

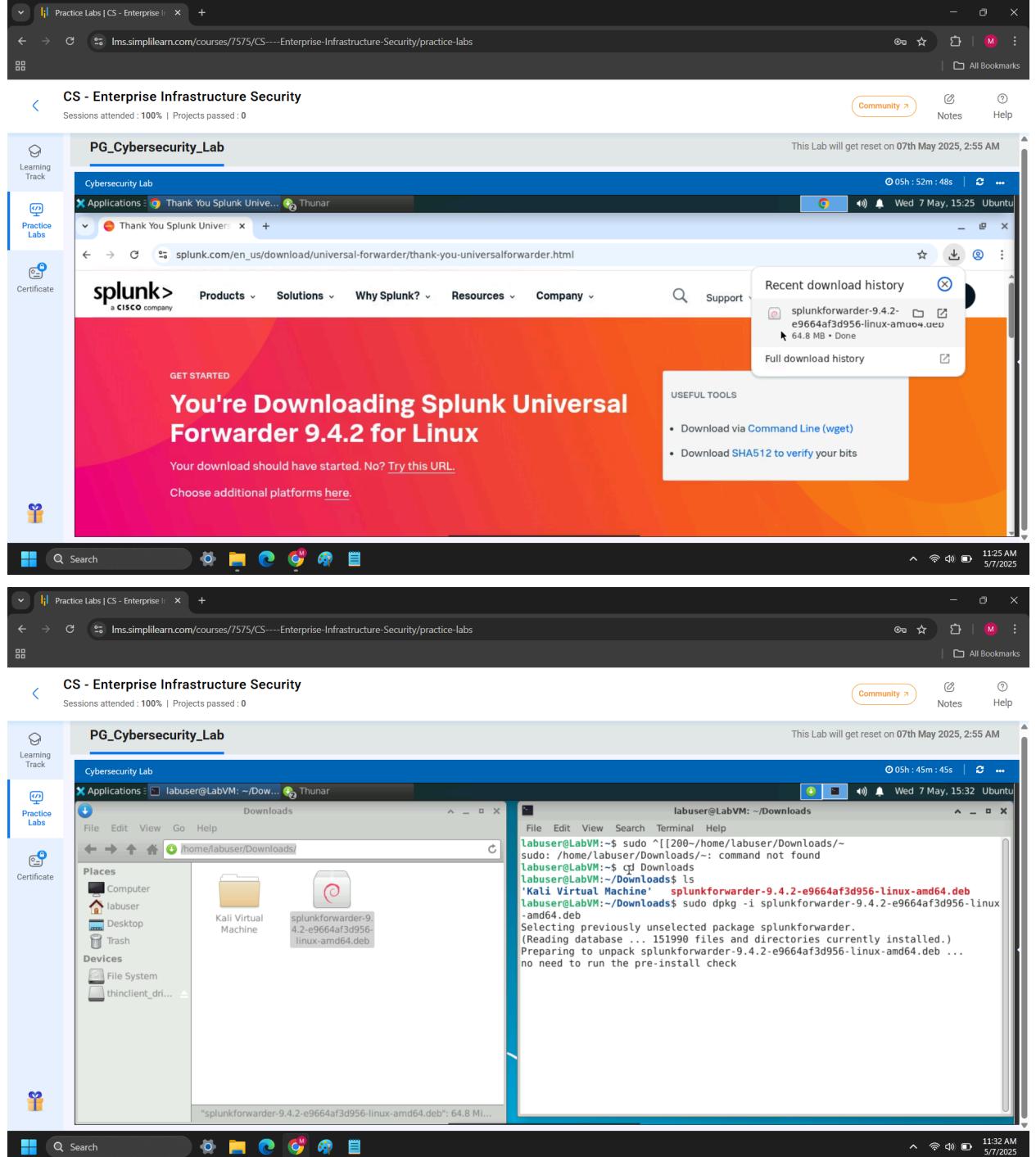
Screenshots for Course End Project: Linux Honeypot

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***

A screenshot of a Linux desktop environment showing a terminal window. The terminal title is 'Applications' and the command entered is 'labuser@LabVM: ~/Downloads\$ sudo apt install fail2ban -y'. The output shows the package being selected and installed.

```
labuser@LabVM:~$ sudo ^[[200~/home/labuser/Downloads/~
labuser@LabVM:~$ sudo dpkg -i splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 151990 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.2) ...
Setting up splunkforwarder (9.4.2) ...
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete
labuser@LabVM:~/Downloads$ sudo apt install fail2ban -y
Reading package lists... 39%
```

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

A screenshot of a Linux desktop environment showing a terminal window. The terminal title is 'Applications' and the command entered is 'labuser@LabVM: ~/Downloads\$ sudo apt install firewalld -y'. The output shows the package being selected and installed, including dependency resolution and file extraction.

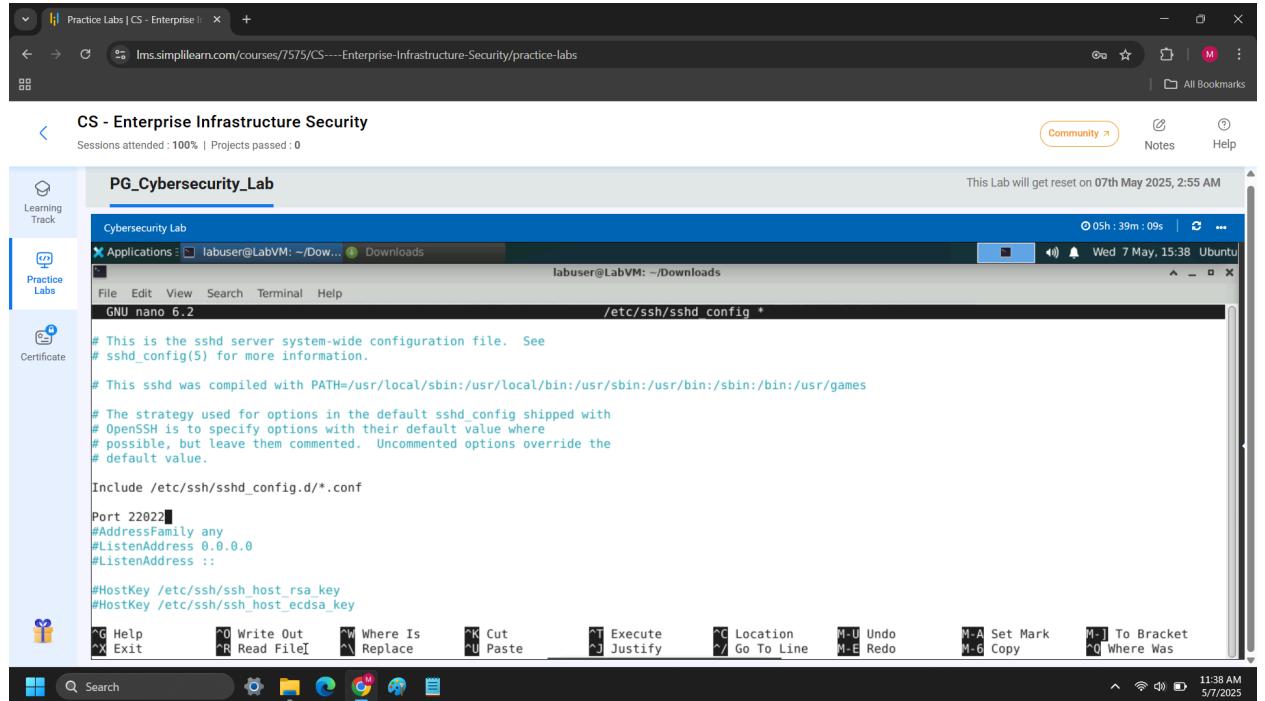
```
labuser@LabVM:~$ sudo apt install firewalld -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gir1.2-nm-1.0 ipset libipset13 libnm0 python3-cap-ng python3-firewall python3-nftables
The following NEW packages will be installed:
  firewalld gir1.2-nm-1.0 ipset libipset13 libnm0 python3-cap-ng python3-firewall python3-nftables
0 upgraded, 8 newly installed, 0 to remove and 7 not upgraded.
Need to get 1188 kB of archives.
After this operation, 6158 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnm0 amd64 1:36.6-0ubuntu2.1 [456 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 gir1.2-nm-1.0 amd64 1:36.6-0ubuntu2.1 [84.1 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 python3-nftables amd64 1:0.2-1ubuntu3 [11.5 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-firewall all 1:1.1-1ubuntul [130 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 firewalld all 1:1.1-1ubuntul [394 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libipset13 amd64 7.15-1build1 [63.4 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-cap-ng amd64 0.7.9-2.2build3 [17.1 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 ipset amd64 7.15-1build1 [32.8 kB]
Fetched 1188 kB in 5s (251 kB/s)
Selecting previously unselected package libnm0:amd64.
(Reading database ... 153102 files and directories currently installed.)
Preparing to unpack .../0-libnm0 1:36.6-0ubuntu2.1 amd64.deb ...
Unpacking libnm0:amd64 (1:36.6-0ubuntu2.1) ...
```

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 /etc/ssh/sshd_config**
2. Changed **#Port 22** to **22022**



```
GNU nano 6.2
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

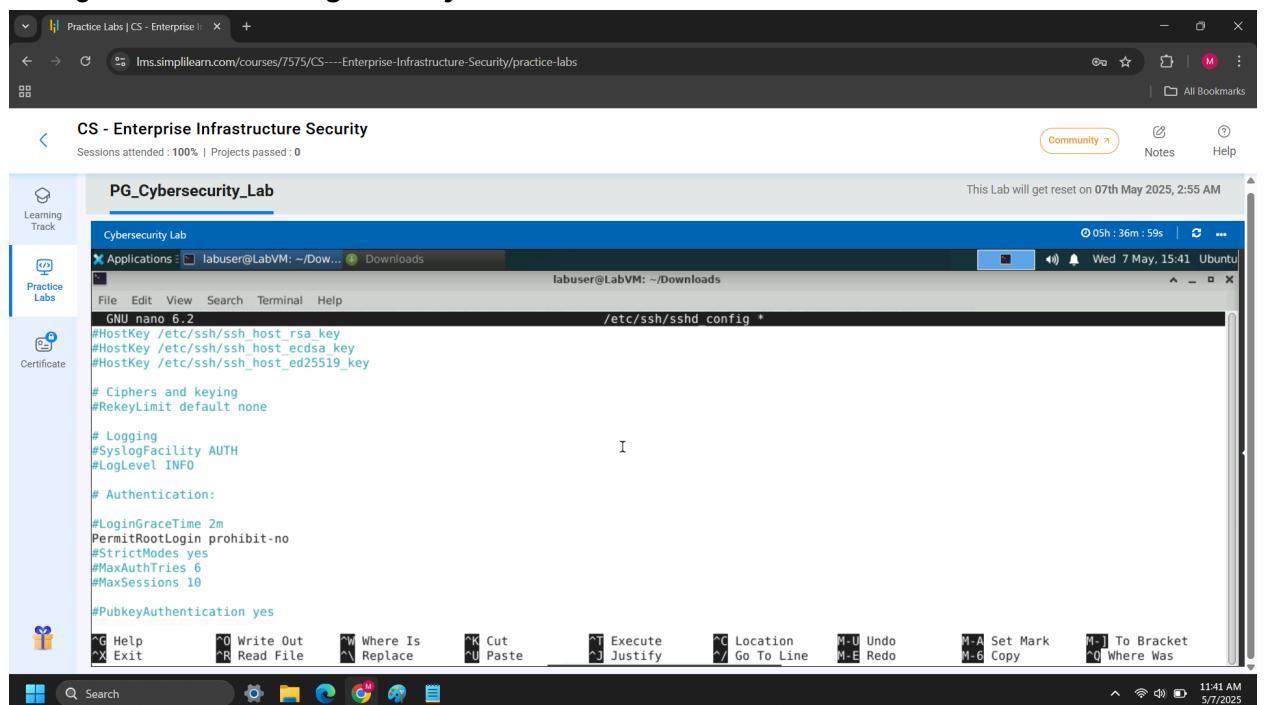
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
```

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



```
GNU nano 6.2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

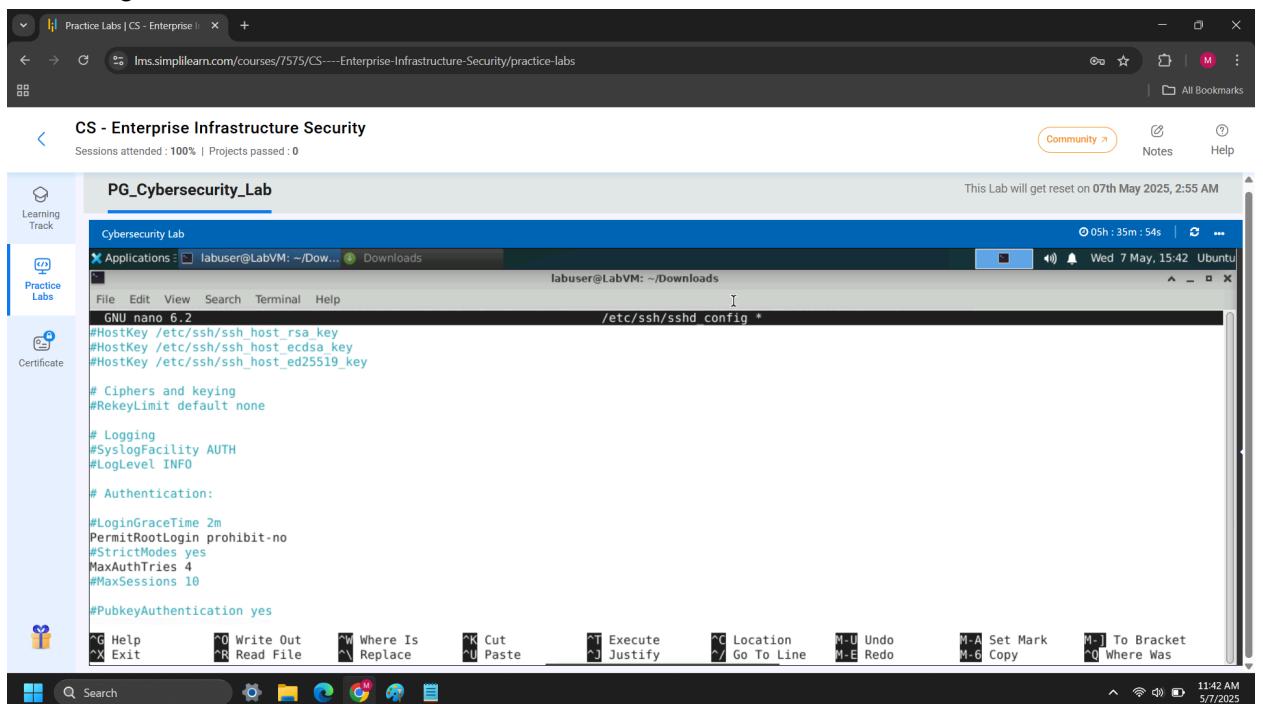
#LoginGraceTime 2m
PermitRootLogin prohibit-no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

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



```
GNU nano 6.2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

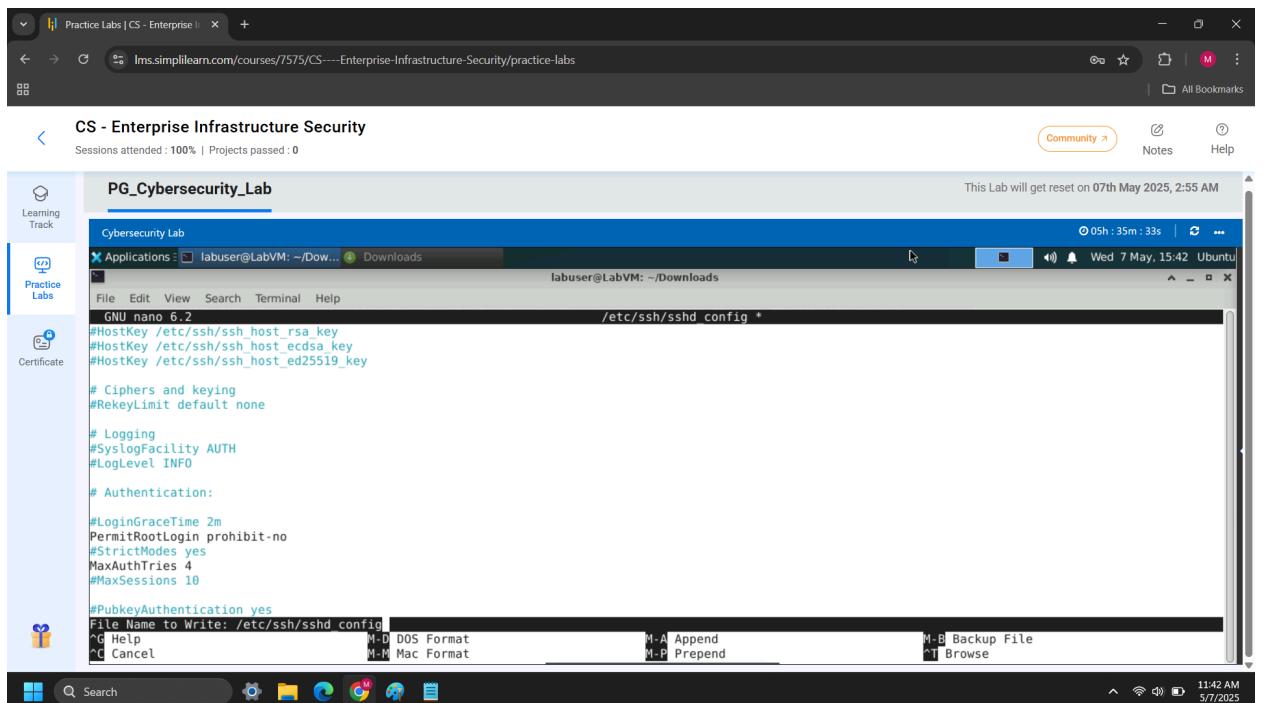
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-no
#StrictModes yes
MaxAuthTries 4
#MaxSessions 10

#PubkeyAuthentication yes
```



```
GNU nano 6.2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-no
#StrictModes yes
MaxAuthTries 4
#MaxSessions 10

#PubkeyAuthentication yes
```

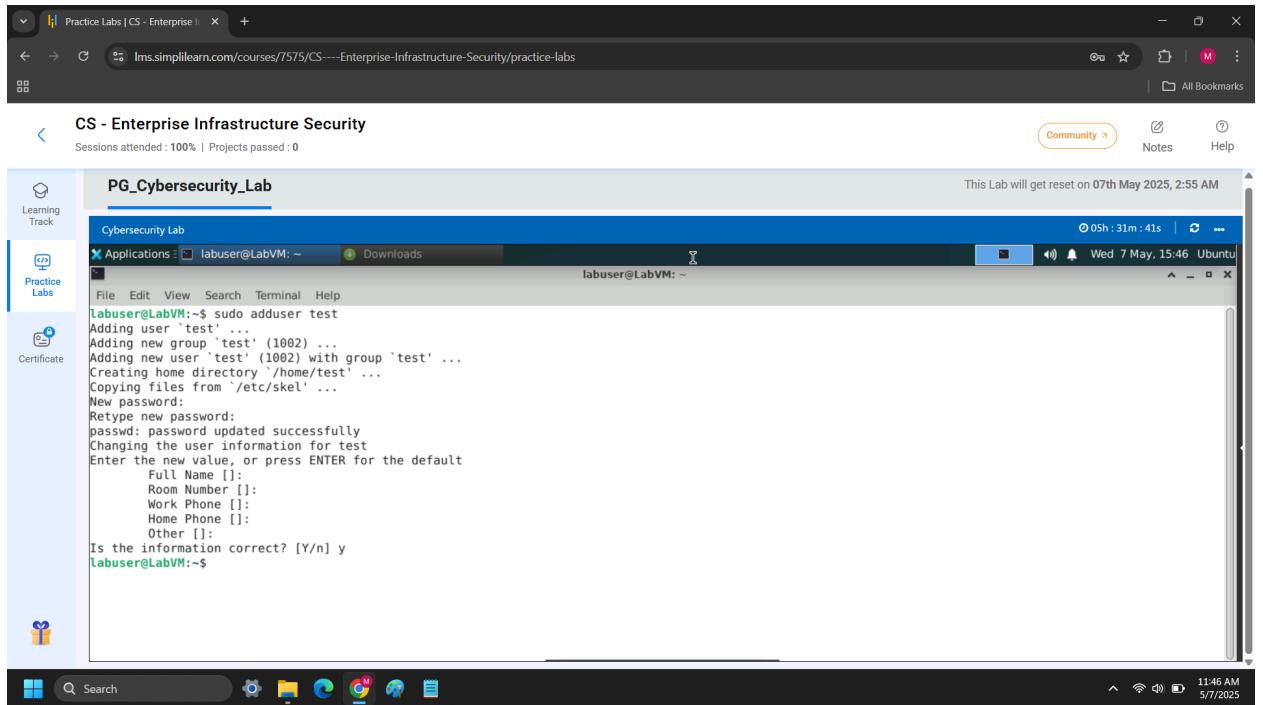
File Name to Write: /etc/ssh/sshd config

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**

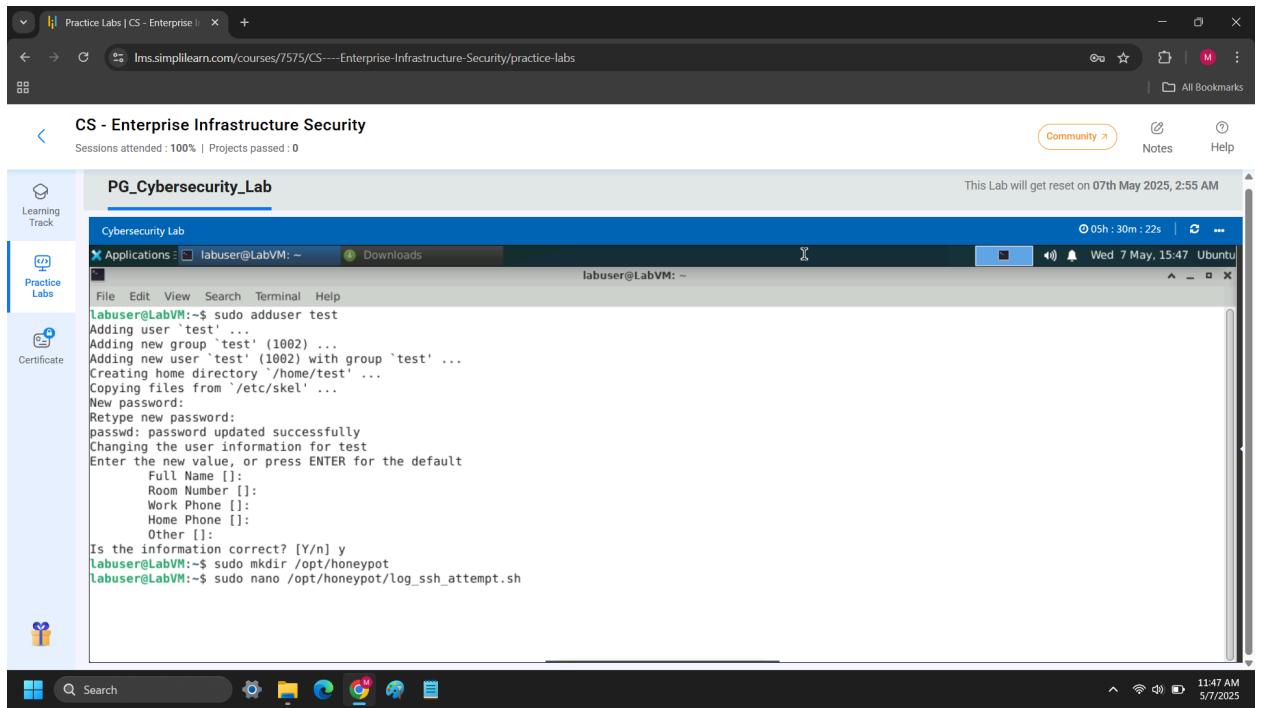


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Applications" and the command being run is "sudo adduser test". The output of the command shows the creation of a new user "test" with a password update and confirmation. The terminal window is part of a desktop interface with a sidebar containing "Learning Track", "Practice Labs", and "Certificate" sections.

```
labuser@LabVM:~$ sudo adduser test
Adding user 'test' ...
Adding new group 'test' (1002) ...
Adding new user 'test' (1002) with group 'test' ...
Creating home directory '/home/test' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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] y
labuser@LabVM:~$
```

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



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Applications" and the command being run is "sudo adduser test". The output of the command shows the creation of a new user "test" with a password update and confirmation. The terminal window is part of a desktop interface with a sidebar containing "Learning Track", "Practice Labs", and "Certificate" sections. Below the terminal window, the command "sudo mkdir /opt/honeypot" is run, followed by "sudo nano /opt/honeypot/log_ssh_attempt.sh" to create the script file.

```
labuser@LabVM:~$ sudo adduser test
Adding user 'test' ...
Adding new group 'test' (1002) ...
Adding new user 'test' (1002) with group 'test' ...
Creating home directory '/home/test' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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] y
labuser@LabVM:~$ sudo mkdir /opt/honeypot
labuser@LabVM:~$ sudo nano /opt/honeypot/log_ssh_attempt.sh
```

Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

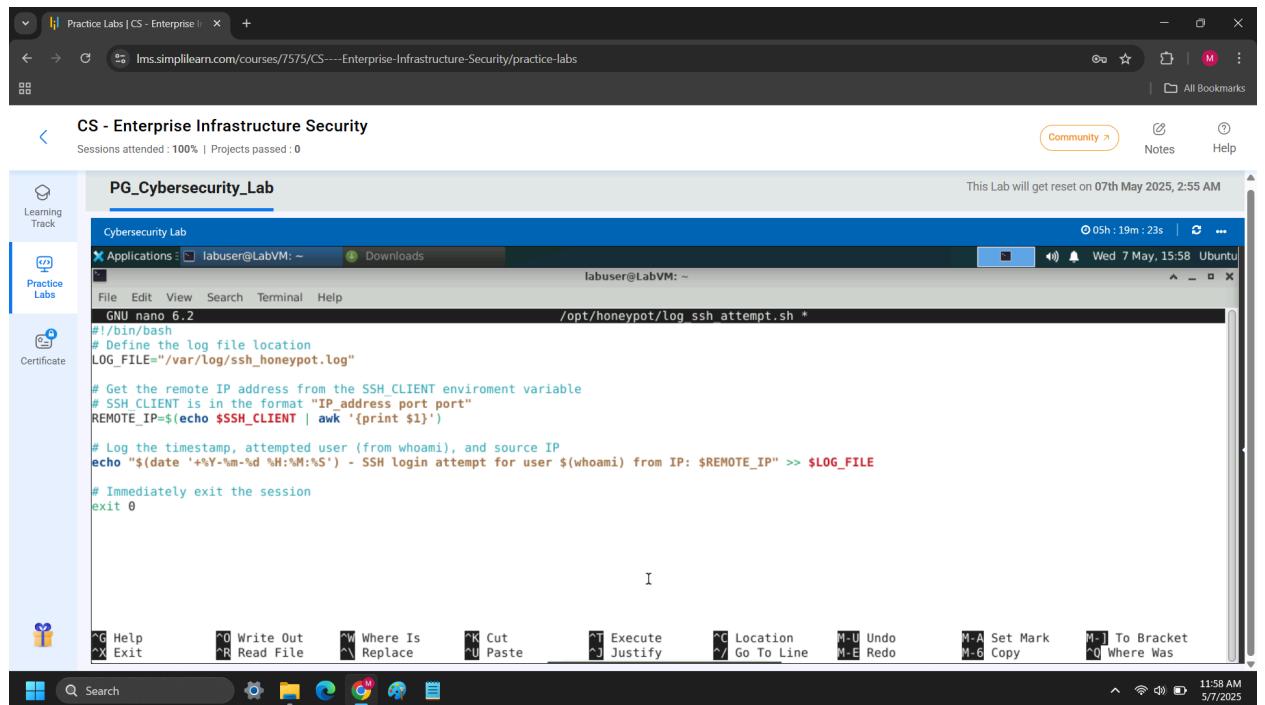
3. Typed the following content into the script & saved file:

```
#!/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
```

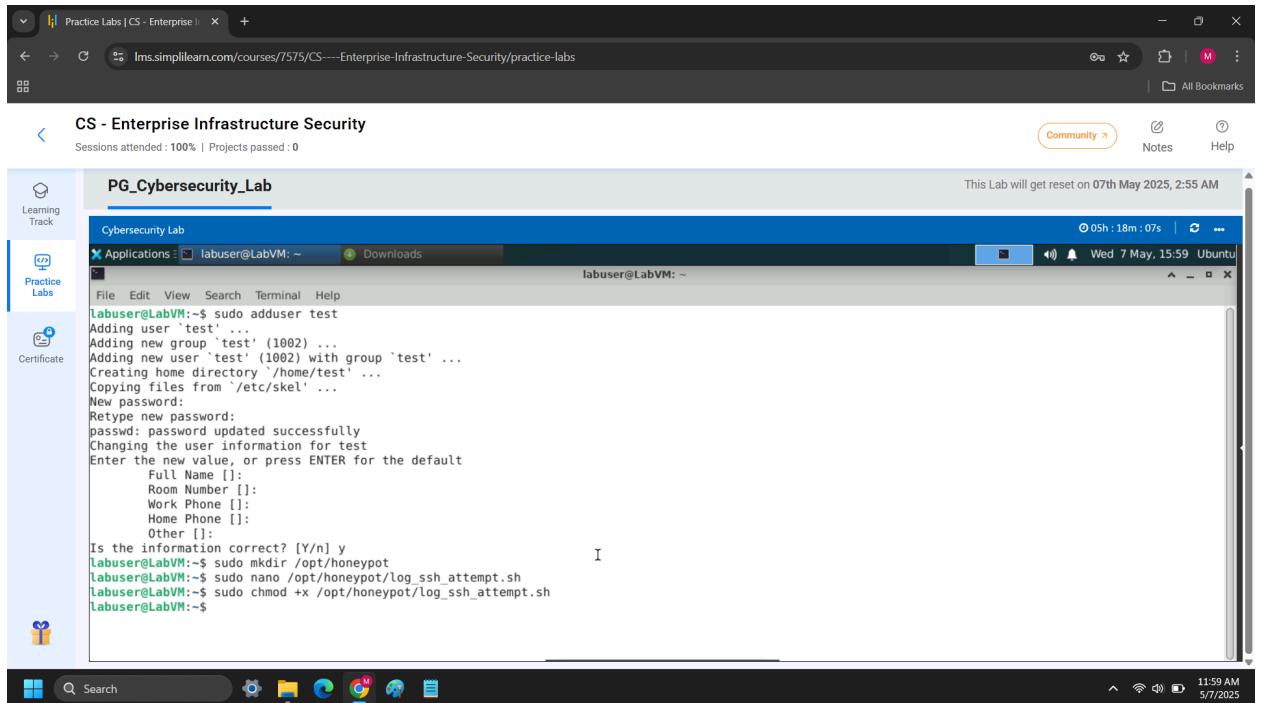
```
exit 0
```



Screenshots for Course End Project: Linux Honeypot

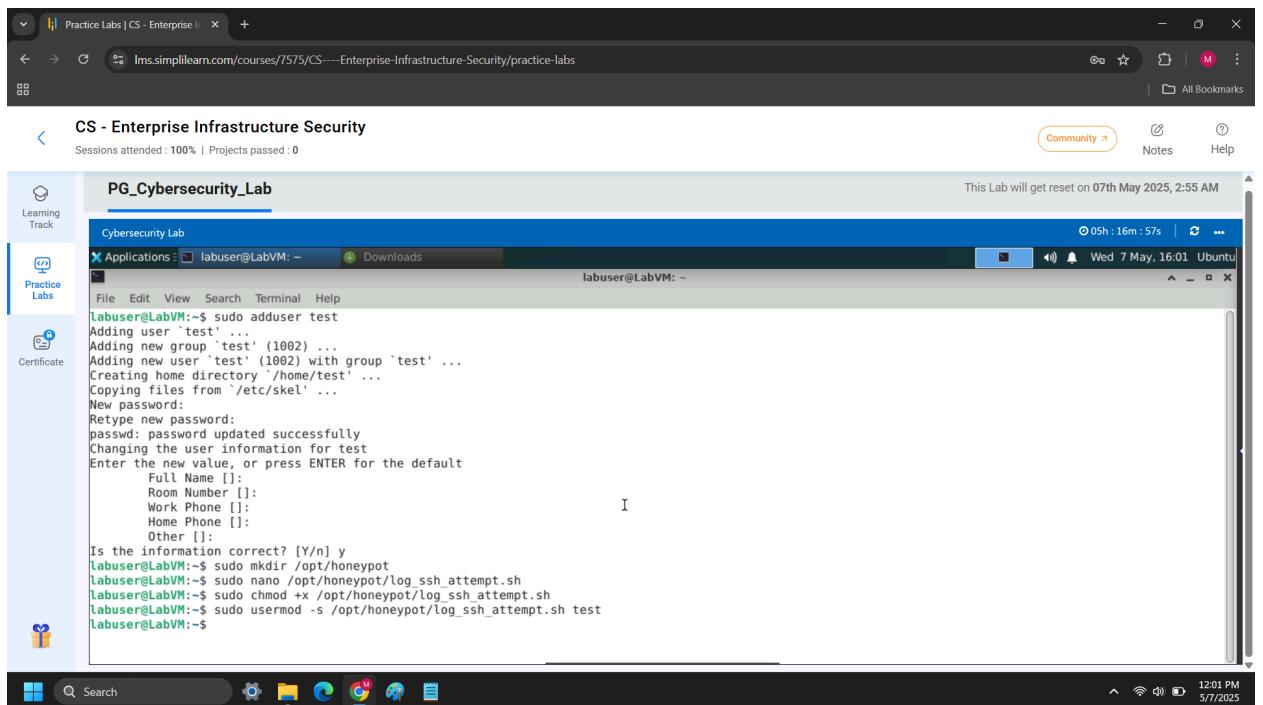
Michael Warner 5/7/25

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



```
labuser@LabVM:~$ sudo adduser test
Adding user `test' ...
Adding new group `test' (1002) ...
Adding new user `test' (1002) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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] y
labuser@LabVM:~$ sudo mkdir /opt/honeypot
labuser@LabVM:~$ sudo nano /opt/honeypot/log_ssh_attempt.sh
labuser@LabVM:~$ sudo chmod +x /opt/honeypot/log_ssh_attempt.sh
labuser@LabVM:~$
```

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**



```
labuser@LabVM:~$ sudo adduser test
Adding user `test' ...
Adding new group `test' (1002) ...
Adding new user `test' (1002) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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] y
labuser@LabVM:~$ sudo mkdir /opt/honeypot
labuser@LabVM:~$ sudo nano /opt/honeypot/log_ssh_attempt.sh
labuser@LabVM:~$ sudo chmod +x /opt/honeypot/log_ssh_attempt.sh
labuser@LabVM:~$ sudo usermod -s /opt/honeypot/log_ssh_attempt.sh test
labuser@LabVM:~$
```

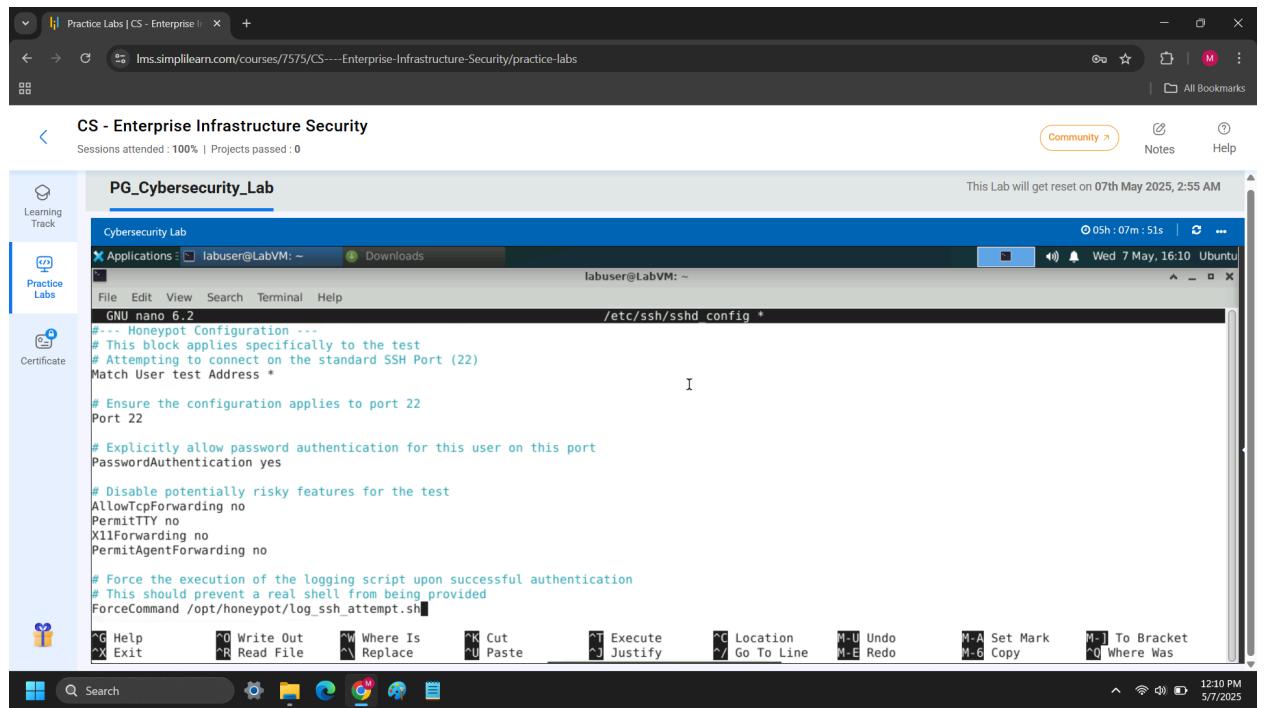
Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

6. Configure SSH for the Honeypot User by using command: **sudo nano /etc/ssh/sshd_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  
X11Forwarding no  
PermitAgentForwarding 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**

A screenshot of a web browser window titled "CS - Enterprise Infrastructure Security". The URL is "lms.simplilearn.com/courses/7575/CS----Enterprise-Infrastructure-Security/practice-labs". The main content area shows a terminal window titled "PG_Cybersecurity_Lab" running on "Ubuntu". The terminal displays the output of the command "sudo firewall-cmd --zone=public --list-all". The output shows the configuration for the "public" zone, including target, interfaces, sources, services, ports, protocols, forward, masquerade, forward-ports, source-ports, icmp-blocks, and rich rules.

```
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
labuser@LabVM:~$
```

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

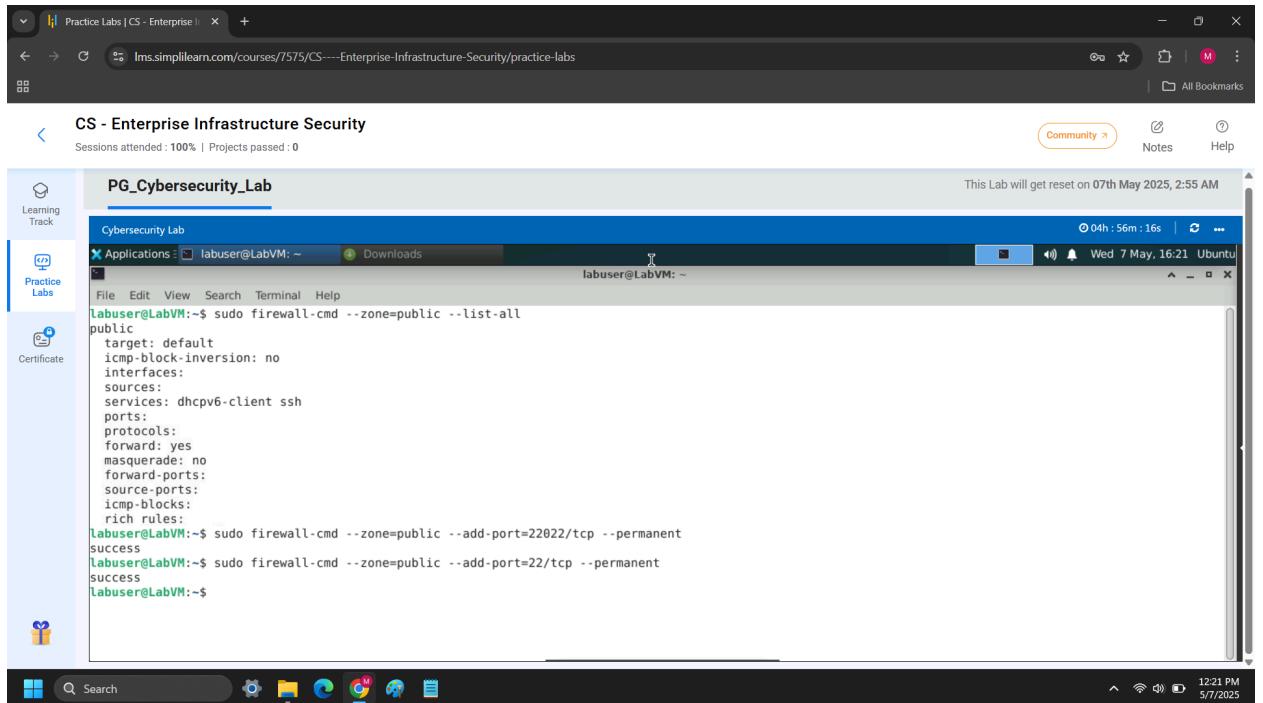
A screenshot of a web browser window titled "CS - Enterprise Infrastructure Security". The URL is "lms.simplilearn.com/courses/7575/CS----Enterprise-Infrastructure-Security/practice-labs". The main content area shows a terminal window titled "PG_Cybersecurity_Lab" running on "Ubuntu". The terminal displays the output of the command "sudo firewall-cmd --zone=public --list-all" followed by "sudo firewall-cmd --zone=public --add-port=22022/tcp --permanent". The output shows the configuration for the "public" zone, including target, interfaces, sources, services, ports, protocols, forward, masquerade, forward-ports, source-ports, icmp-blocks, and rich rules, with the addition of the new port rule.

```
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
labuser@LabVM:~$ sudo firewall-cmd --zone=public --add-port=22022/tcp --permanent
success
labuser@LabVM:~$
```

Screenshots for Course End Project: Linux Honeypot

Michael Warner 5/7/25

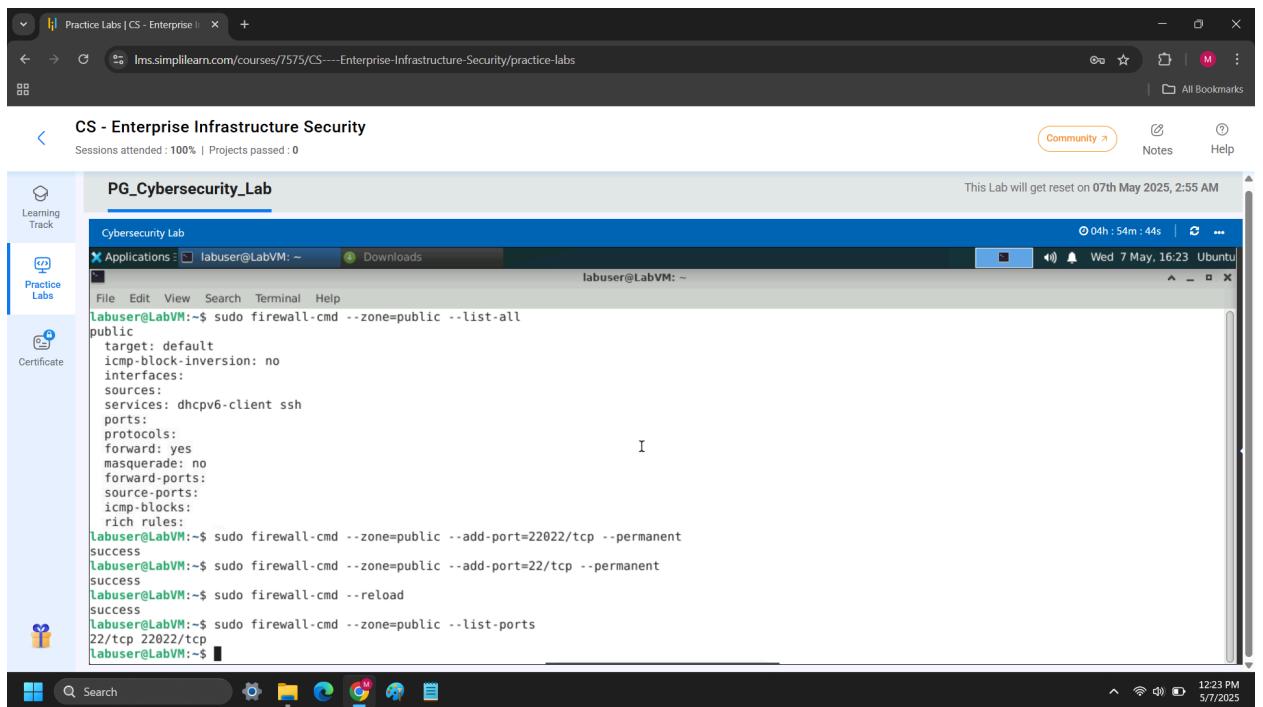
- Adding the standard SSH port 22 for the honeypot; using command: **sudo firewall-cmd --zone=public --add-port=22/tcp --permanent**



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "PG_Cybersecurity_Lab". The terminal content shows the execution of the following commands:

```
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
labuser@LabVM:~$ sudo firewall-cmd --zone=public --add-port=22022/tcp --permanent
success
labuser@LabVM:~$ sudo firewall-cmd --zone=public --add-port=22/tcp --permanent
success
labuser@LabVM:~$
```

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



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "PG_Cybersecurity_Lab". The terminal content shows the execution of the following commands:

```
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
labuser@LabVM:~$ sudo firewall-cmd --zone=public --add-port=22022/tcp --permanent
success
labuser@LabVM:~$ sudo firewall-cmd --zone=public --add-port=22/tcp --permanent
success
labuser@LabVM:~$ sudo firewall-cmd --reload
success
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-ports
22/tcp 22022/tcp
labuser@LabVM:~$
```

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**

A screenshot of a Linux desktop environment showing a terminal window titled "PG_Cybersecurity_Lab". The terminal shows the following commands being run:

```
labuser@LabVM:~$ sudo firewall-cmd --reload
success
labuser@LabVM:~$ sudo firewall-cmd --zone=public --list-ports
22/tcp 22022/tcp
labuser@LabVM:~$ sudo ufw allow 22022/tcp
Rules updated
Rules updated (v6)
labuser@LabVM:~$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
labuser@LabVM:~$ sudo ufw enable
Firewall is active and enabled on system startup
labuser@LabVM:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
22022/tcp    ALLOW     Anywhere
22/tcp       ALLOW     Anywhere
22022/tcp (v6) ALLOW     Anywhere (v6)
22/tcp (v6)   ALLOW     Anywhere (v6)

labuser@LabVM:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
labuser@LabVM:~$
```

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**

A screenshot of a Linux desktop environment showing a terminal window titled "PG_Cybersecurity_Lab". The terminal shows the following commands being run:

```
-- 
22022/tcp    ALLOW     Anywhere
22/tcp       ALLOW     Anywhere
22022/tcp (v6) ALLOW     Anywhere (v6)
22/tcp (v6)   ALLOW     Anywhere (v6)

labuser@LabVM:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
labuser@LabVM:~$ sudo nano /etc/fail2ban/jail.local
labuser@LabVM:~$ sudo systemctl restart fail2ban
labuser@LabVM:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:          sshd
labuser@LabVM:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:      0
| |- File list:          /var/log/auth.log
`- Actions
  |- Currently banned: 0
  |- Total banned:      0
  `|- Banned IP list:
```

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`**

CS - Enterprise Infrastructure Security

Sessions attended : 100% | Projects passed : 0

Community ↗ Notes Help

PG_Cybersecurity_Lab

Cybersecurity Lab

This Lab will get reset on 07th May 2025, 2:55 AM

04h:46m:17s | Wed 7 May 2025, 16:31 Ubuntu

Applications labuser@LabVM: ~ Downloads labuser@LabVM: ~

File Edit View Terminal Help

```
~- Jail list: sshd
labuser@LabVM:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- File list: /var/log/auth.log
- Actions
| |- Currently banned: 0
| |- Total banned: 0
| - Banned IP list:
labuser@LabVM:~$ sudo tail -f /var/log/auth.log
May 7 16:30:21 LabVM sudo: labuser : TTY:pts/0 ; PWD=/home/labuser ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
May 7 16:30:21 LabVM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 7 16:30:21 LabVM sudo: pam_unix(sudo:session): session closed for user root
May 7 16:30:31 LabVM sudo: root : PWD=/home/labuser ; USER=labuser ; COMMAND=/bin/bash --login -c 'env DISPLAY\\=\\:10\\.0 xprintidle'
May 7 16:30:31 LabVM sudo: pam_unix(sudo:session): session opened for user labuser(uid=1000) by (uid=0)
May 7 16:30:31 LabVM sudo: pam_unix(sudo:session): session closed for user labuser
May 7 16:31:31 LabVM sudo: root : PWD=/home/labuser ; USER=labuser ; COMMAND=/bin/bash --login -c 'env DISPLAY\\=\\:10\\.0 xprintidle'
May 7 16:31:31 LabVM sudo: pam_unix(sudo:session): session opened for user labuser(uid=1000) by (uid=0)
May 7 16:31:31 LabVM sudo: pam_unix(sudo:session): session closed for user labuser
May 7 16:31:32 LabVM sudo: labuser : TTY:pts/0 ; PWD=/home/labuser ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
May 7 16:31:32 LabVM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
```

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

CS - Enterprise Infrastructure Security

Sessions attended : 100% | Projects passed : 0

Community Notes Help

PG_Cybersecurity_Lab

This Lab will get reset on 07th May 2025, 2:55 AM

04h: 24m: 29s Wed 7 May, 16:53 Ubuntu

Cybersecurity Lab

Applications labuser@LabVM: ~ Downloads

GNU nano 6.2 /opt/splunkforwarder/etc/system/local/inputs.conf

```
[monitor:///var/log/auth.log]
sourcetype = linux_secure
index = main

[monitor:///var/log/ssh_honeypot.log]
sourcetype = ssh_honeypot_log
index = main

[monitor:///var/log/fail2ban.log]
sourcetype = fail2ban
index = main
```

File Edit View Search Terminal Help

^G Help ^O Write Out ^W Where Is ^X Cut ^R Read File ^U Replace ^K Paste [Read 11 lines] ^E Execute ^C Location M-U Undo M-A Set Mark M-J To Bracket M-B Copy M-Q Where Was

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

