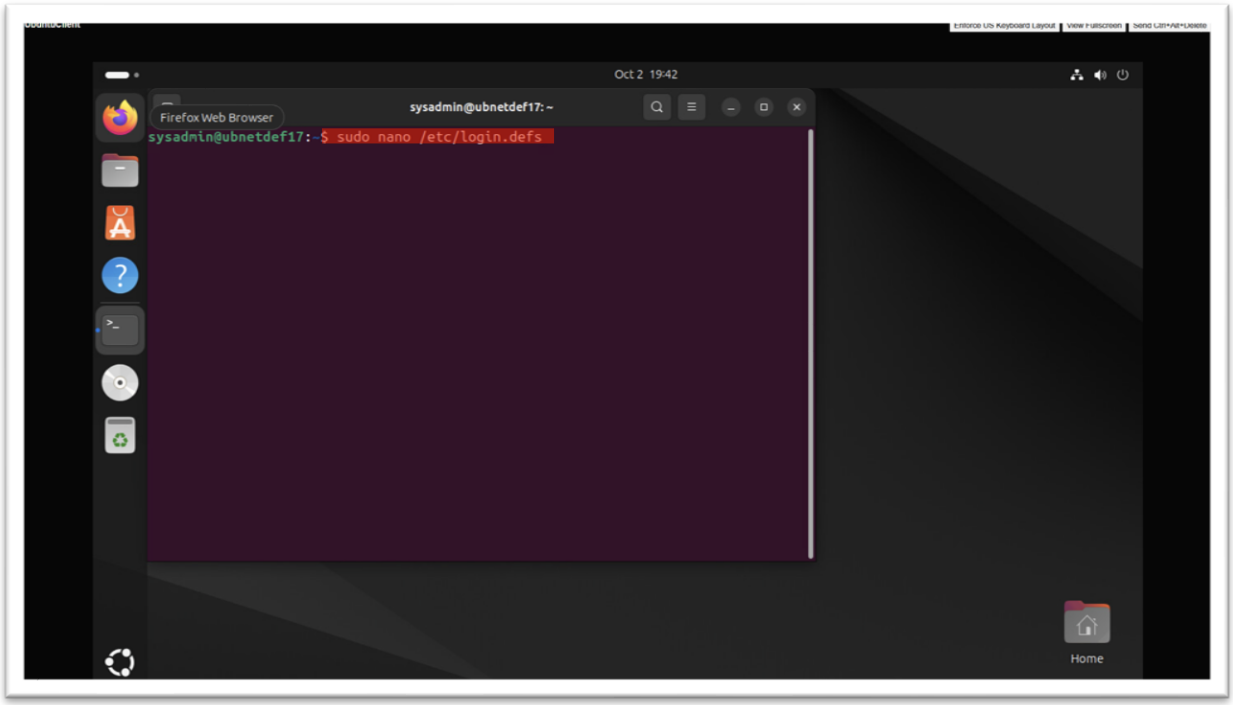

Figure 23: Screenshot of "sudo nano /etc/login.defs" to edit password policy.

- Now edit the number in "PASS_MAX_DAYS" to 70 days and then press ctrl+X then save it and press Enter to exit Sudo as shown below.

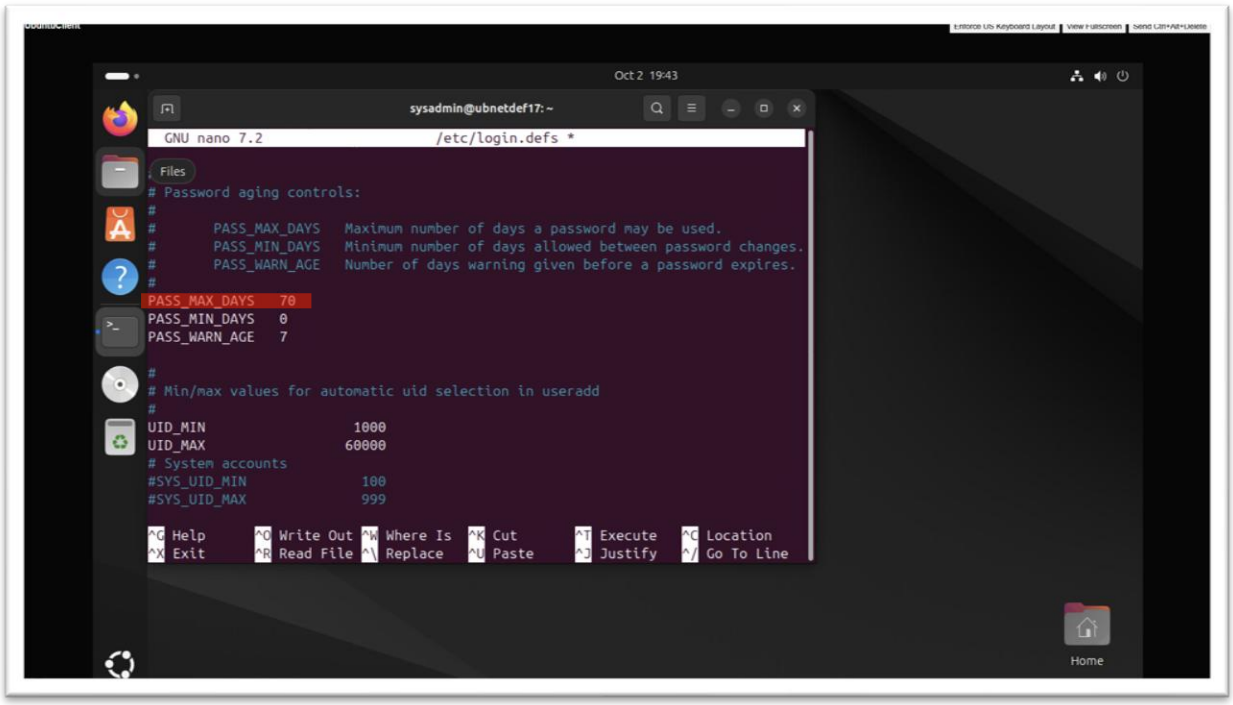

Figure 24: Screenshot of editing "PASS_MAX_DAYS" to 70 days to change password policy.

- Now enter “Apply Security Updates Only” to the “sysadmin” i.e. “sudo apt install unattended-upgrades” and we can observe that it is able to run as shown in Figure 25.

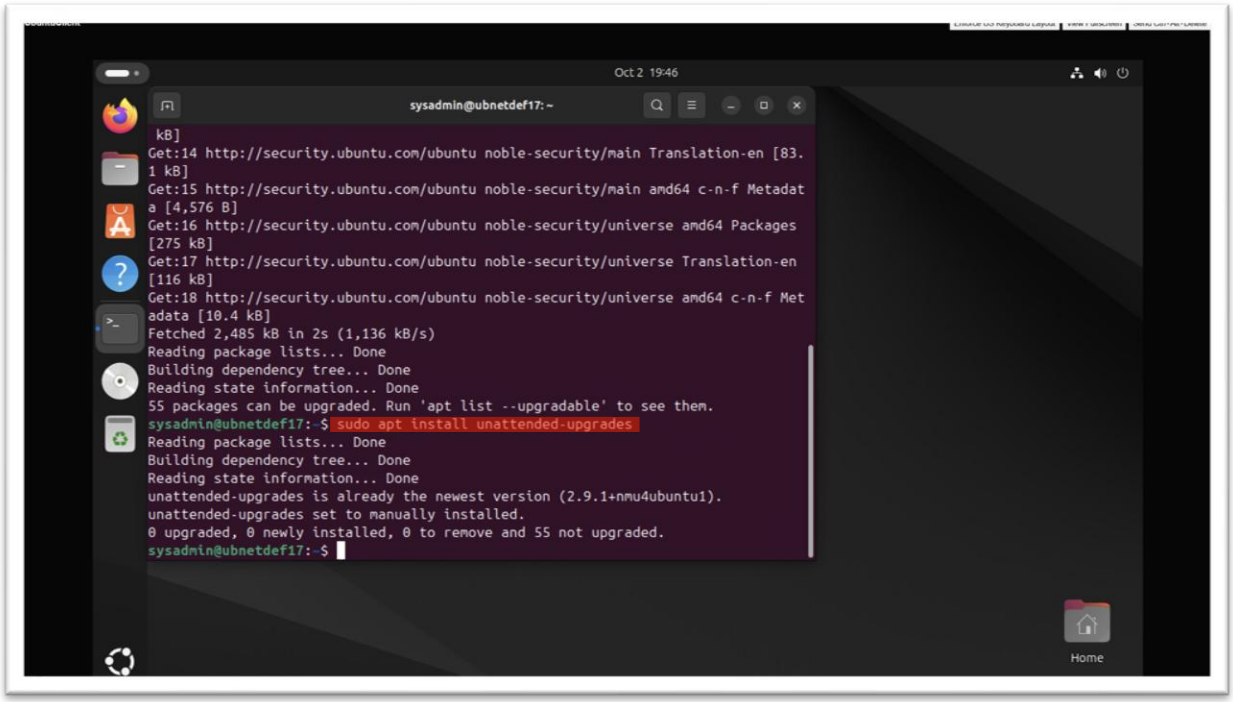

Figure 25: Screenshot of “sudo apt install unattended-upgrades” to Apply Security Updates Only.

- Now we change the user to fahmed29 as shown in Figure 26 and we enter “sudo vim” in that but we don’t get output as we can observe in Figure 27.

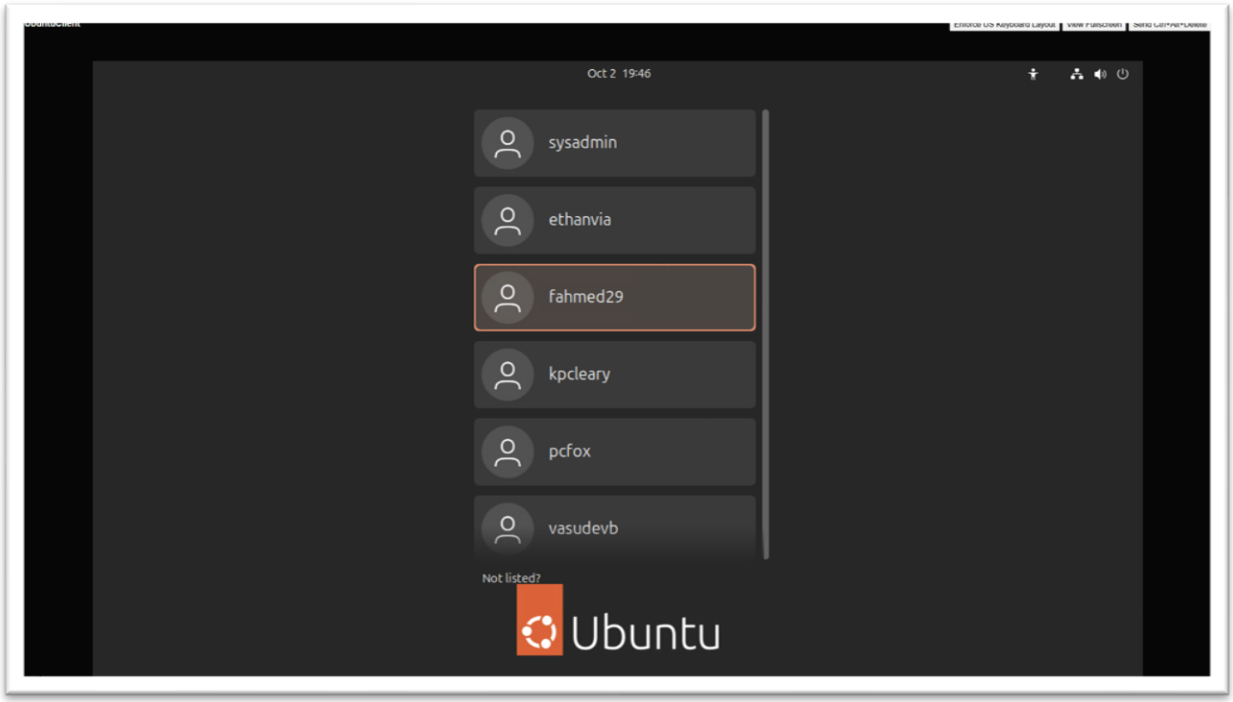

Figure 26: Screenshot of selecting different user “fahmed29”.

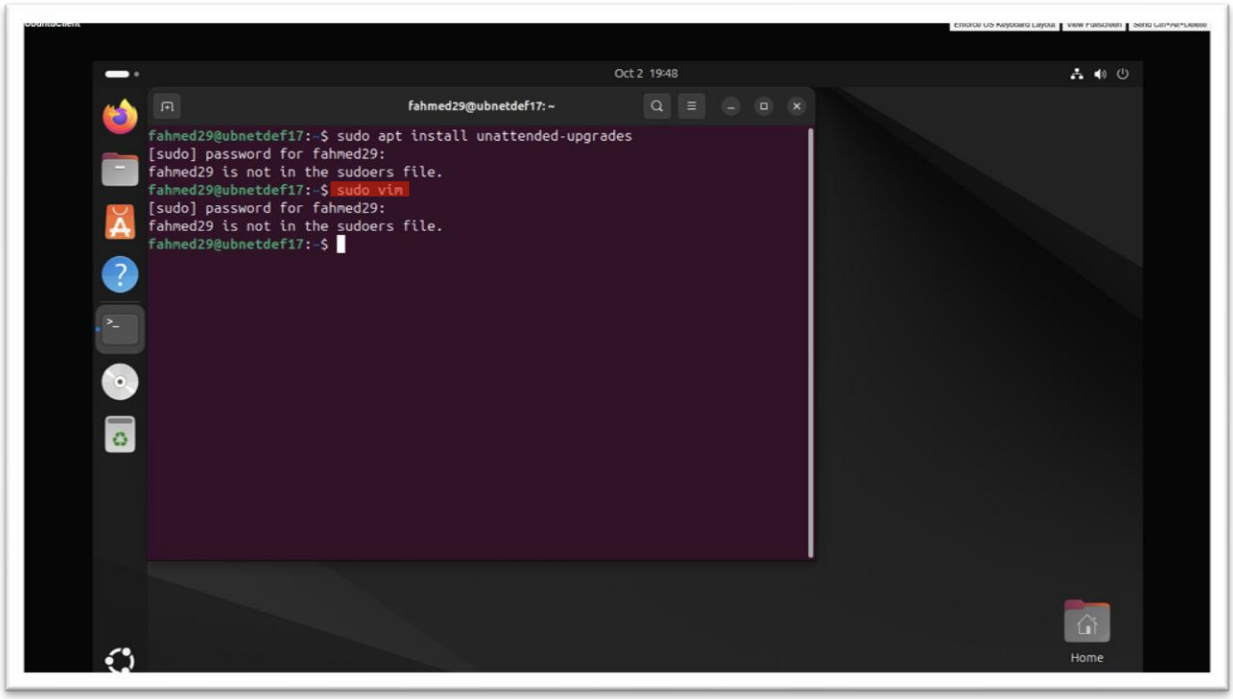

Figure 27: Screenshot of "sudo vim" to verify the output in different user.

- Now we type command "sudo visudo" to edit all the permissions as highlighted in Figure 28.

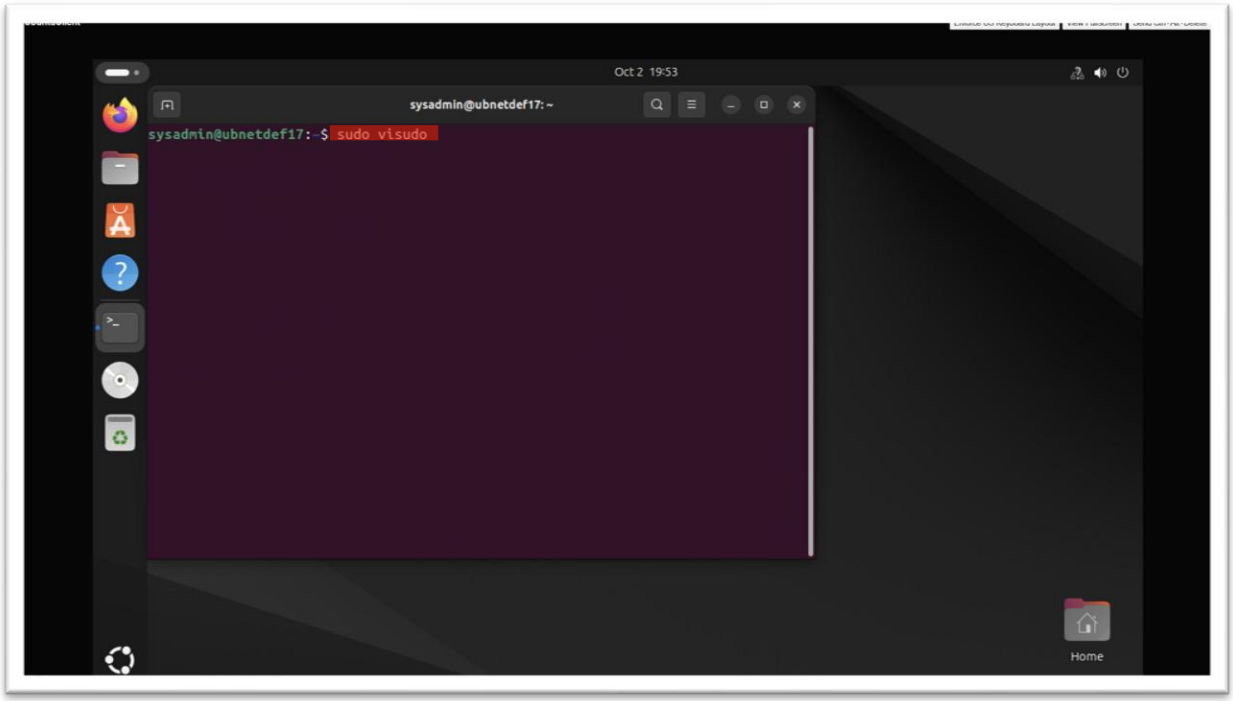

Figure 28: Screenshot of "sudo visudo" to edit permissions.

- So, we type new line under “group sudo permission” – “%BlackTeam ALL=(ALL:ALL) ALL” as shown in Figure 29 to give full permission.

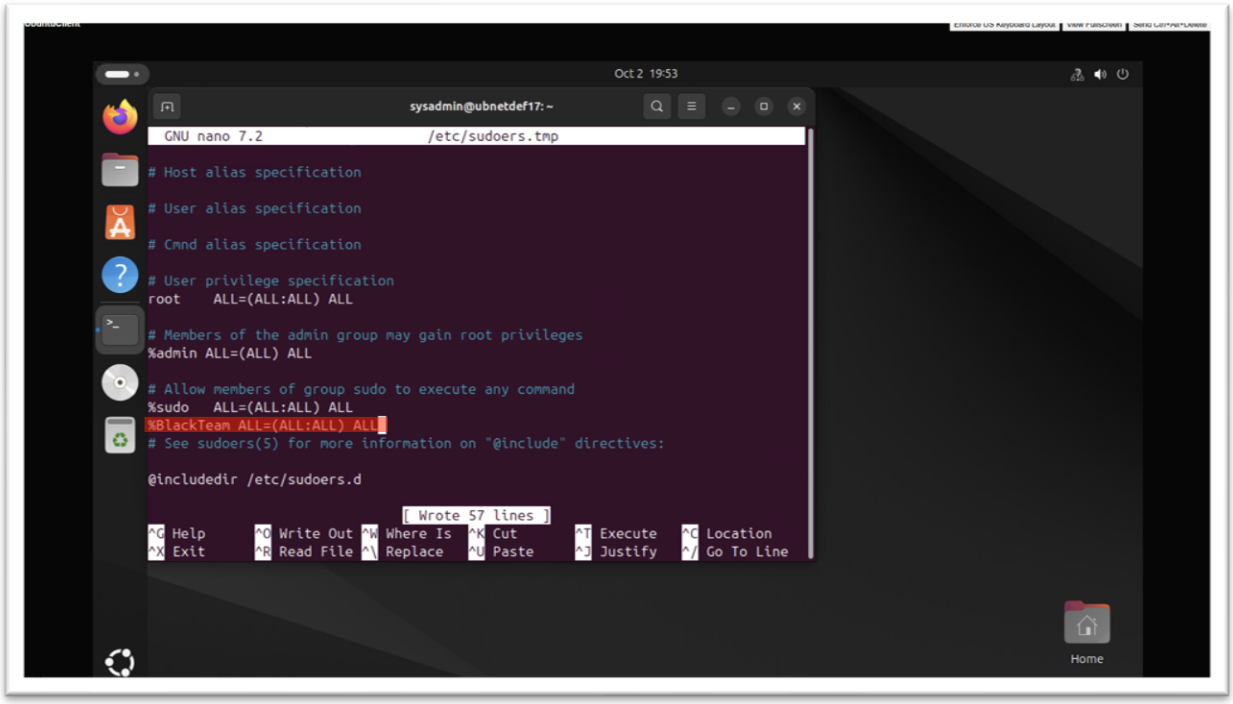

Figure 29: Screenshot of entering “%BlackTeam ALL=(ALL:ALL) ALL” to give all permissions.

- Now we enter “sudo chmod 700 $(which whoami) to give file permissions for whoami to allow only root user to read, write, and execute it as highlighted in Figure 30.

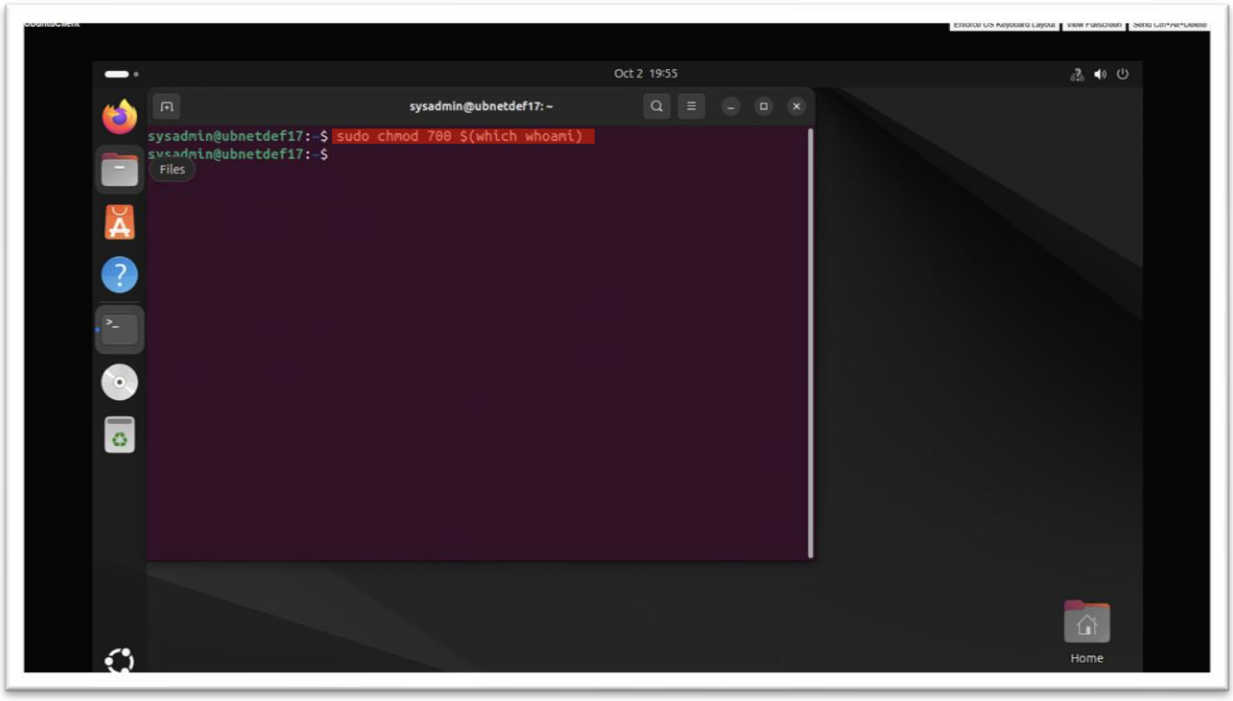

Figure 30: Screenshot of using “sudo chmod 700 $(which whoami) to give root permissions.

- So after that, we use “sudo chmod 750 /etc/hostname” to give file permissions for /etc/hostname to allow members of the BlackTeam group to read and execute it as highlighted in Figure 31.

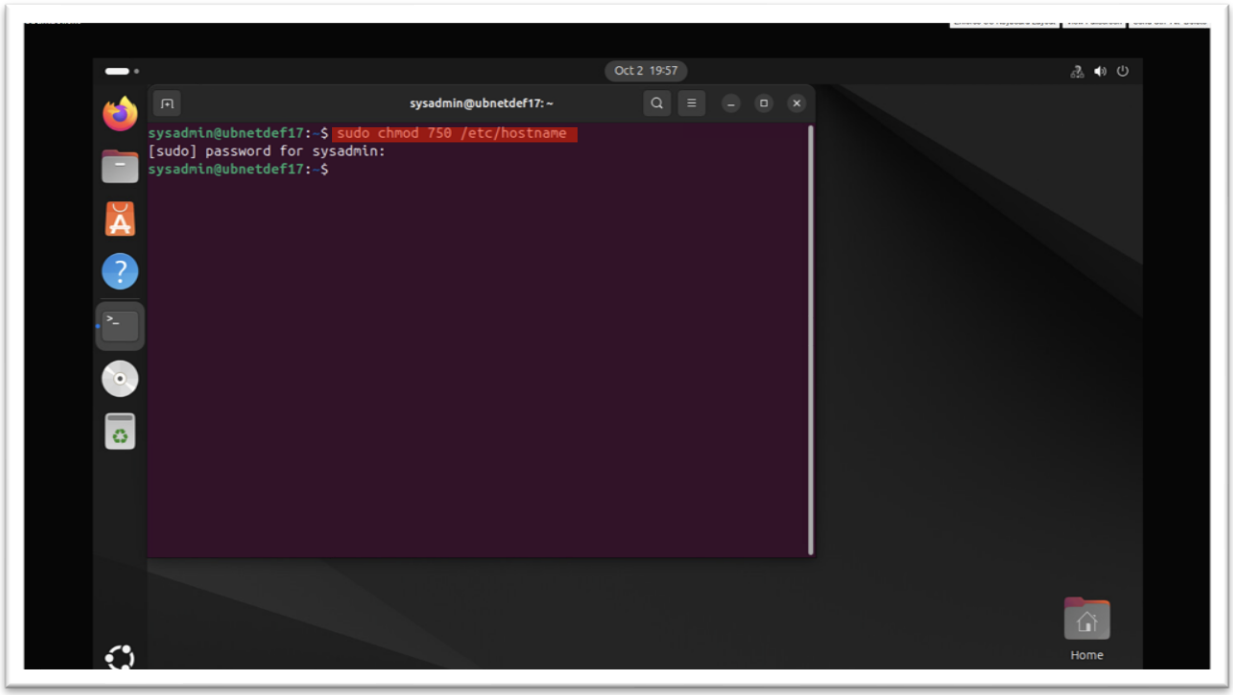

Figure 31: Screenshot of entering “sudo chmod 750 /etc/hostname” to give BlackTeam permissions.

- After that, type “sudo chown pcfox:pcfox /etc/hostname to change the ownership of /etc/hostname to pcfox in highlighted in Figure 32.

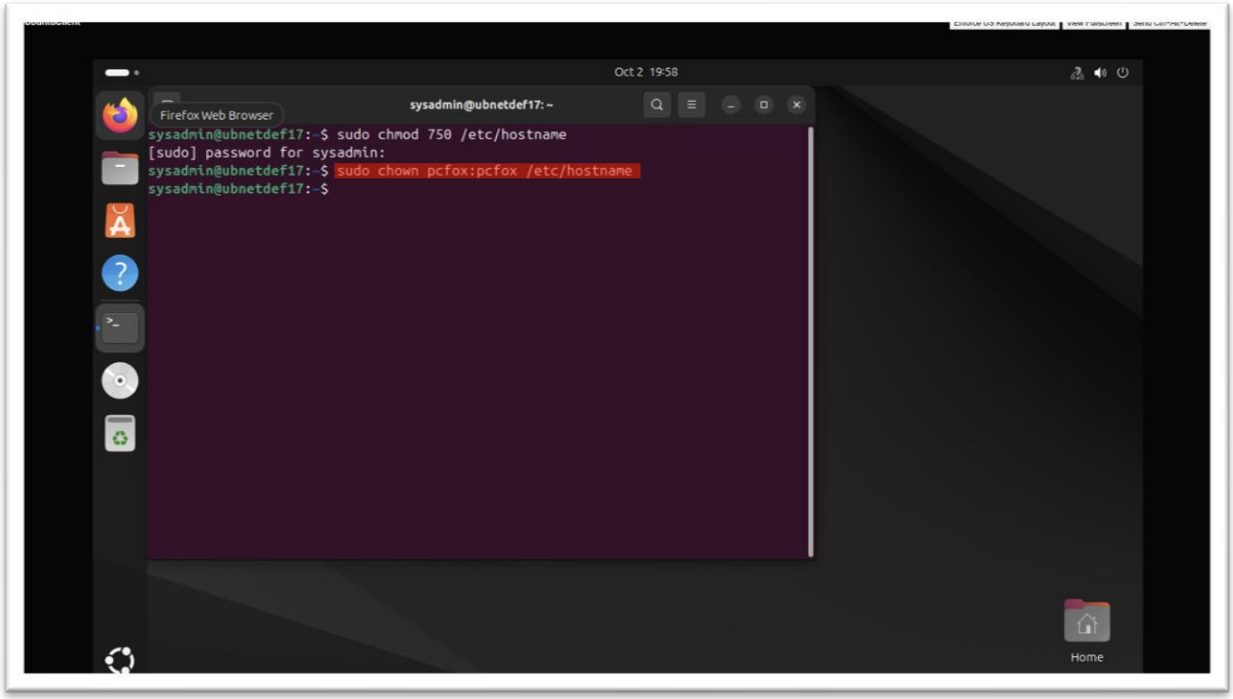

Figure 32: Screenshot of “sudo chown pcfox:pcfox /etc/hostname” to change ownership.

- Now, enter “sudo apt install libpam-pwquality” to install this library to edit password properties in highlighted in Figure 33.

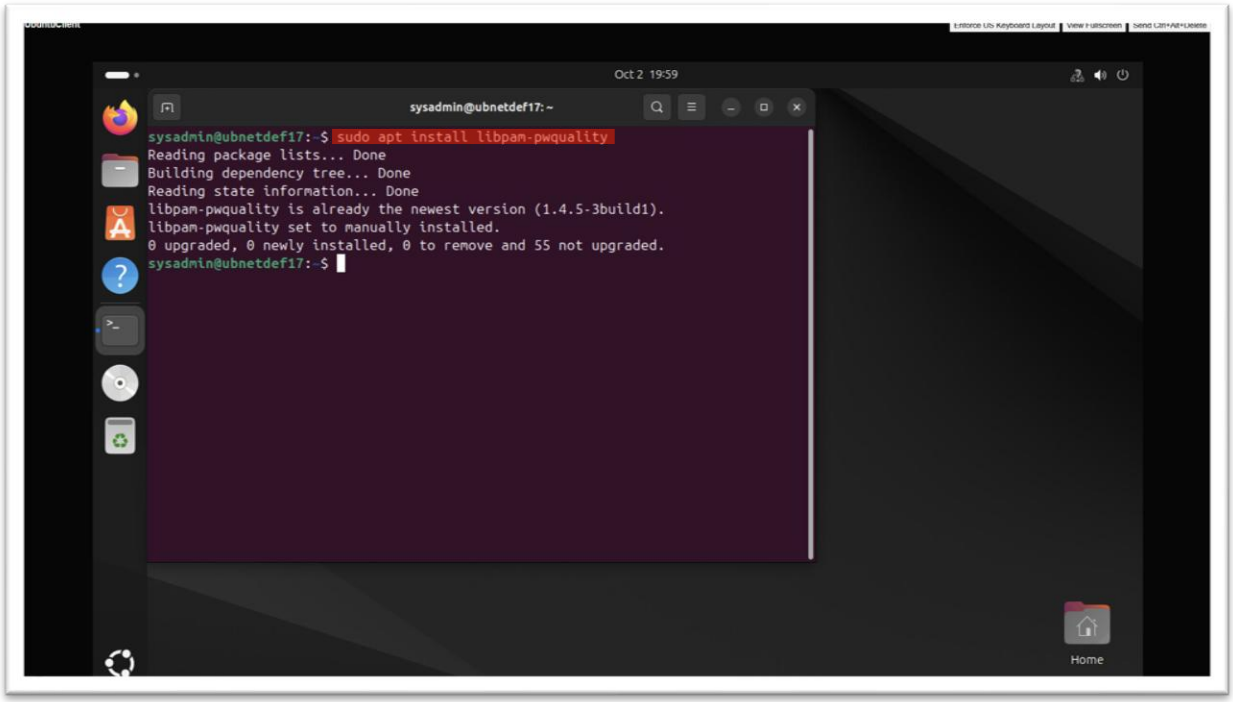

Figure 33: Screenshot of “sudo apt install libpam-pwquality” to install library.

- Now we edit the security file to change password properties by entering “sudo nano /etc/security/pwquality.conf” as highlighted in Figure 34.

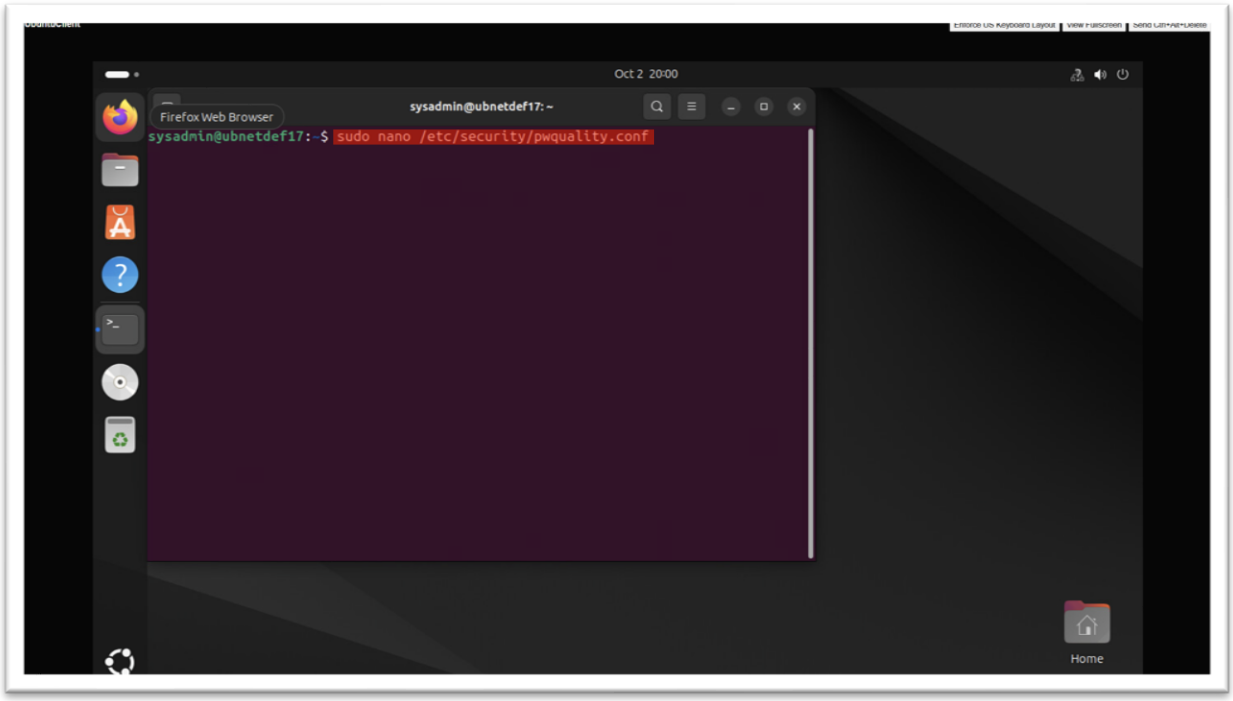

Figure 34: Screenshot of typing “sudo nano /etc/security/pwquality.conf” to edit password properties.

- Now we change “minlen= 10” to accept minimum length of 10 characters in shown in Figure 35.

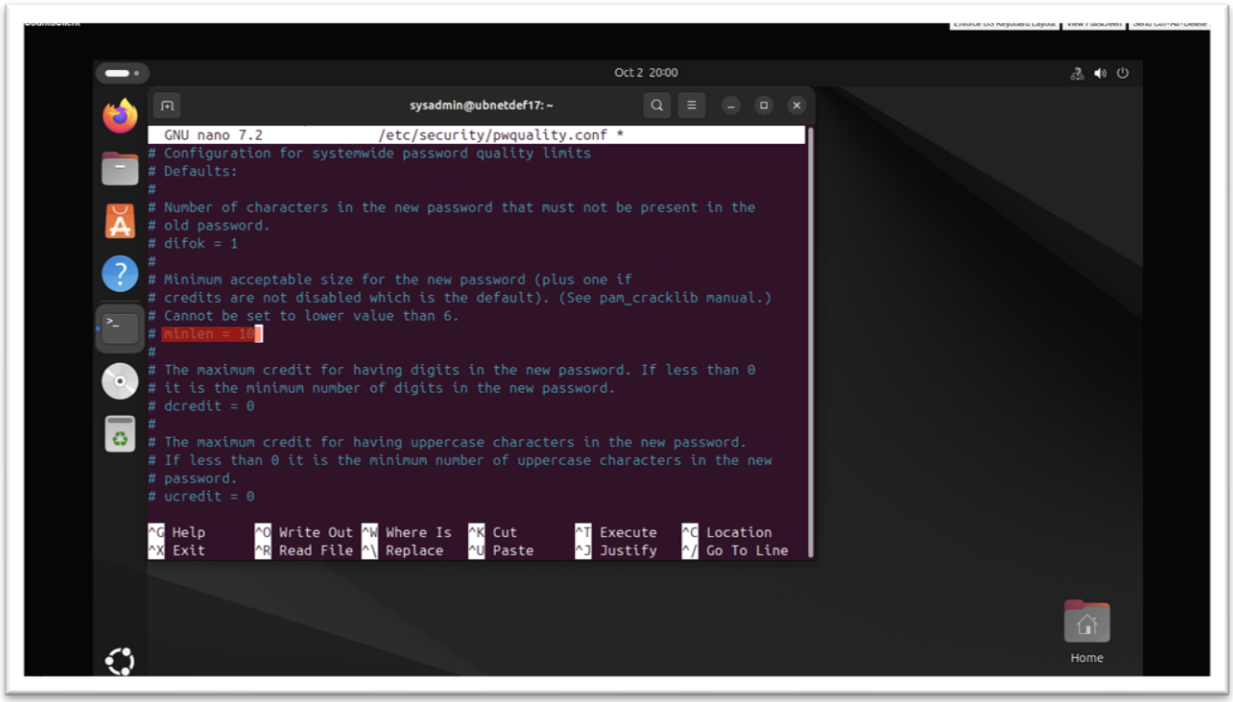

Figure 35: Screenshot of changing value of “minlen to 10” to accept minimum length.

- After that we modify value of “dcredit= -2” to accept password with atleast two digits as shown in Figure 36.

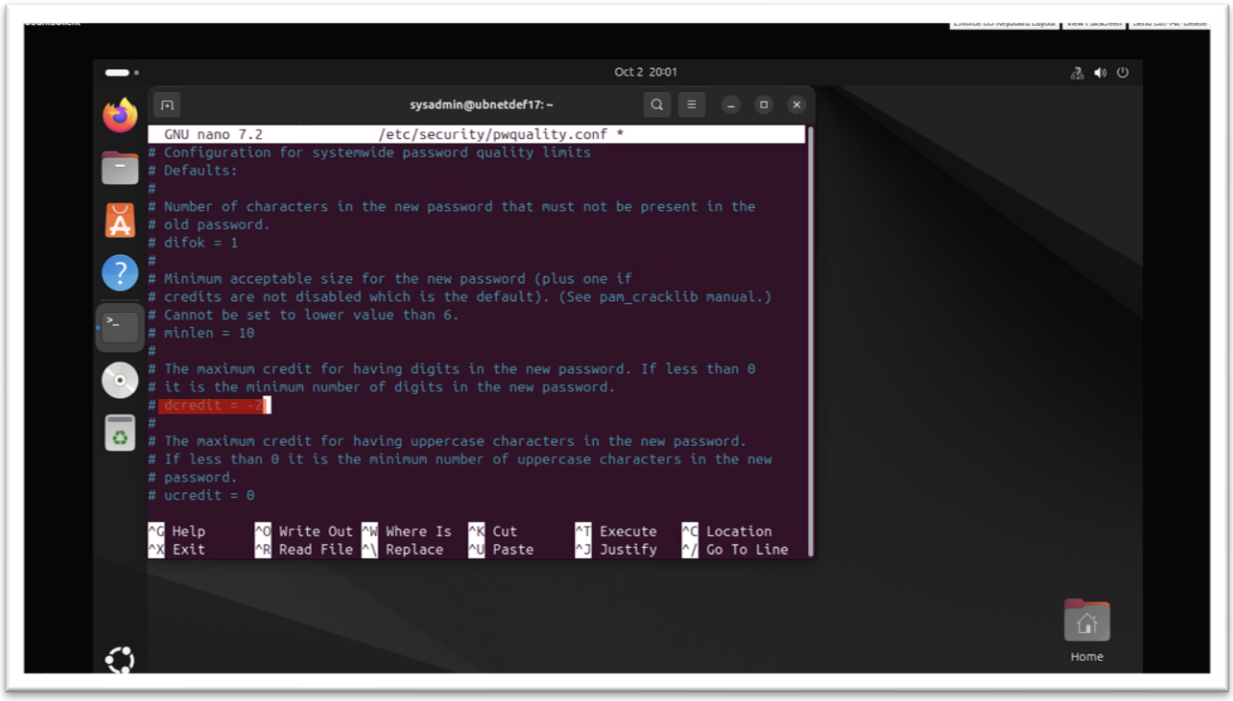

Figure 36: Screenshot of changing value of “dcredit to -2” to accept two digit.

- Finally, we modify value of “ucredit= -1” to accept passwords with atleast one upper case letter as shown in Figure 37.

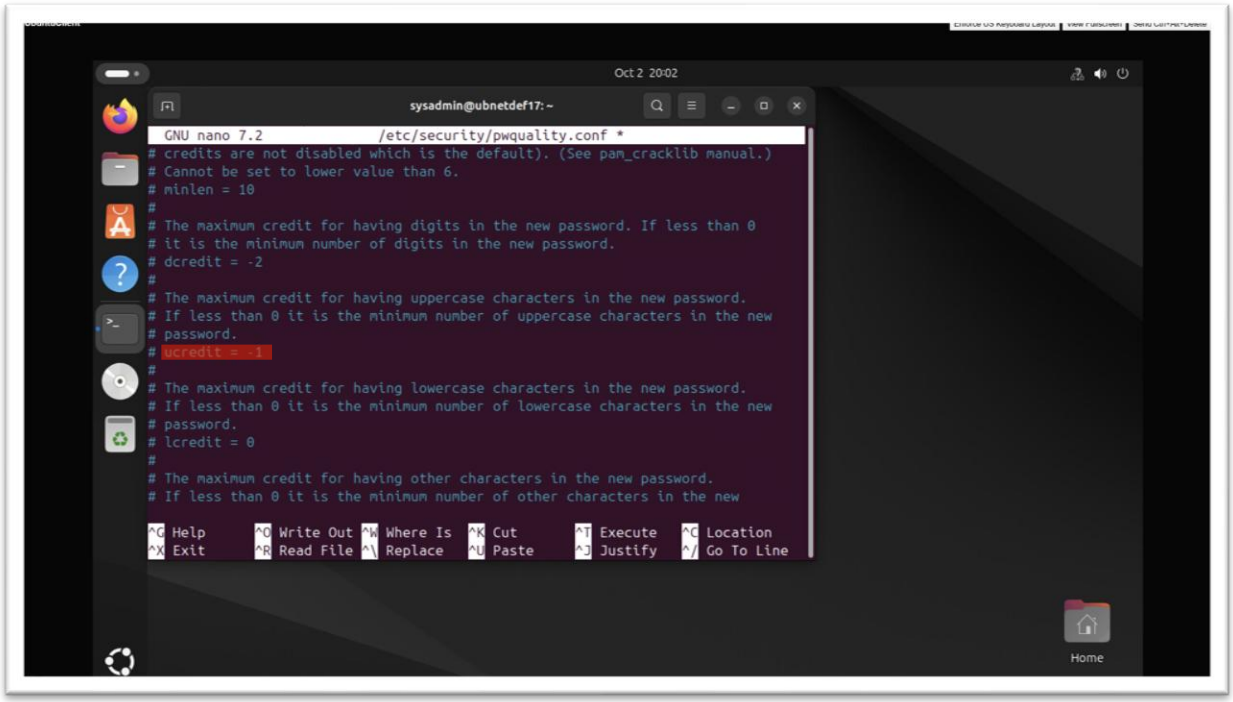

Figure 37: Screenshot of changing value of “ucredit to -1” to accept atleast one UpperCase.

5. Updated Topology

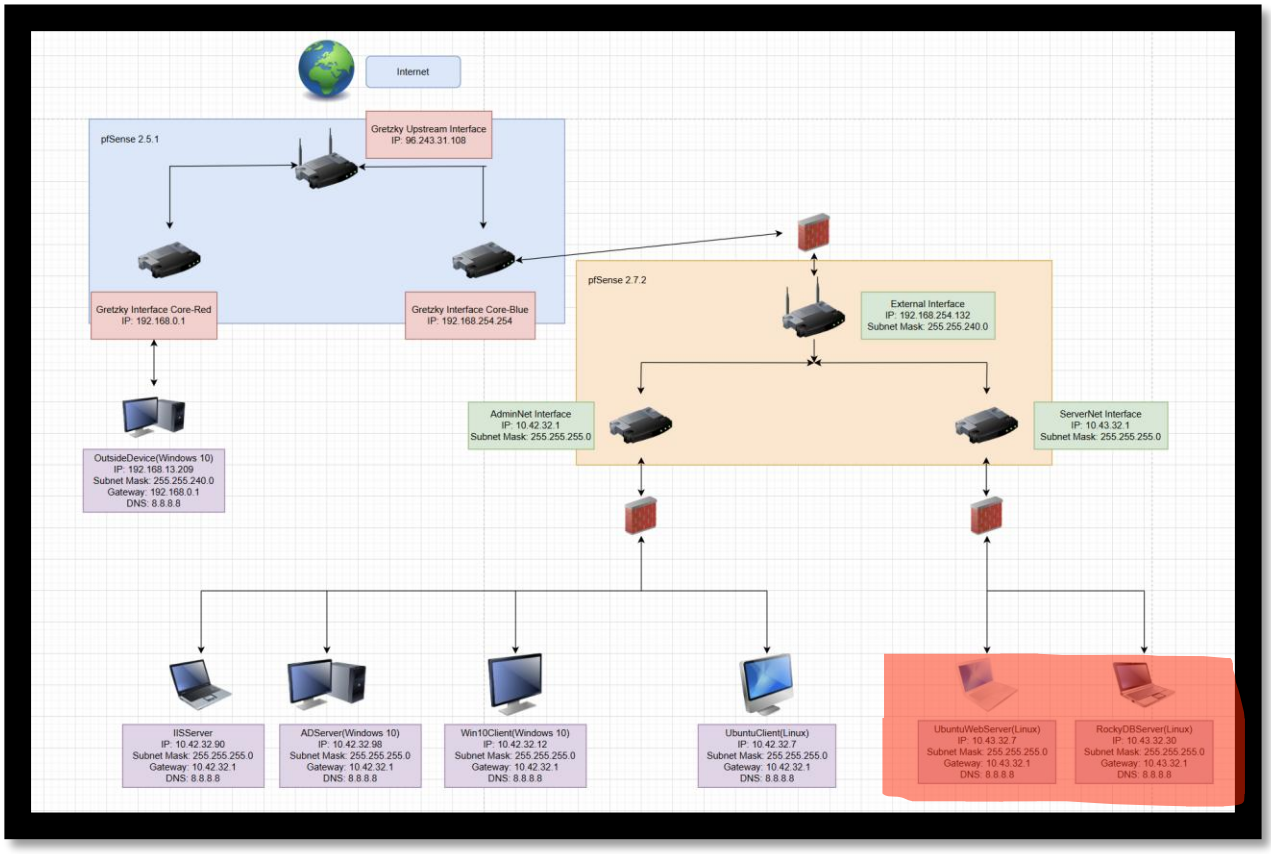

Figure 38: Screenshot of Updated Topology

- Two new devices “UbuntuWebServer” and “RockyBDServer” are added to the ServerNet Interface (as shown in Figure 38).
- One more new device “OutsideDevice” is connected in different network to “Gretzky Core-Red”
- Now, we have two different network interfaces,
  - One is “Blue” which is main system to connect every device from old topology
  - This one is “Red” which connects “OutsideDevice” to the network as shown in Figure 38.
- Because of two different network systems, there are three Gretzky Interface- Red, Blue and Upstream.

6. EAS 595 Additional Tasks

- Now type “cat /var/log/apache2/access.log” to verify that access logs exist as shown in Figure 39. And from same figure we can see that there is an access log that exist but its empty as no logs exists for now.

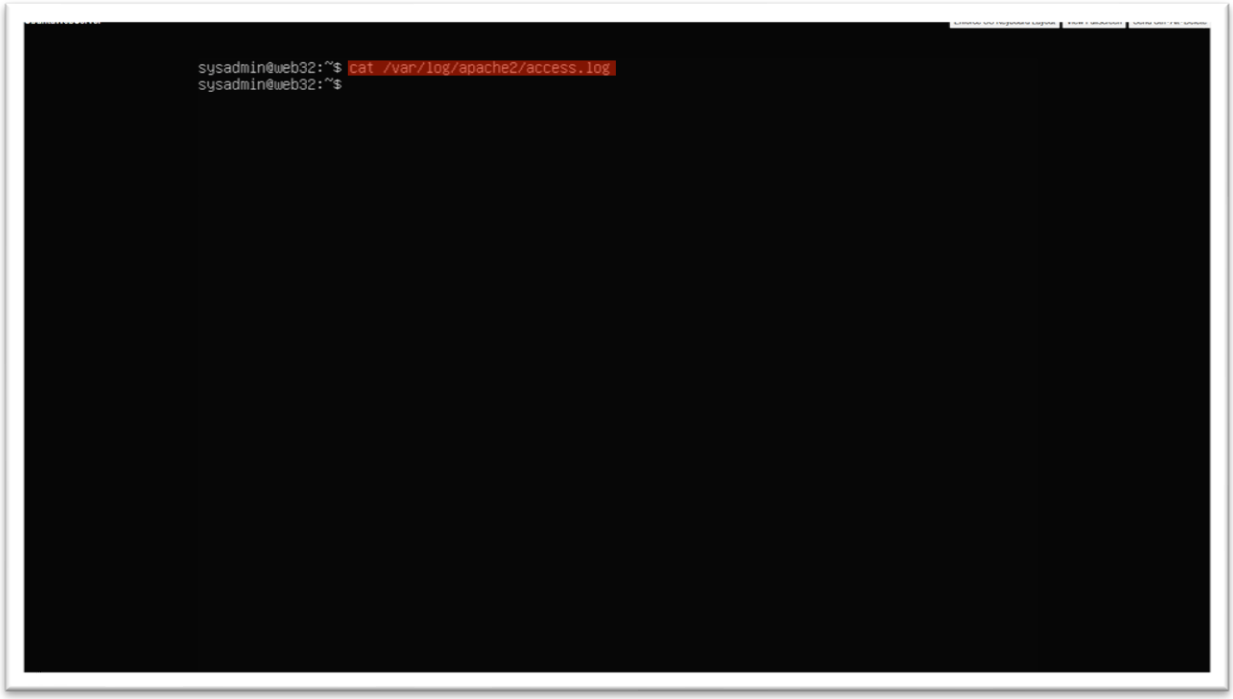

Figure 39: Screenshot of “cat /var/log/apache2/access.log” to verify access logs.

- Now we create a directory to store logs in the sysadmin user's home directory. By entering command “mkdir /home/sysadmin/log_backups”

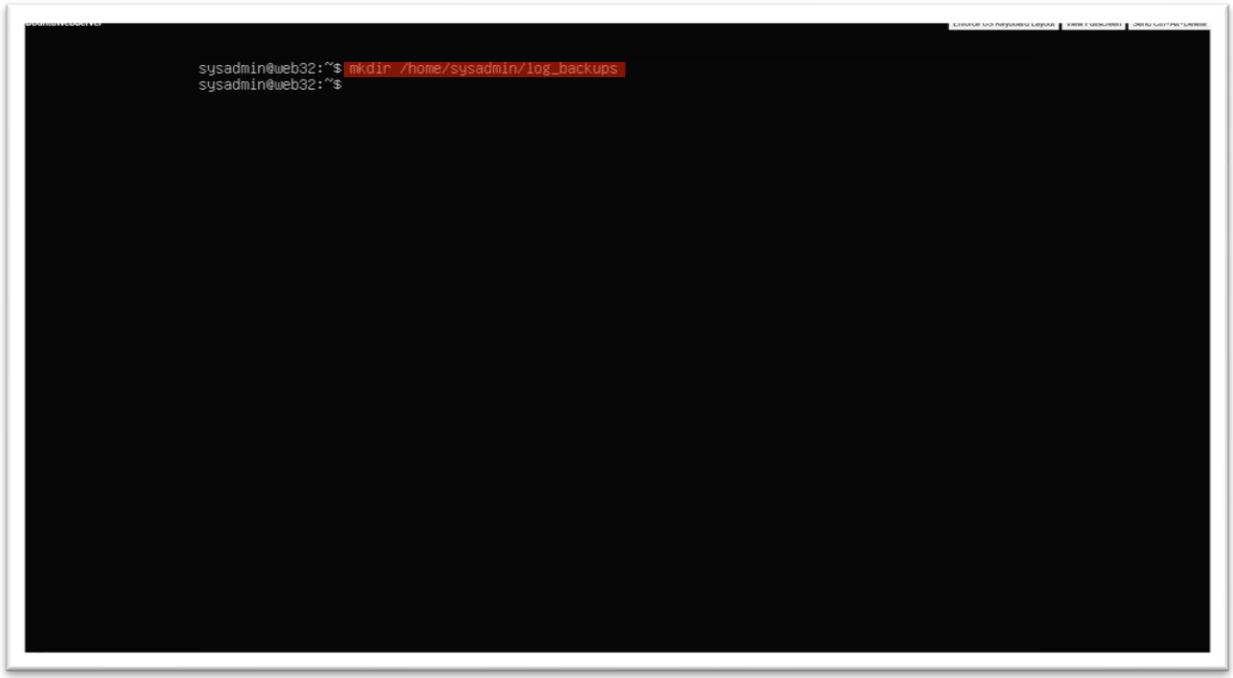

Figure 40: Screenshot of "mrdir /home/sysadmin/log_backups" to create a directory in user's home.

- After that we enter "nano /home/sysadmin/backuplog.sh" to create a script named backuplog and edit the script to make it like as shown in Figure 41.

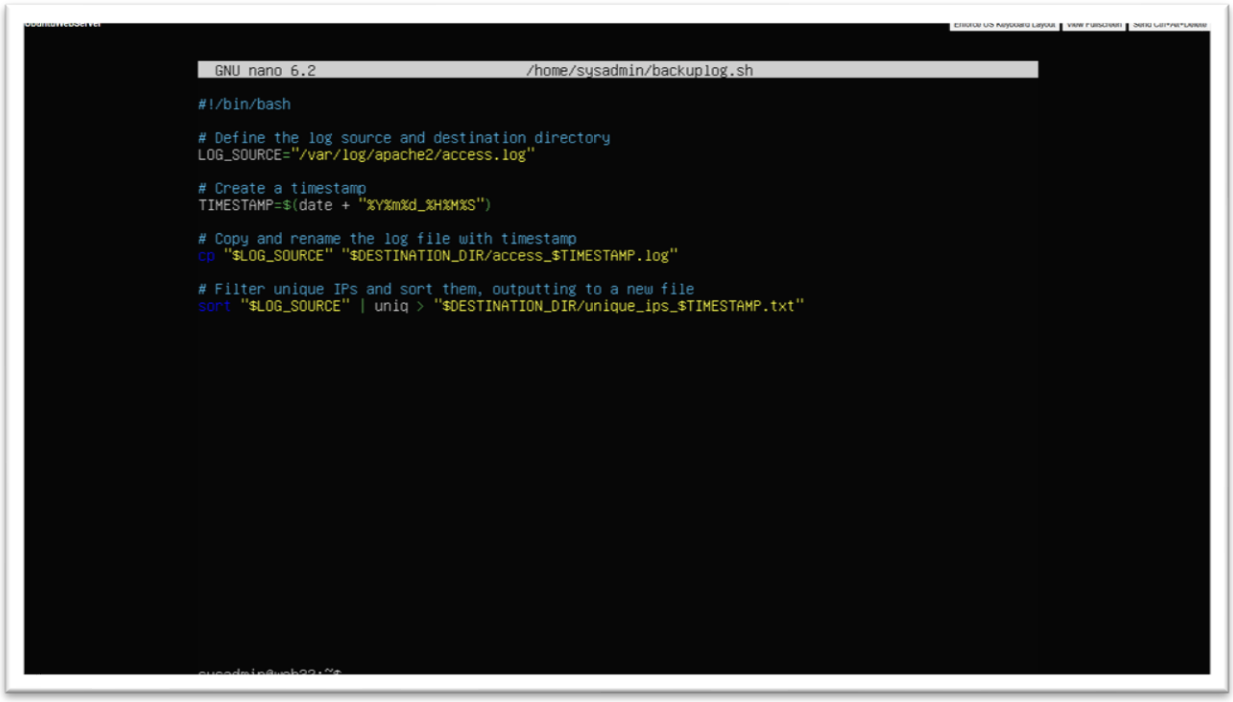

Figure 41: Screenshot of editing the script for backuplog.

- Now we get proper permissions to that script using "chmod +x /home/sysadmin/backuplog.sh" as highlighted in Figure 42.

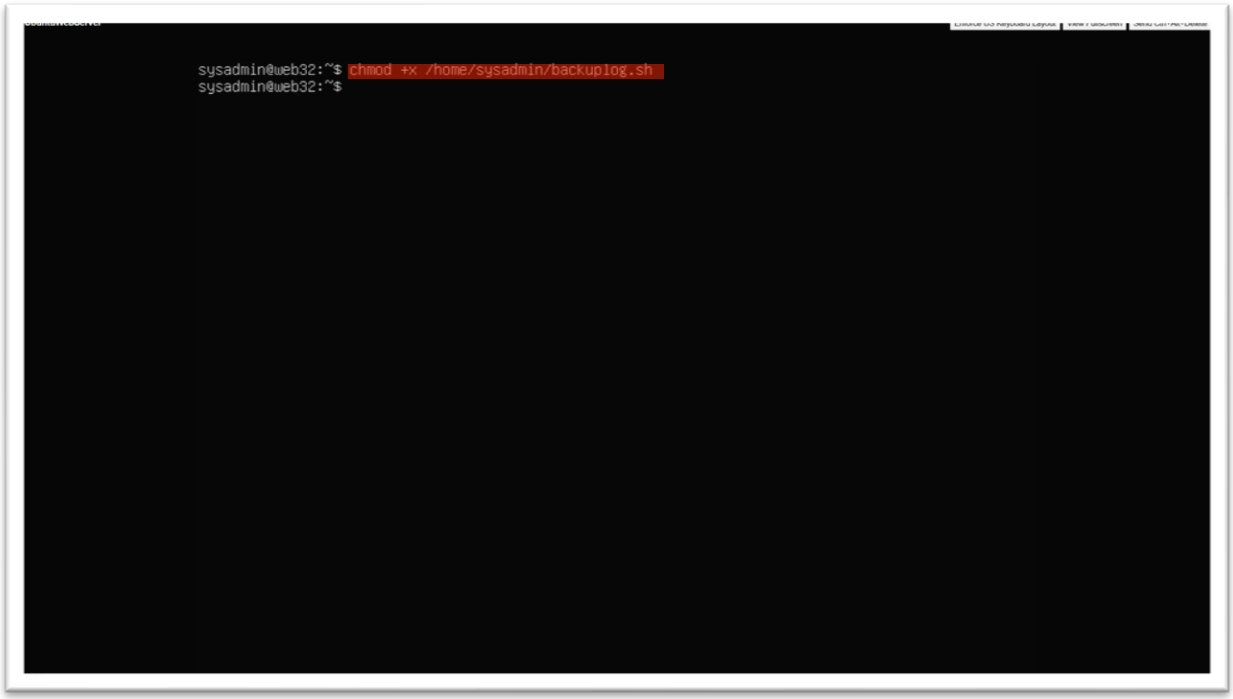

Figure 42: Screenshot of "chmod +x /home/sysadmin/backuplog.sh" to give permisions to the script.

- Now we can verify the permissions by using command "ls -la /home/sysadmin/backuplog.sh" as highlighted below in Figure 43 and as we can observe the output consists of "-rwxrwxr-x" which proves the permissions given to that script.

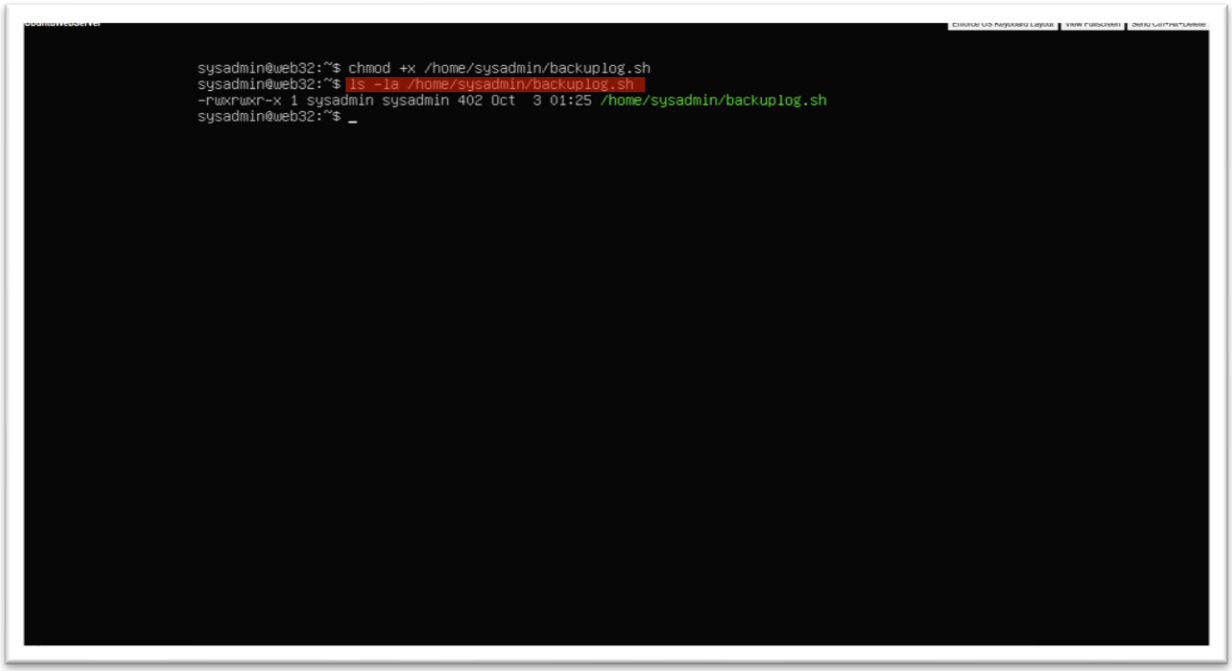

Figure 43: Screenshot of "ls -la /home.sysadmin/backuplog.sh" to verify permissions for script.

- As we want to edit Cron Job, we type "crontab -e" (choose nano if asked so after entering that command) as highlighted in Figure 44.

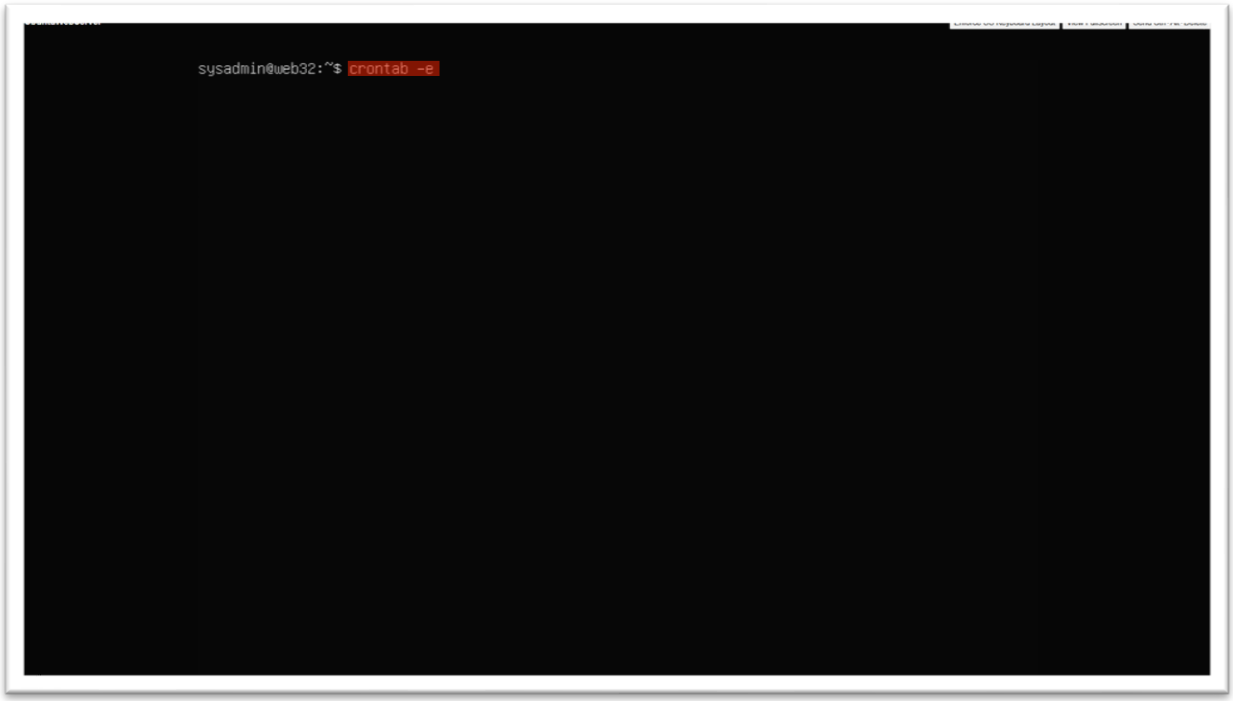

Figure 44: Screenshot of editing Cron Job using "crontab -e".

- Now enter a new line at the end of nano- "5 4 * * * /home/sysadmin/backuplog.sh" to schedule the script to run daily at 4:05 AM as highlighted below.

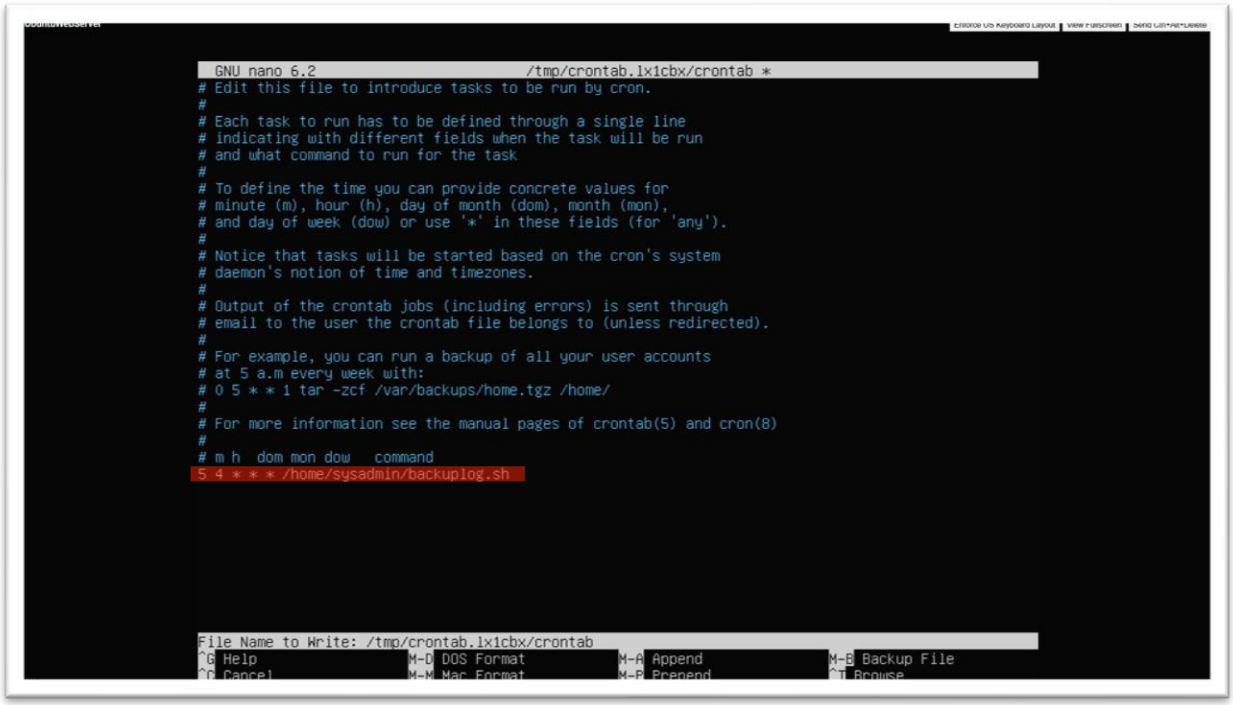

Figure 45: Screenshot of entering a new line "5 4 * * * /home/sysadmin/backuplog.sh" to make script run daily at 4:05 AM.

- After that, we check the list by inputting "crontab -l" and the final result as shown in Figure 46.

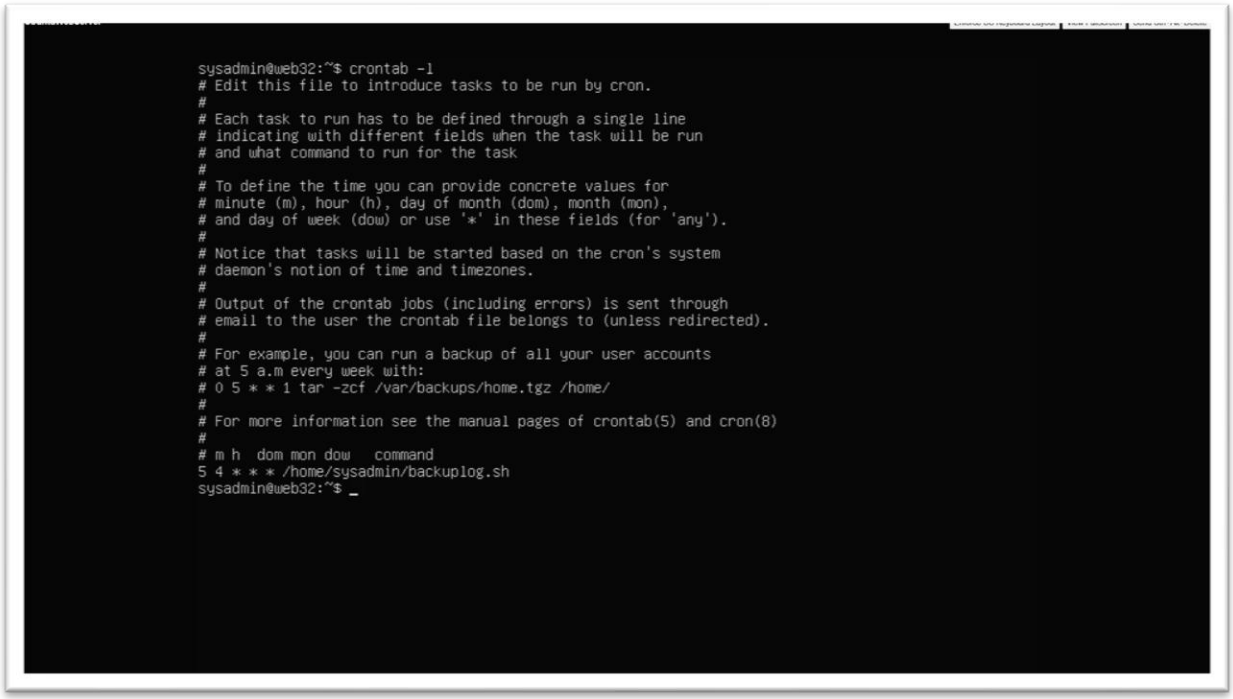

Figure 46: Screenshot of Final Result by inputting "crontab -l".