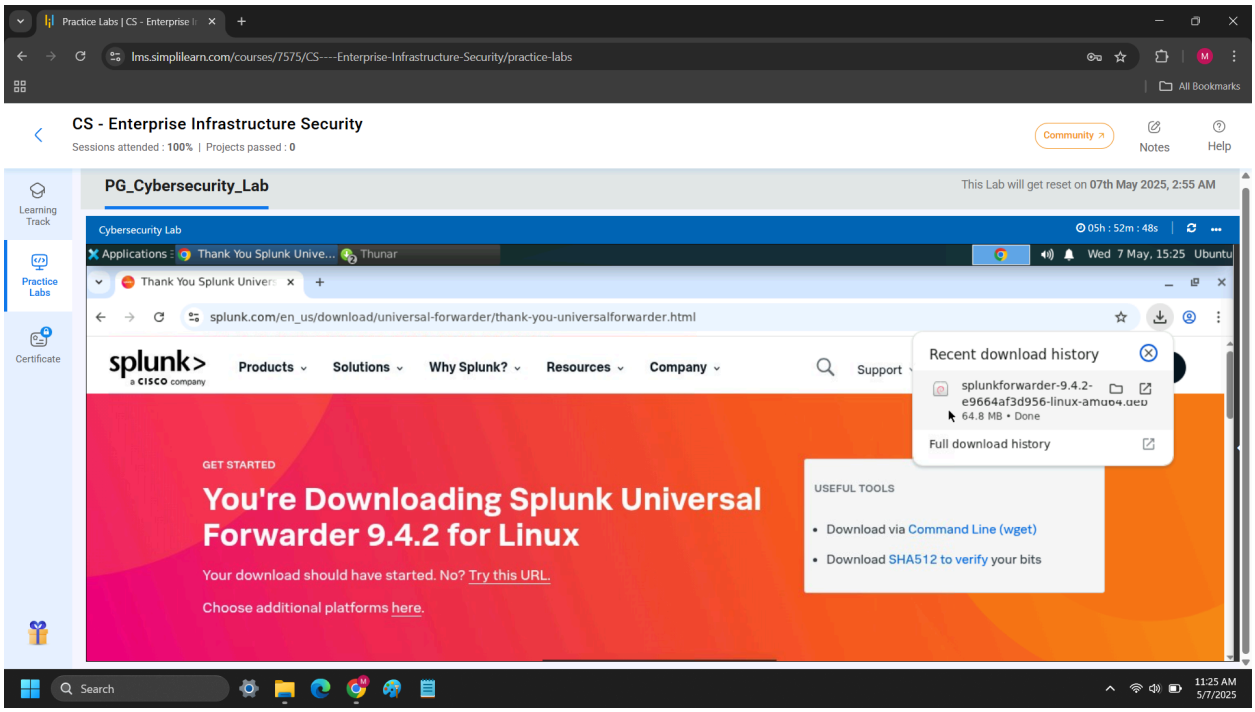
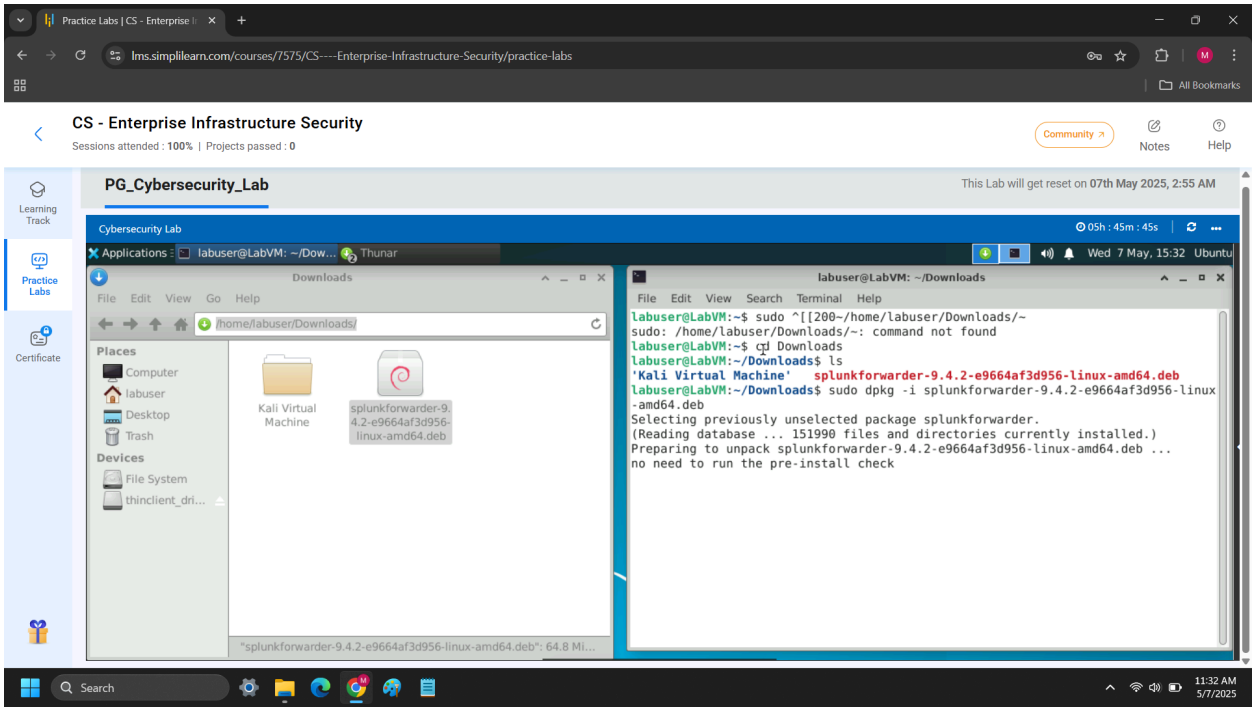
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

Phase #1: Setting up

1. Install SplunkForwarder by going to splunk's website and using the following command to unpack the installer:
   sudo dpkg -i splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb

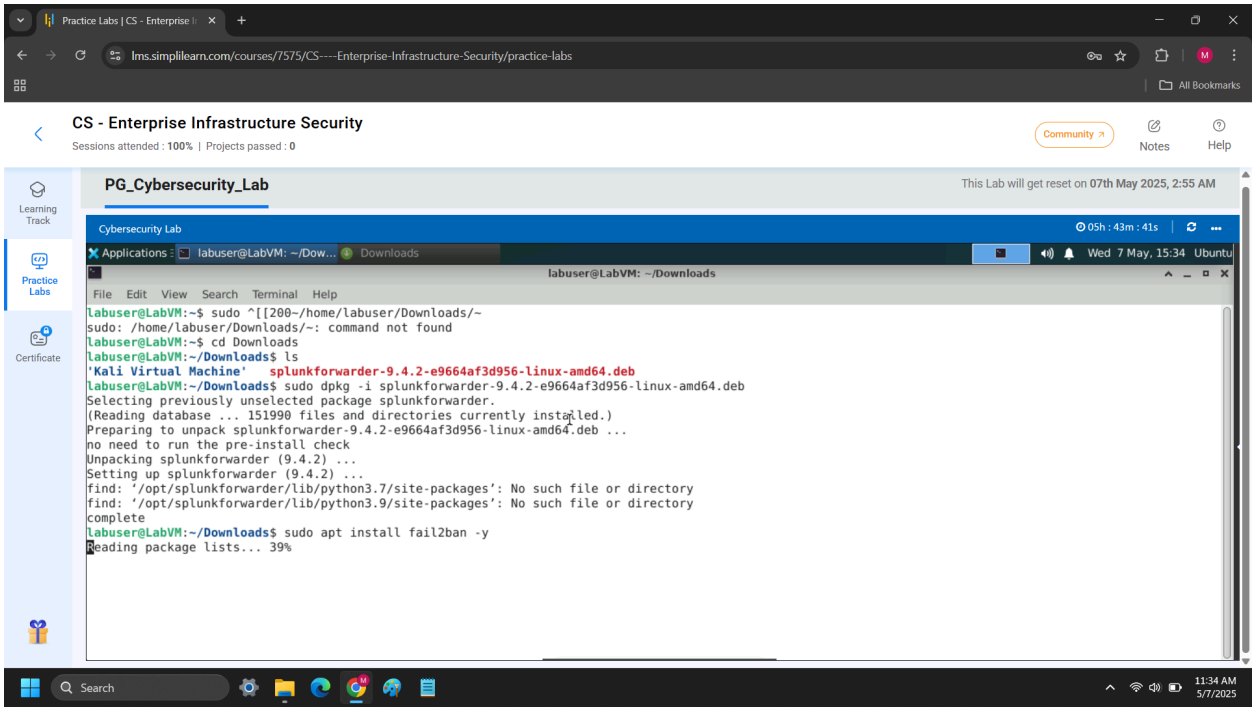




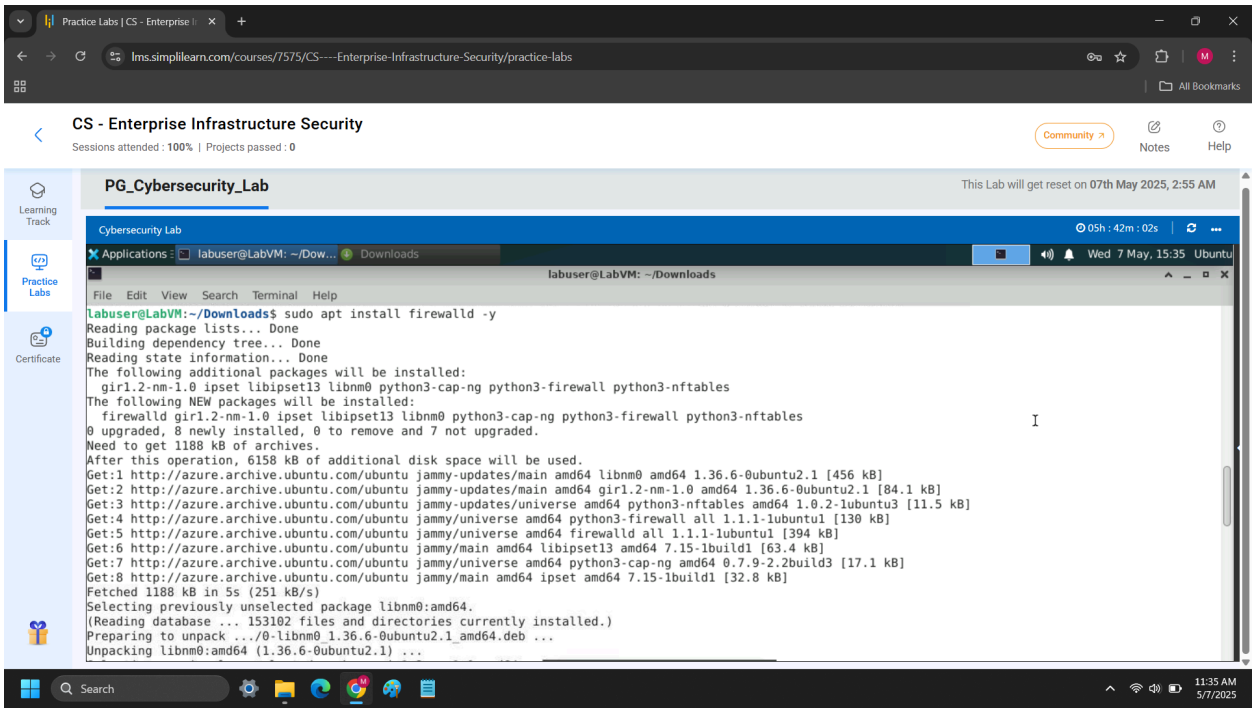
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

2. Install Fail2Ban using : ***sudo apt install fail2ban -y***



3. Install Firewalld using : ***sudo apt install firewalld -y***



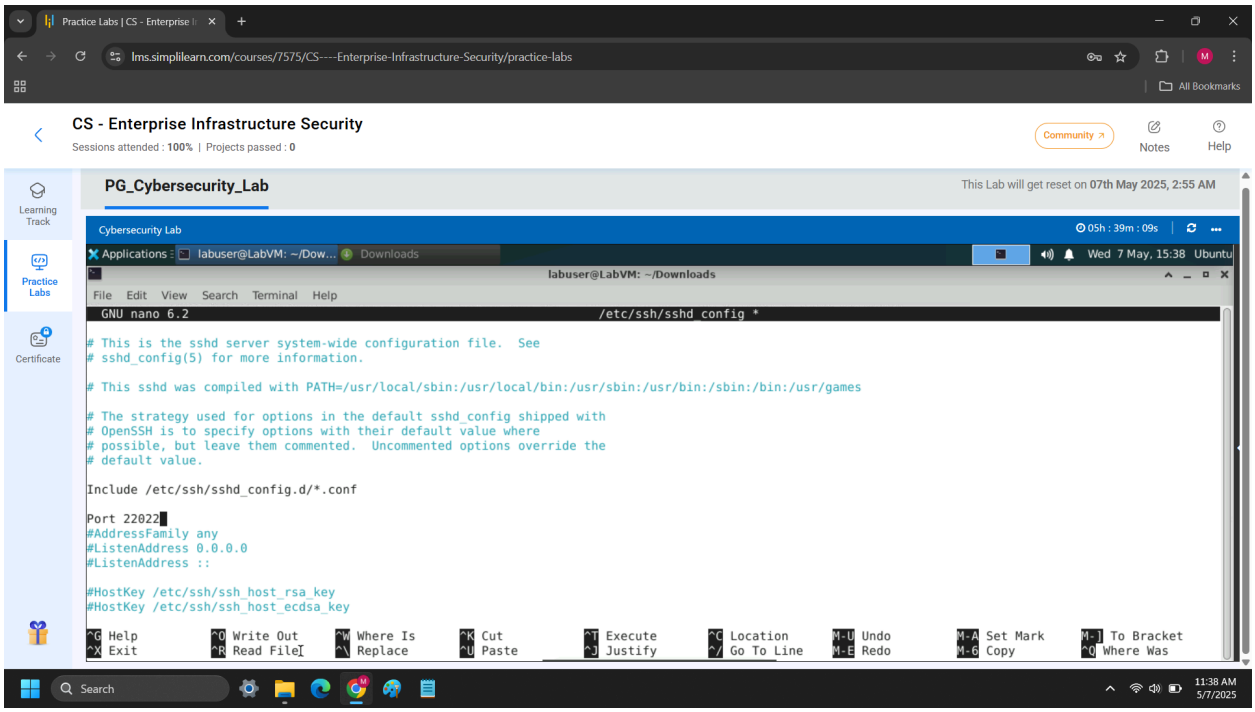
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

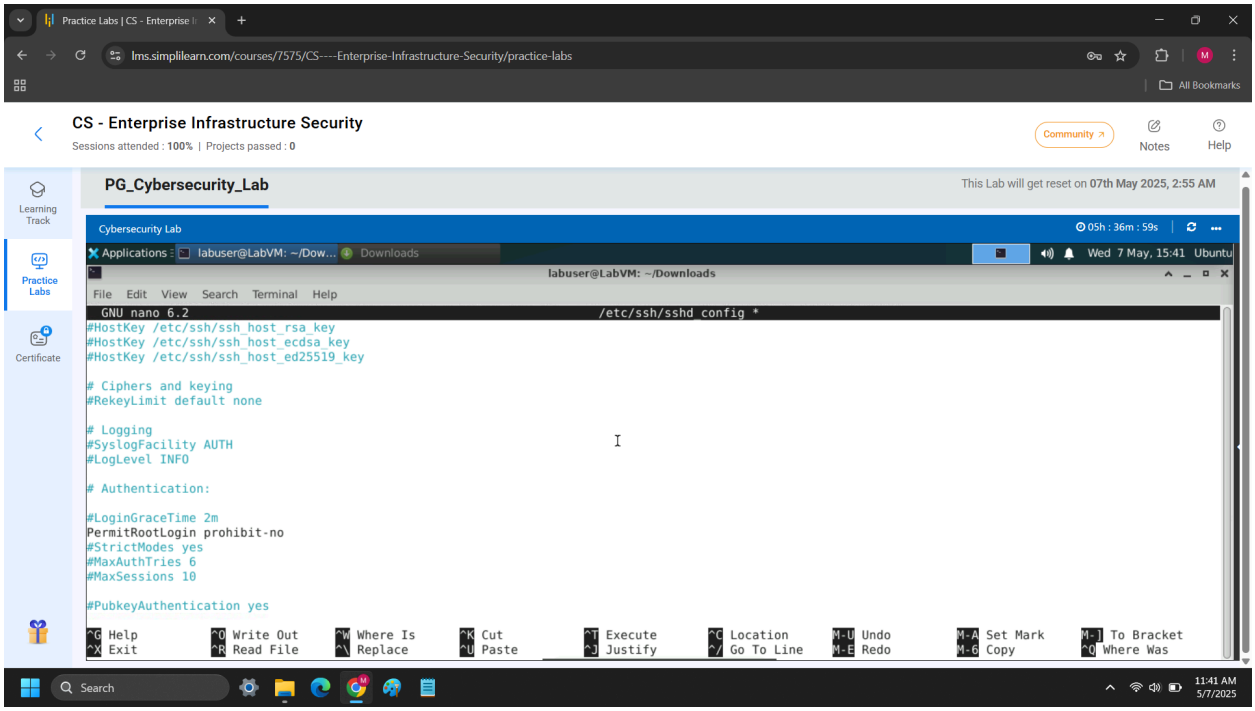
Phase #2: SSH Hardening

1. Open default SSH port settings using bash command: ***sudo nano /ect/ssh/sshd_config***

2. Changed ***#Port 22*** to ***22022***



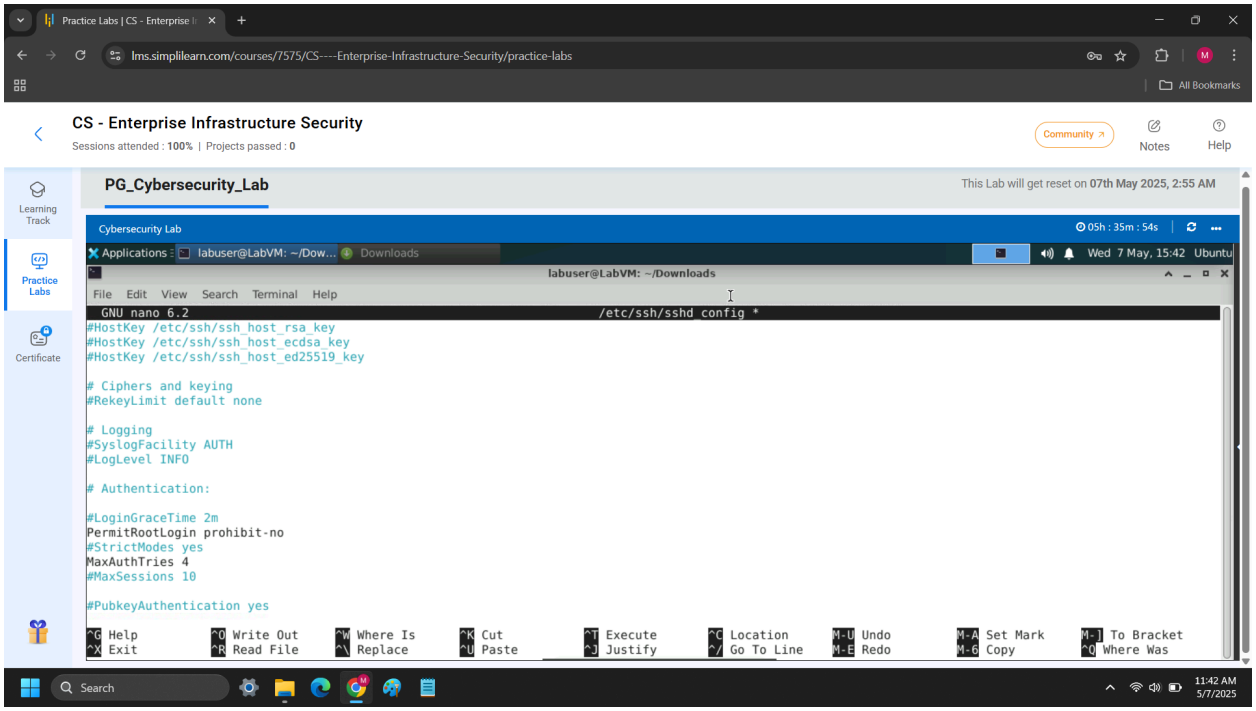
3. Changed ***PermitRootLogin*** from ***yes*** to ***no***

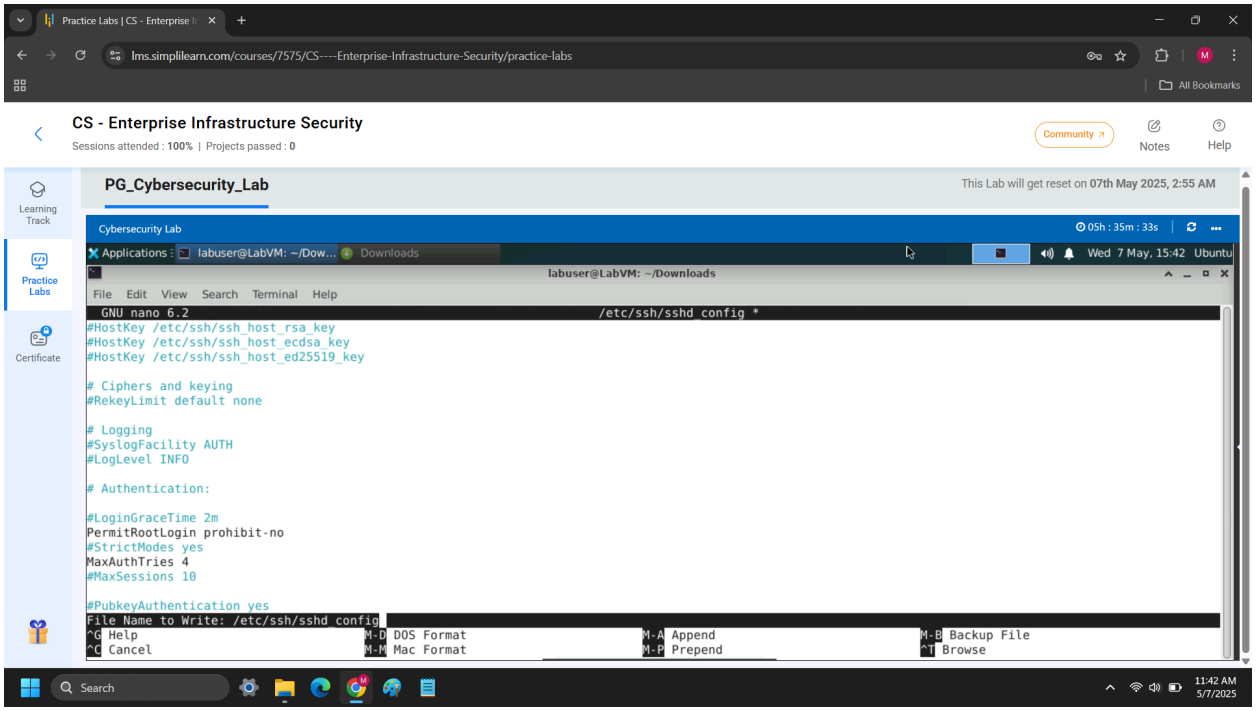


Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

4. Added login limits: ***MaxAuthTries 4*** & saved with ***Ctrl + X***, then ***Y*** to confirm



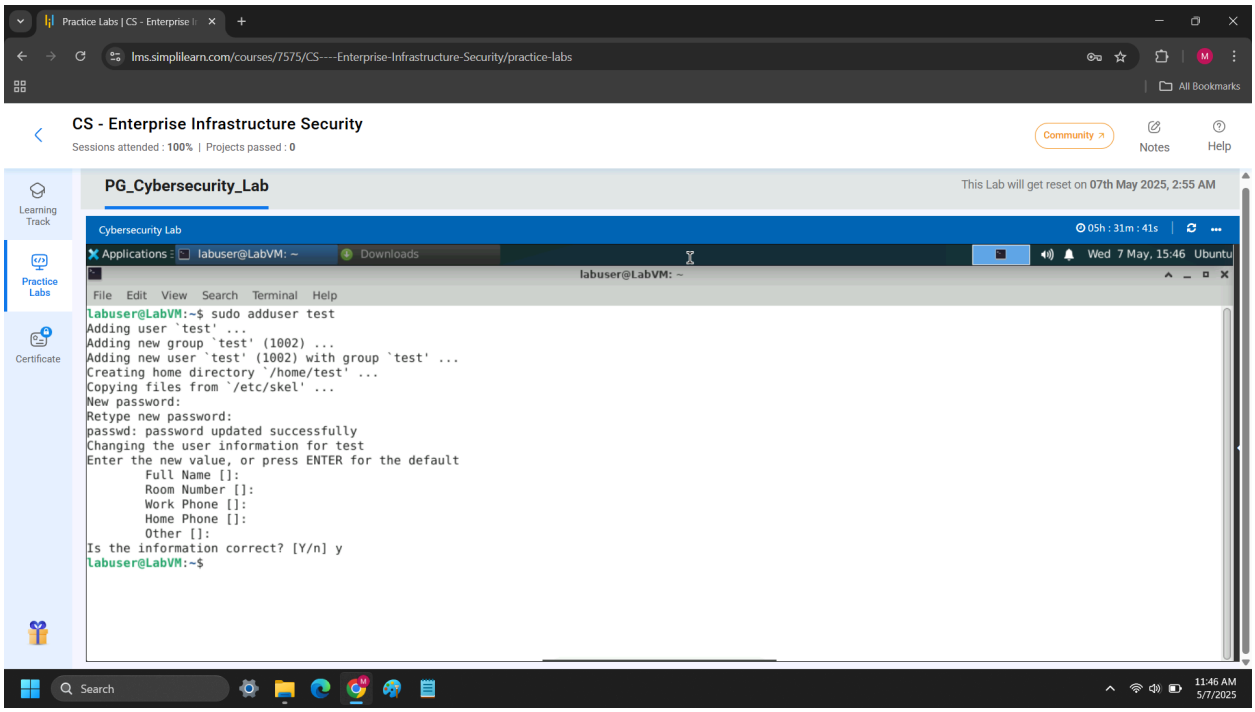


Screenshots for Course End Project: Linux Honeypot

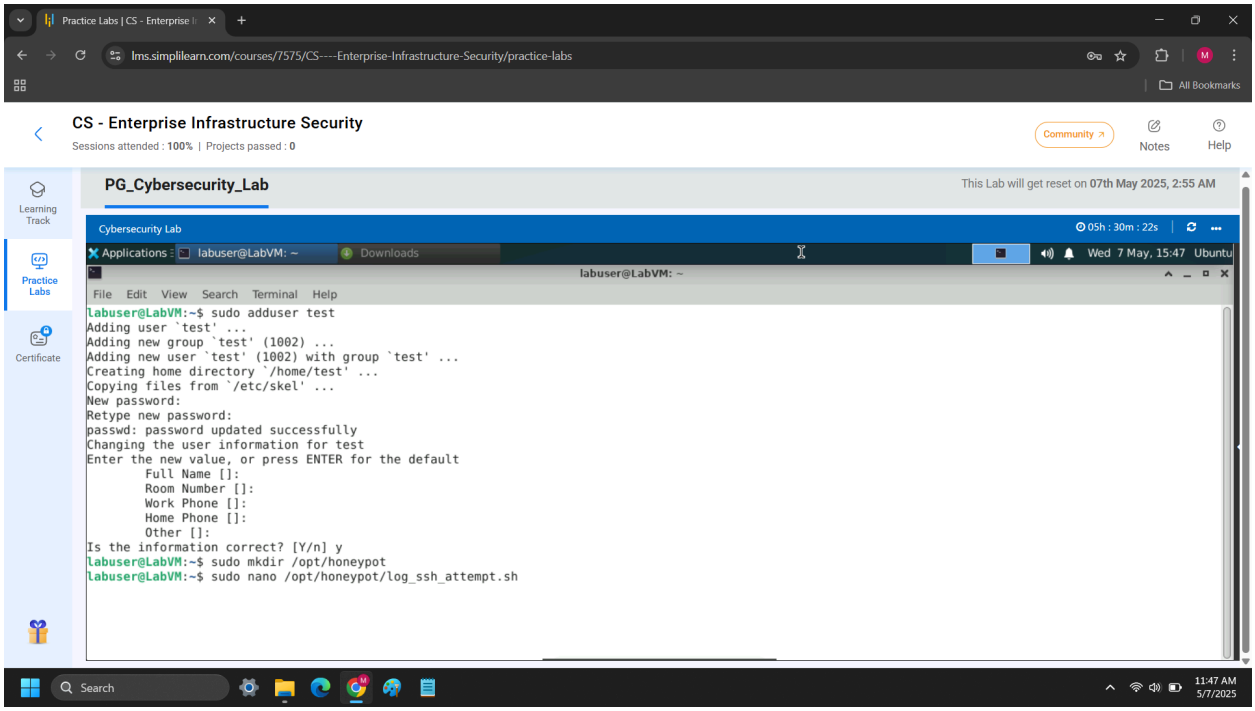
Michael Warner 5/7/25

Phase #3: Deploy SSH Honeypot + Configuring the Firewall

1. Created a dedicated honeypot user; using command: ***sudo adduser test***



2. Created a Logging Script; using command: ***sudo mkdir /opt/honeypot*** to store honeypot related files & using command: ***sudo nano /opt/honeypot/log_ssh_attempt.sh*** to create the script files



Screenshots for Course End Project: Linux Honeypot

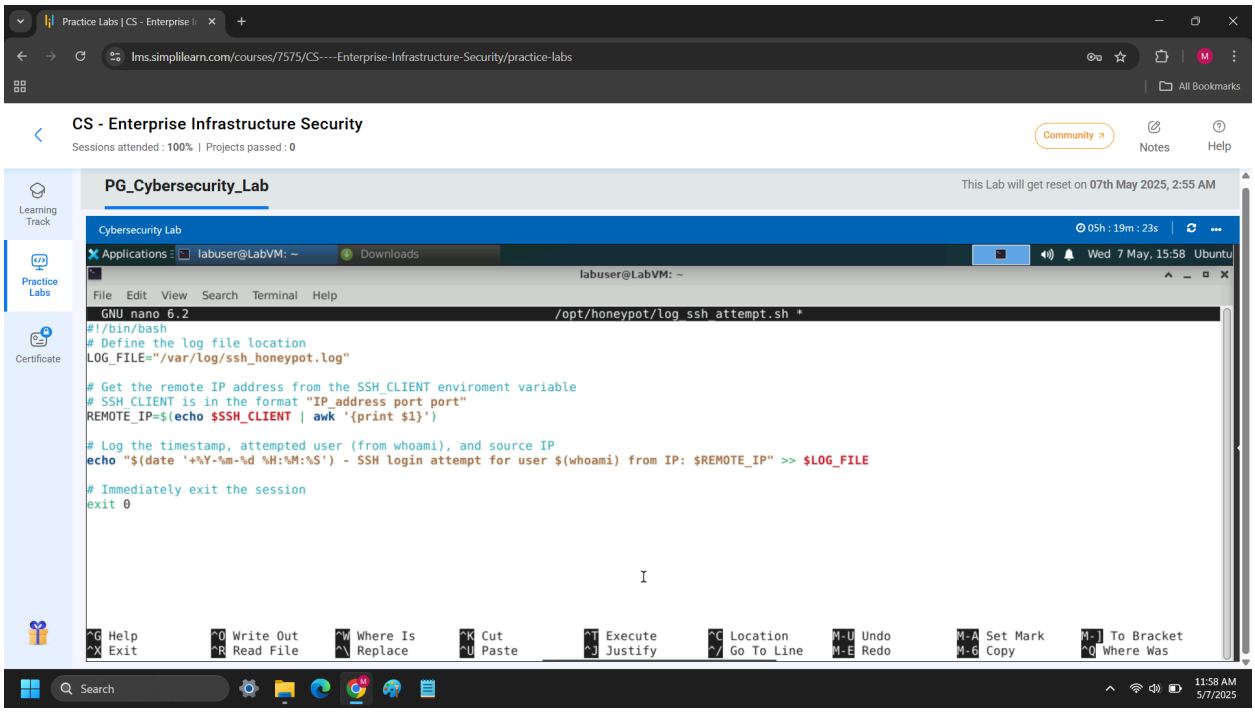
Michael Warner 5/7/25

3. Typed the following content into the script & saved file:
   #!/bin/bash
   LOG_FILE=”/var/log/ssh_honeypot.log

   REMOTE_IP=$(echo $SSH_CLIENT | awk’{print $1}’)

   Echo “$(date ‘+%Y-%m-%d %H:%M:%S’) - SSH login attempt for user $(whoami) from IP: $REMOTE_IP” >> $LOG_FILE

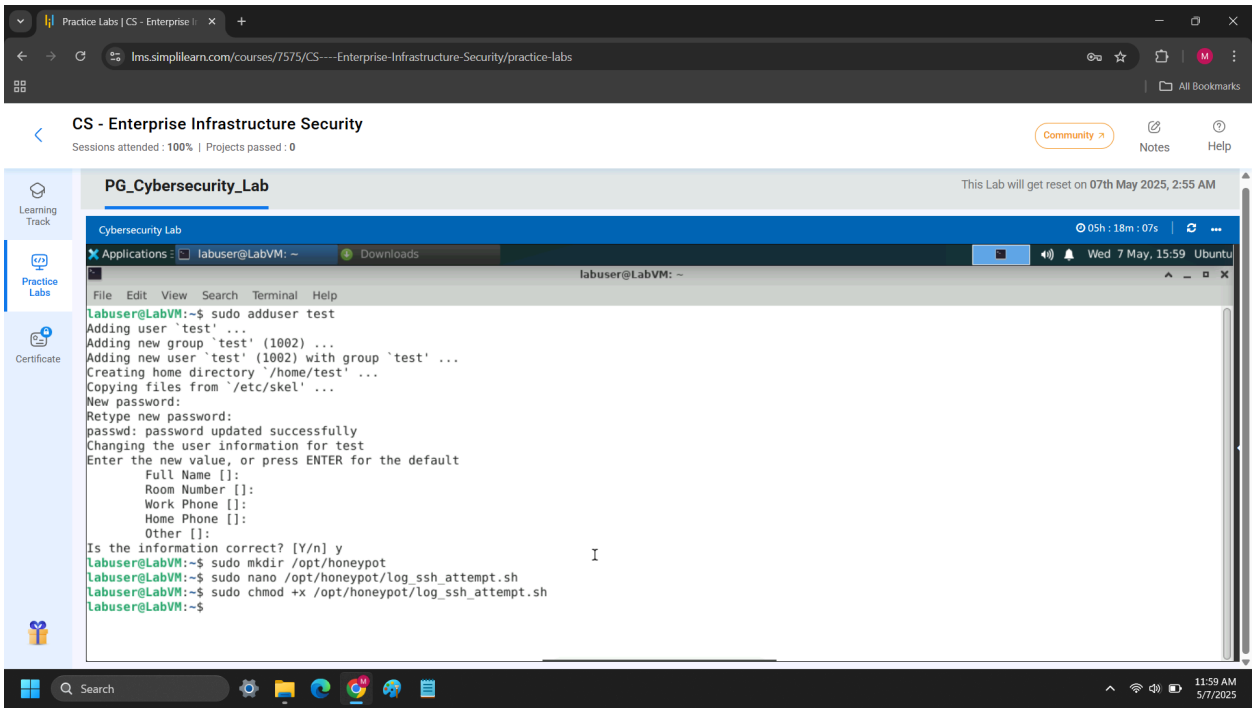
   exit 0



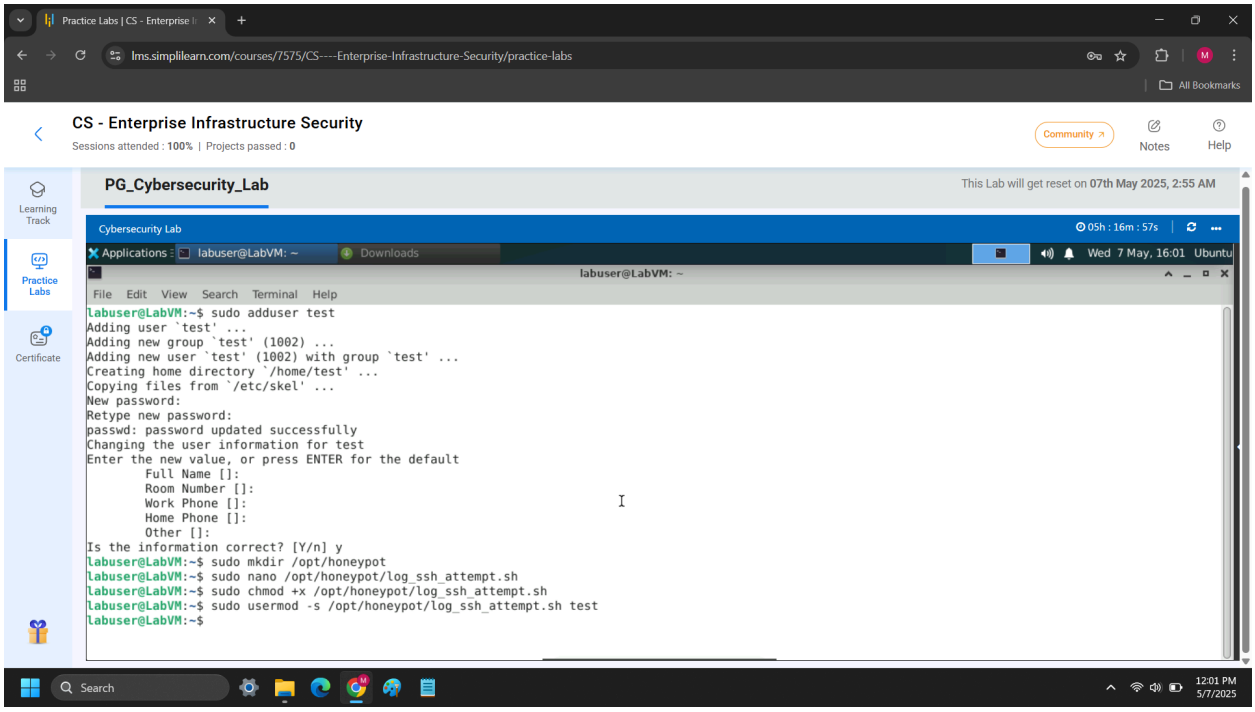
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

4. Making the script executable with command: ***sudo chmod +x /opt/honeypot/log_ssh_attempt.sh***



5. Changing the default shell for the honeypot user to the script; using command: ***sudo usermod -s /opt/honeypot/log_ssh_attempt.sh honeypot_user***



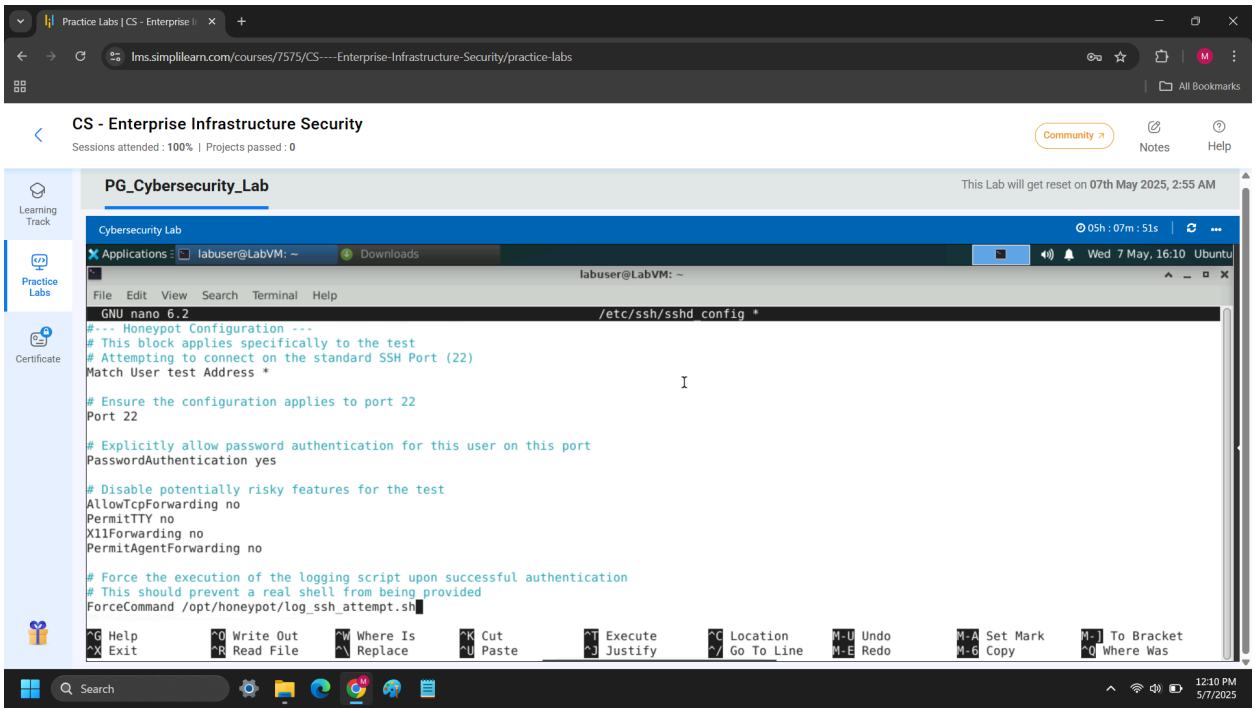
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

6. Configure SSH for the Honeypot User by using command: ***sudo nano /etc/ssh/sshs_config*** to bring up the file. Added a match block at the end of the file and saved the updates; the snippet is as follows:
Match User honeypot_user Address * Port 22

PasswordAuthentication yes
AllowTcpForwarding no
PermitTTY no
X11Fowarding no
PermitAgentFowarding no

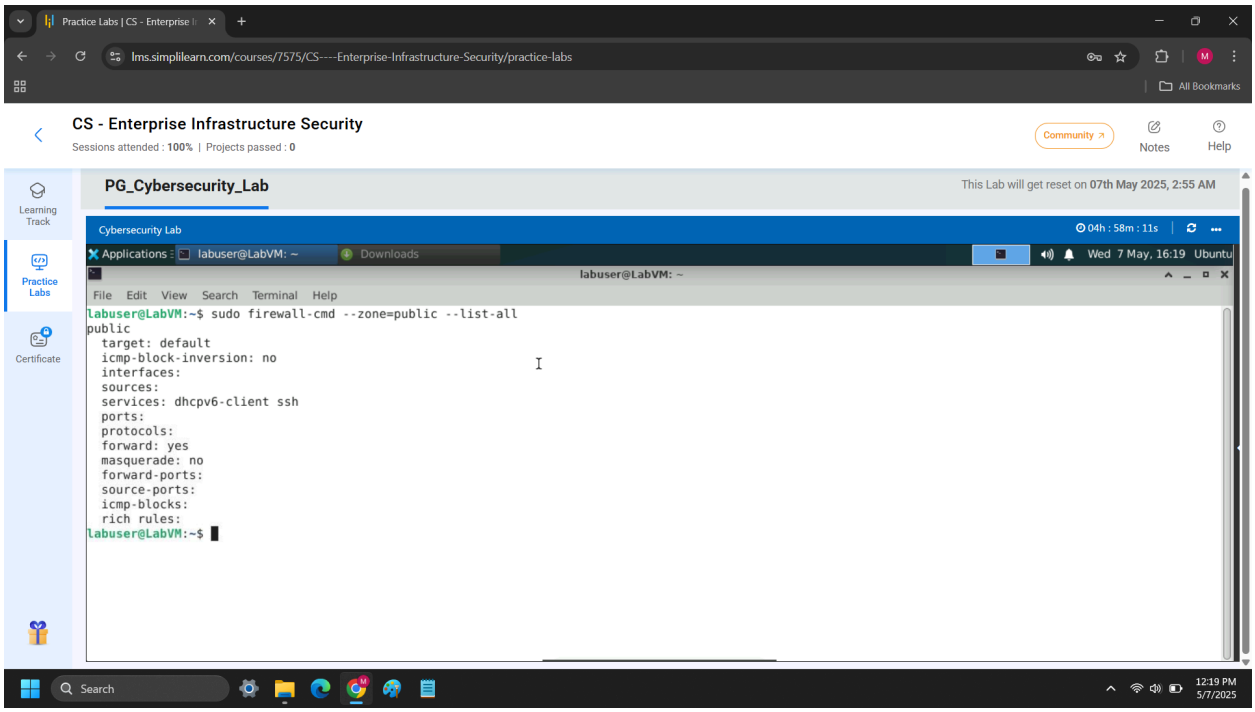
ForceCommand /opt/honeypot/log_ssh_attempt.sh



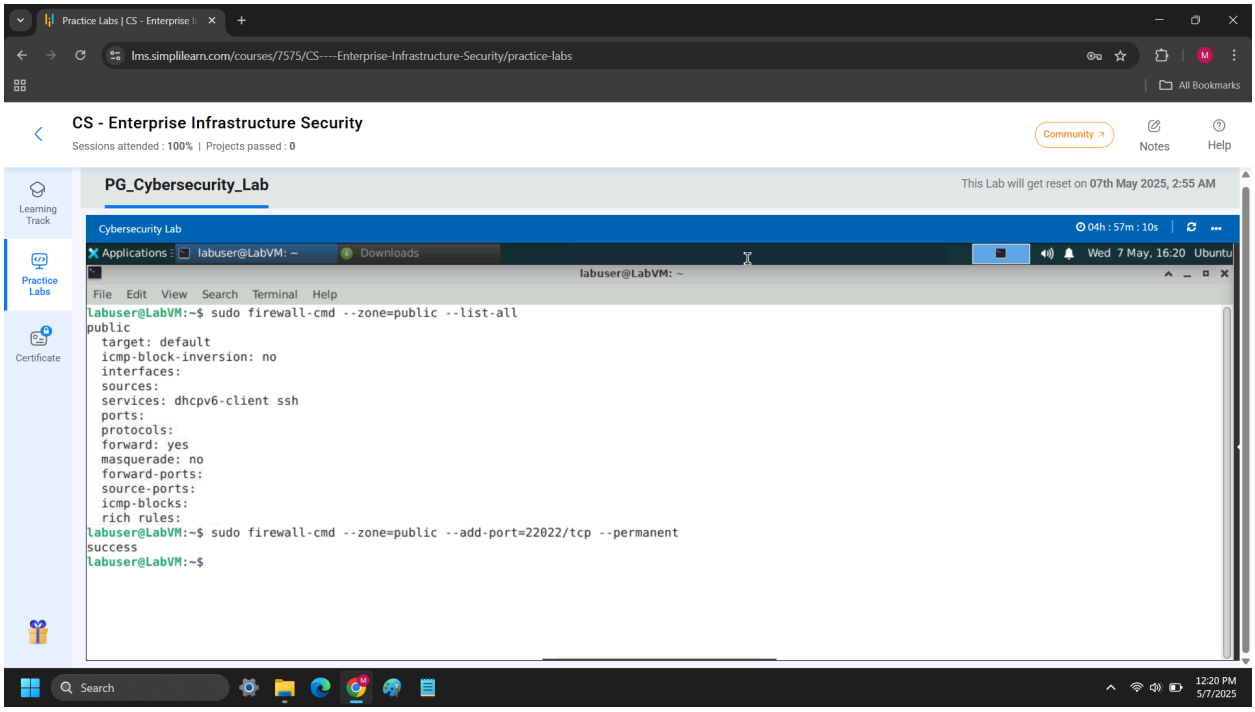
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

7. Checking current open ports/services on Firewalld; using command: ***sudo firewall-cmd --zone=public --list-all***



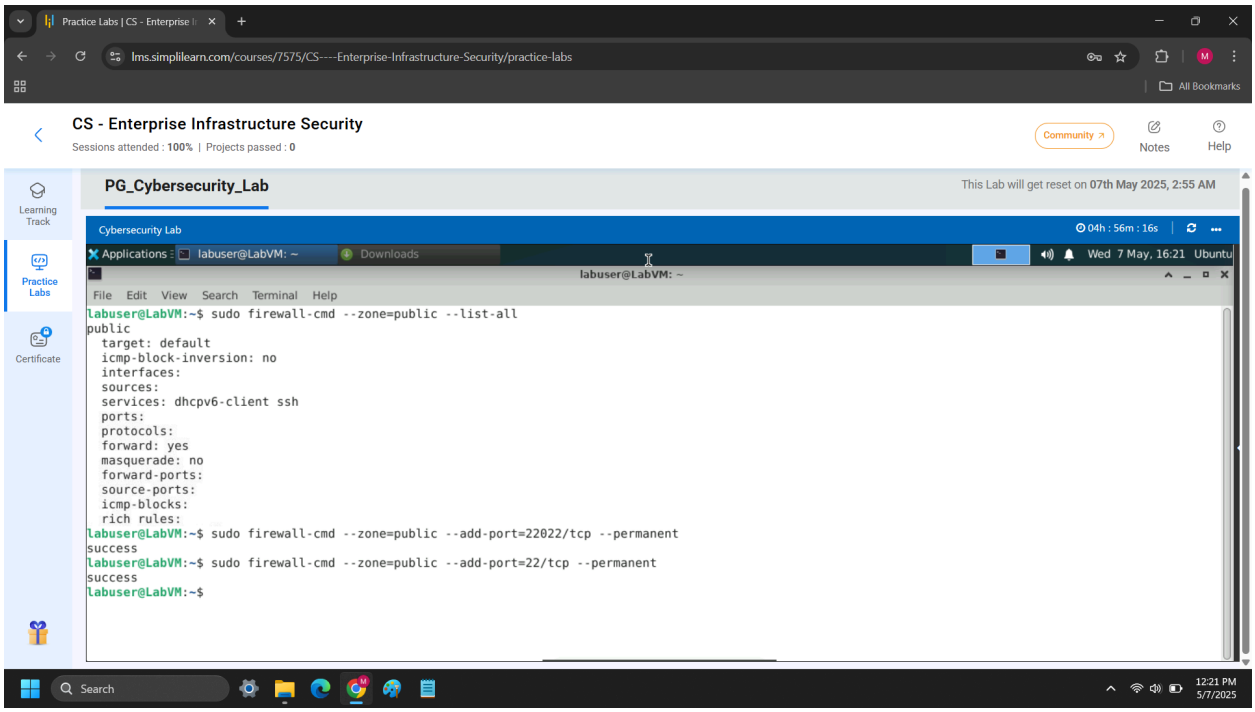
8. Adding the new SSH port; using command: ***sudo firewall-cmd --zone=public --add-port=22022/tcp --permanent***



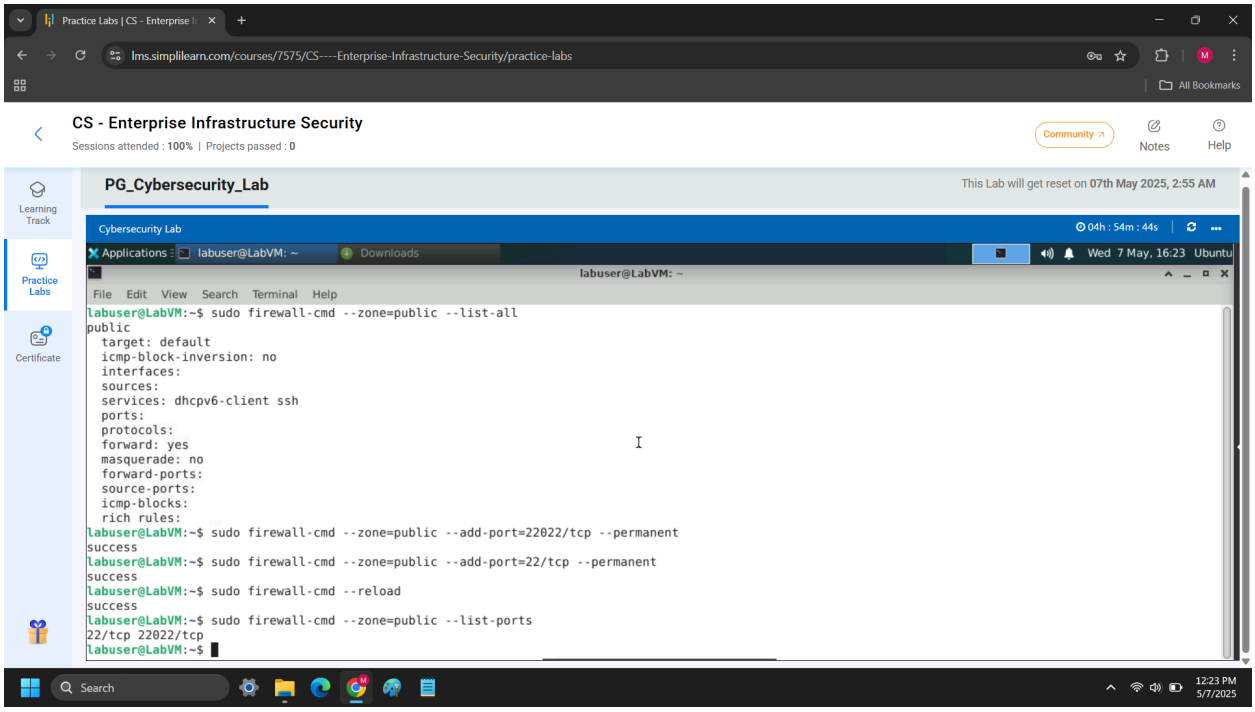
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

9. Adding the standard SSH port 22 for the honeypot; using command: ***sudo firewall-cmd --zone=public --add-port=22/tcp --permanent***



10. Refreshing Firewalld with command: ***sudo firewall-cmd --reload*** & verifying the changes with command: ***sudo firewall-cmd --zone=public --list-ports***

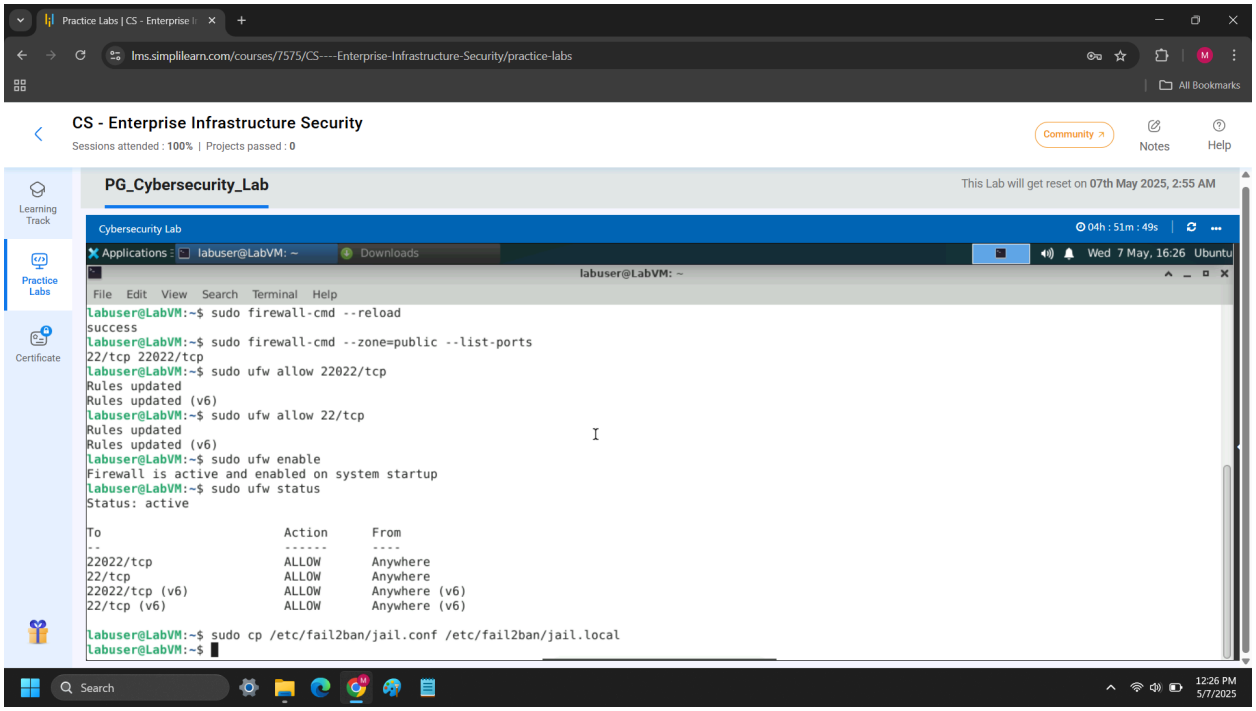


Screenshots for Course End Project: Linux Honeypot

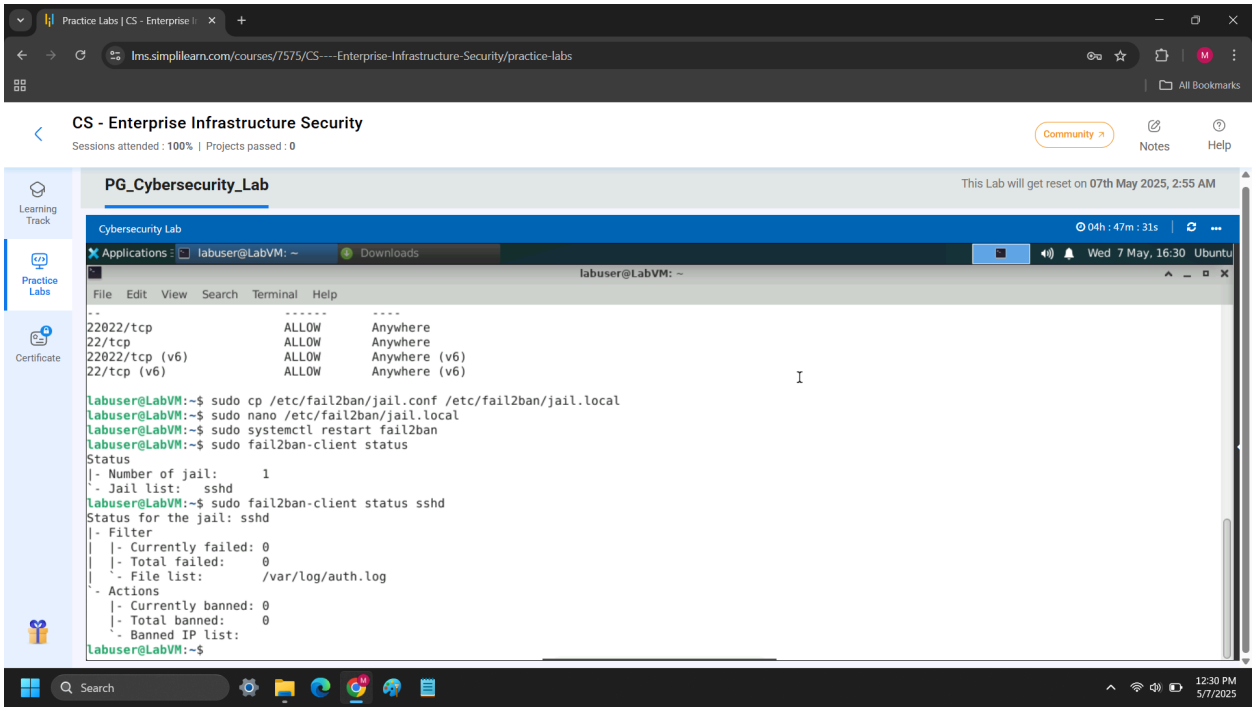
Michael Warner 5/7/25

Phase #4: Fail2Ban Configuration

1. Create a local configuration file, using command: ***sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local***



2. Double checked Configuring the SSH jail; no updates needed
3. Restarted Fail2Ban using command: ***sudo systemctl restart fail2ban***
4. Verified Fail2Ban status using command: ***sudo fail2ban-client status***
5. Checking the status of the sshd jail using command: ***sudo fail2ban-client status sshd***

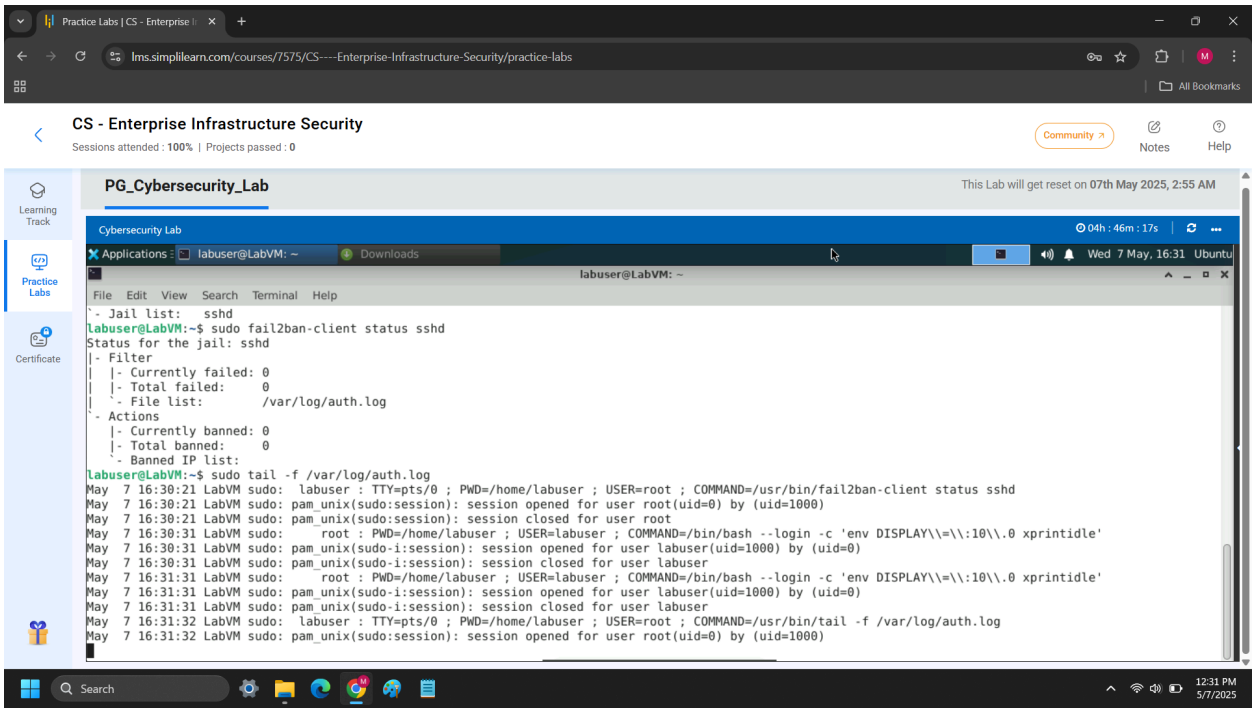


Screenshots for Course End Project: Linux Honeypot

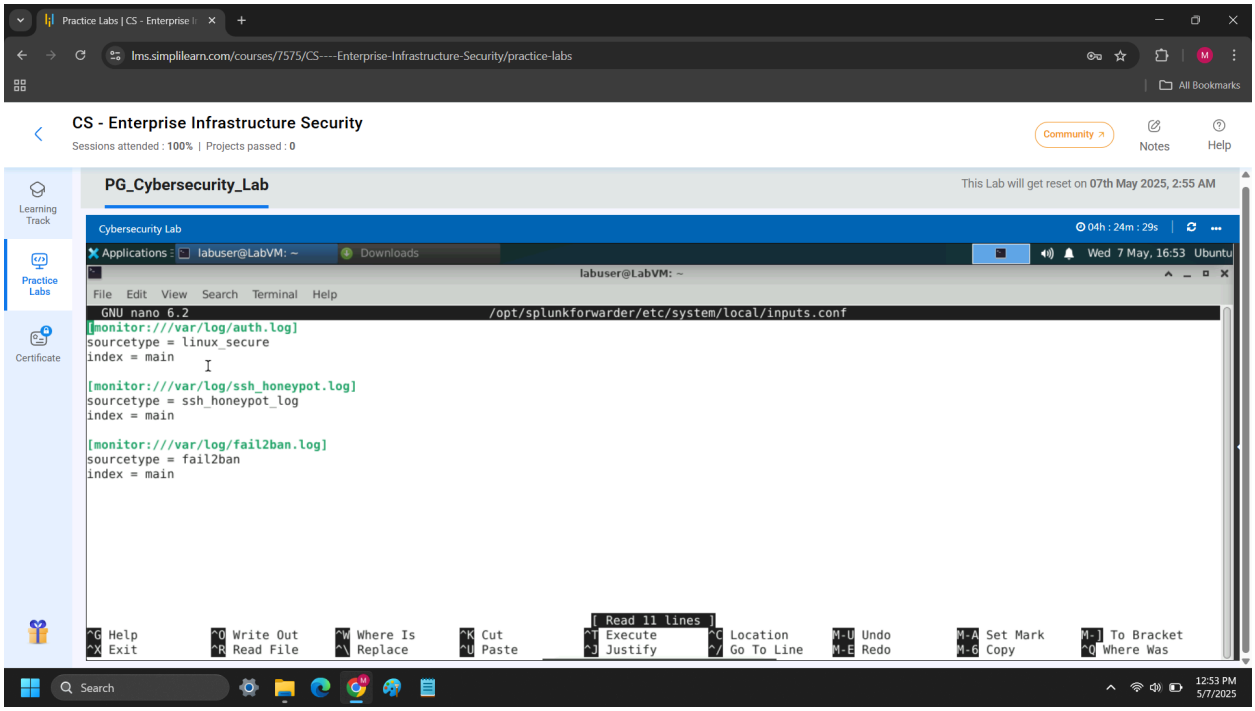
Michael Warner 5/7/25

Phase #5: Monitor of Logs & Integration into Splunk

1. Pulled up SSH authentication logs using command: ***sudo tail -f /var/log/auth.log***
2. Pulled up Fail2Ban's log file using command: ***sudo tail -f /var/log/fail2ban.log***



3. Configuring the Forwarder to Monitor Log Files using command: ***sudo nano /opt/splunkforwarder/etc/system/local/inputs.conf*** & added this stanzas for our log



Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

4. Telling Forwarder where Splunk Indexer is using command: ***sudo nano /opt/splunkforwarder/etc/system/local/outputs.conf &*** added this stanza pointing to whichever splunk index is needed