CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-1

Performing Reconnaissance from the WAN

Student Info:
Name : Akhila Parankusham
Student ID: 00810899
Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

Banner Grabbing

We'll start a connection to the pfSense firewall's external IP address in order to get banner data. The network will also be examined and open ports will be found using nmap.

Service Detection

Our goal is to identify the software and operating system that are present on the internal computers that are protected by the firewall that faces externally.

Remote Desktop Protocol

We will launch a Remote Desktop Protocol (RDP) session and access the Microsoft Windows Server using the supplied credentials.

Objectives

The primary objective of the reconnaissance mission was to gather information about the target networks and systems with an emphasis on locating potential security flaws.

Lab Description Details:

1. Lab Environment Setup**:** Setting up a regulated network environment with different network services, such as email, FTP, and web servers.
2. Banner Grabbing Essentials: Exploration of the core idea behind banner snatching, with emphasis on its crucial function in the reconnaissance process.
3. Knowledge of Tools: A working knowledge of how to use banner capture software in the target network, such as Telnet, Netcat, and Nmap.
4. Knowledge of data interpretation: Gaining proficiency in interpreting and extrapolating meaning from the data gathered by banner capturing, such as service version, category, and setup.
5. Exploitation insights for vulnerabilities: Gaining knowledge of the methods by which the information acquired through banner capture can be used successfully to locate and possibly exploit vulnerabilities present in the target network.

Step 1: Log in to the Kali Linux.

Enter the credentials. Username: **root**

Password: **toor**

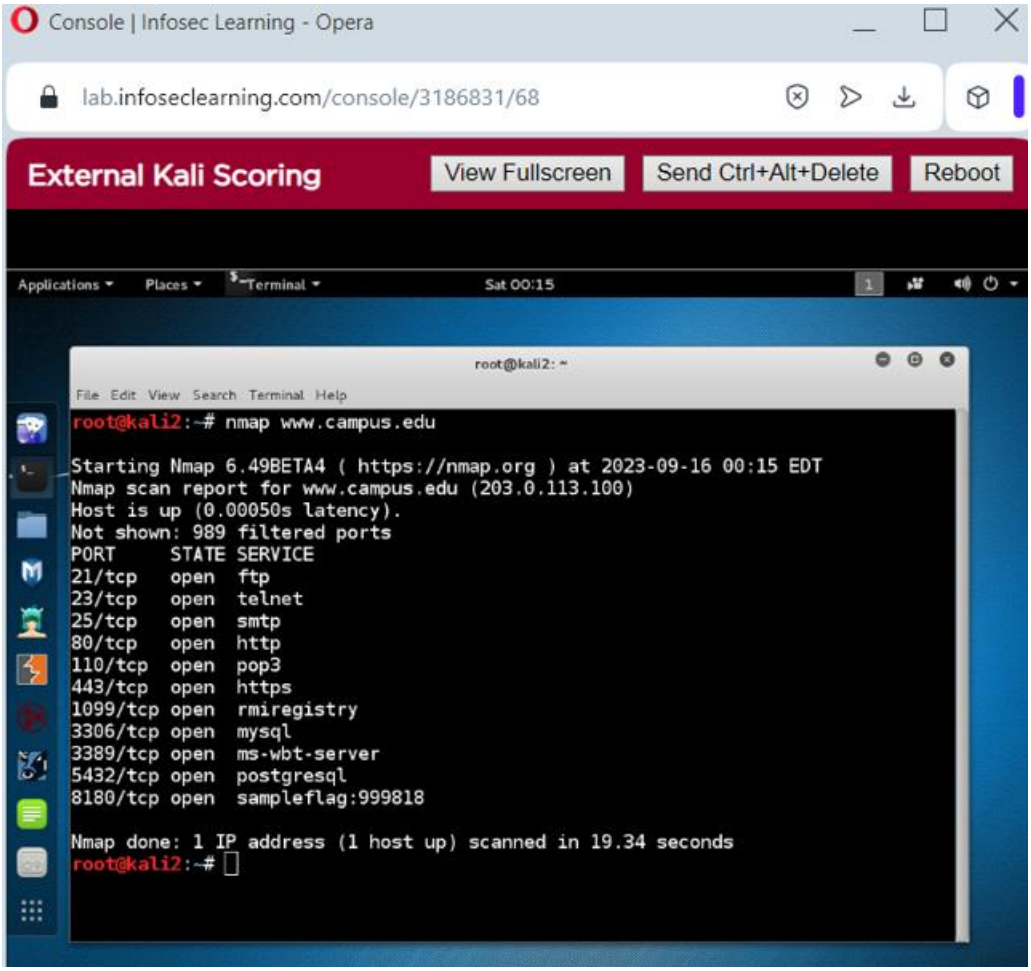
Step 2: Open the terminal.

Step 3: Determine the open ports.

Network is: www.campus.edu

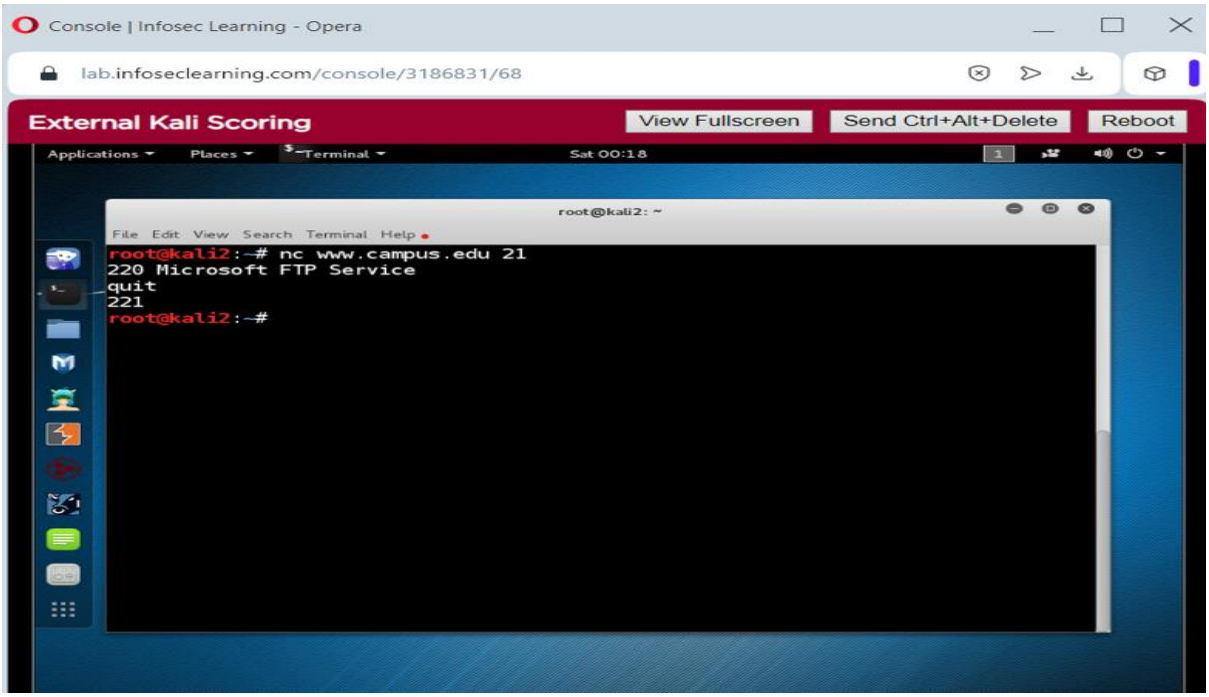
Step 4: Perform a scan using nmap.

#nmap www.campus.edu



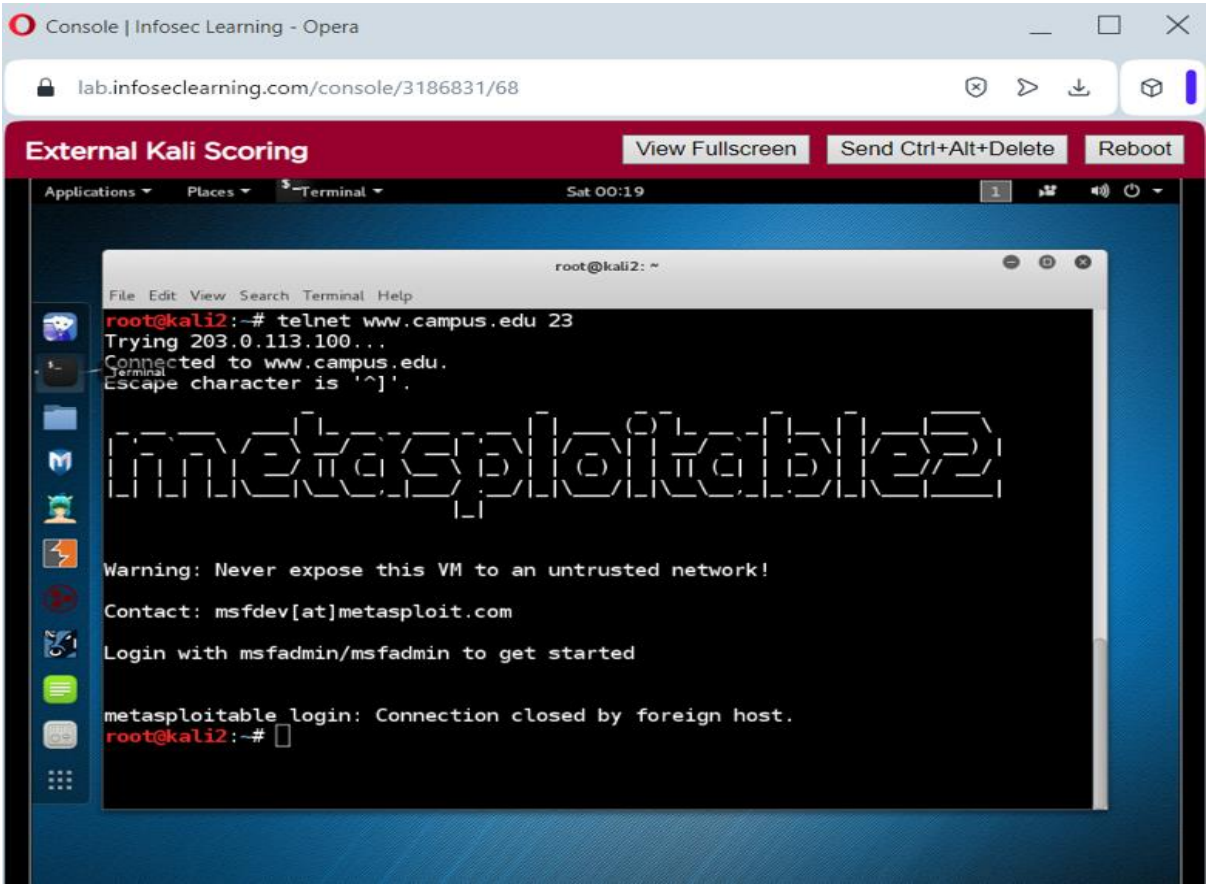
Step 5: Perform a scan with netcat

#nc www.campus.edu 21



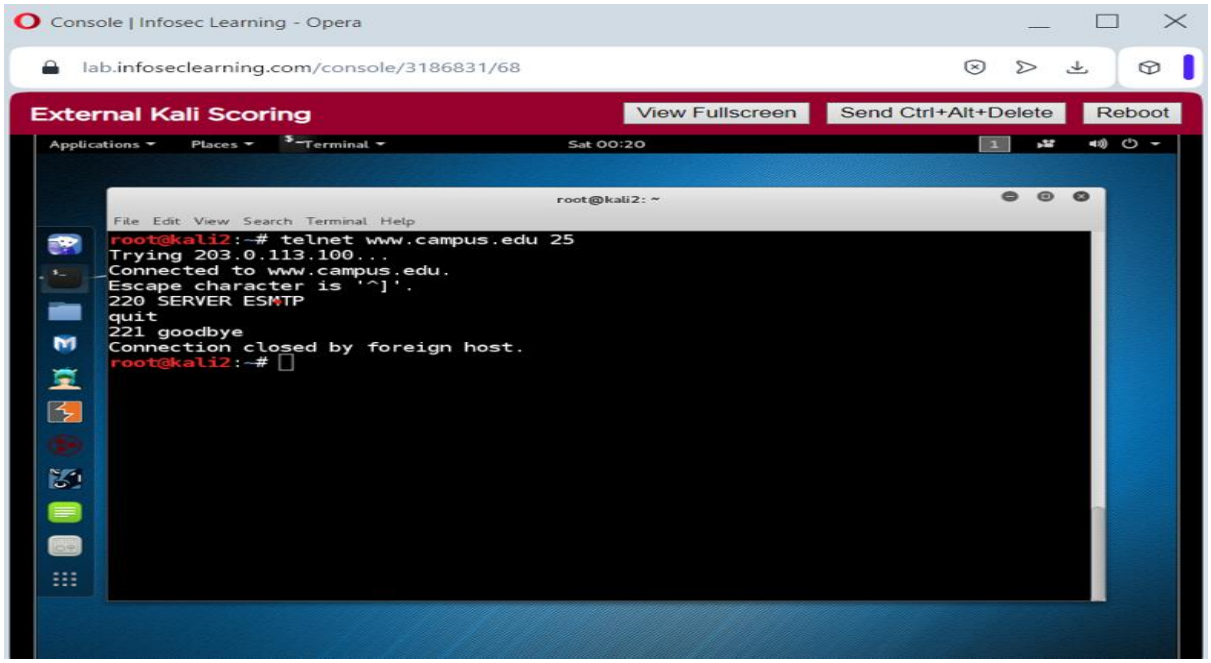
Step 6: Connect to the telnet service, username and password will be displayed.

telnet www.campus.edu 23



Step 7: Perform a telnet scan to get additional information.

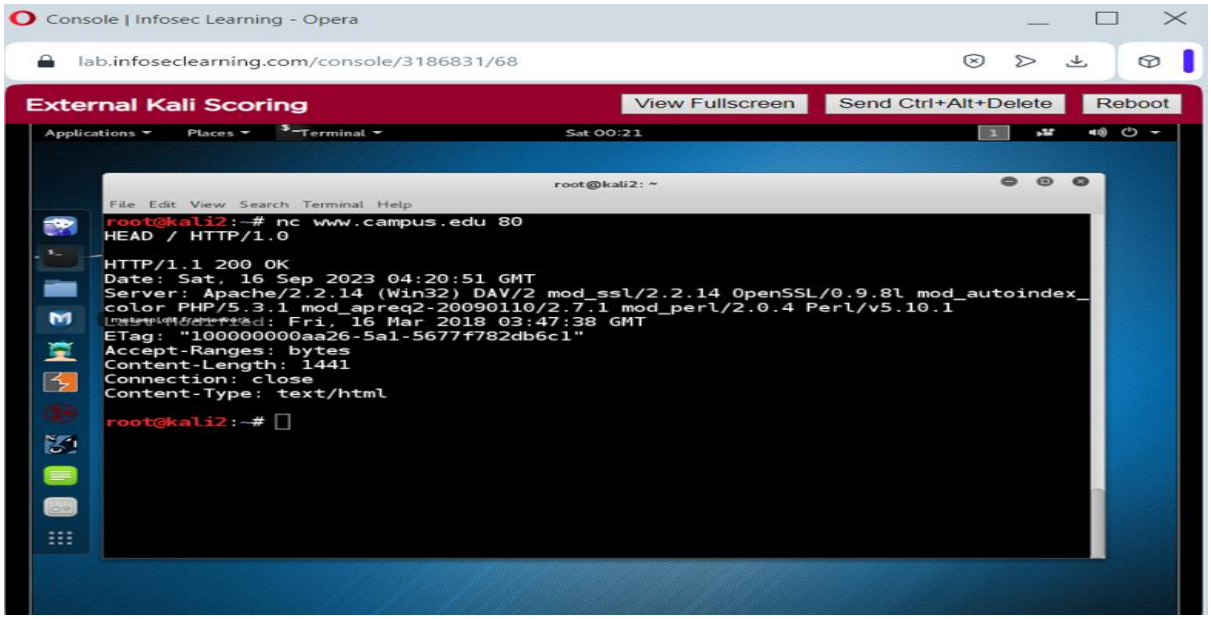
telnet www.campus.edu 25



Step 8: Perform netcat scan to gather additional information.

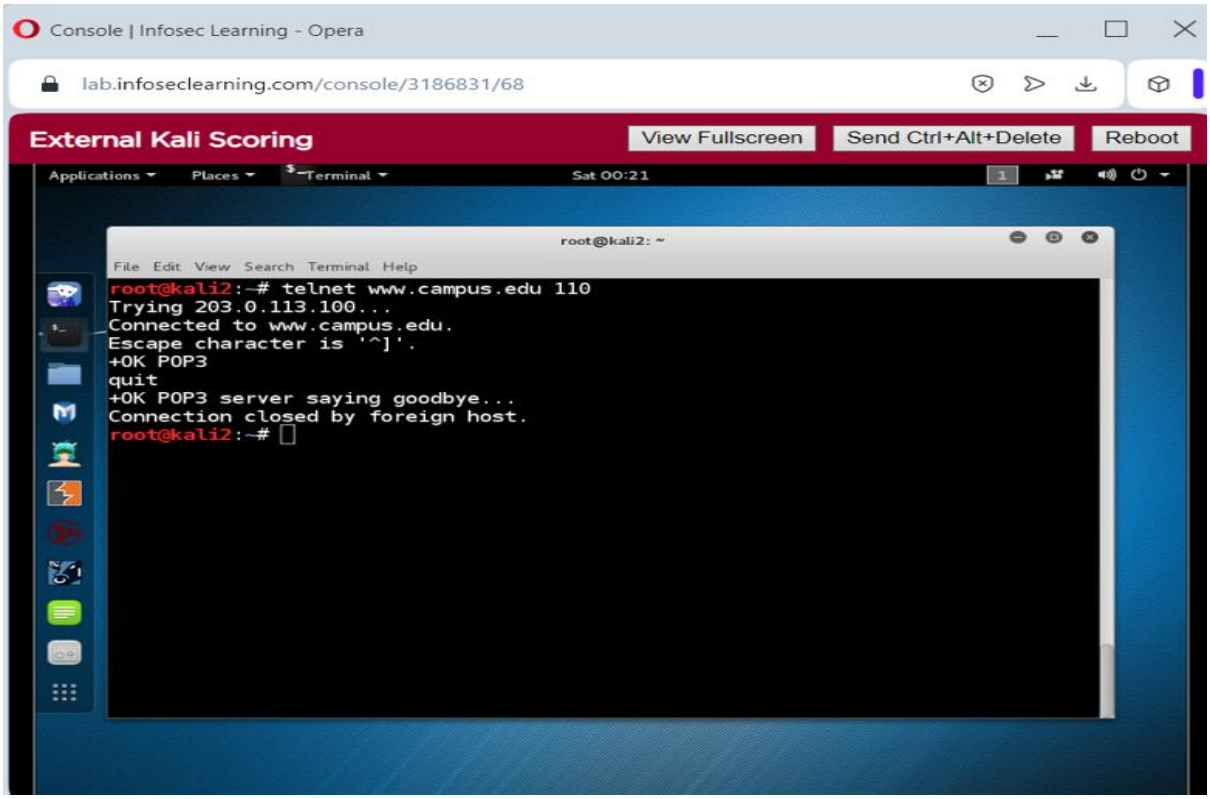
nc www.campus.edu 80

HEAD /HTTP/1.0



Step 9: Perform a telnet scan to get additional information.

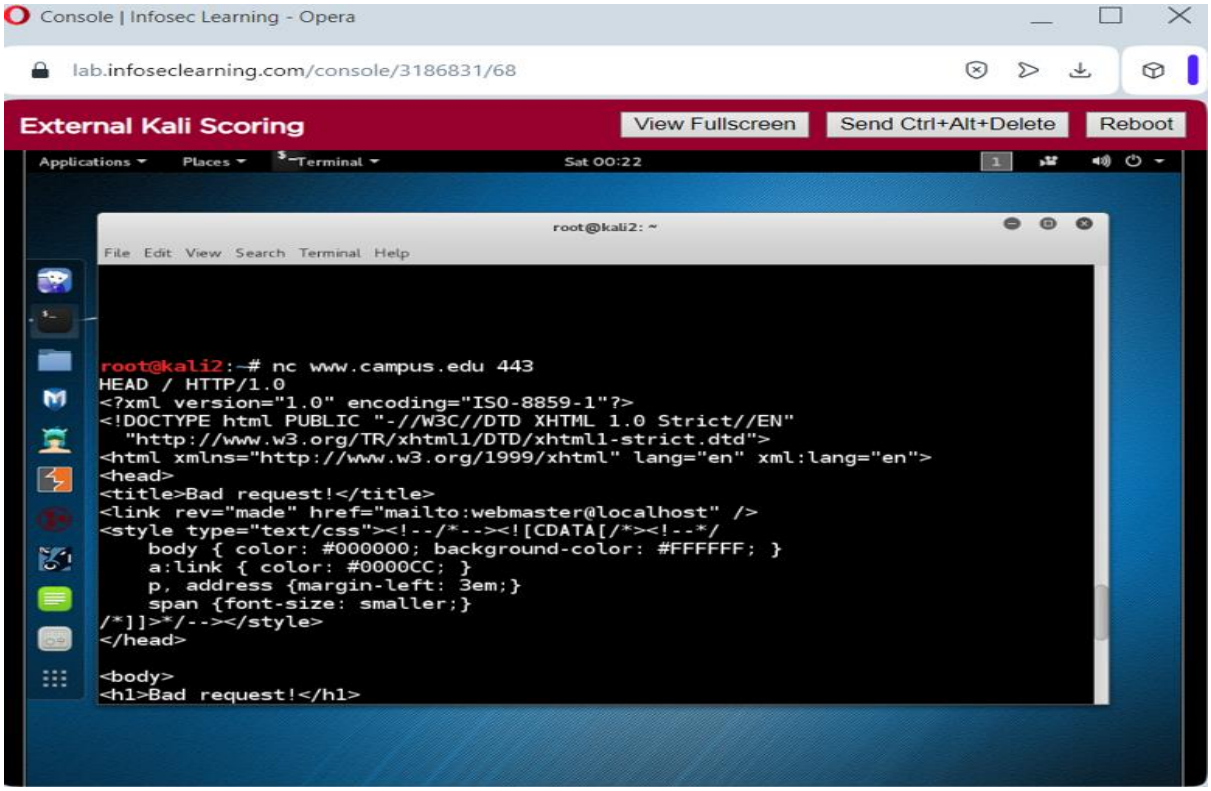
telnet www.campus.edu 110

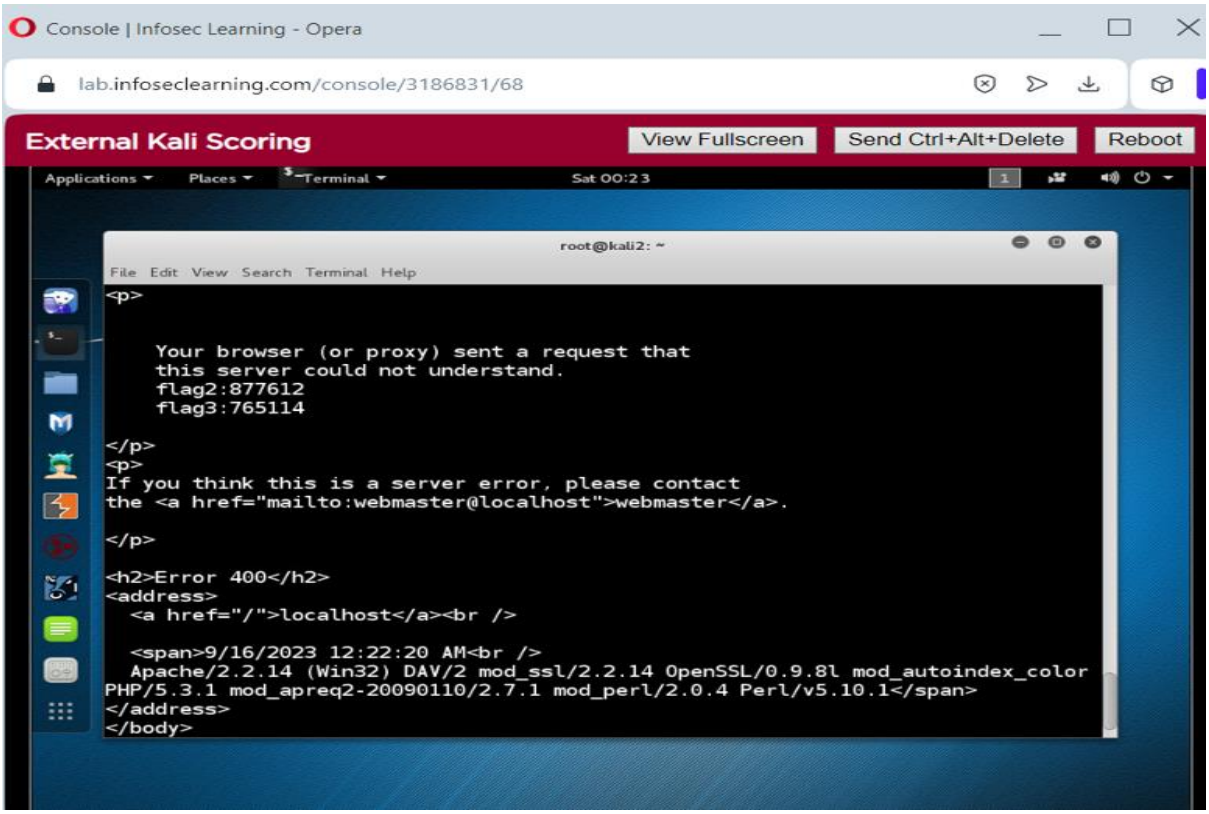


Step 10: Perform netcat scan to gather additional information.

nc www.campus.edu 443

HEAD /HTTP/1.0


Console | Infosec Learning - Opera
lab.infoseclearning.com/console/3186831/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Sat 00:22
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# nc www.campus.edu 443
HEAD / HTTP/1.0
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Bad request!</title>
<link rev="made" href="mailto:webmaster@localhost" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
body { color: #000000; background-color: #FFFFFF; }
a:link { color: #0000CC; }
p, address {margin-left: 3em;}
span {font-size: smaller;}
/*]]>*/--></style>
</head>
<body>
<h1>Bad request!</h1>


Console | Infosec Learning - Opera
lab.infoseclearning.com/console/3186831/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Sat 00:23
root@kali2: ~
File Edit View Search Terminal Help

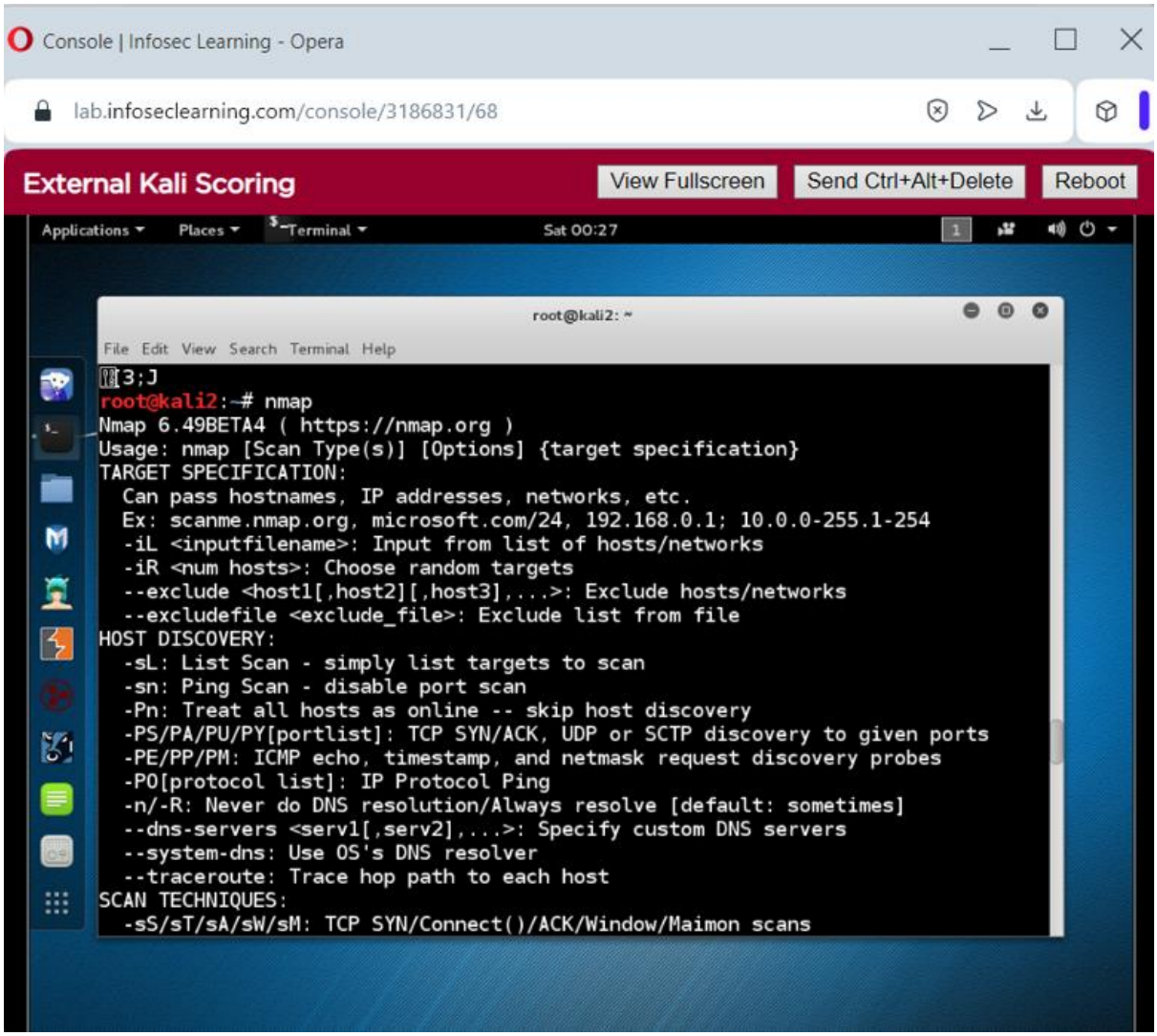
Your browser (or proxy) sent a request that
this server could not understand.
flag2:877612
flag3:765114

If you think this is a server error, please contact
the webmaster.

<h2>Error 400</h2>
<address>
localhost
9/16/2023 12:22:20 AM
Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color
PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
</address>
</body>

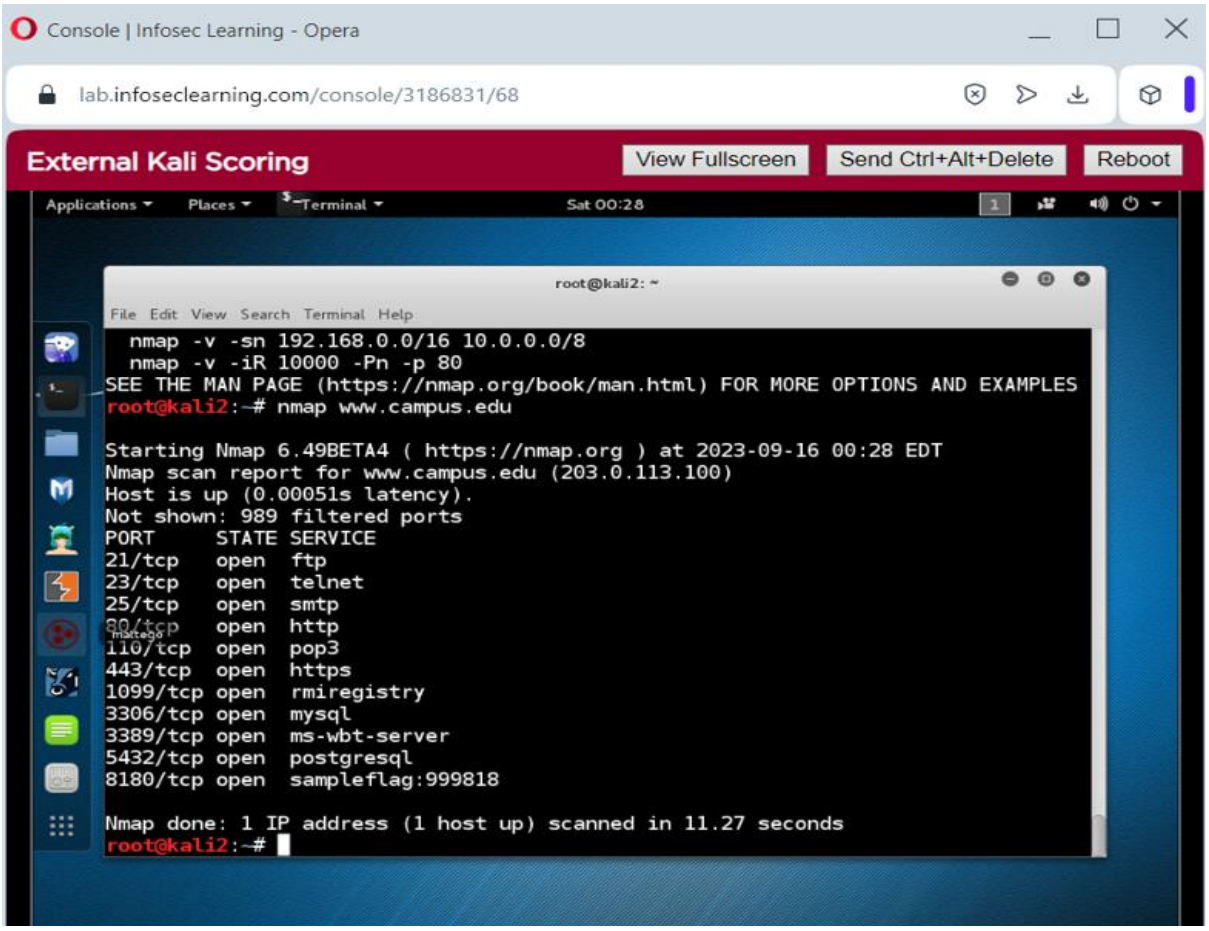
Step 11: Identifying available switches using nmap

nmap



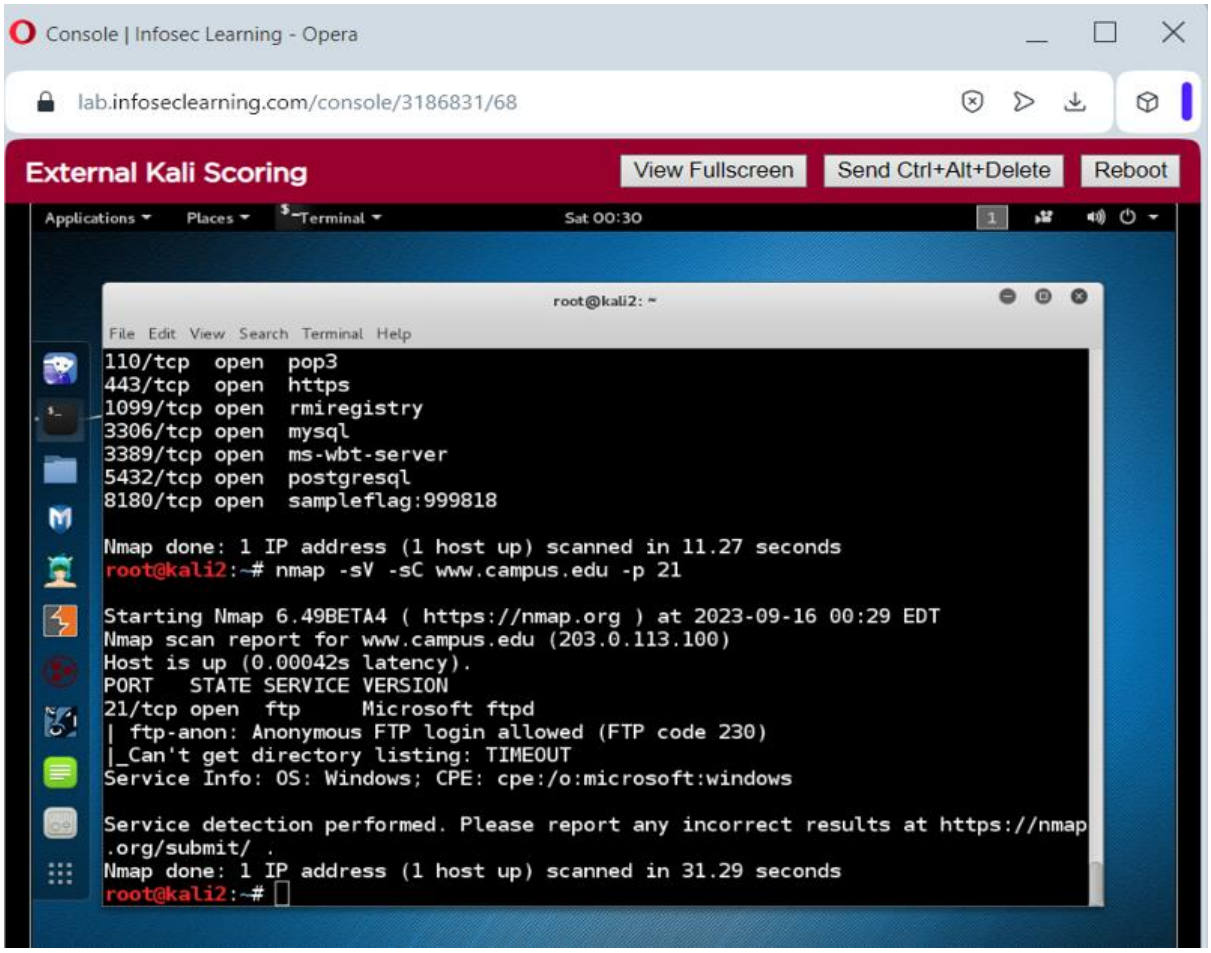
Step 12: Determine the open ports to harvest more information.

nmap www.campus.edu



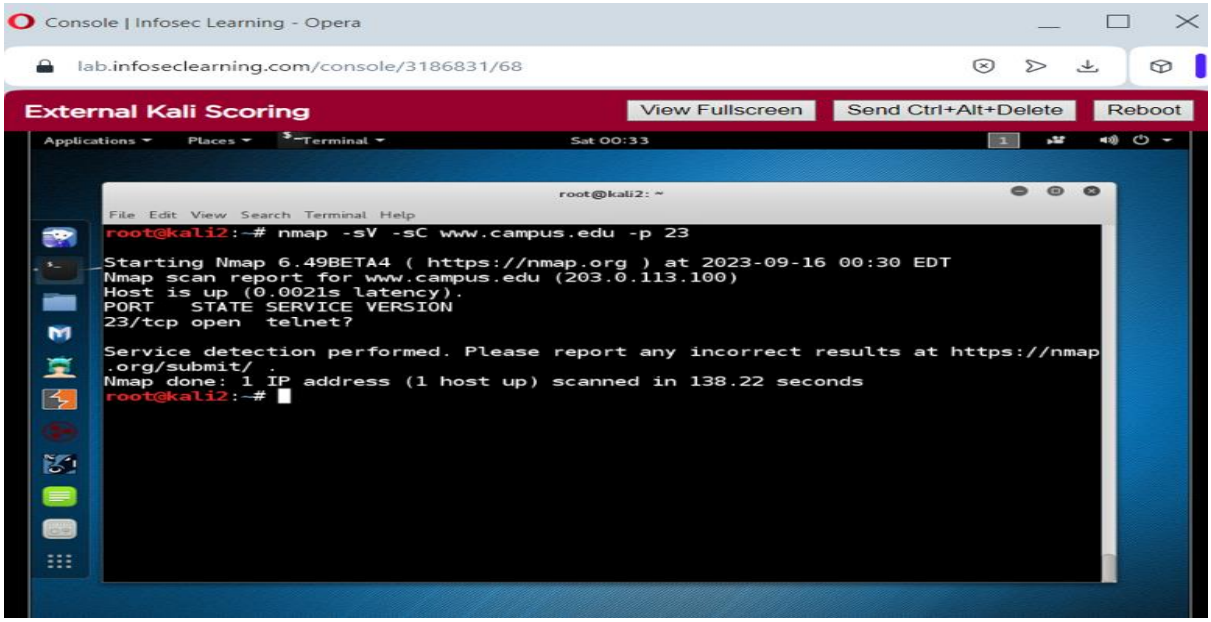
Step 13: Perform a service and script scan of the target on port 21 using nmap.

nmap -sV -sC www.campus.edu -p 21



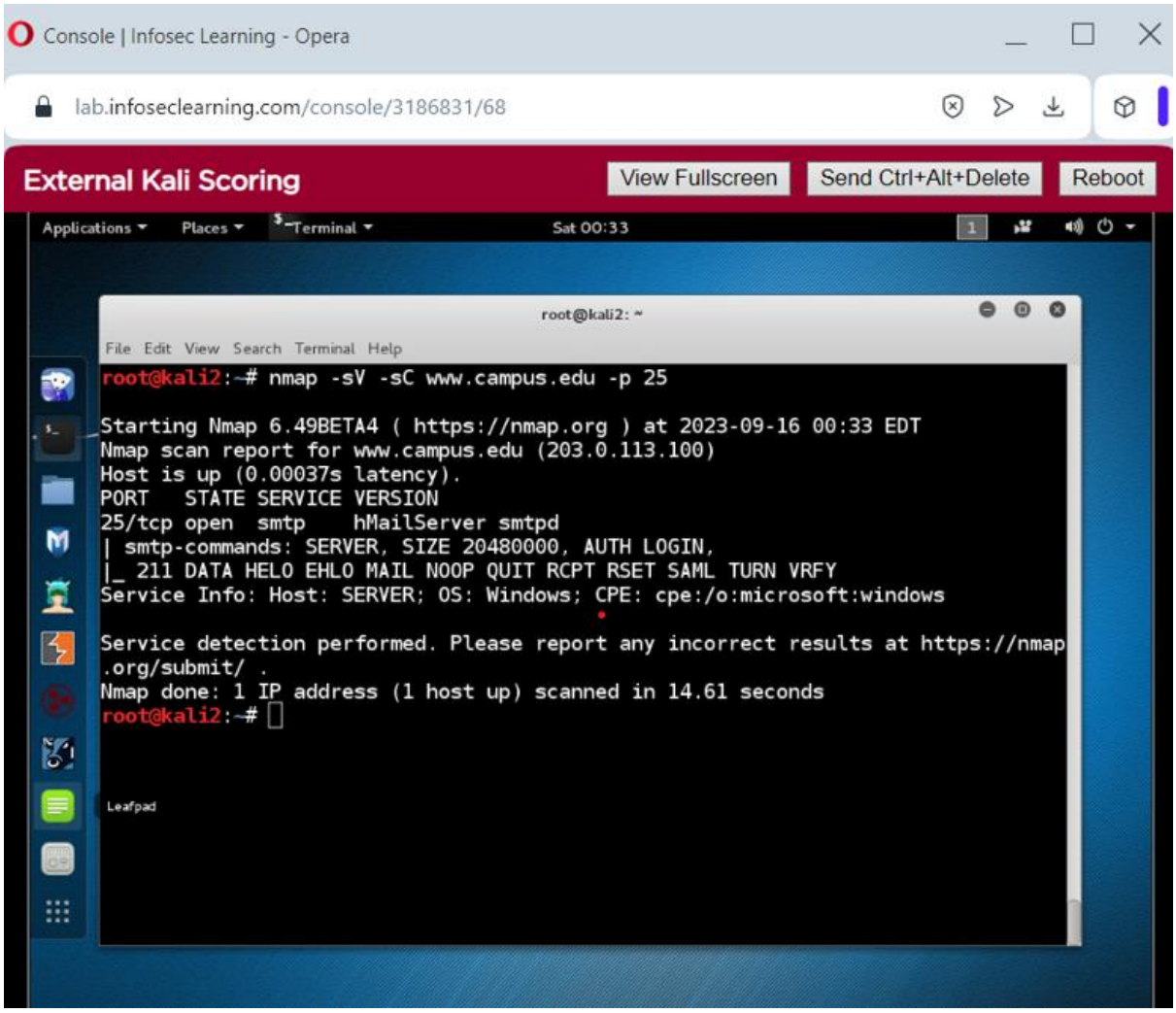
Step 14: Perform a service and script scan of the target on port 23 using nmap.

nmap -sV -sC www.campus.edu -p 23



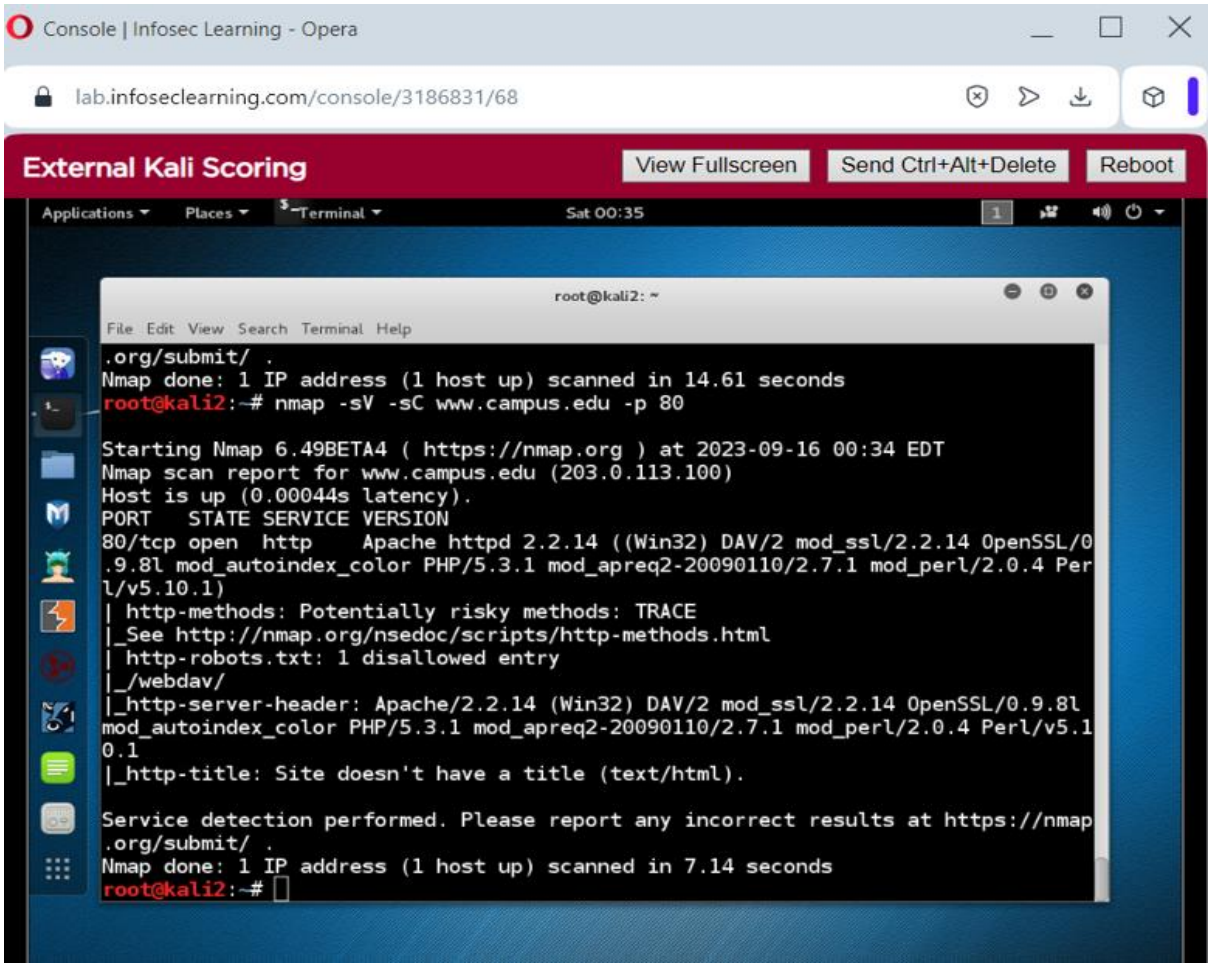
Step 15: Perform a service and script scan of the target on port 25 using nmap.

nmap -sV -sC www.campus.edu -p 25



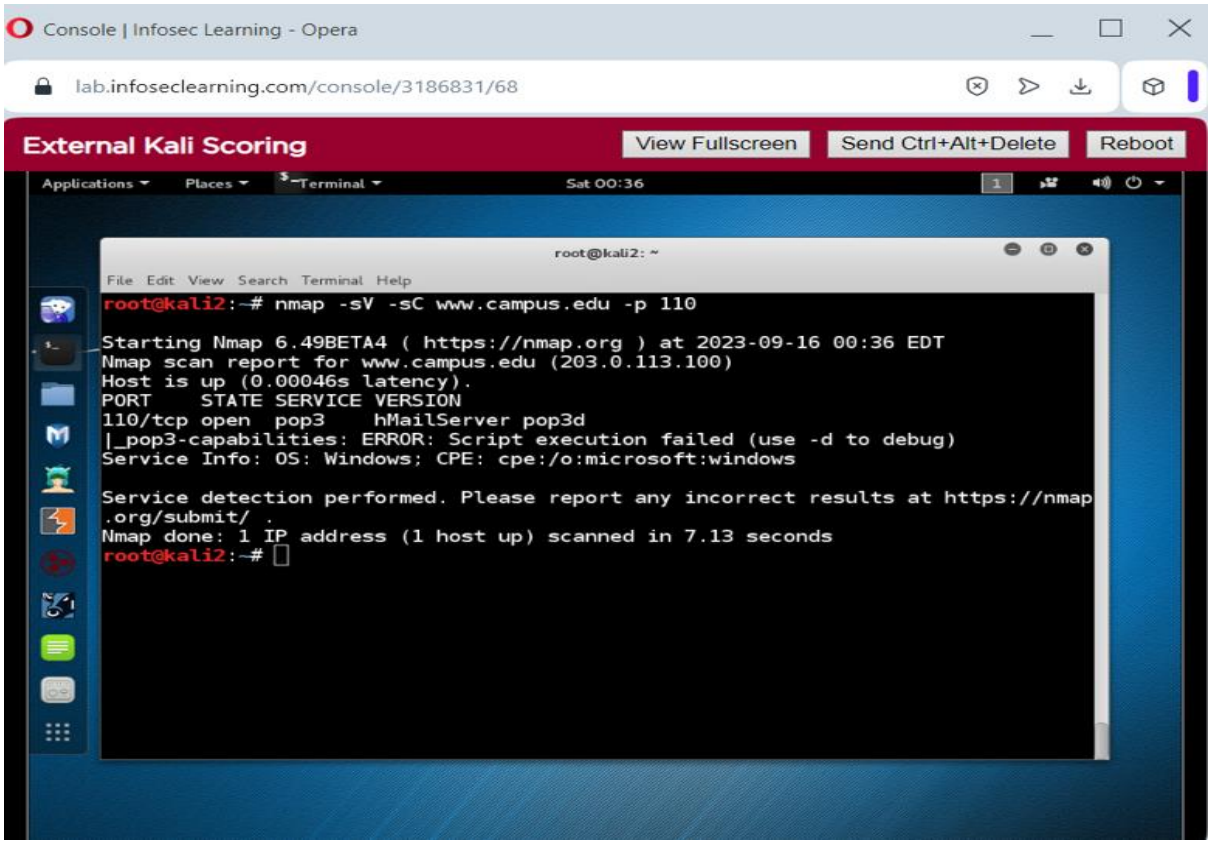
Step 16: Perform a service and script scan of the target on port 80 using nmap.

nmap -sV -sC www.campus.edu -p 80



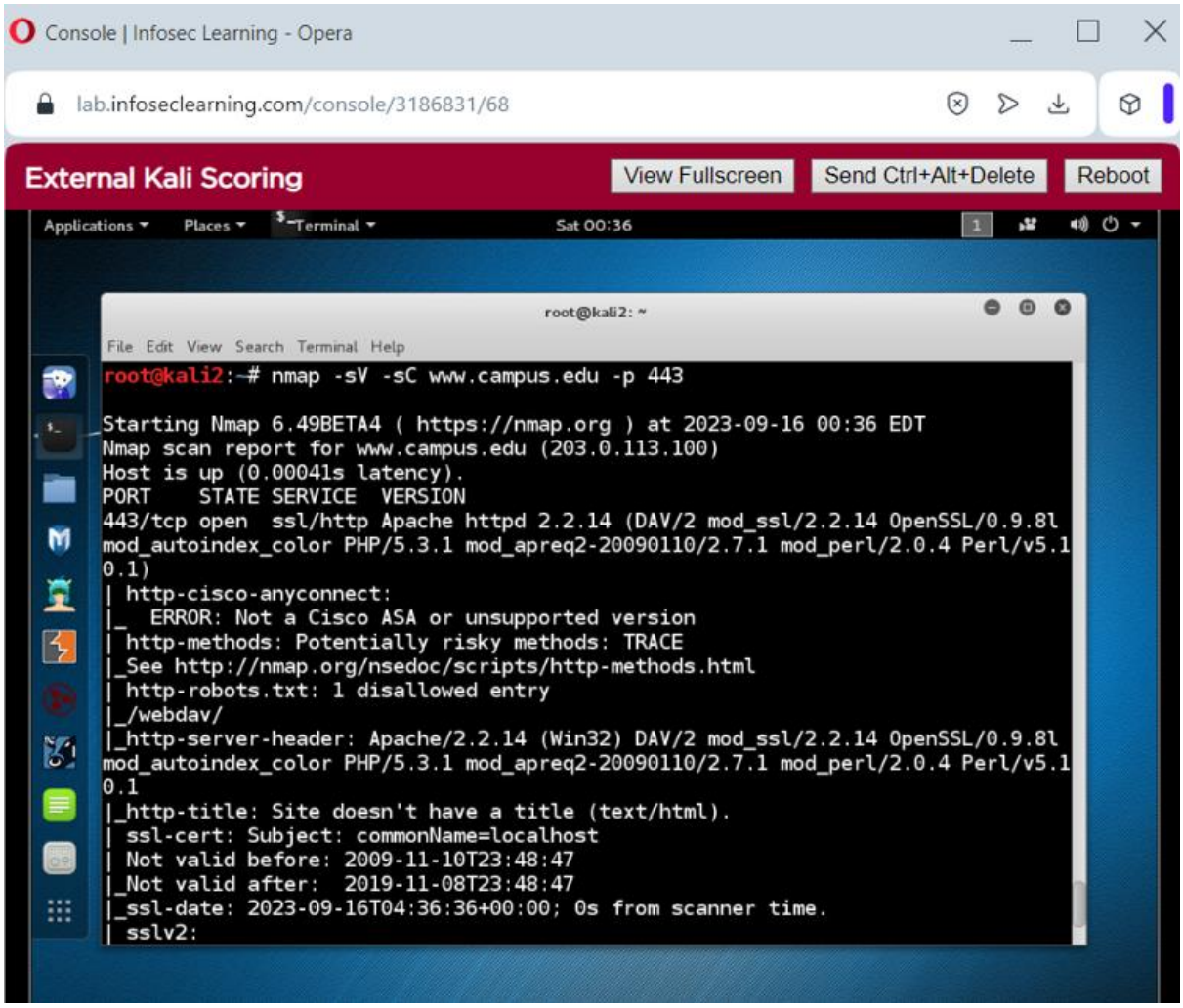
Step 17: Perform a service and script scan of the target on port 110 using nmap.

nmap -sV -sC www.campus.edu -p 110



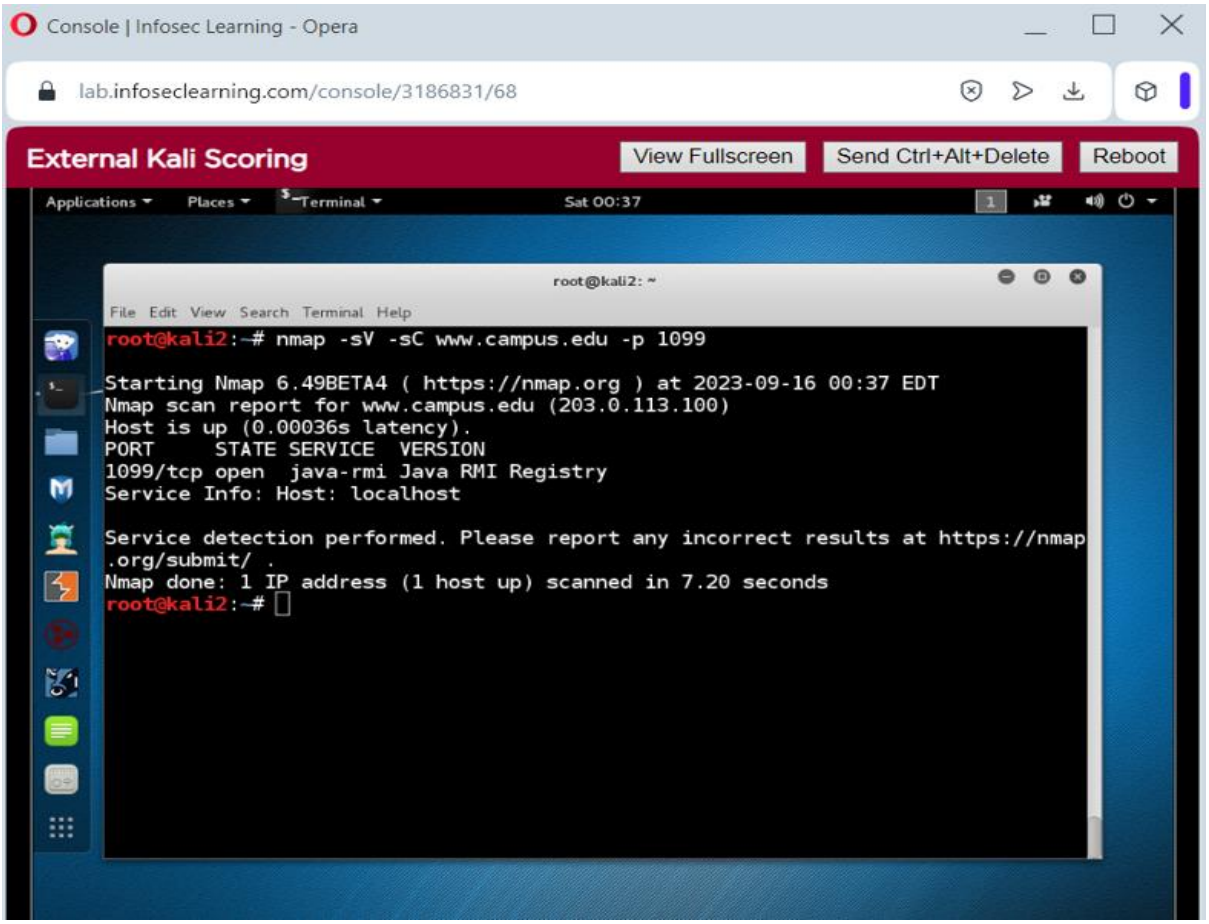
Step 18: Perform a service and script scan of the target on port 443 using nmap.

nmap -sV -sC www.campus.edu -p 443



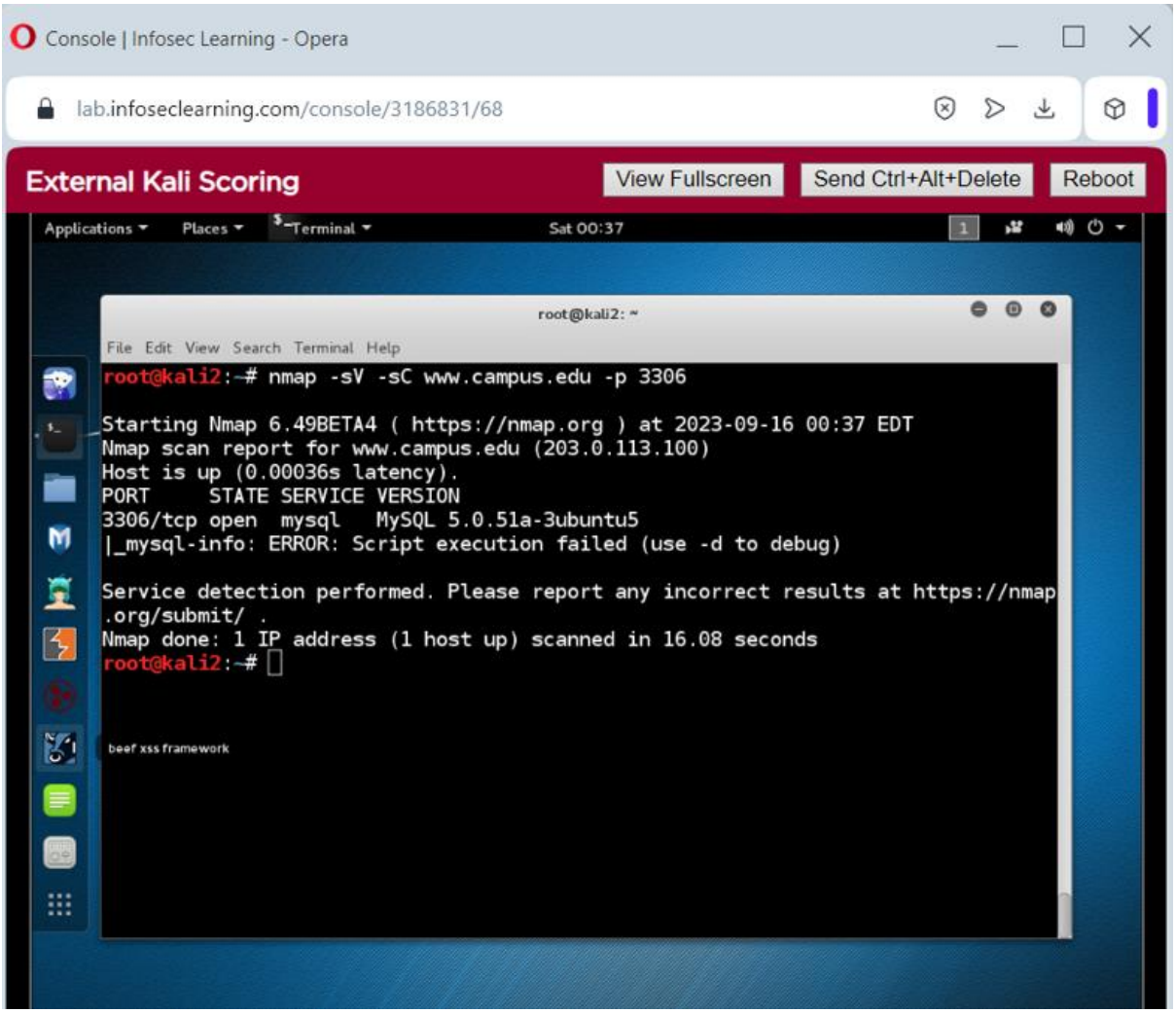
Step 19: Perform a service and script scan of the target on port 1099 using nmap.

nmap -sV -sC www.campus.edu -p 1099



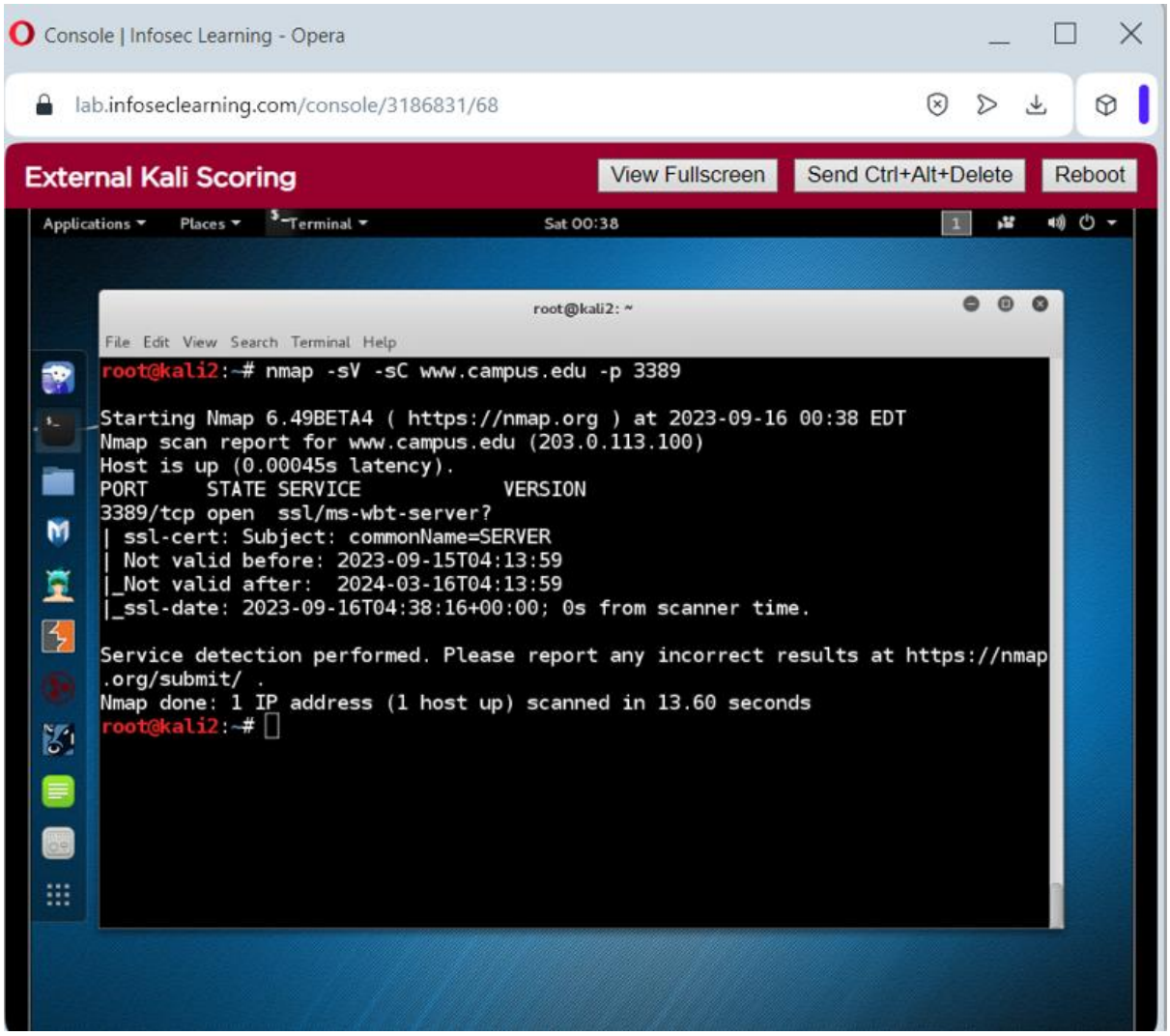
Step 20: Perform a service and script scan of the target on port 3306 using nmap.

nmap -sV -sC www.campus.edu -p 3306



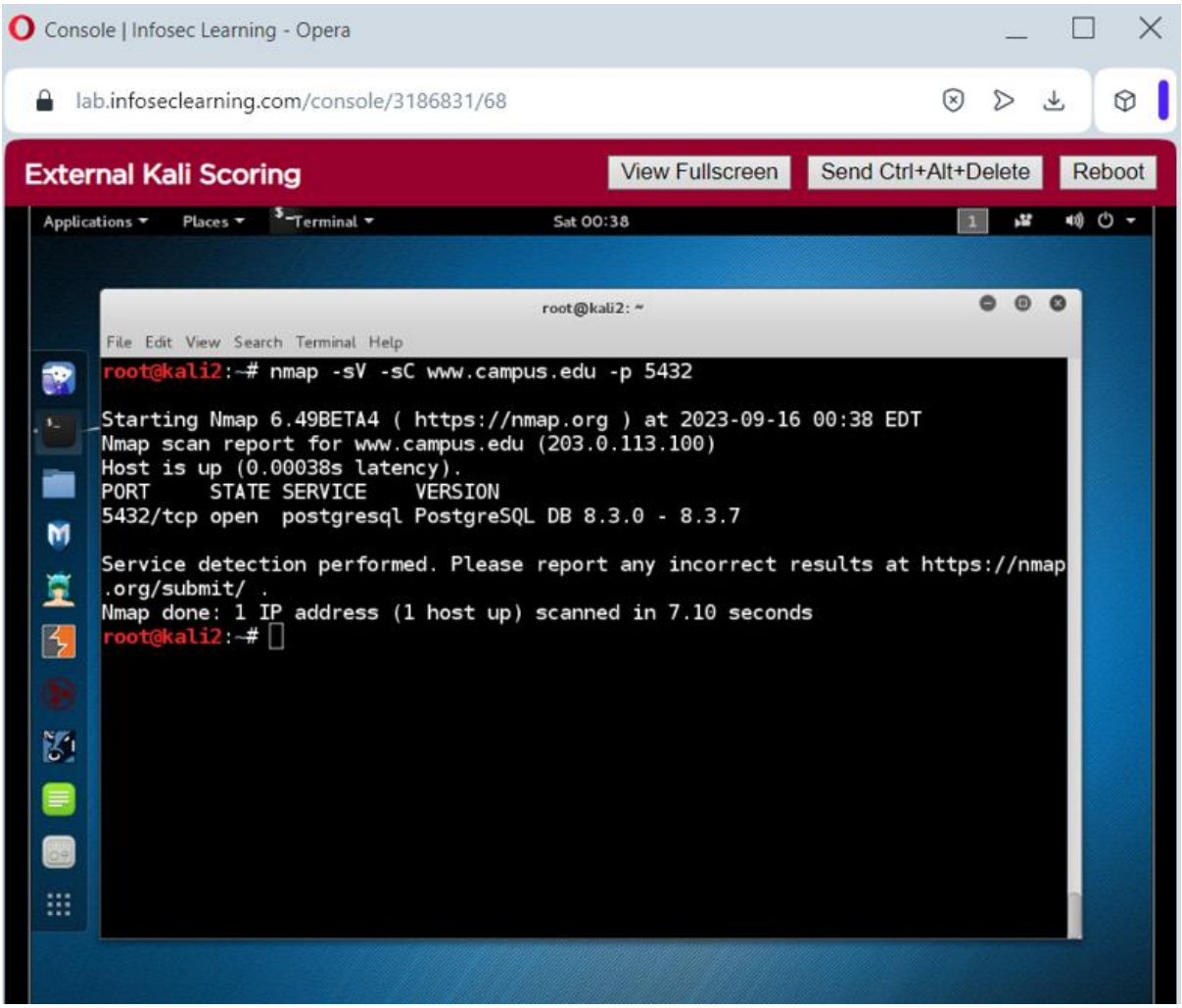
Step 21: Perform a service and script scan of the target on port 3389 using nmap.

nmap -sV -sC www.campus.edu -p 3389



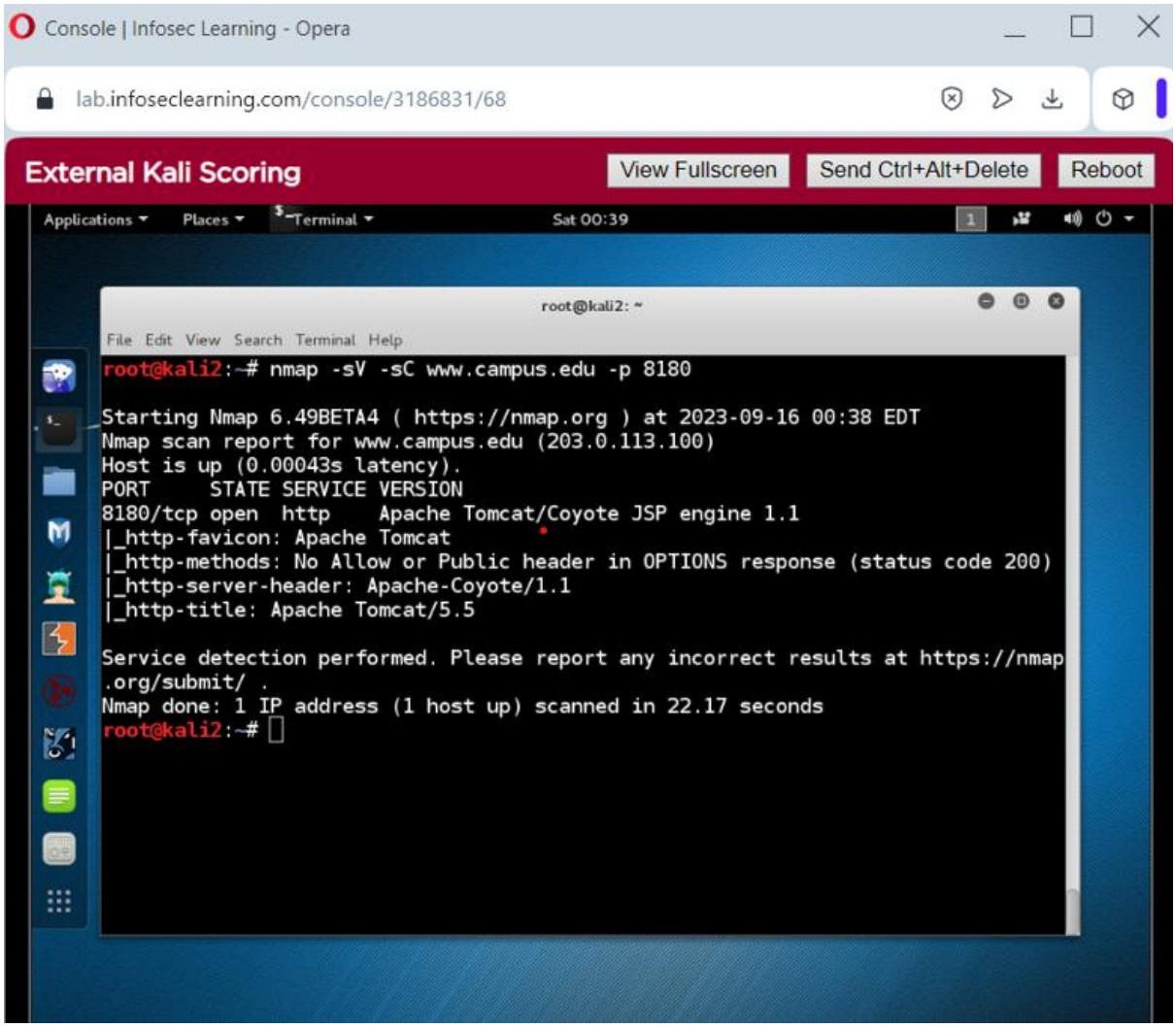
Step 22: Perform a service and script scan of the target on port 5432 using nmap.

nmap -sV -sC www.campus.edu -p 5432



Step 23: Perform a service and script scan of the target on port 8180 using nmap.

nmap -sV -sC www.campus.edu -p 8180



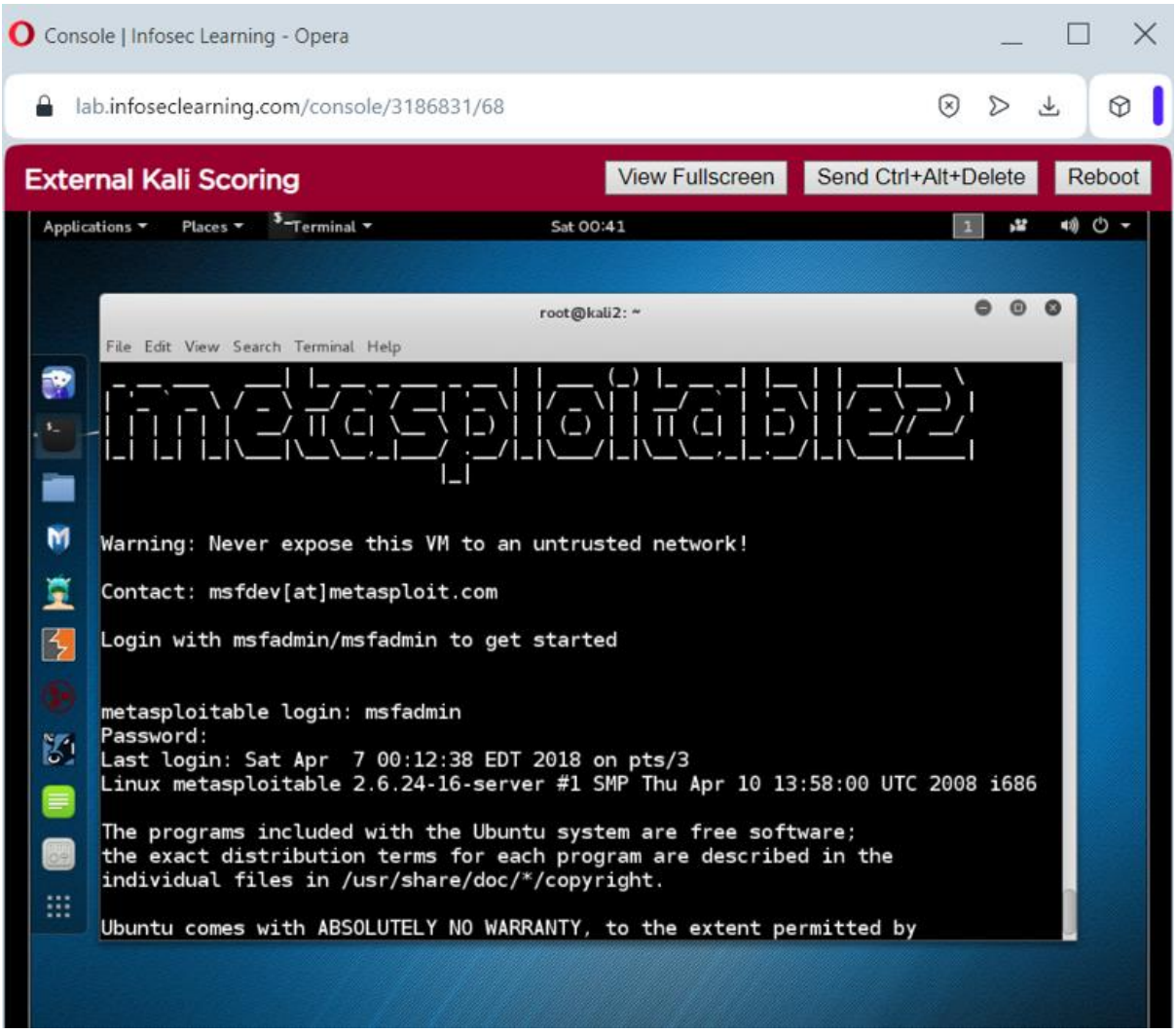
Step 24: Connect to the telnet server.

telnet www.campus.edu

Login into metasploitable. Enter the details.

login: msfadmin

password: msfadmin



Step 25: View the id for the root account.

```
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
```

Step 26: View the hashes in the shadow file.

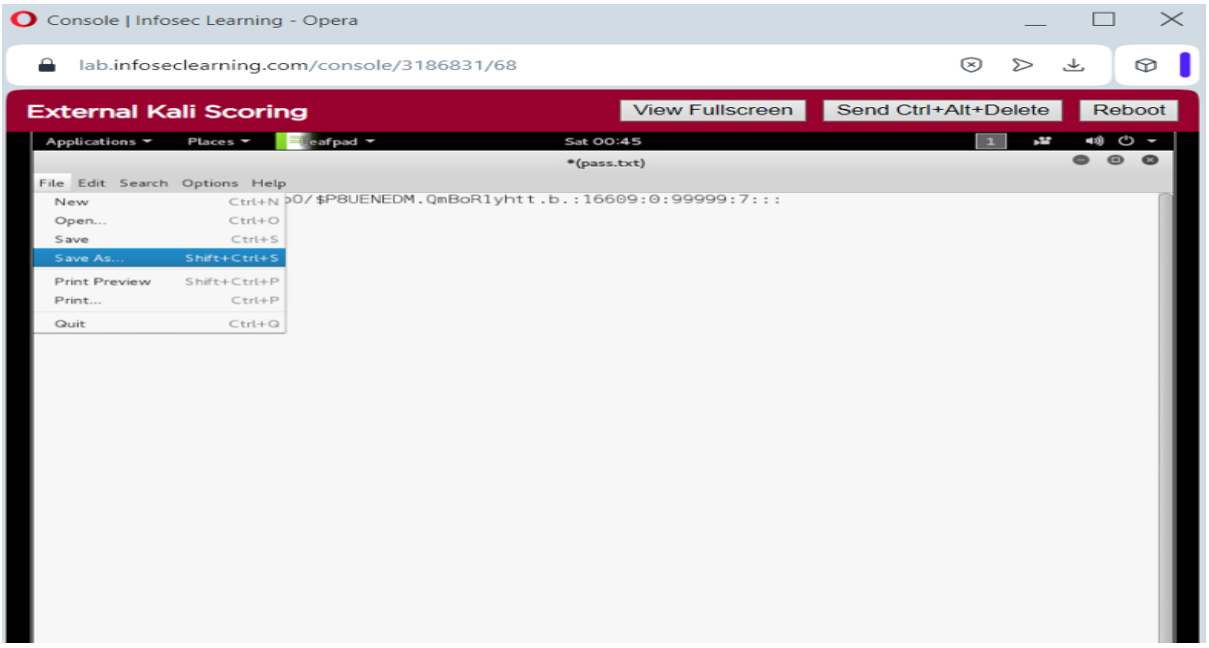
$ sudo tail /etc/shadow

```
msfadmin@metasploitable:~$ sudo tail /etc/shadow
sudo: unable to resolve host metasploitable
[sudo] password for msfadmin:
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
gdm:*:16467:0:99999:7:::
messagebus:*:16467:0:99999:7:::
polkituser:*:16467:0:99999:7:::
haldaemon:*:16467:0:99999:7:::
administrator:$1$aMci2pO/$P8UENEDM.QmBoR1yhtt.b.:16609:0:99999:7:::
flag4:!:17628:0:99999:7:::
flag5:!:17628:0:99999:7:::
flag6:!:17628:0:99999:7:::
```

Step 27: Exit the telnet sessions.

```
msfadmin@metasploitable:~$ exit
logout
Connection closed by foreign host.
```

Step 28: Create a text file named pass.txt. Select the file and save it.



Step 29: Crack the hash in pass.txt.

john pass.txt

```
root@kali2:~# leafpad pass.txt
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[illegible]ord          (administrator)
1g 0:00:00:00 DONE 2/3 (2023-09-16 00:46) 4.761g/s 18204p/s 18204c/s 18204C/s na
tional..rock
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:~#
```

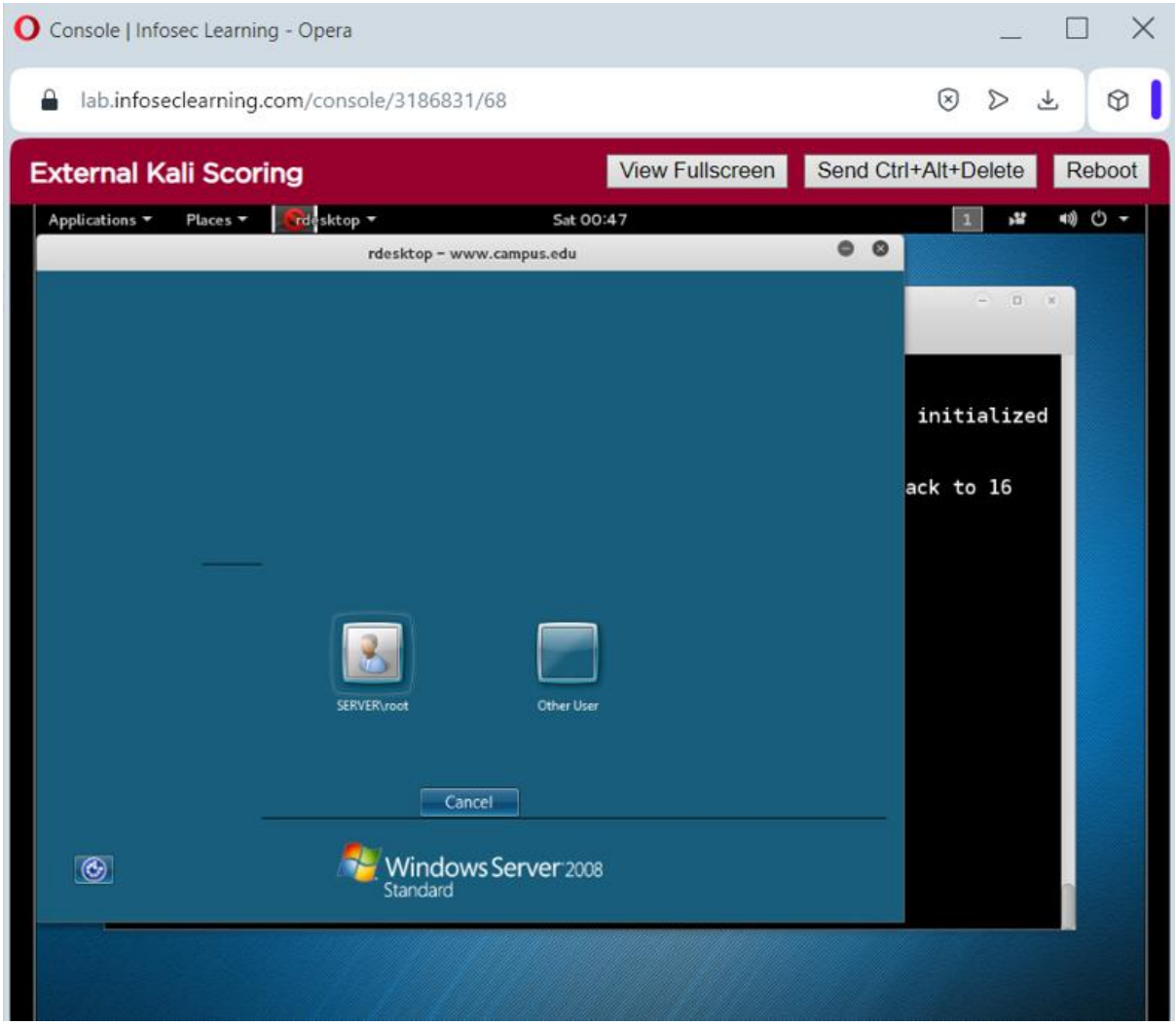
Step 30: Perform a service and script scan of the target on port 3389 using nmap.

nmap -sV -sC www.campus.edu -p 3389

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-09-16 00:46 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00039s latency).
PORT     STATE SERVICE           VERSION
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=SERVER
| Not valid before: 2023-09-15T04:13:59
|_Not valid after:  2024-03-16T04:13:59
|_ssl-date: 2023-09-16T04:47:05+00:00; 0s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

Step 31: Connect to the target on port 3389.

rdesktop www.campus.edu

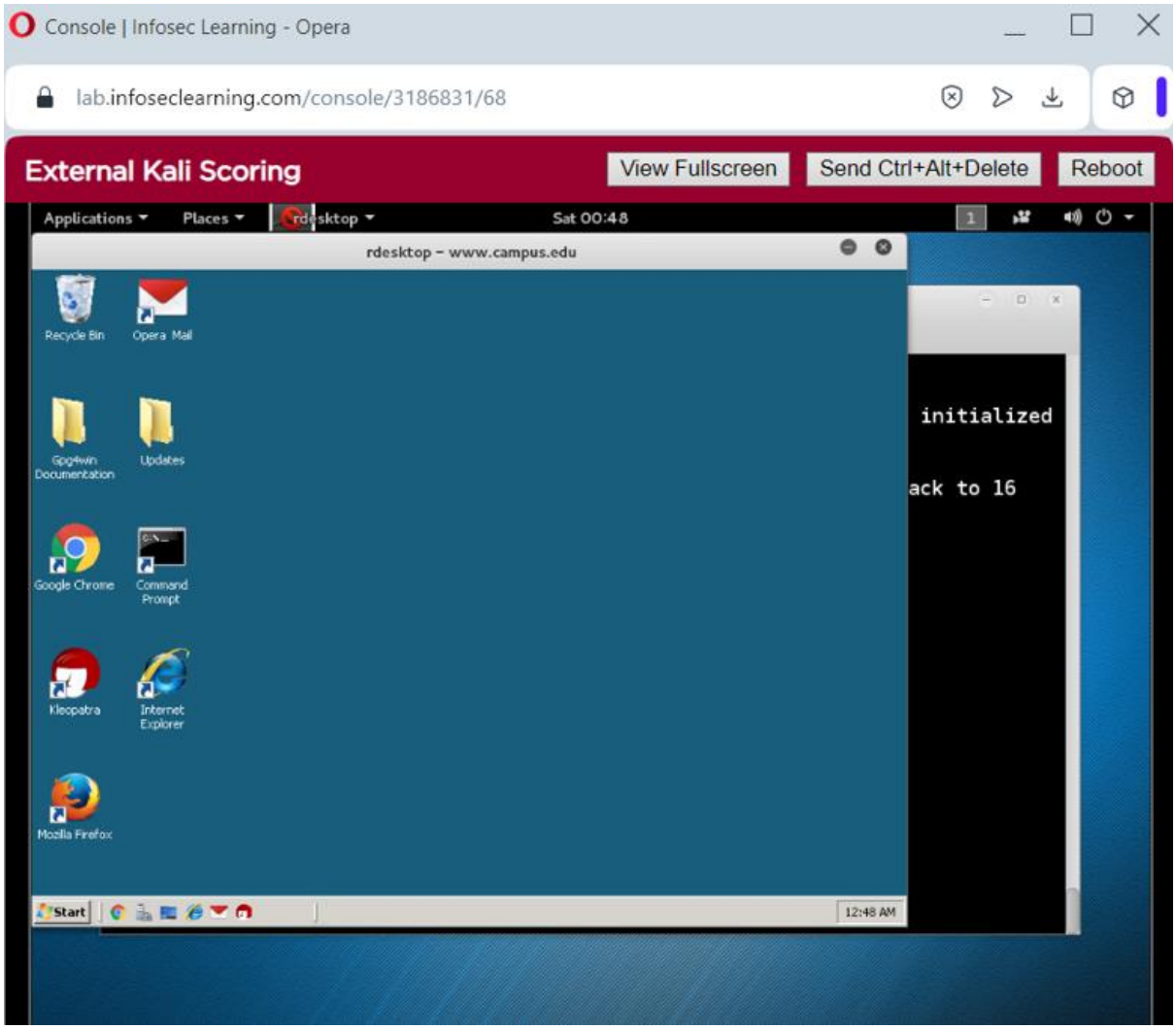


Step 32: Click on other user and enter the login details.

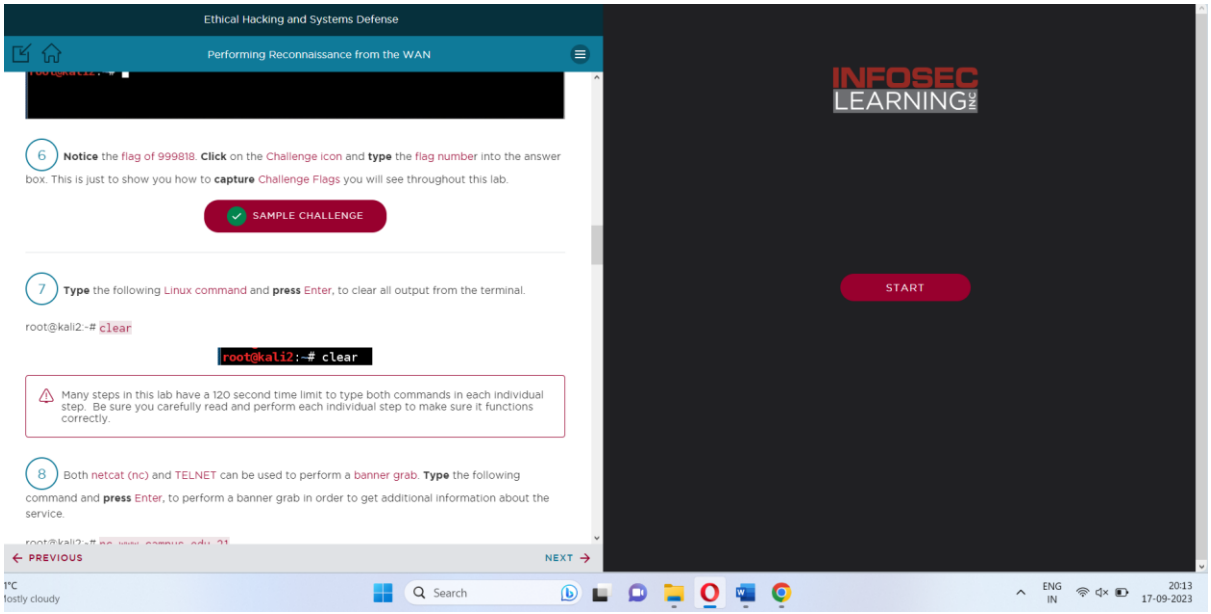
Username: administrator@camous.edu

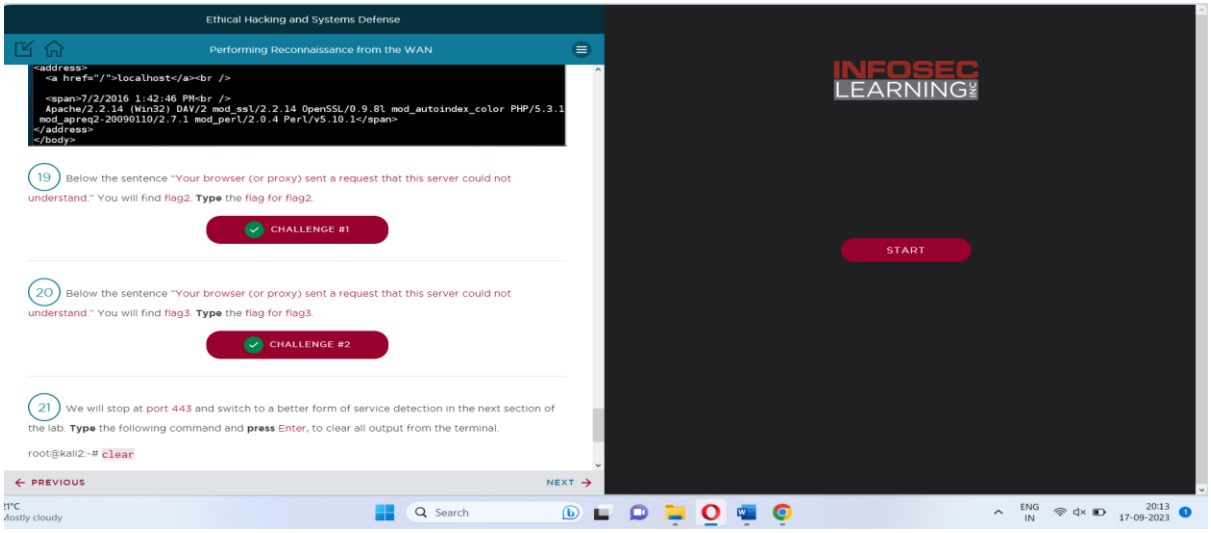
Password: P@ssw0rd

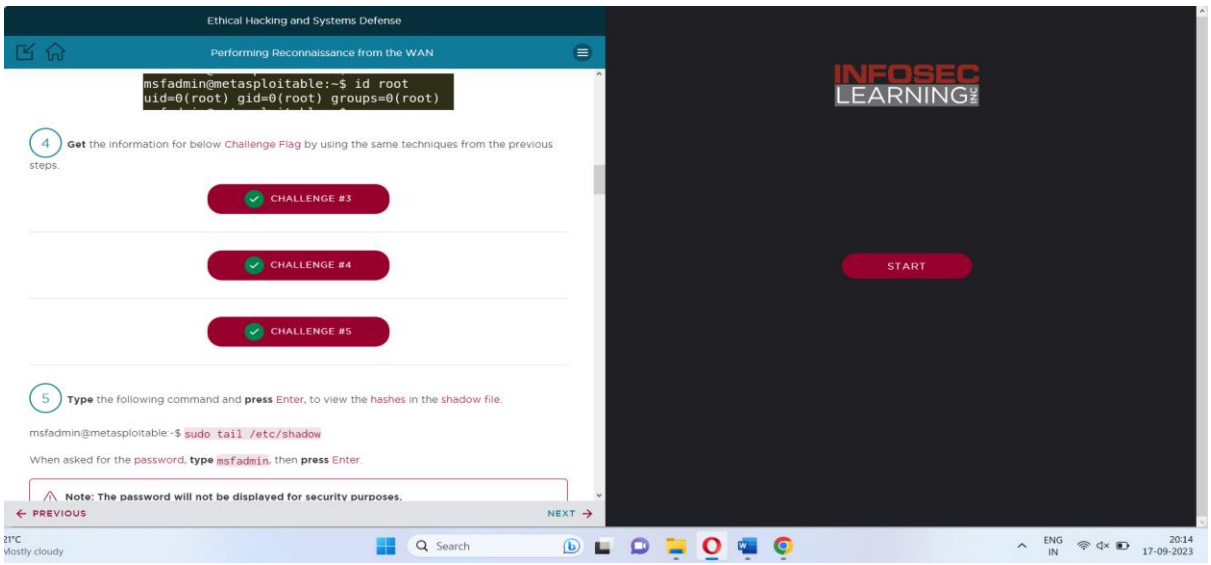
We are logged into the system.



Supporting Evidence







Conclusion & Wrap-up

The lab provides a thorough examination of the methods and tools used in the hands-on activities, highlighting the difficulties and constraints unique to WAN-based reconnaissance. Its goal is to give readers a thorough grasp of the value of reconnaissance, the successes and drawbacks of various strategies, and the challenges that must be overcome for real-world reconnaissance to be successful.

CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-1

Scanning the Network on the LAN

Student Info:
Name : Akhila Parankusham
Student ID: 00810899
Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

Nmap/Zenmap: Our method involves using Nmap to do a ping scan, which enables us to identify the IP addresses attached to LAN-connected PCs. We will also use Nmap/Zenmap to scan the LAN and identify the open Transmission Control Protocol (TCP) ports on various devices.

Metasploit and Armitage: We will make use of the features of Metasploit and Armitage in order to exploit system flaws.

Objectives

This lab exercise's main goal is to conduct scans on multiple hosts running the Windows operating system within a Local Area Network (LAN). Kali, a Linux distribution, will be used to do this. To further exploit any potential flaws in the target system, we will employ Armitage and Metasploit.

Lab Description Details

1. Network scanning methods: Using a variety of network exploration tools and approaches, such as ping and port scans, to obtain understanding of the network's architecture.
2. OS Recognition: Determining the operating systems and the versions of those operating systems that are utilized by the devices connected to the network.
3. Port and Service Detection: This procedure helps to identify potential security vulnerabilities by locating active ports and services on each device connected to the network.
4. Network Charting: Charting a network using network mapping to provide a graphic depiction of the structure of the network and device connections.
5. Security Evaluation: Security evaluation involves examining the network for any potential security risks or vulnerabilities, such as out-of-date software, exposed ports that could be vulnerable to known exploits, or weak authentication procedures, and putting the required security controls in place to strengthen the network's defenses.

Step 1: Log in to the Kali Linux.

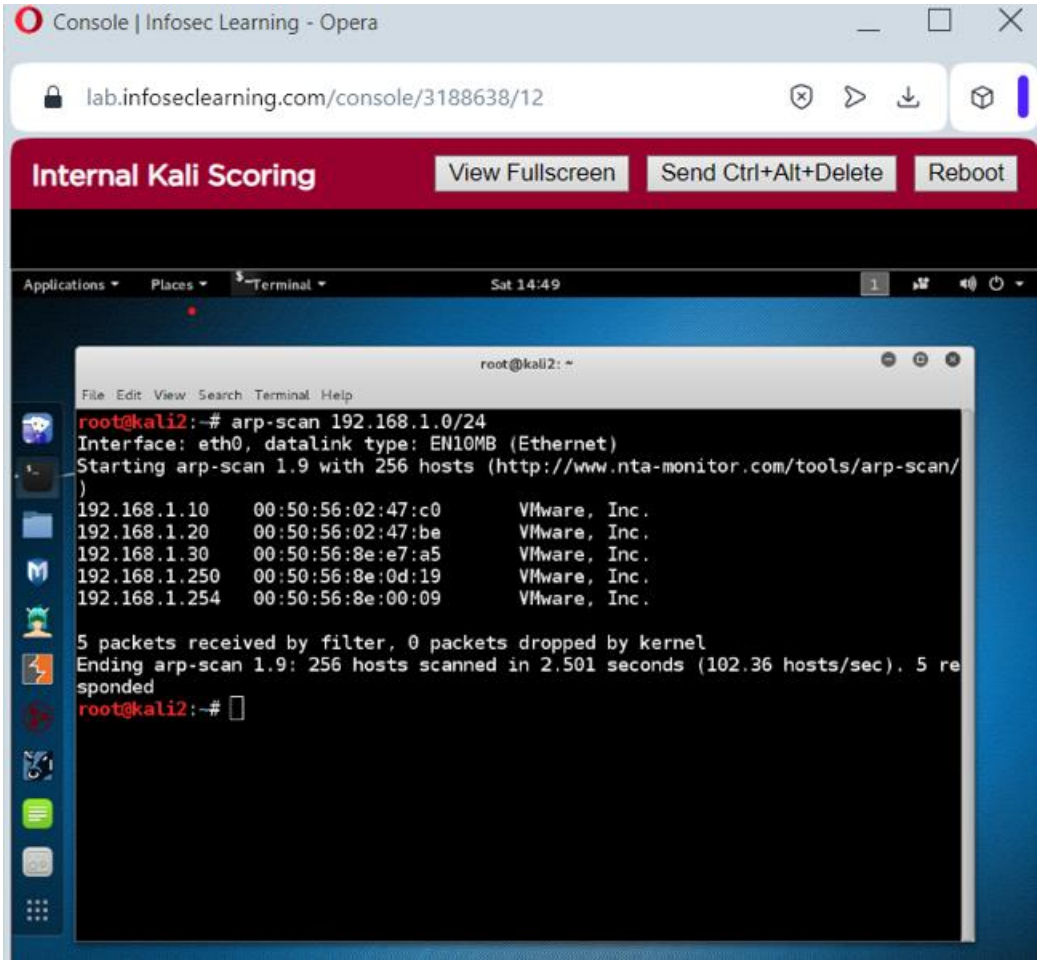
Enter the credentials. Username: **root**

Password: **toor**

Step 2: Open the terminal.

Step 3: Perform ARP scan.

arp-scan 192.168.1.0/24



Step 4: Perform a TCP scan of 192.168.1.10 and determine the open ports.

nmap -sT 192.168.1.10

```
root@kali2:~# nmap -sT 192.168.1.10

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-09-16 14:51 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00020s latency).
Not shown: 971 filtered ports
PORT      STATE SERVICE
7/tcp     open  echo
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
```

Step 5: Perform a TCP scan of 192.168.1.20 and determine the open ports.

nmap -sT 192.168.1.20

```
root@kali2:~# nmap -sT 192.168.1.20

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-09-16 14:56 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00033s latency).
Not shown: 992 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:50:56:02:47:BE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.14 seconds
```

Step 6: Perform a TCP scan of 192.168.1.30 and determine the open ports.

nmap -sT 192.168.1.30

```
root@kali2:~# nmap -sT 192.168.1.30

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-09-16 14:57 EDT
Nmap scan report for 192.168.1.30
Host is up (0.00015s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
```

Step 7: Perform a TCP scan of 192.168.1.254 and determine the open ports.

nmap -sT 192.168.1.254

```
root@kali2:~# nmap -sT 192.168.1.254

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-09-16 14:58 EDT
Nmap scan report for 192.168.1.254
Host is up (0.00028s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:8E:00:09 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.24 seconds
```

Step 8: Perform an OS scan of 192.168.1.10 to determine the OS of the host.

#nmap -0 192.168.1.10 | tail

```
root@kali2:~# nmap -0 192.168.1.10 | tail
nmap: unrecognized option '-0'
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Step 9: Perform an OS scan of 192.168.1.20 to determine the OS of the host.

#nmap -0 192.168.1.20 | tail

```
root@kali2:~# nmap -O 192.168.1.20 | tail
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 7|8|Vista|2008|Phone|2012 (93%)
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:micros
oft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_20
08::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windo
ws Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista S
P2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft Windows Phone 7.5 or 8.0 (92%),
Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Ser
ver 2008 SP1 (89%), Microsoft Windows 7 (89%), Microsoft Windows 7 SP1 (89%), Microsoft Win
dows Vista SP0 - SP1 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.70 seconds
```

Step 10: Perform an OS scan of 192.168.1.30 to determine the OS of the host.

#nmap -0 192.168.1.30 | tail

```
root@kali2:~# nmap -O 192.168.1.30 | tail
8180/tcp open  flag4:232441
MAC Address: 00:50:56:8E:E7:A5 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.78 seconds
```

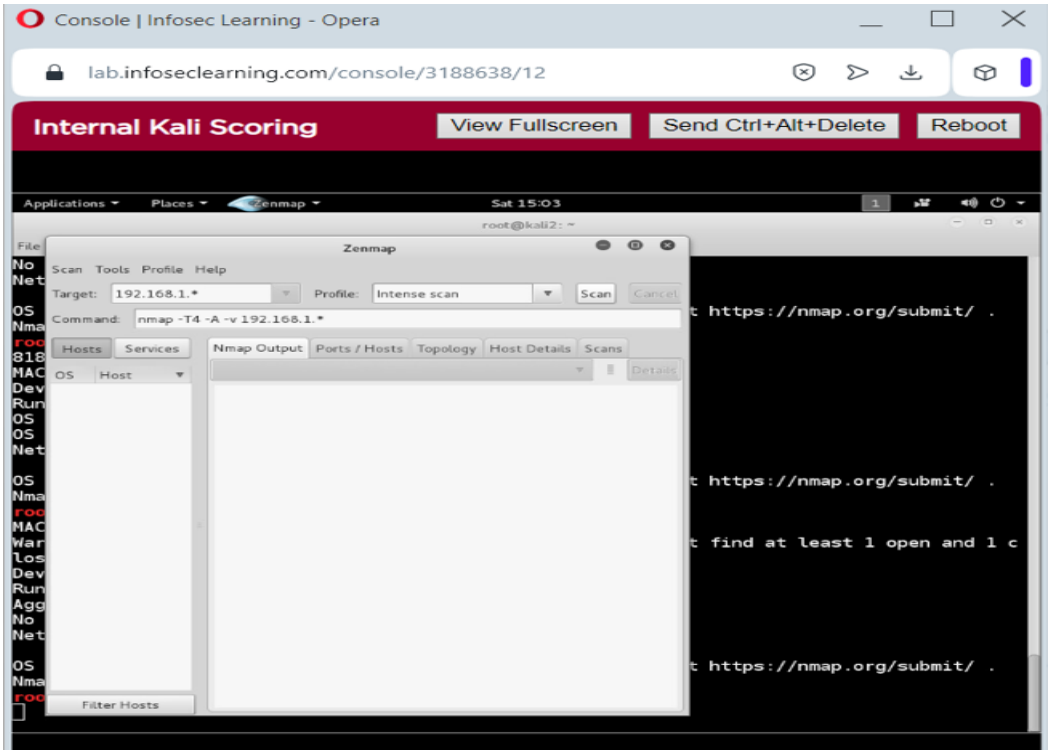
Step 11: Perform an OS scan of 192.168.1.254 to determine the OS of the host.

#nmap -0 192.168.1.254 | tail

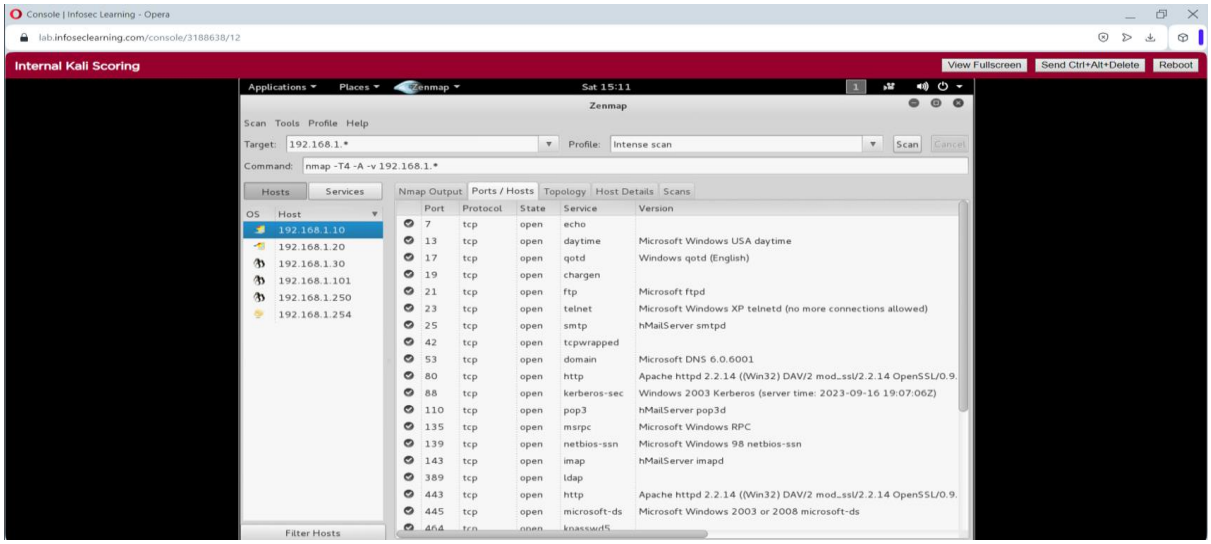
```
root@kali2:~# nmap -O 192.168.1.254 | tail
MAC Address: 00:50:56:8E:00:09 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: specialized
Running (JUST GUESSING): Comau embedded (92%)
Aggressive OS guesses: Comau C4G robot control unit (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.82 seconds
```

Step 12: Open Zenmap and launch an intense scan on 192.168.1.*

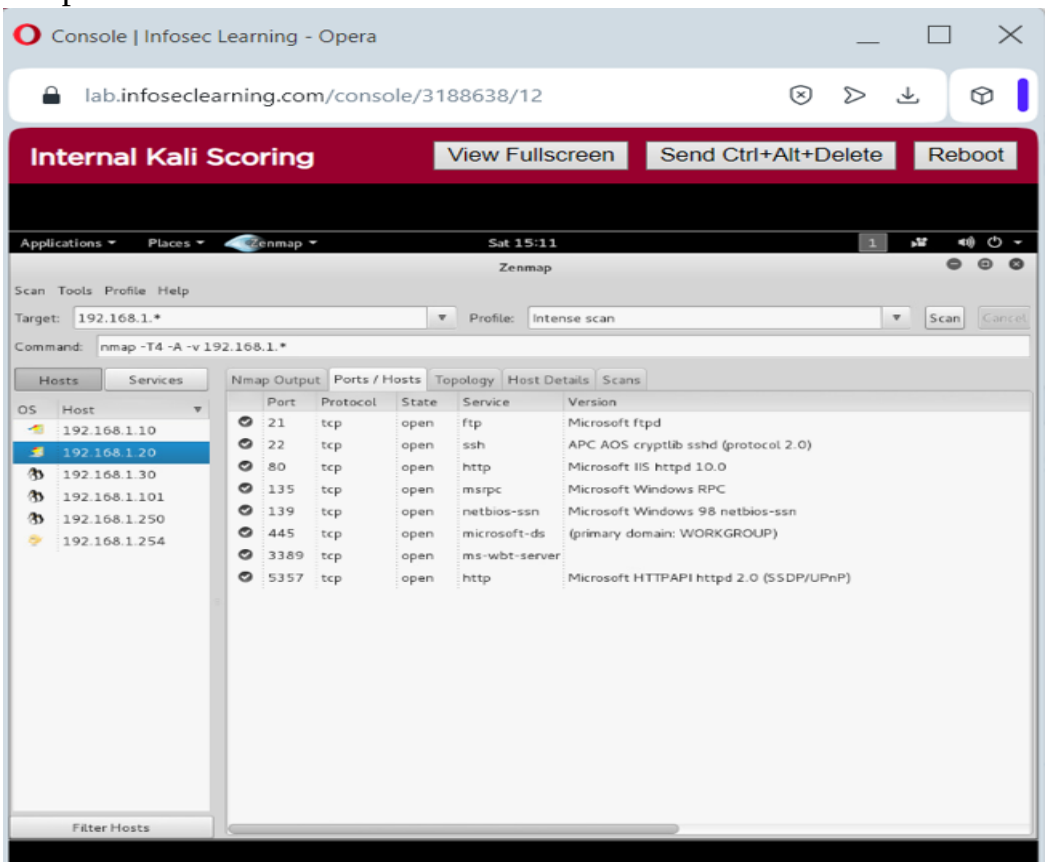
zenmap



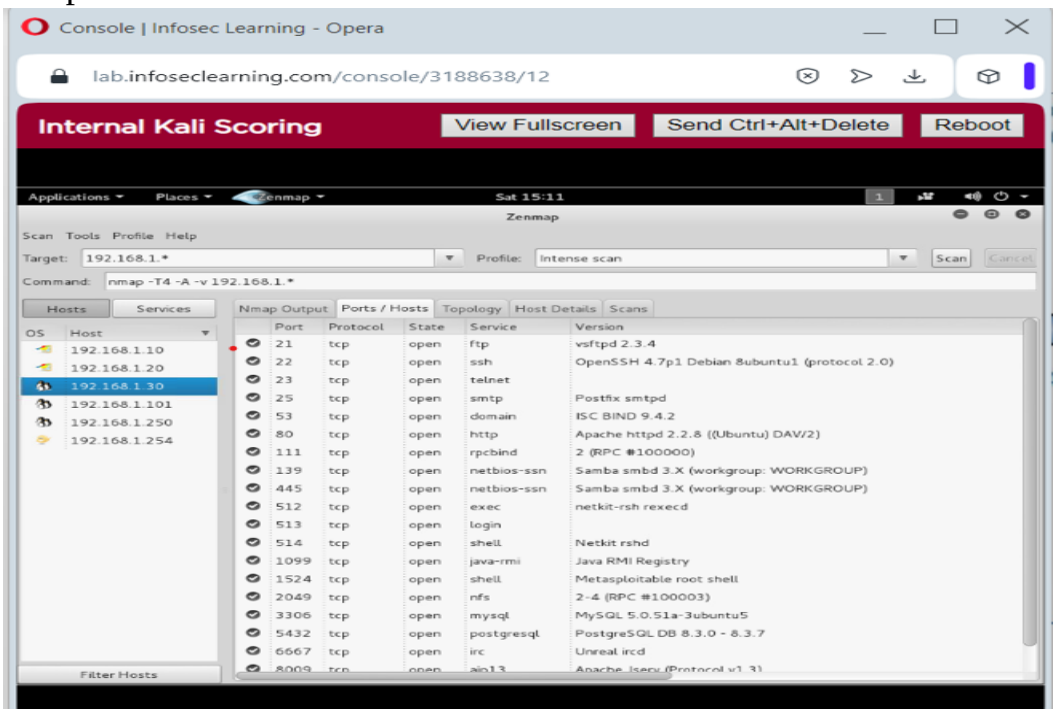
Step 13: Click on first host and then click the ports/hosts tab to view the open ports.



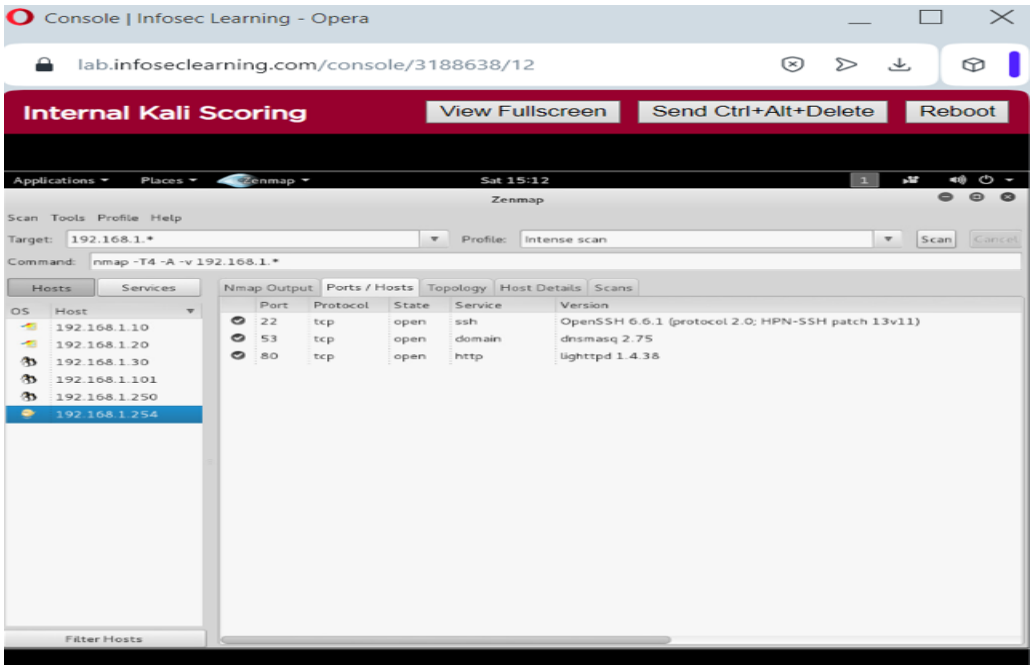
Step 14: Click on second host and then click the ports tab to view the open ports.



Step 15: Click on third host and then click the ports tab to view the open ports.



Step 16: Click on fifth host and then click the ports tab to view the open ports.

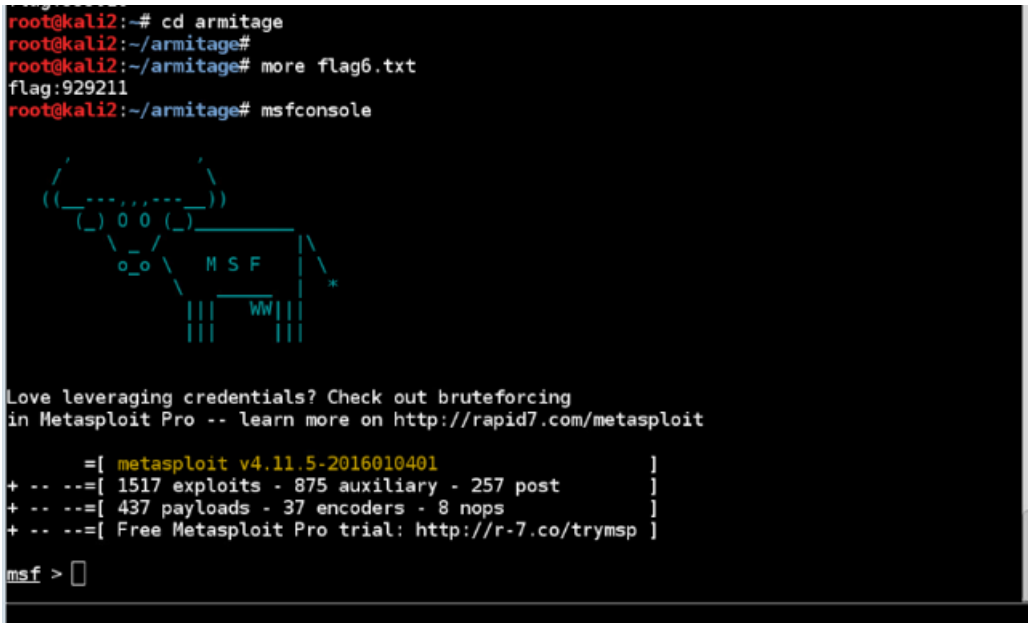


Step 17: Start the postgresql service and check the files and folders.

service postgresql start

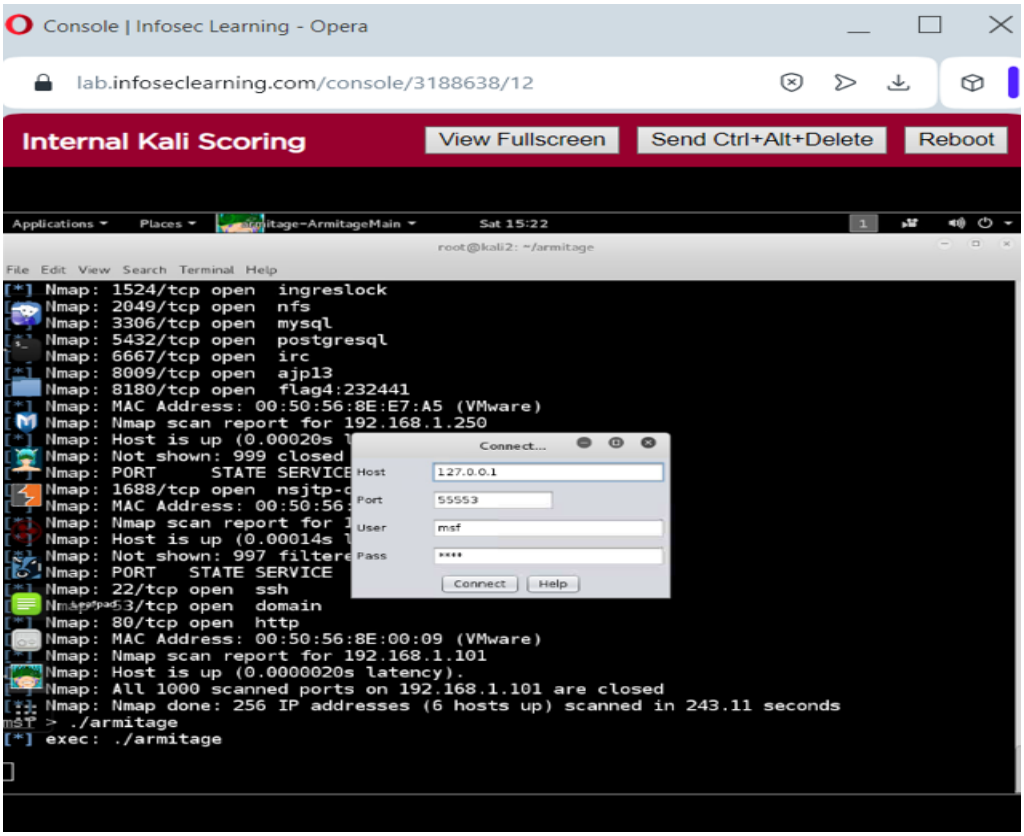
Step 18: Switch to the Metasploit interface.

/armitage#msfconsole

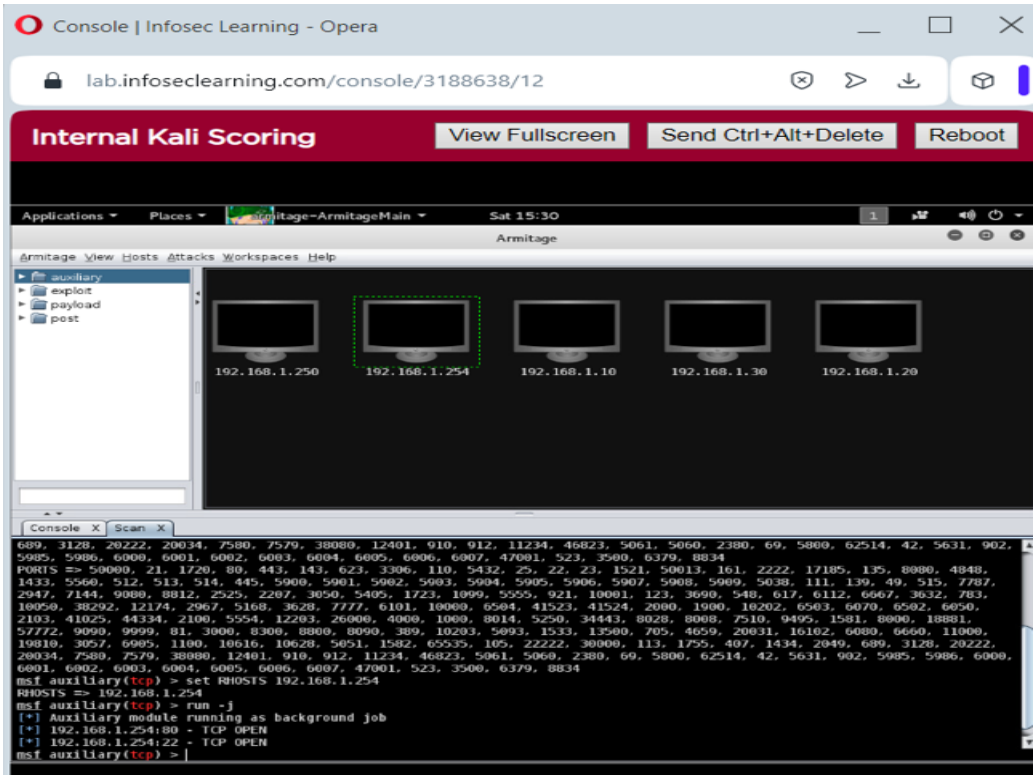


Step 19: Start a database nmap scan.

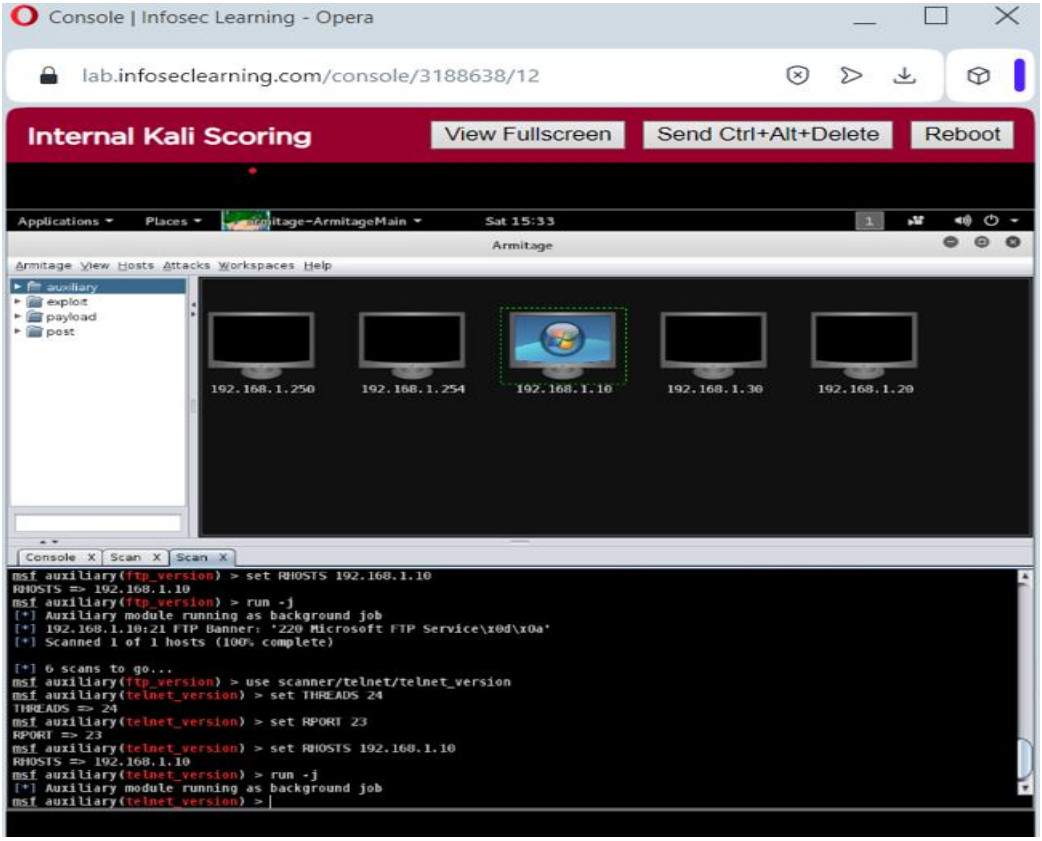
db_nmap 192.168.1.*



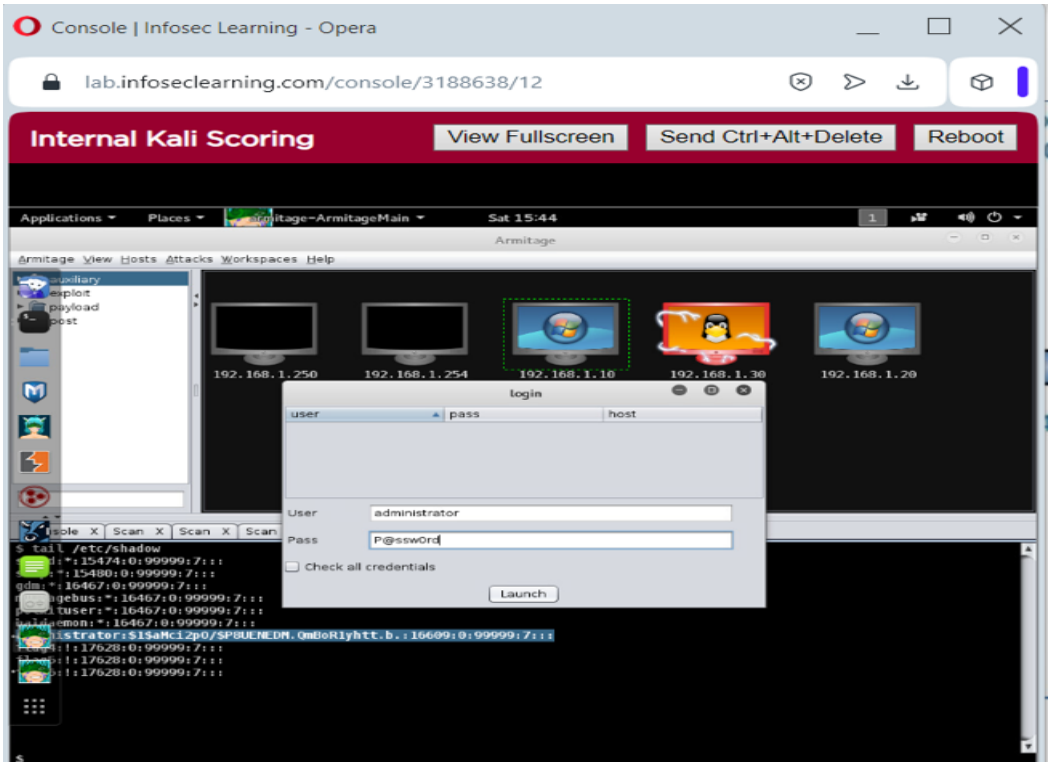
Step 20: Scan the host 192.168.1.254 to detect the OS.



Step 21: Scan the host 192.168.1.10 to detect the OS.



Step 22: Scan the host 192.168.1.30 to detect the OS.



Step 23: To compromise the hosts:

192.168.1.30 > Attack > Misc > java_rmi_server > Launch

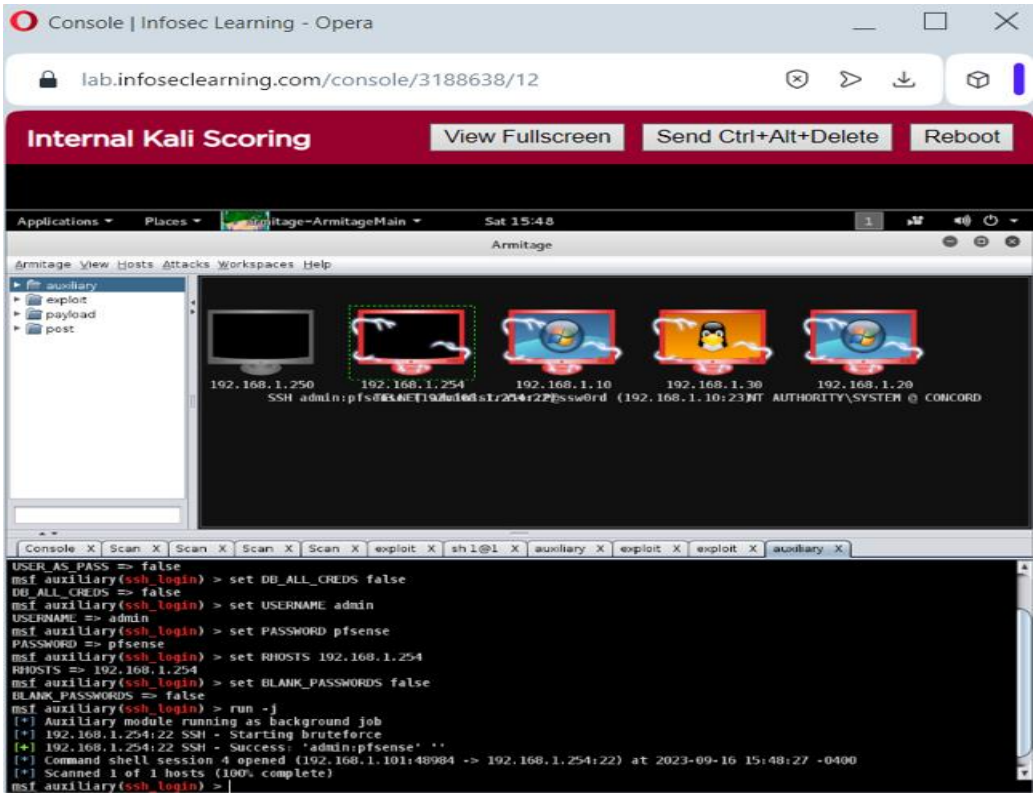
192.168.1.30 > Meterpreter 1 > Interact > Command Shell > tail /etc/shadow >copy the hash file and crack the hash file with John The Rippper (administrator:P@ssw0rd)

192.168.1.10 > Login > telnet > login with administrator:P@ssw0rd > Launch

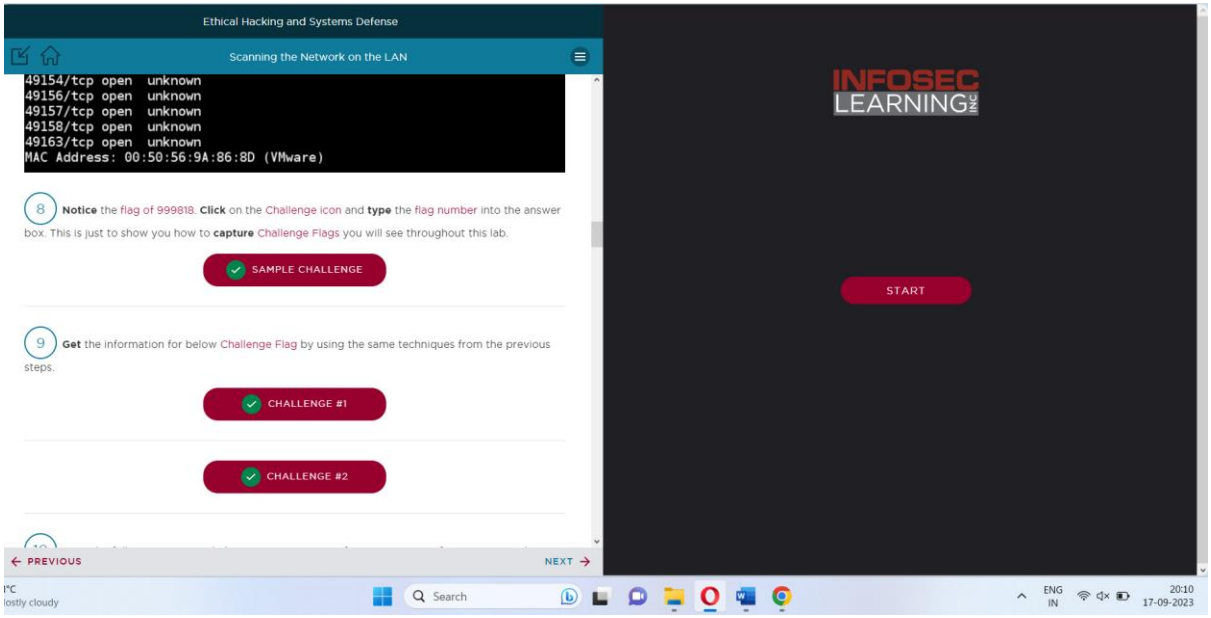
192.168.1.20 > Login > psexec > login with administrator:P@ssw0rd > Launch

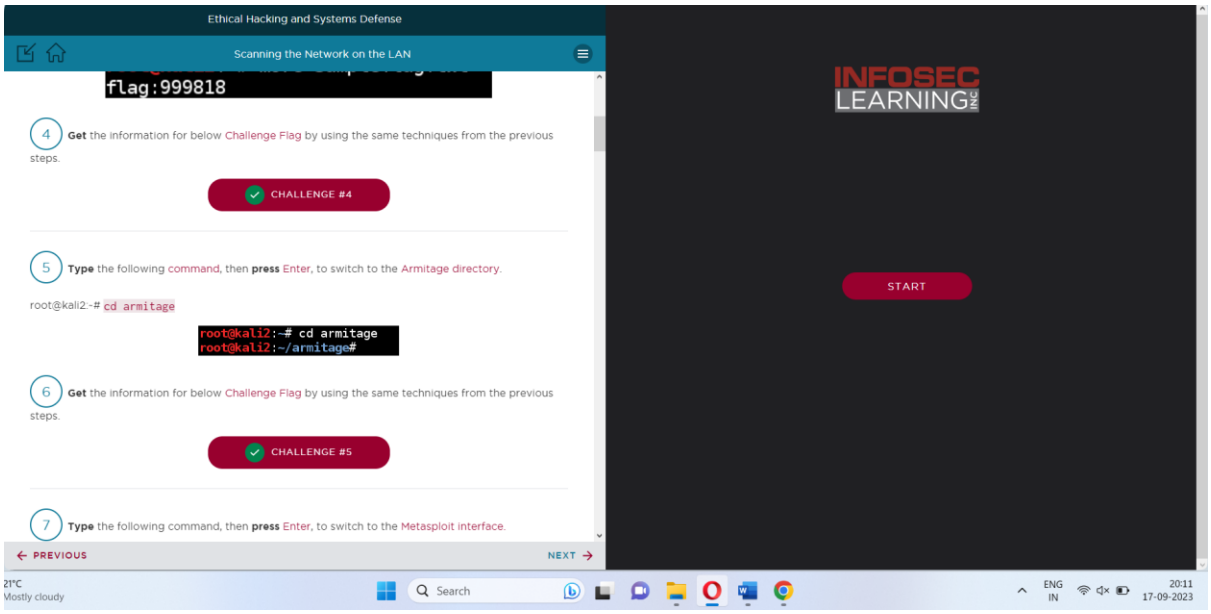
192.168.1.254 > Login> ssh > Login with default pfsense credentials (admin:pfsense) > Launch

All the hosts has been compromised.



Supporting Evidence





Conclusion & Wrap-up

The primary goal of scanning a Local Area Network (LAN) is to gather in-depth data about the structure and components of the network. This information is necessary for determining the network's current state of security and identifying any vulnerabilities. Based on these findings, one can thereafter proactively develop customised security policies and risk mitigation strategies.

CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-1

Capturing and Analyzing Network Traffic Using a Sniffer

Student Info:
Name : Akhila Parankusham
Student ID: 00810899
Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

Ifconfig

Identify the network interface and configure it.

Protocols

ftp, telnet and mail protocols used to generate the traffic.

Wireshark

Capture and analyze the traffic.

Objectives

The major goals of gathering and analyzing network traffic with a sniffer are to gain a deeper understanding of network activity, discover potential security threats, troubleshoot network issues, and improve network performance. By mastering the techniques and tools of network sniffing, network administrators can strengthen their capacity to maintain network security and ensure network dependability.

Lab Description Details

1. Understanding Network Behavior: Recognizing patterns in network traffic and the actions of network devices and services will help you understand network behavior.

2. Determining security risks: Potential security threats and weaknesses can be discovered by examining network traffic.

3. Network troubleshooting: The process of locating problem regions and determining the source of network difficulties using network traffic analysis.

4. Increasing network performance: To maximize network performance, network traffic bottlenecks must be identified and eliminated.

5. Acquiring knowledge of network sniffing tools and procedures: to get practical knowledge of network sniffing methods and tools and become an expert user of these devices for capturing and analyzing network information.

6. Recognizing the importance of network sniffing: Recognizing the value of network sniffing for network security.

Step 1: Log in to the Kali Linux.

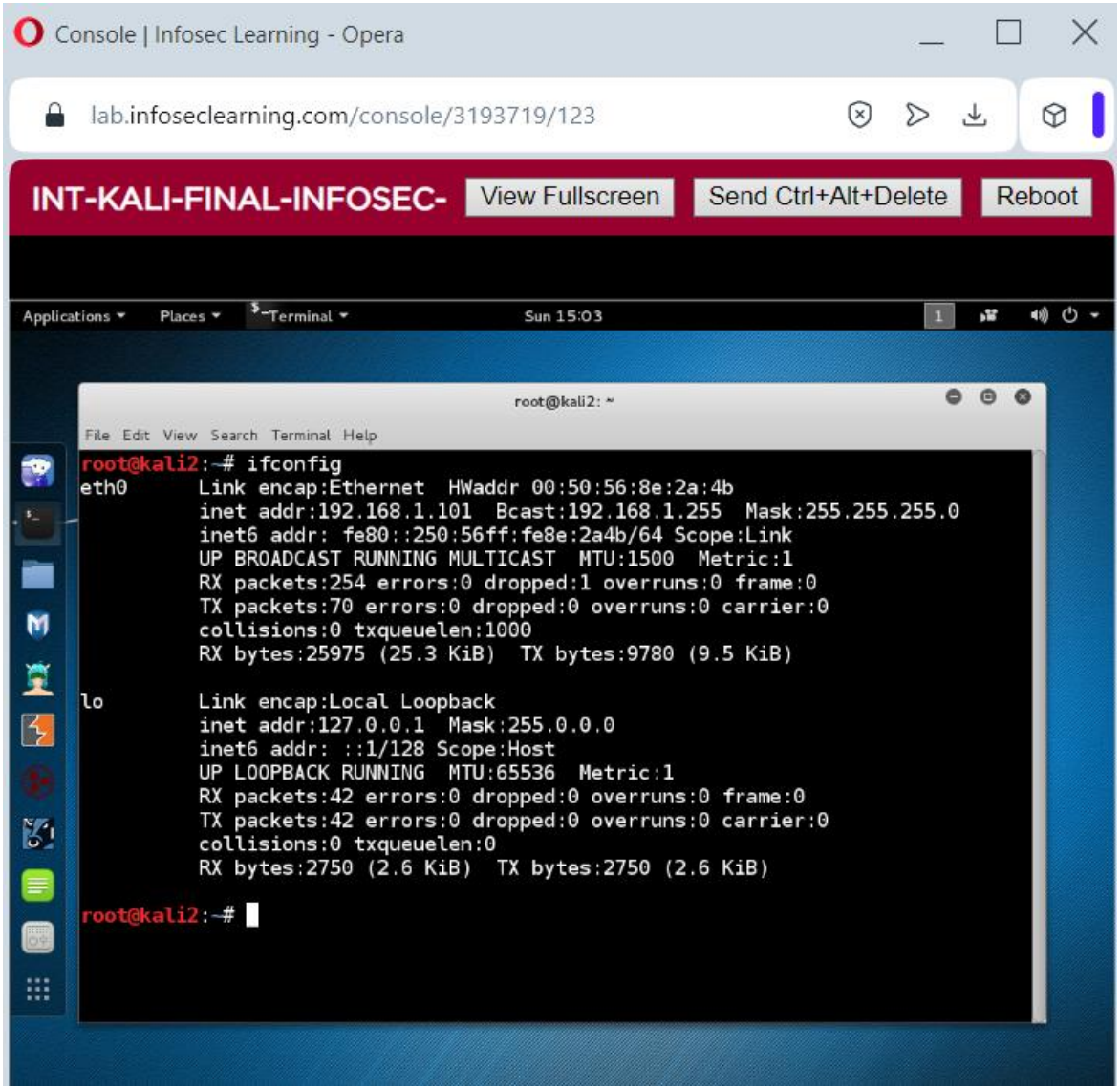
Enter the credentials. Username: **root**

Password: **toor**

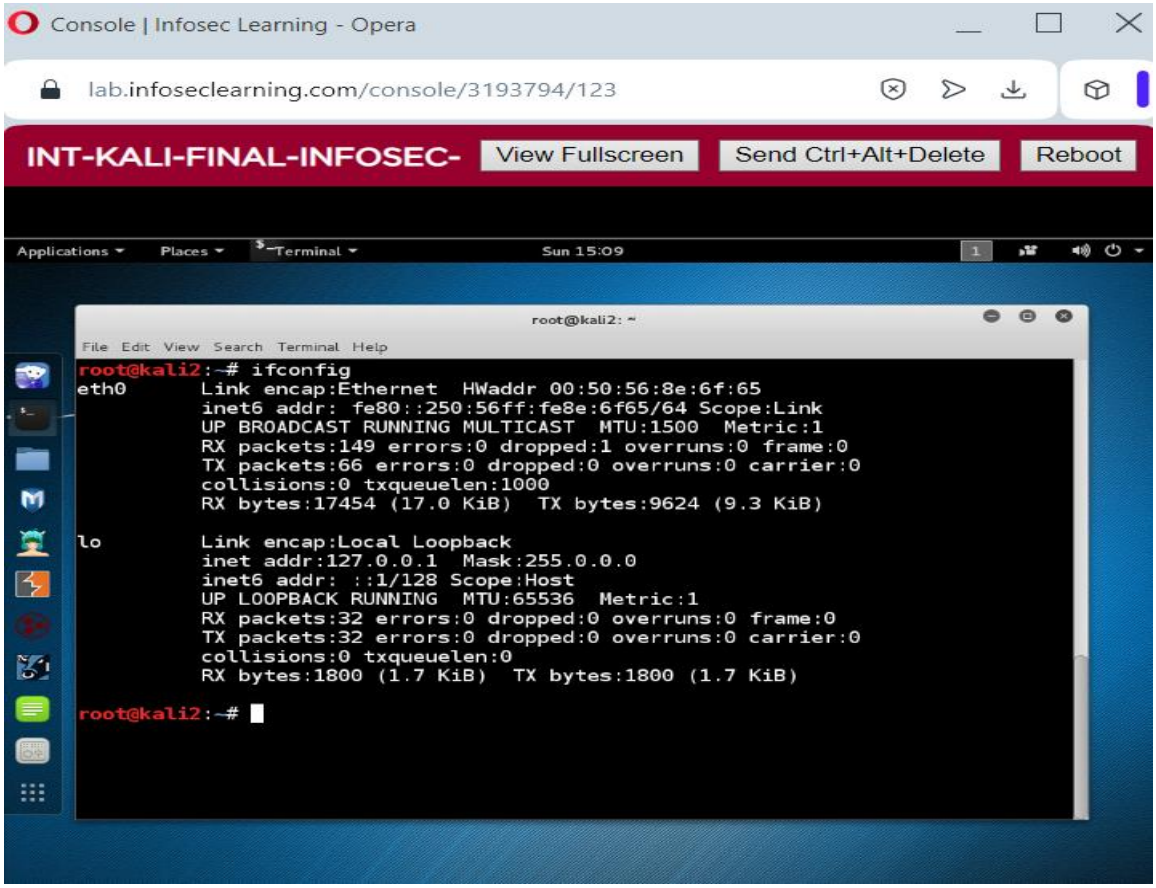
Step 2: Open the terminal.

Step 3: Check for the IP address of the system.

#ifconfig

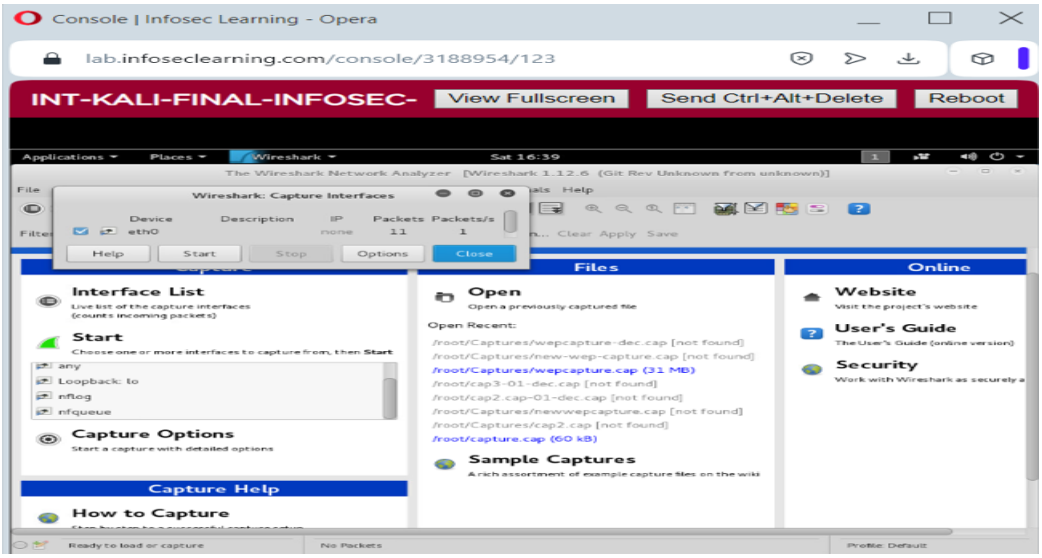


Step 4: Enter # ifconfig eth0 0.0.0.0 up to verify that no IPv4 address is listed for eth0 and then if config



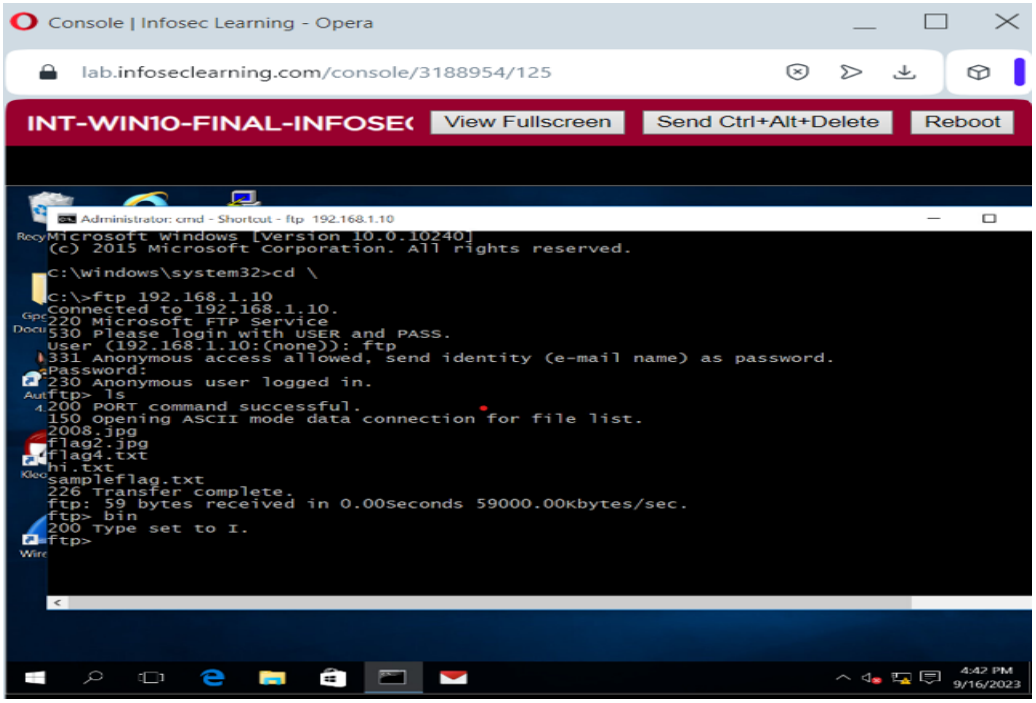
Step 5: Open Wireshark and capture the eth0 data by clicking the start button.

>Wireshark > Capture > Interfaces > select eth0 > start



Step 6: Run cmd-shortcut as administrator and ftp to windows server.

>ftp 192.168.1.10
ftp> ls
ftp> bin (Switch to binary mode to download the picture file)
ftp> get 2008.jpg
ftp> bye (leave the ftp session and exit the ftp sub-prompt)



Step 7: Open the File explorer

>File explorer > This PC > Local Disk (C:) > 2008.jpg > flag 999818

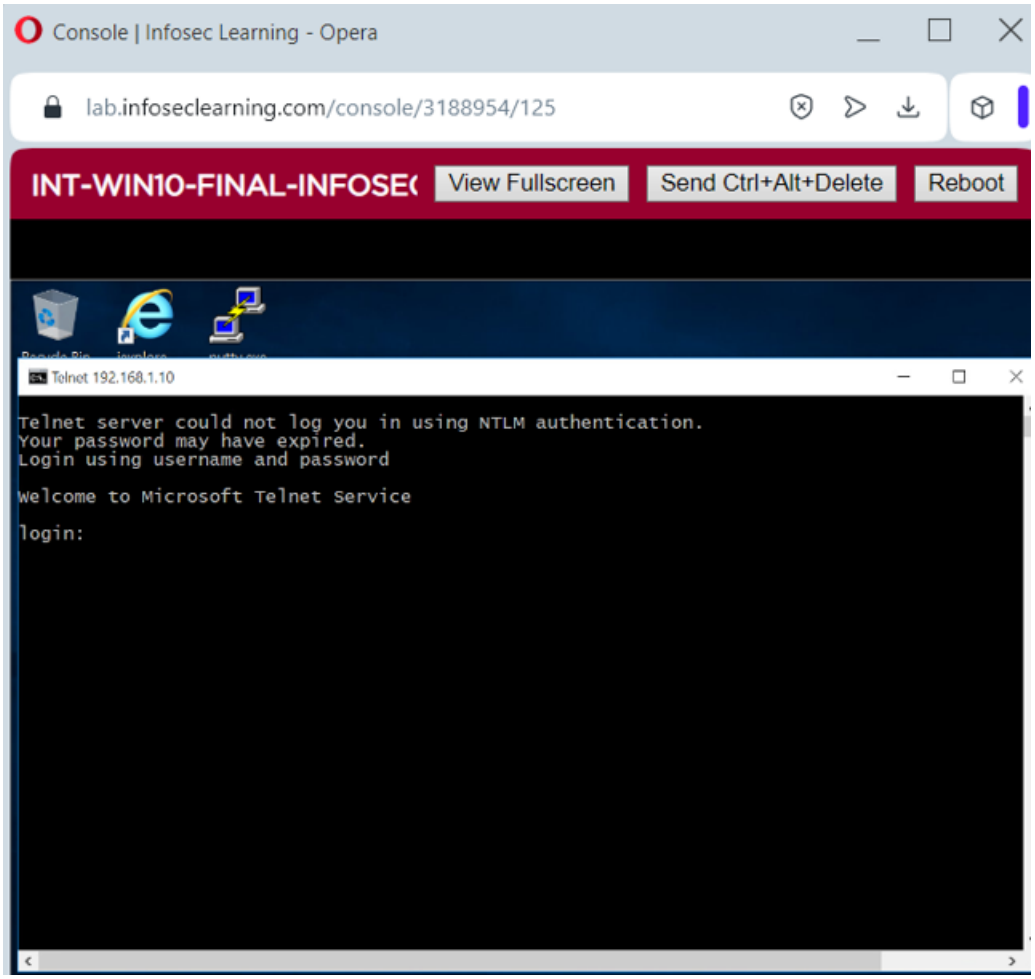
Step 8: Repeat the Step5 and Step 6 to complete the challenge 1 flag. (i.e., flag 80212)

16 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #1

Step 9: Open the cmd-shortcut and connect to the windows server using telnet.

>telnet 192.168.1.10 > enter y to continue > Login to windows server using administrator:P@ssw0rd.

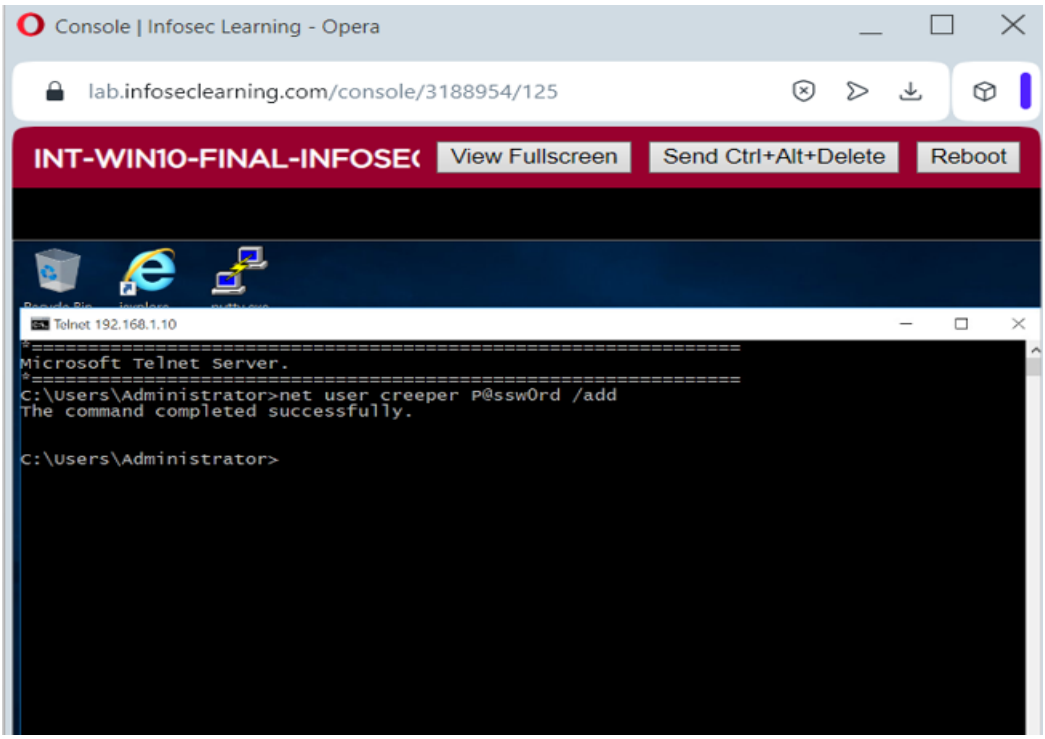


Step 10: Add a user account creeper to the windows server.

>net user creeper P@ssw0rd /add

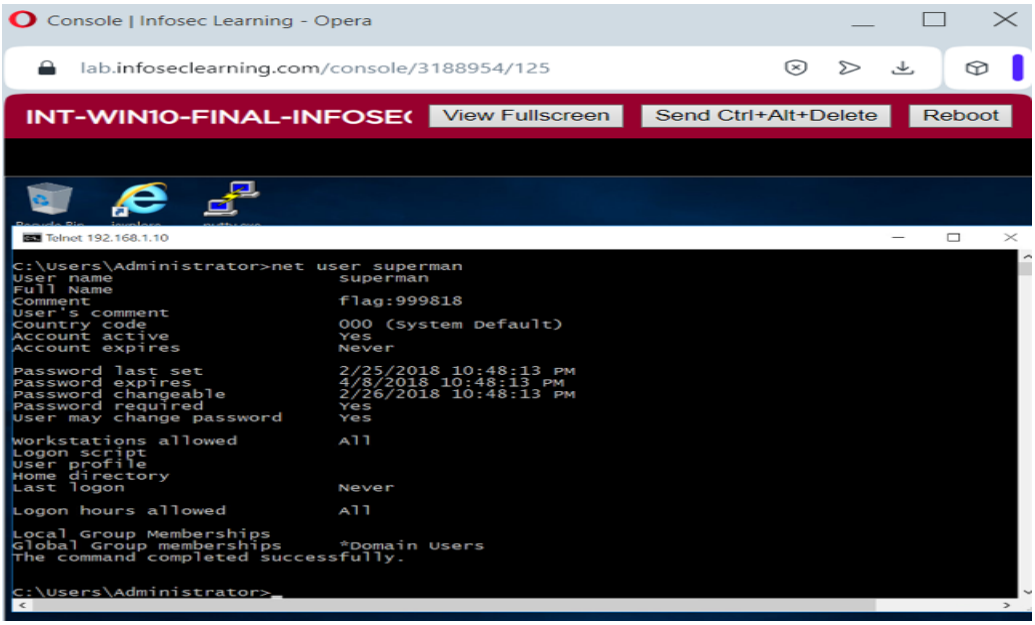
Add creeper to the Enterprise Admins group.

>net group “domain admins” creeper adds



Step 11: View the superman information account and complete the challenge

>net user superman



Step 12: View the aquaman information account and complete the challenge

>net user aquaman

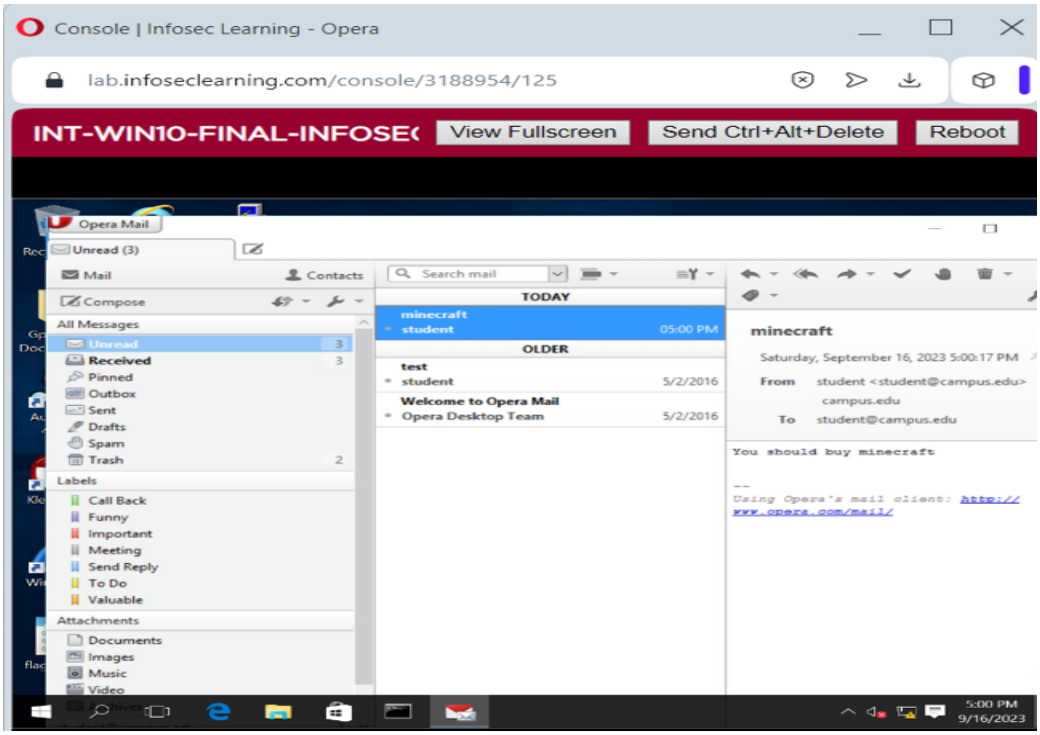
25 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #2

Step 13: Leave the telnet session on the windows server.

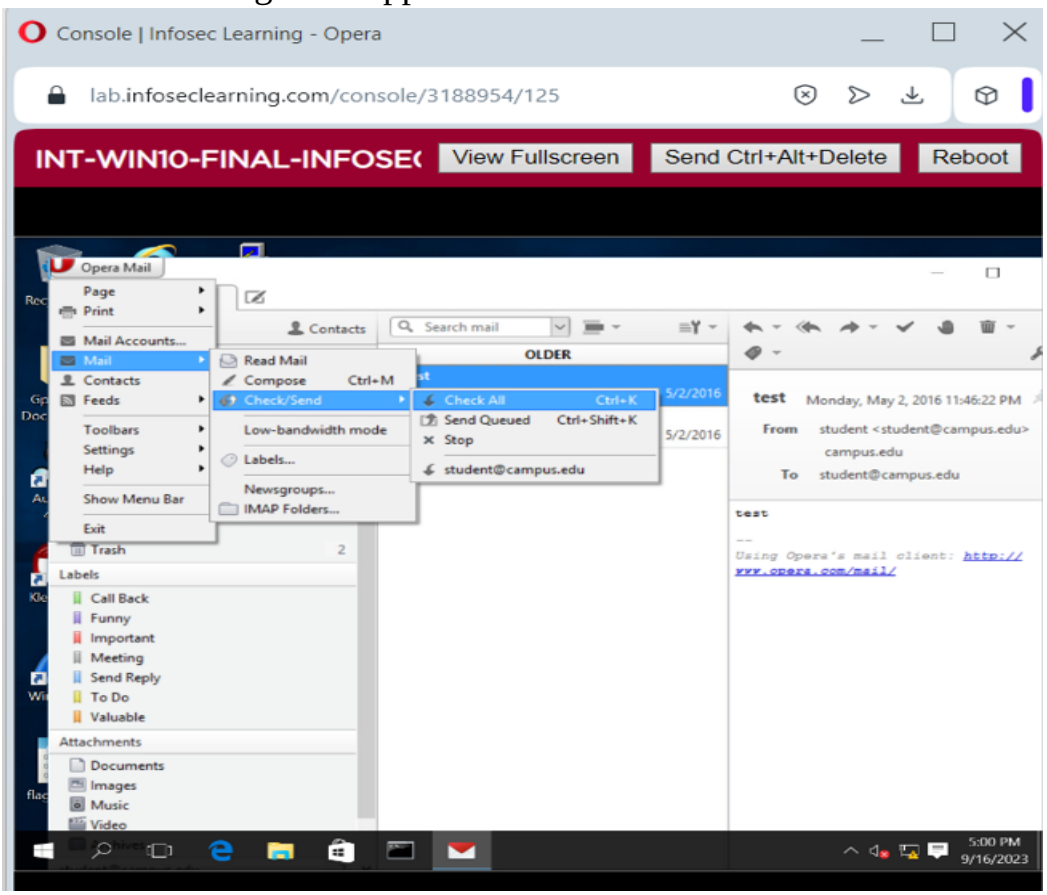
Step 14: Open the Opera mail and click the compose button to compose the mail.

To box: student@campus.edu
Subject box: minecraft
Body: You should buy Minecraft
and send the mail.

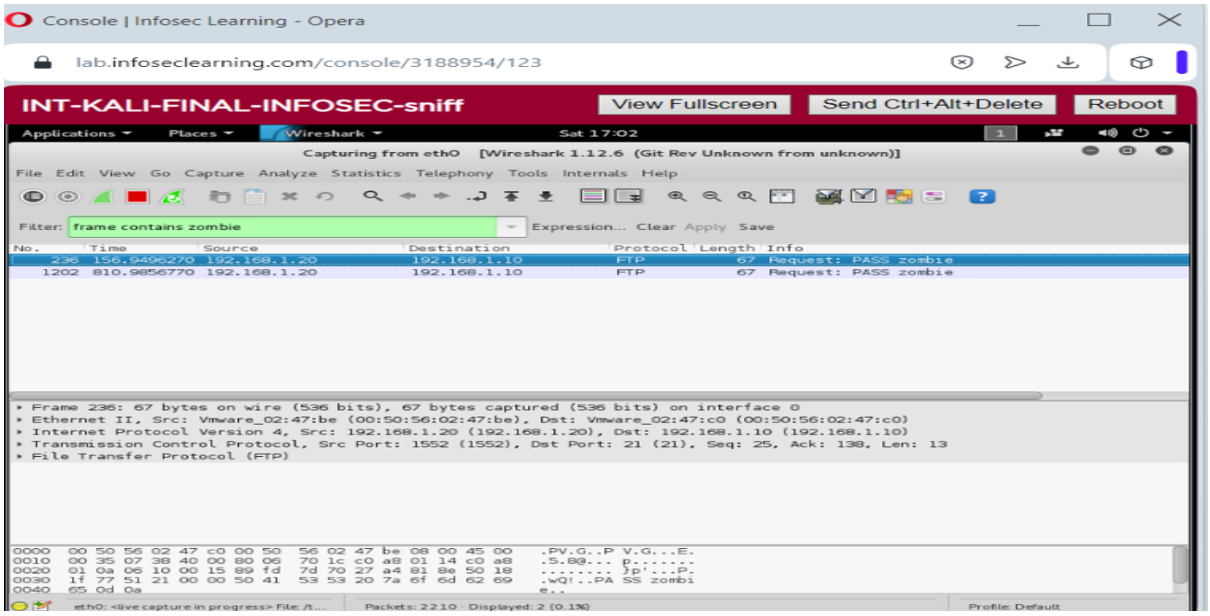


Step 15: Click Opera mail > Mail>Check/send >Check All

Minecraft message will appear in the list.

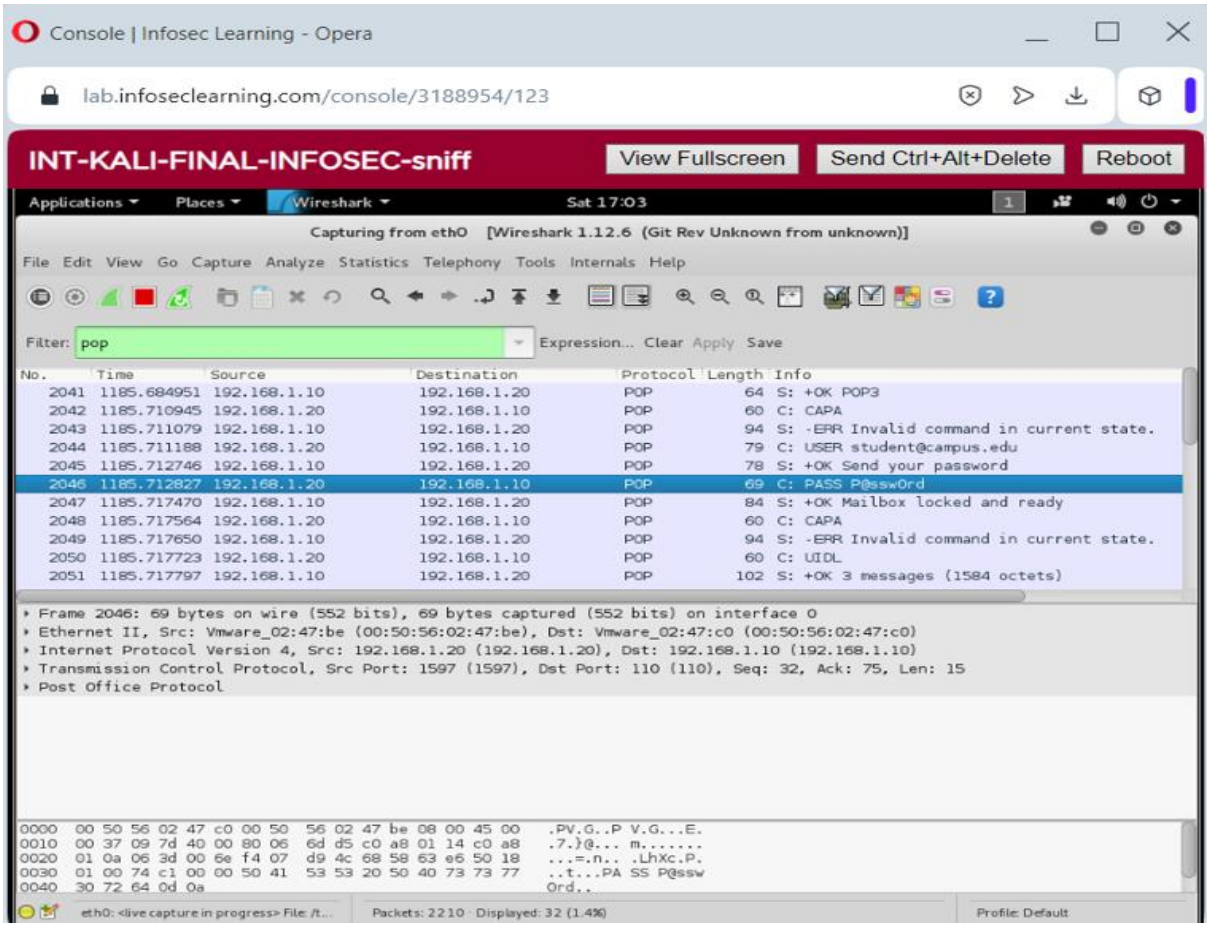


Step 16: In the Wireshark filter pane type ‘’frame contains zombie’’ to get the user’s zombie password.

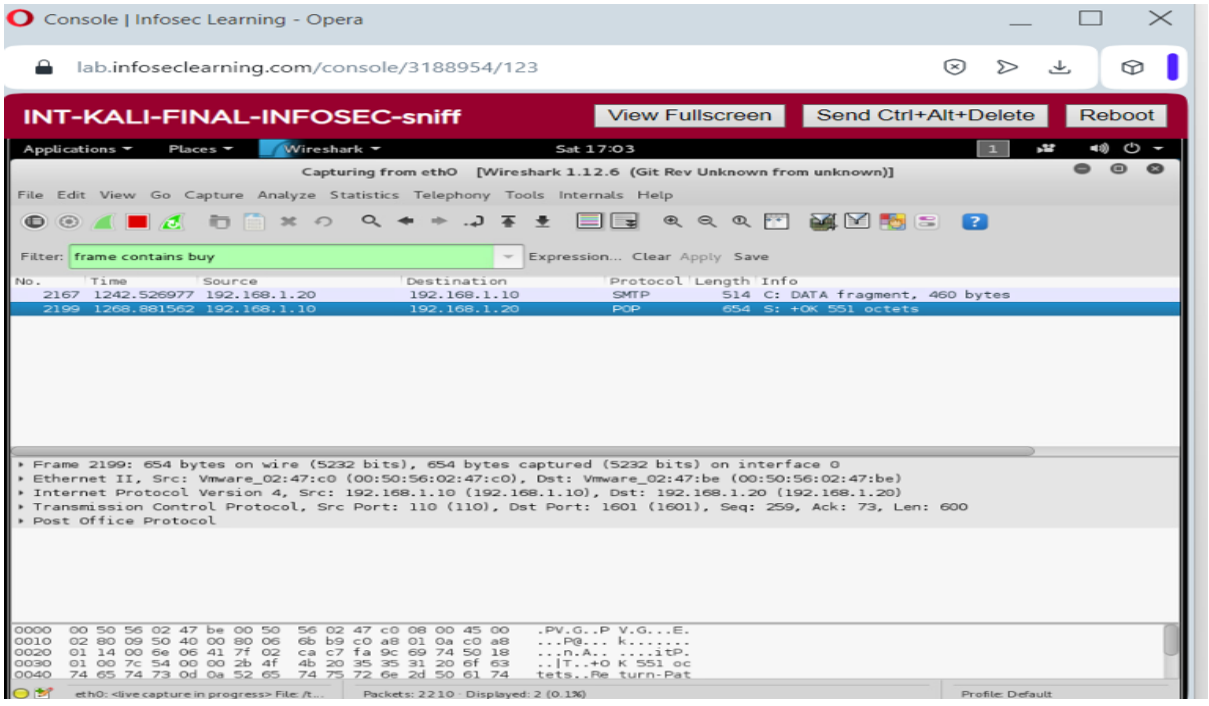


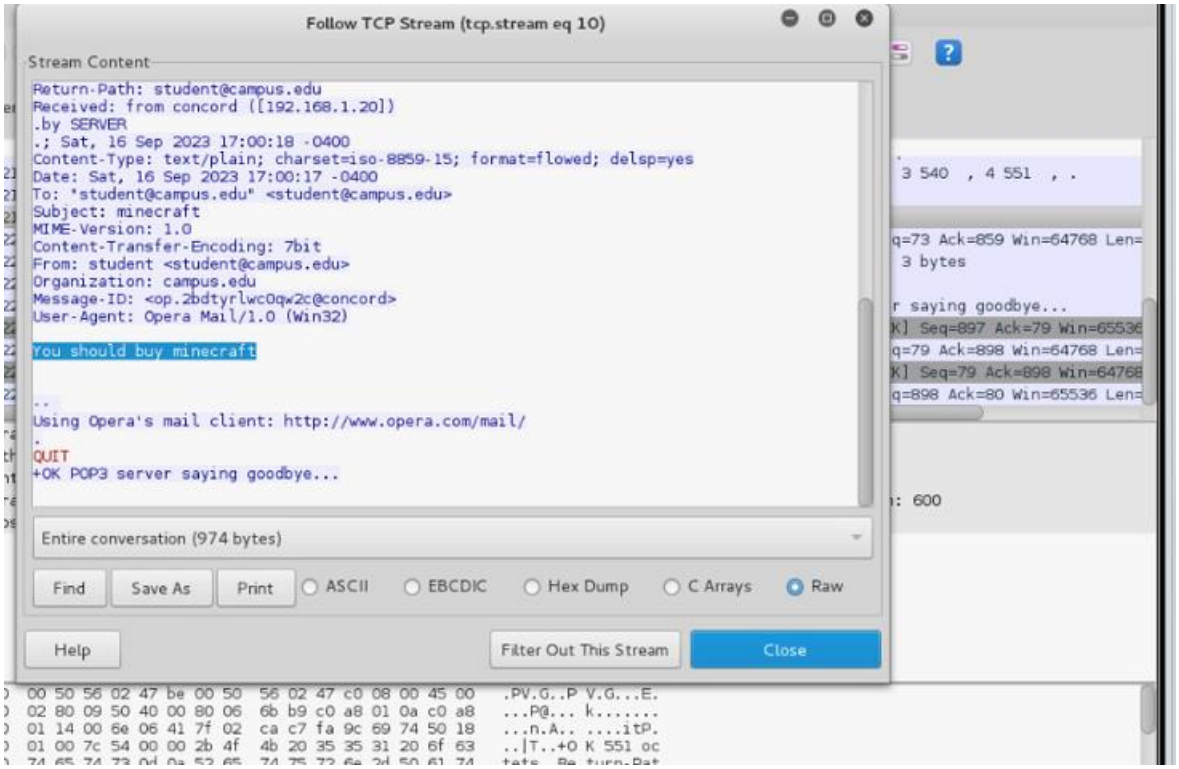
Step 17: Examine the email traffic using POP.

Wireshark filter pane > POP > apply (to view the student’s password of P@ssw0rd).

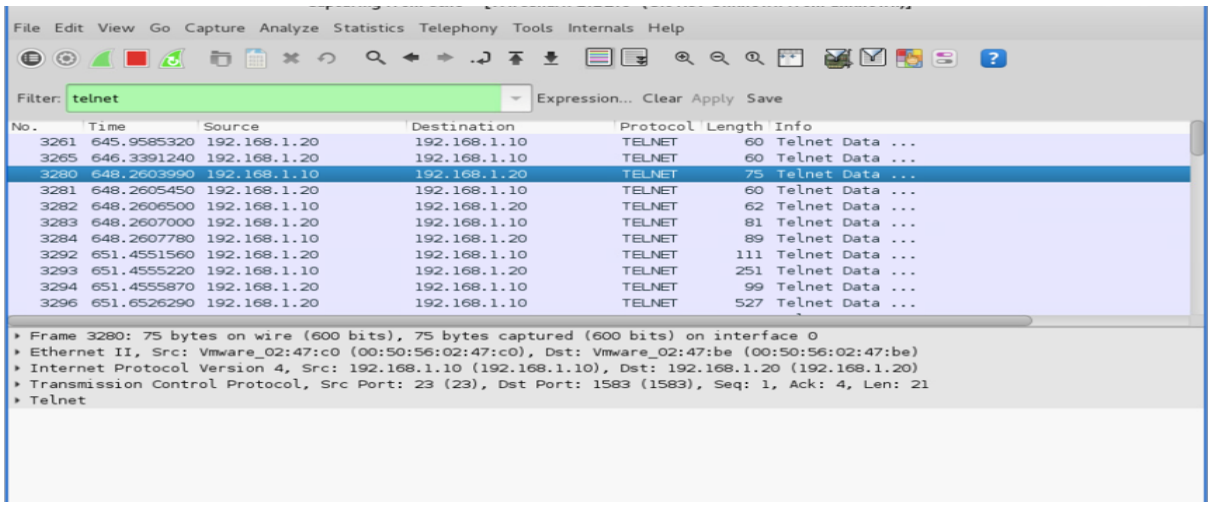


Step 18: Wireshark filter pane > frame contains buy > apply > POP frame > Follow TCP Stream





Step 19: Wireshark filter pane > telnet > apply > telnet frame > Follow TCP Stream



Step 20: Stop the Wireshark and open capture.cap file and complete the challenges.

>file > open > continue without saving > home > capture.cap

16 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #3

17

Get the information for below Challenge Flag by using the same techniques from the previous steps.

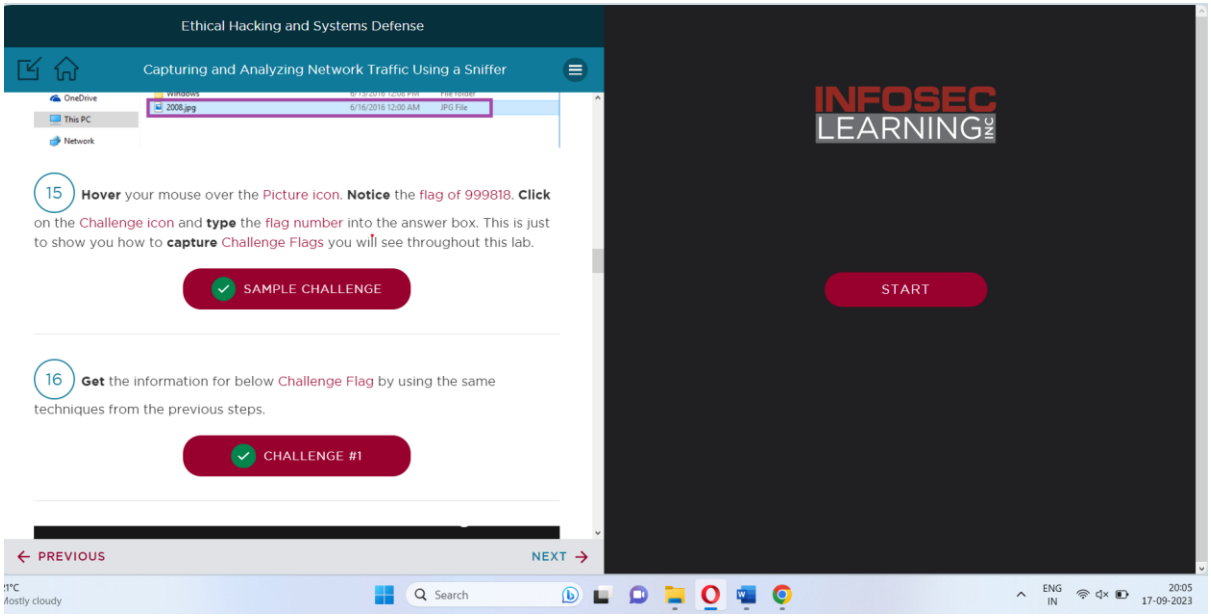
CHALLENGE #4

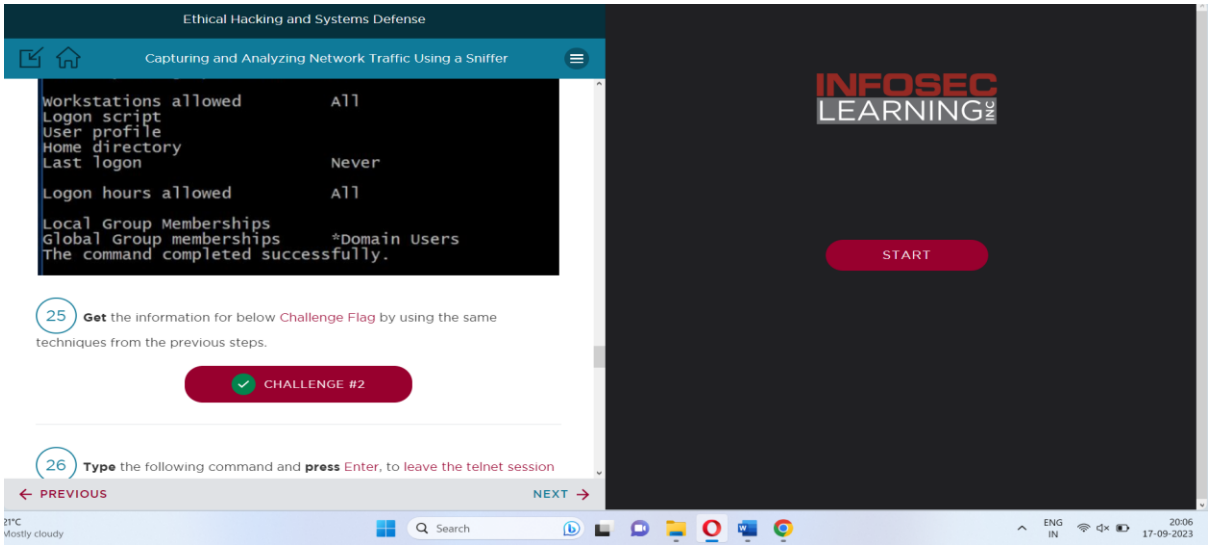
18

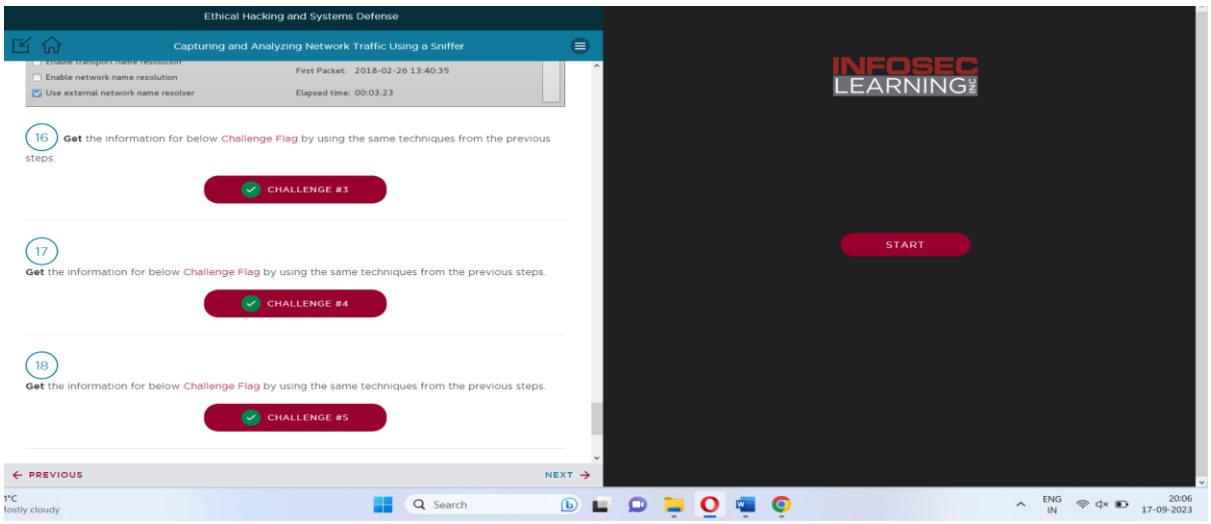
Get the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #5

Supporting Evidence







Conclusion & Wrap-up

The lab provides a thorough study of the techniques and tools utilized in the demos and clarifies the challenges and limitations of performing reconnaissance from a WAN. The goal is to offer a clear understanding of the importance of reconnaissance, the successes and failures of various approaches, and the challenges that must be overcome in order to properly conduct reconnaissance in actual situations.