Lab 6 - Capturing and Analyzing Network Traffic Using a Sniffer

Objective:

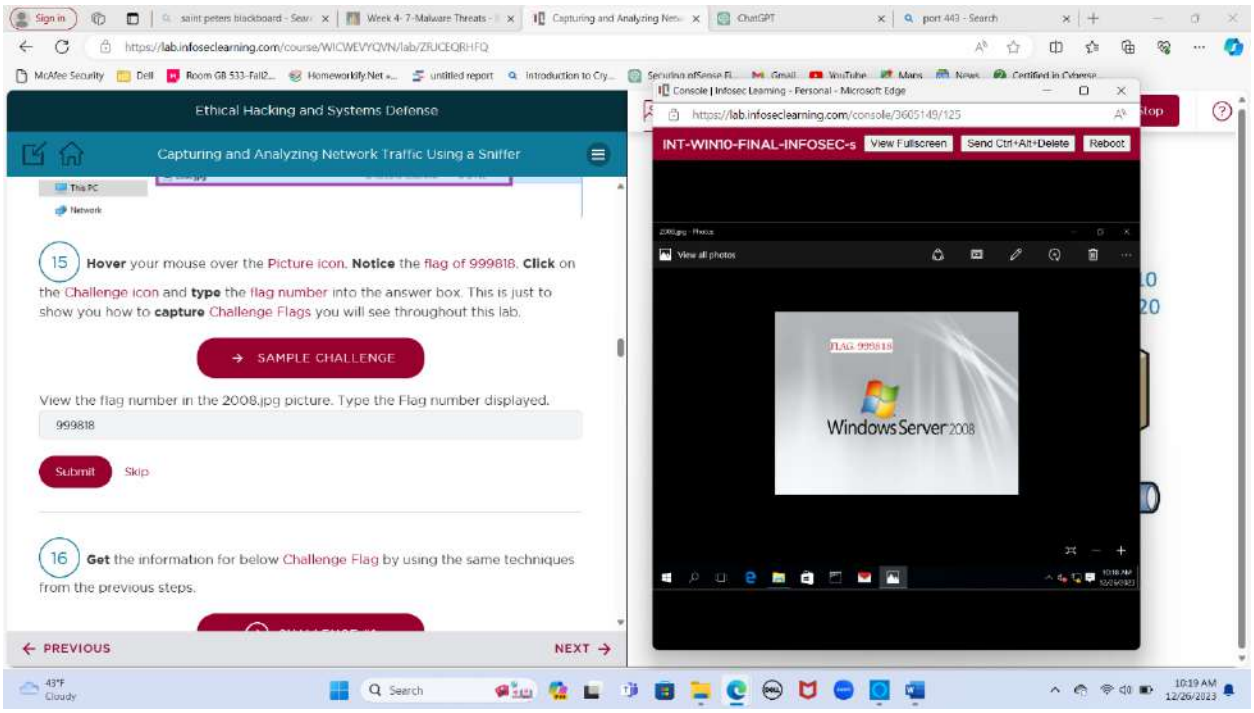
1. Starting the Sniffer
2. Generating the Traffic
3. Analysing the Traffic

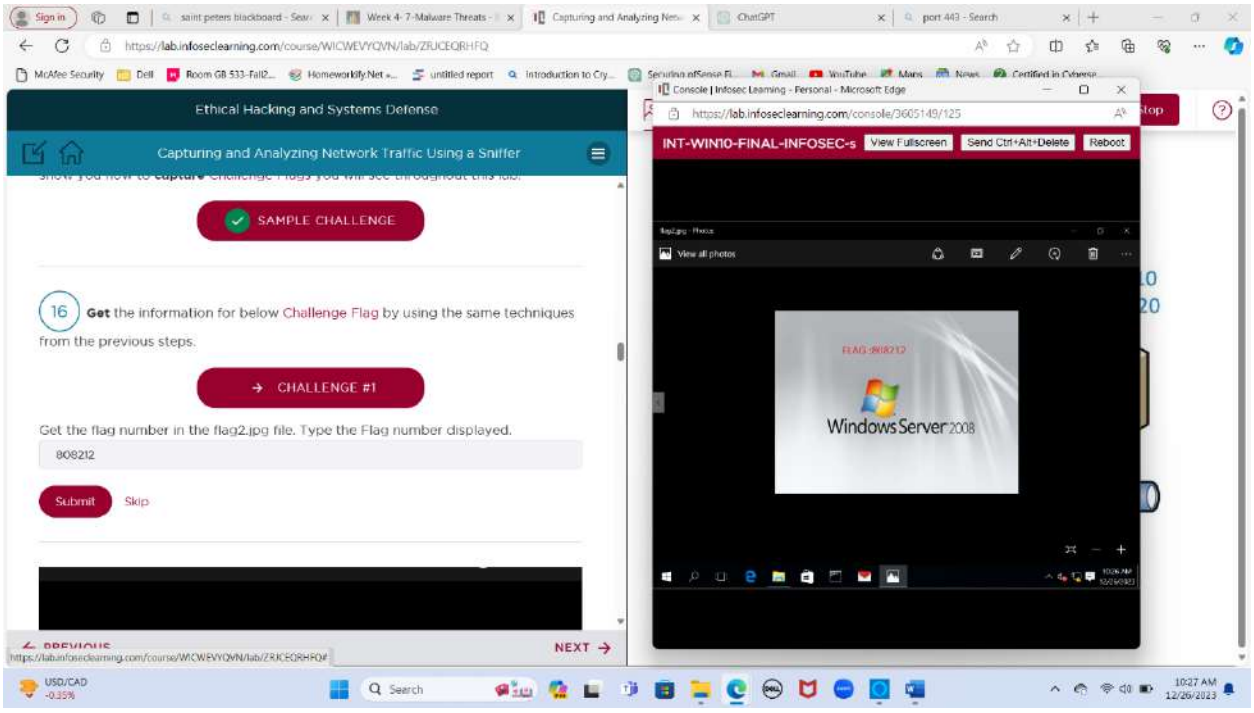
Takeaways:

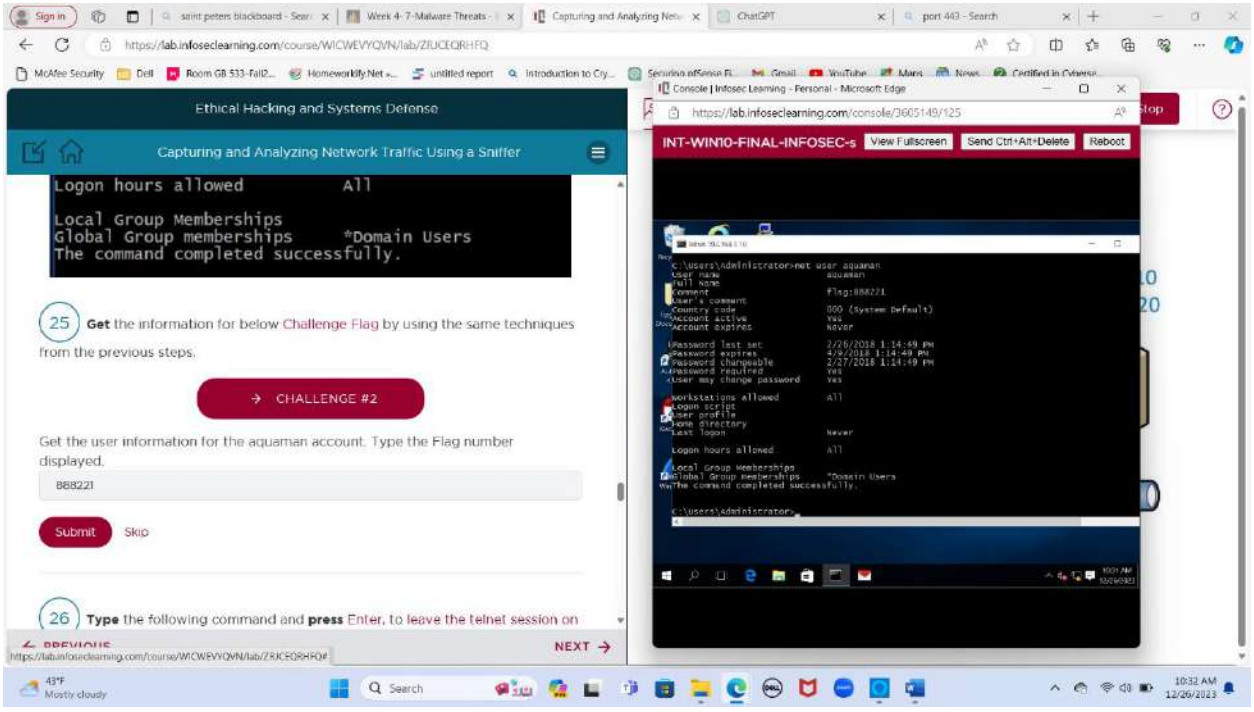
1. Wireshark is a powerful network protocol analyzer used for capturing and inspecting network traffic in real-time. It allows users to examine data packets traversing a network, aiding in network troubleshooting, security analysis, and protocol development.
2. FTP, short for File Transfer Protocol, is a standard network protocol used for transferring files between a client and a server on a computer network. It enables users to upload, download, and manage files on a remote server over a network connection.
3. Telnet is a network protocol used to establish a remote connection and access resources or manage devices over a network, typically the internet. It allows users to log into and interact with a remote computer or server, but due to security vulnerabilities, its usage has declined in favor of more secure protocols like SSH (Secure Shell).
4. The "net group" command in Windows is a command-line utility used to manage groups within a network environment. It enables administrators to create, modify, view, and manage group memberships and permissions on a Windows system or domain.
5. A TCP stream refers to a sequence of data transmitted between two devices over a TCP (Transmission Control Protocol) connection. It represents the continuous flow of

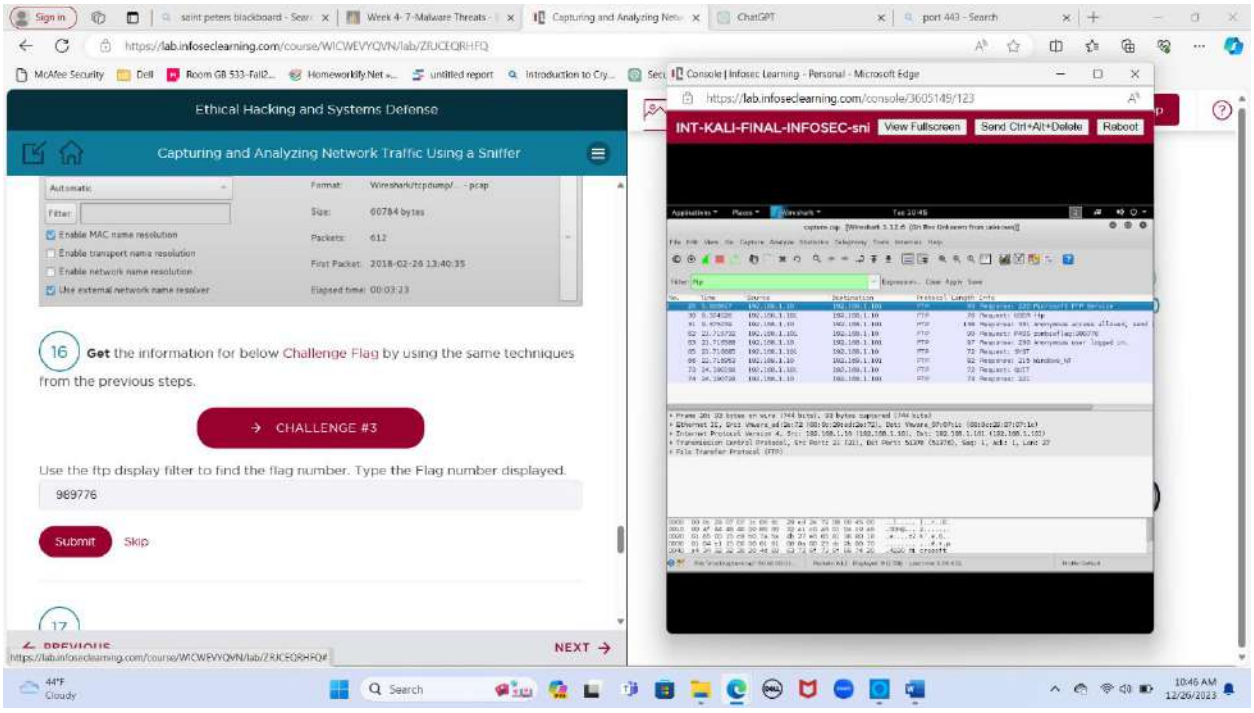
information sent and received between the sender and receiver, maintaining the reliability and order of data delivery in a network communication session.

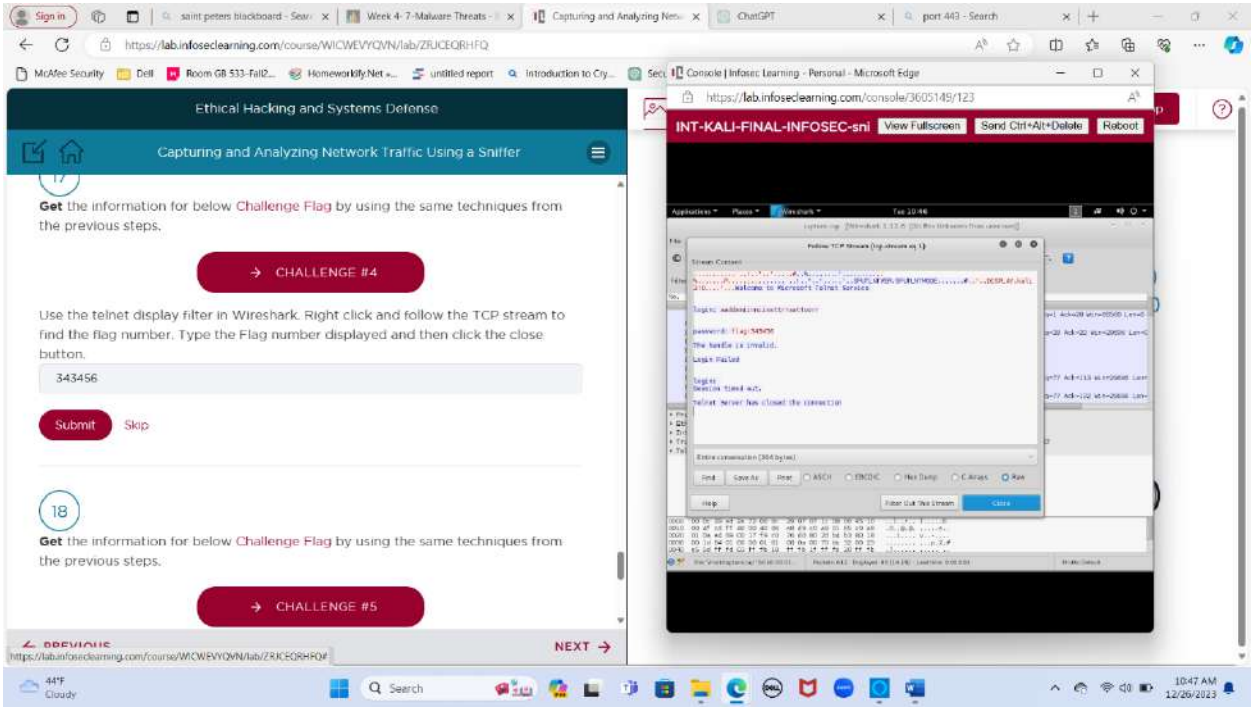
Challenges:

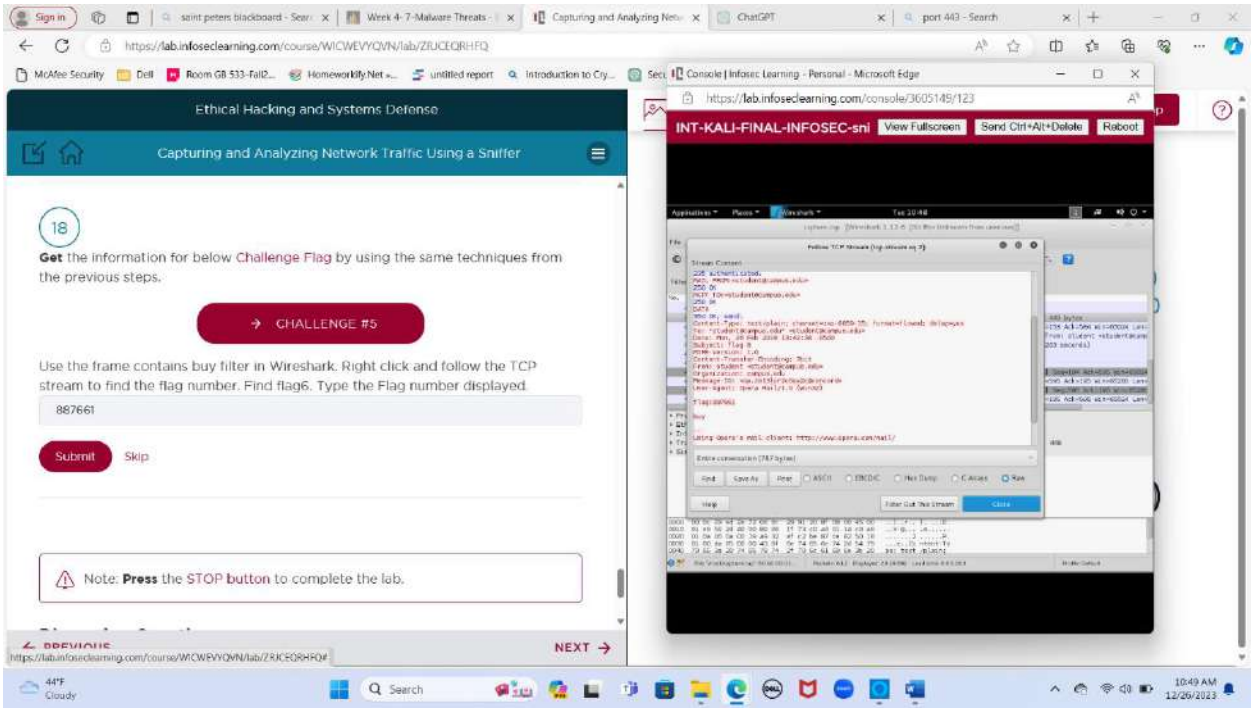



Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
SAMPLE CHALLENGE
16 Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #1
Get the flag number in the flag2.jpg file. Type the Flag number displayed.
808212
Submit
Skip
PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Windows Server 2008

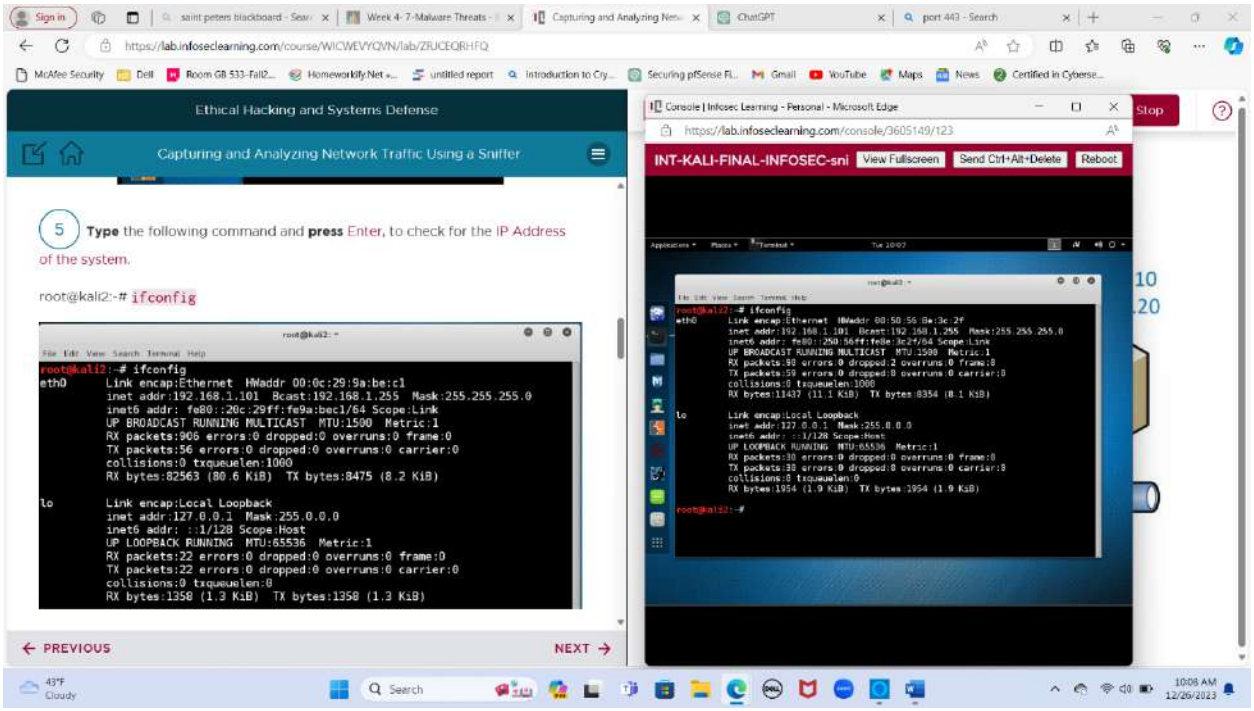

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
Logon hours allowed All
Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.
25 Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #2
Get the user information for the aquaman account. Type the Flag number displayed.
888221
Submit
Skip
26 Type the following command and press Enter, to leave the telnet session on
PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3605145/123
INT-KALI-FINAL-INFOSEC-snl
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
16 Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #3
Use the ftp display filter to find the flag number. Type the Flag number displayed.
989776
Submit
Skip
NEXT →

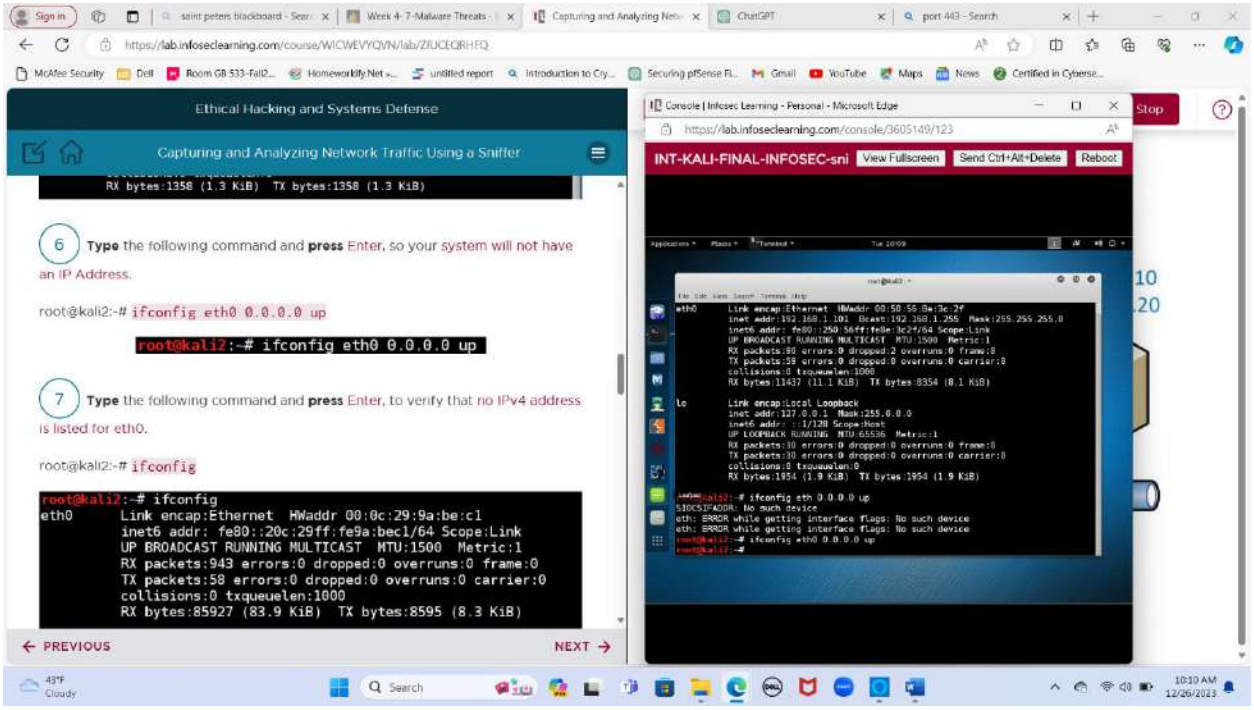

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3605145/123
INT-KALI-FINAL-INFOSEC-snl
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #4
Use the telnet display filter in Wireshark. Right click and follow the TCP stream to find the flag number. Type the Flag number displayed and then click the close button.
343456
Submit
Skip
18
Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #5
NEXT →

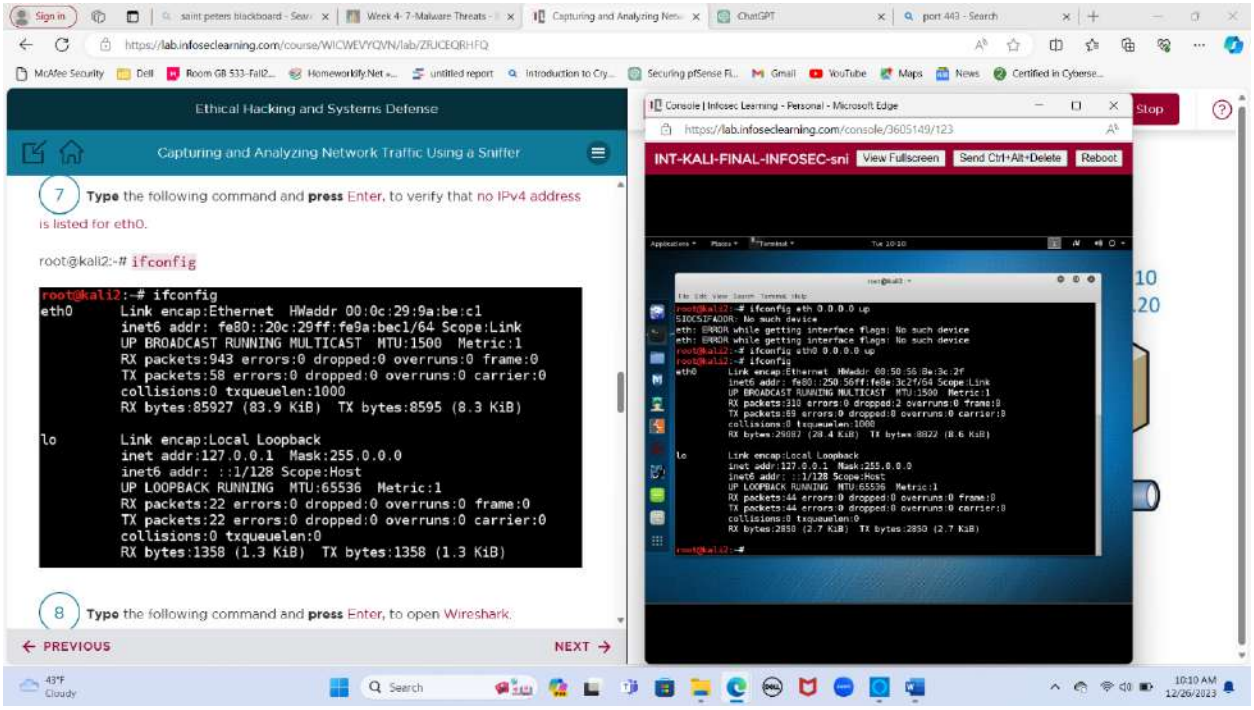


Screenshots:

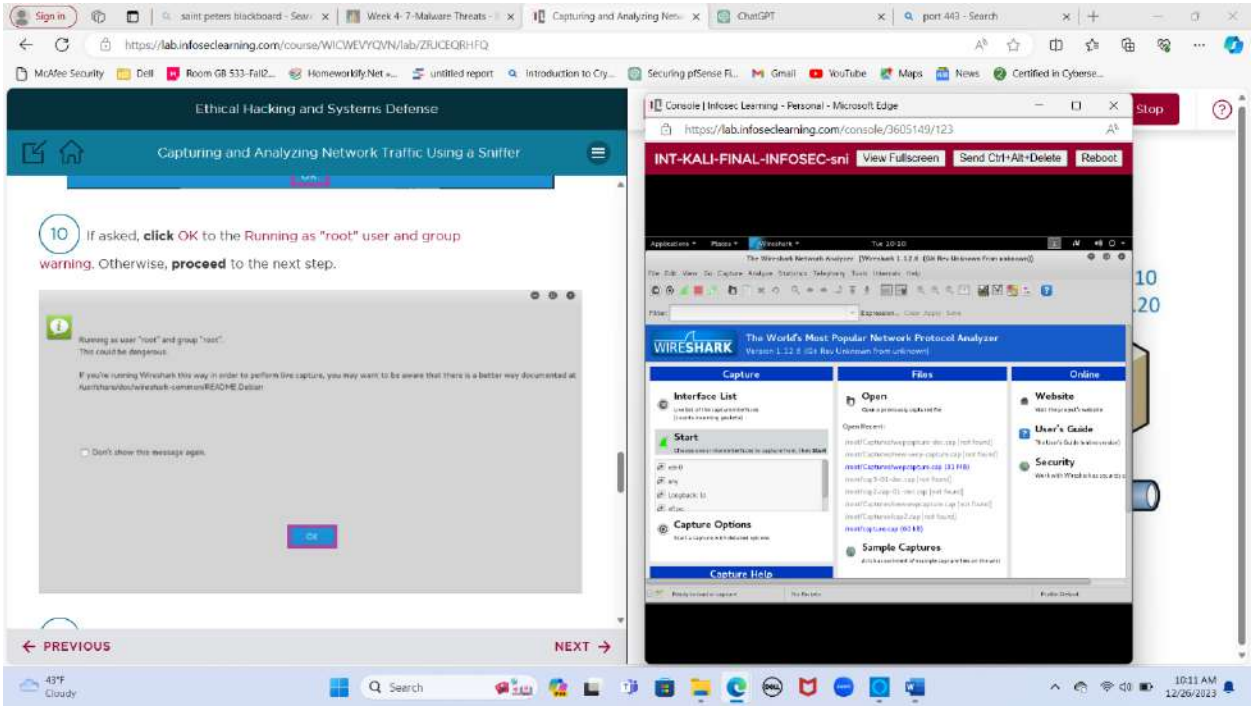


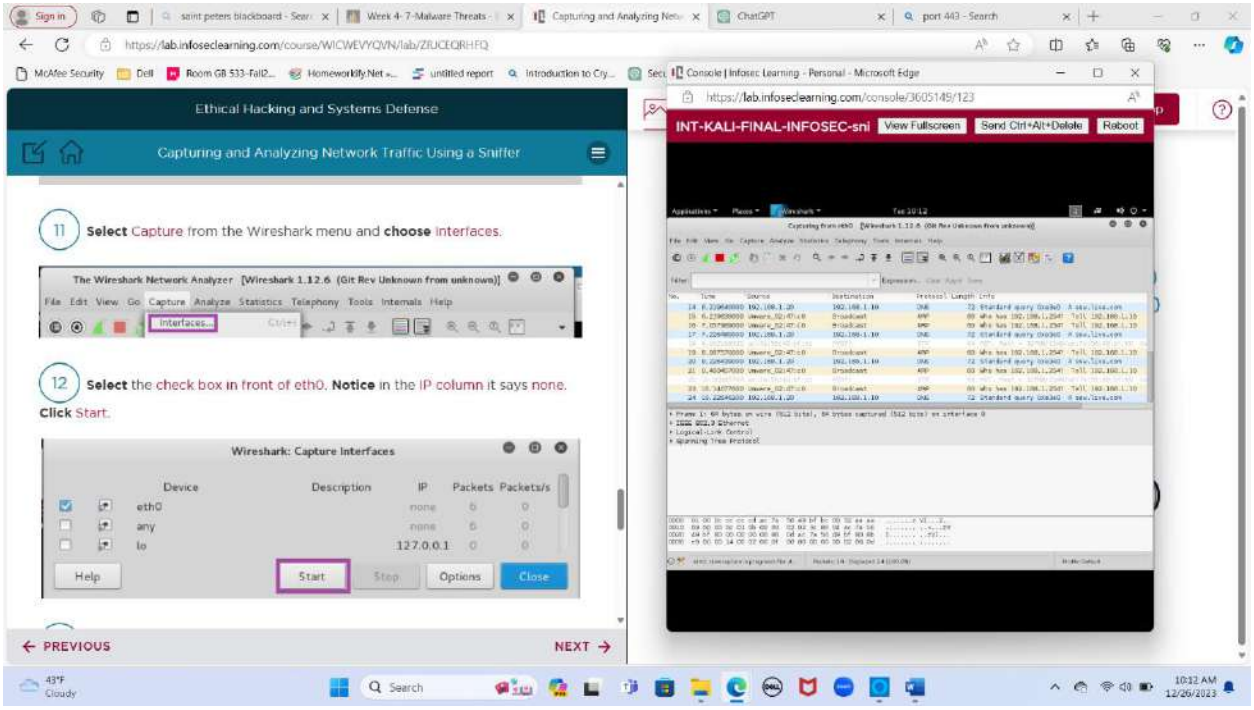
Removing the IP address:

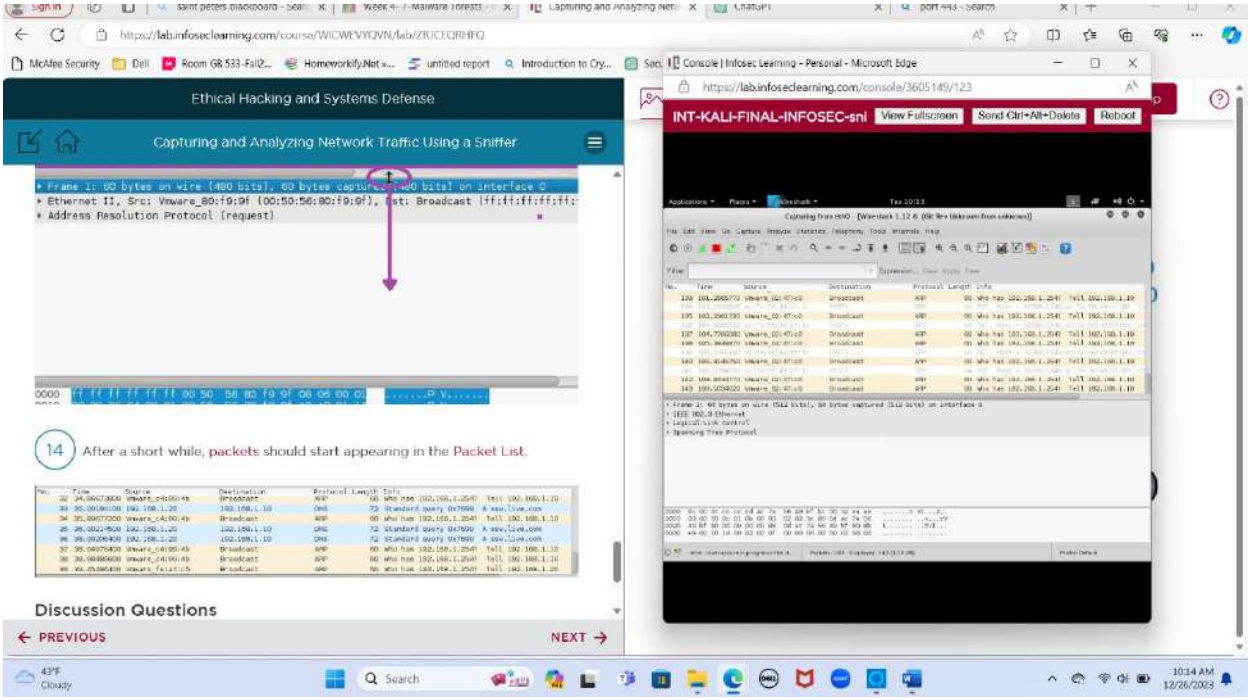


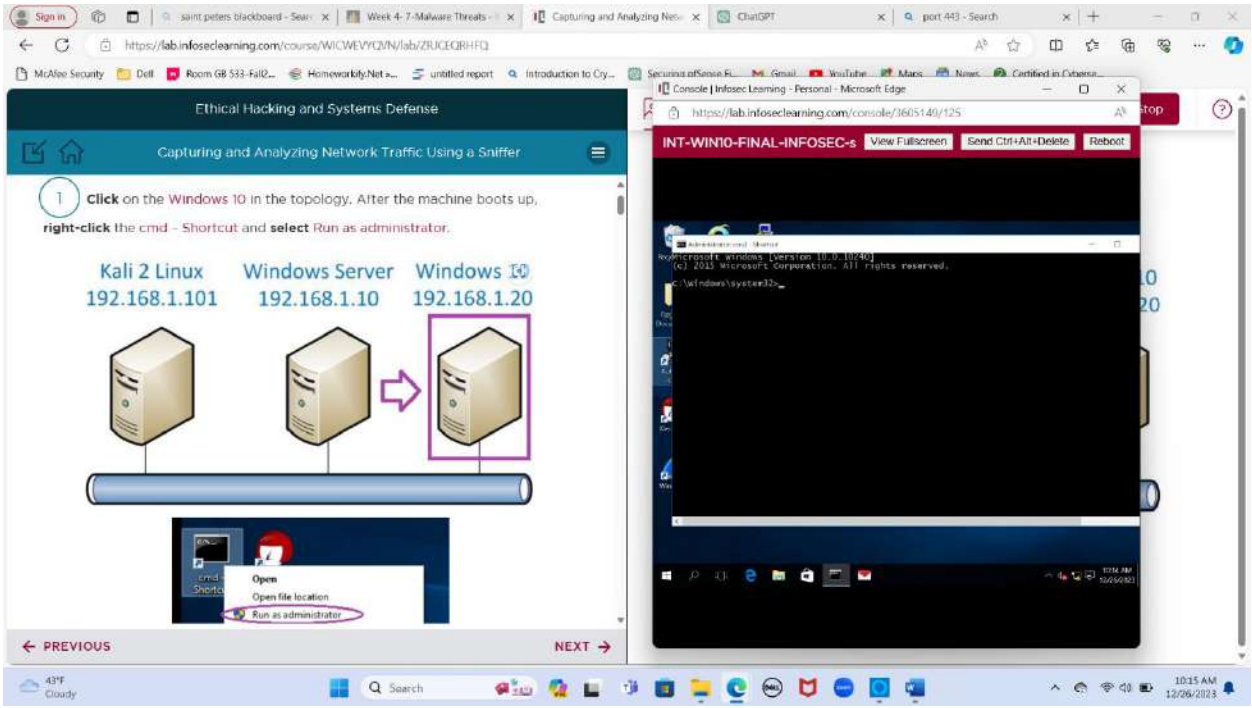


Wireshark:

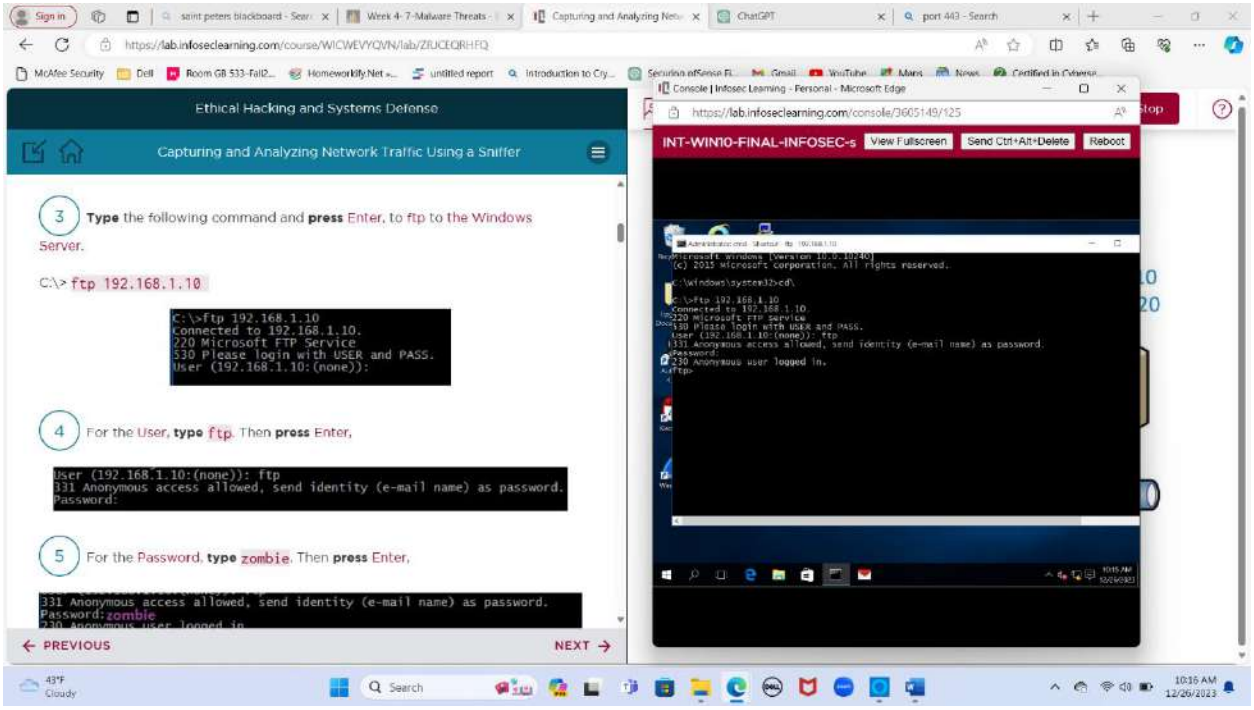

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
10 If asked, click OK to the Running as "root" user and group warning. Otherwise, proceed to the next step.
PREVIOUS
NEXT
INT-KALI-FINAL-INFOSEC-sni
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Files
Online
Interface List
Start
Capture Options
Open
Sample Captures
Website
User's Guide
Security
Capture Help

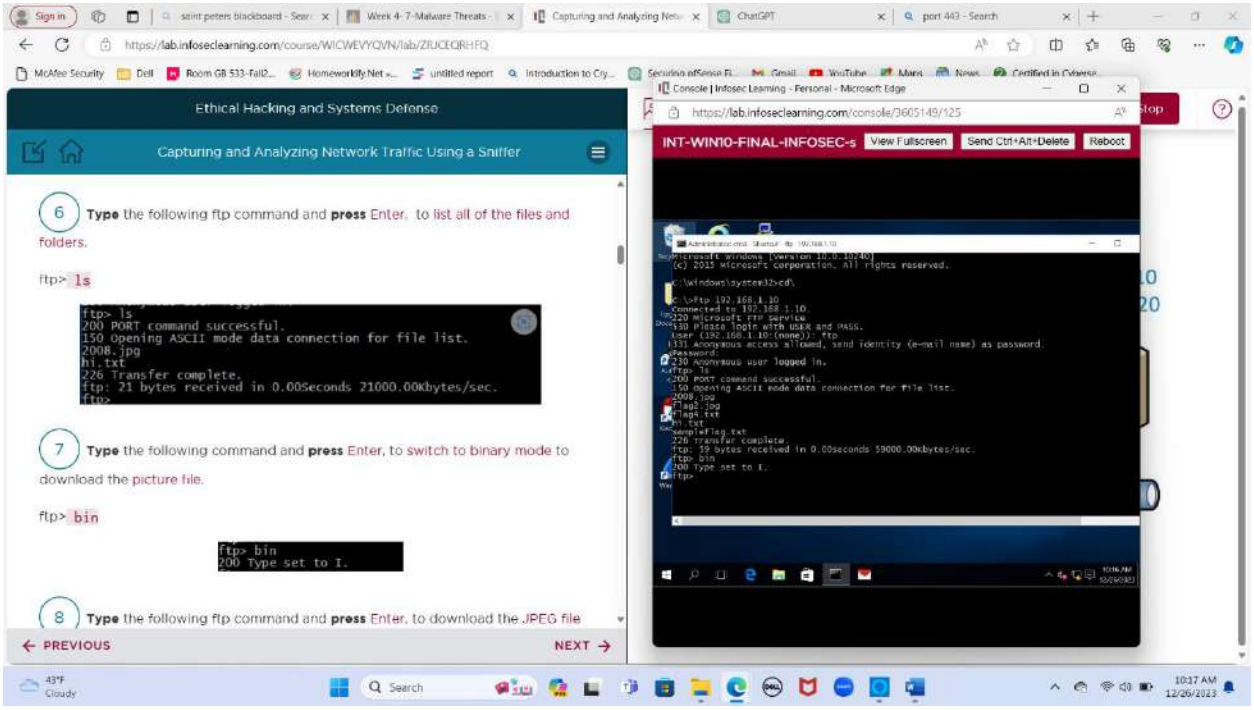

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
11 Select Capture from the Wireshark menu and choose Interfaces.
The Wireshark Network Analyzer [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces...
12 Select the check box in front of eth0. Notice in the IP column it says none. Click Start.
Wireshark: Capture Interfaces
Device
Description
IP
Packets
Packets/s
eth0
any
lo
127.0.0.1
Help
Start
Stop
Options
Close
PREVIOUS
NEXT
INT-KALI-FINAL-INFOSEC-sni
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

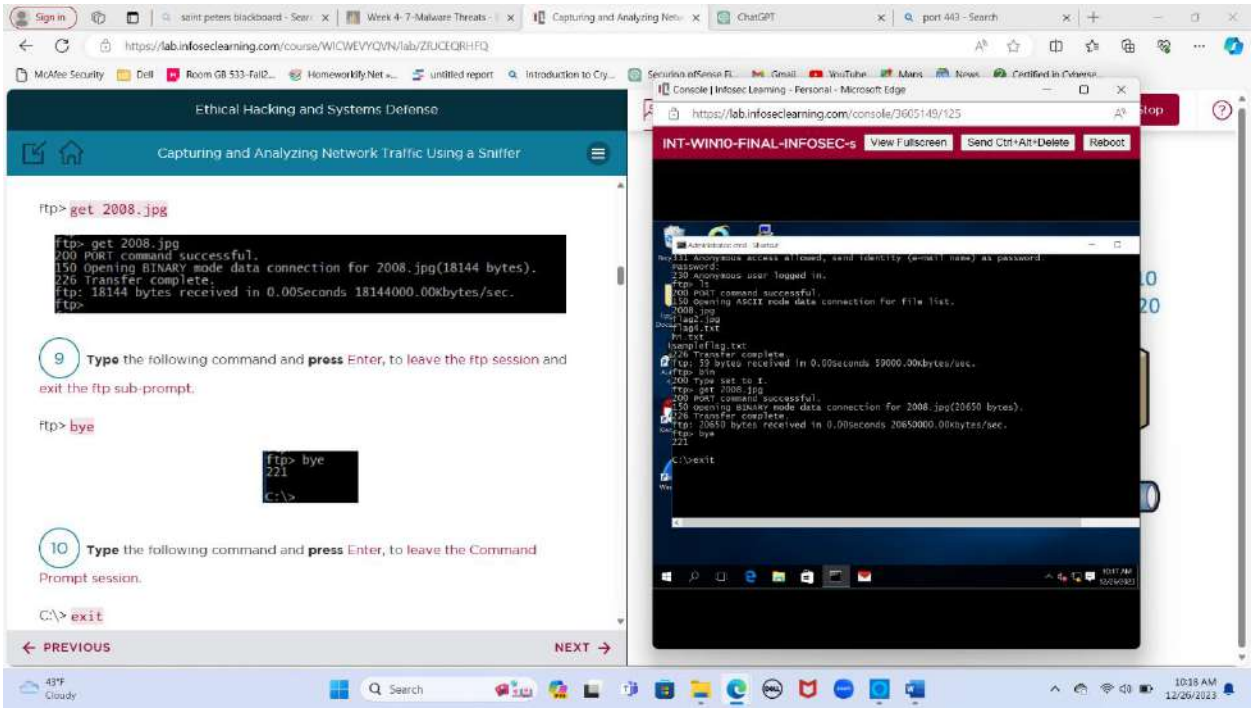

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_80:f9:9f (00:50:56:80:f9:9f), Dst: Broadcast (ff:ff:ff:ff:ff:
Address Resolution Protocol (request)
14 After a short while, packets should start appearing in the Packet List.
Discussion Questions
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3605149/123
INT-KALI-FINAL-INFOSEC-sni
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
1 Click on the Windows 10 in the topology. After the machine boots up, right-click the cmd - Shortcut and select Run as administrator.
Kali 2 Linux
192.168.1.101
Windows Server
192.168.1.10
Windows 10
192.168.1.20
Open
Open file location
Run as administrator
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3605149/125
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>

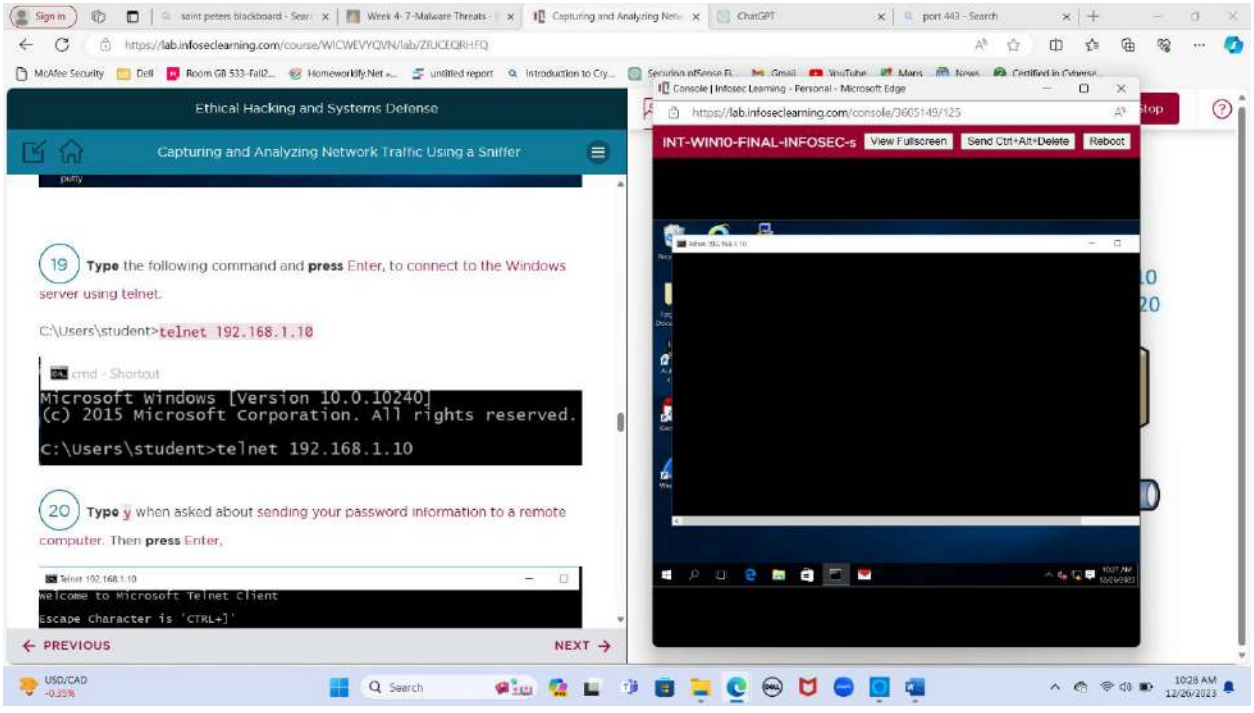
FTP

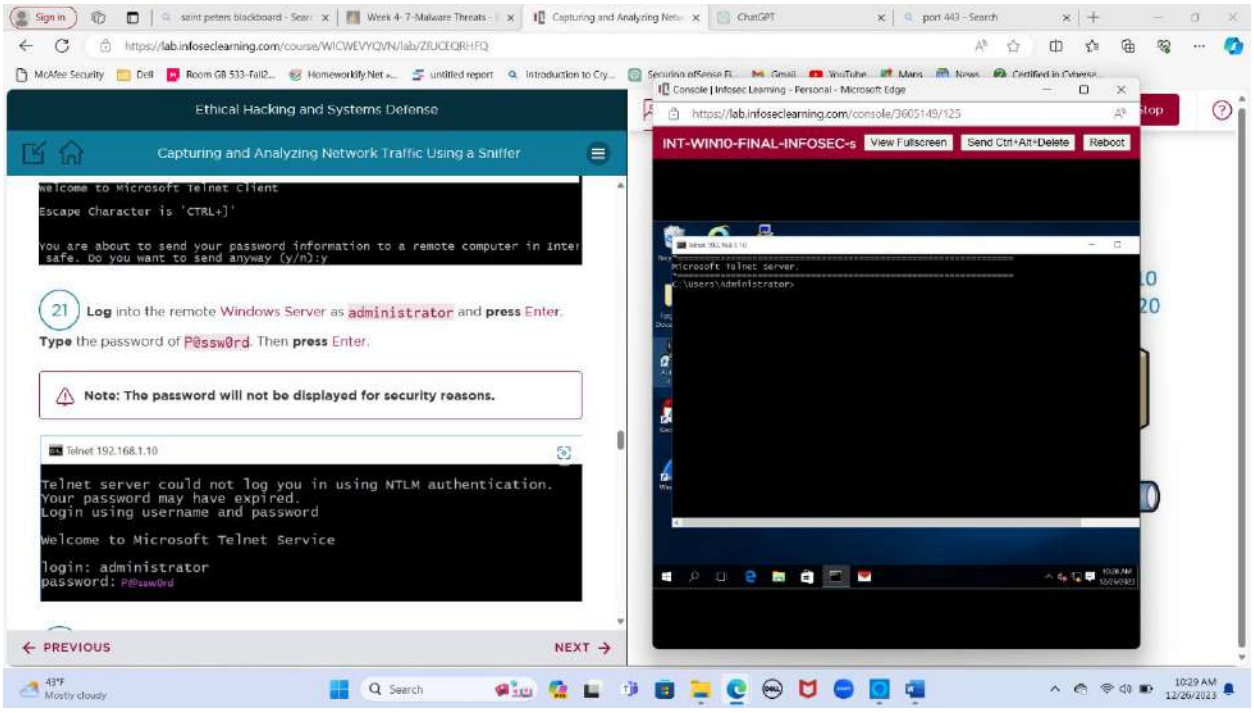

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
3 Type the following command and press Enter, to ftp to the Windows Server.
C:\> ftp 192.168.1.10
C:\>ftp 192.168.1.10
Connected to 192.168.1.10.
220 Microsoft FTP Service
530 Please login with USER and PASS.
User (192.168.1.10:(none)):
4 For the User, type ftp. Then press Enter,
User (192.168.1.10:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
5 For the Password, type zombie. Then press Enter,
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:zombie
230 Anonymous user logged in.
PREVIOUS
NEXT
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
6 Type the following ftp command and press Enter, to list all of the files and folders.
ftp> ls
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
2008.jpg
hi.txt
226 Transfer complete.
ftp: 21 bytes received in 0.00Seconds 21000.00Kbytes/sec.
ftp>
7 Type the following command and press Enter, to switch to binary mode to download the picture file.
ftp> bin
ftp> bin
200 Type set to I.
8 Type the following ftp command and press Enter, to download the JPEG file
PREVIOUS
NEXT
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

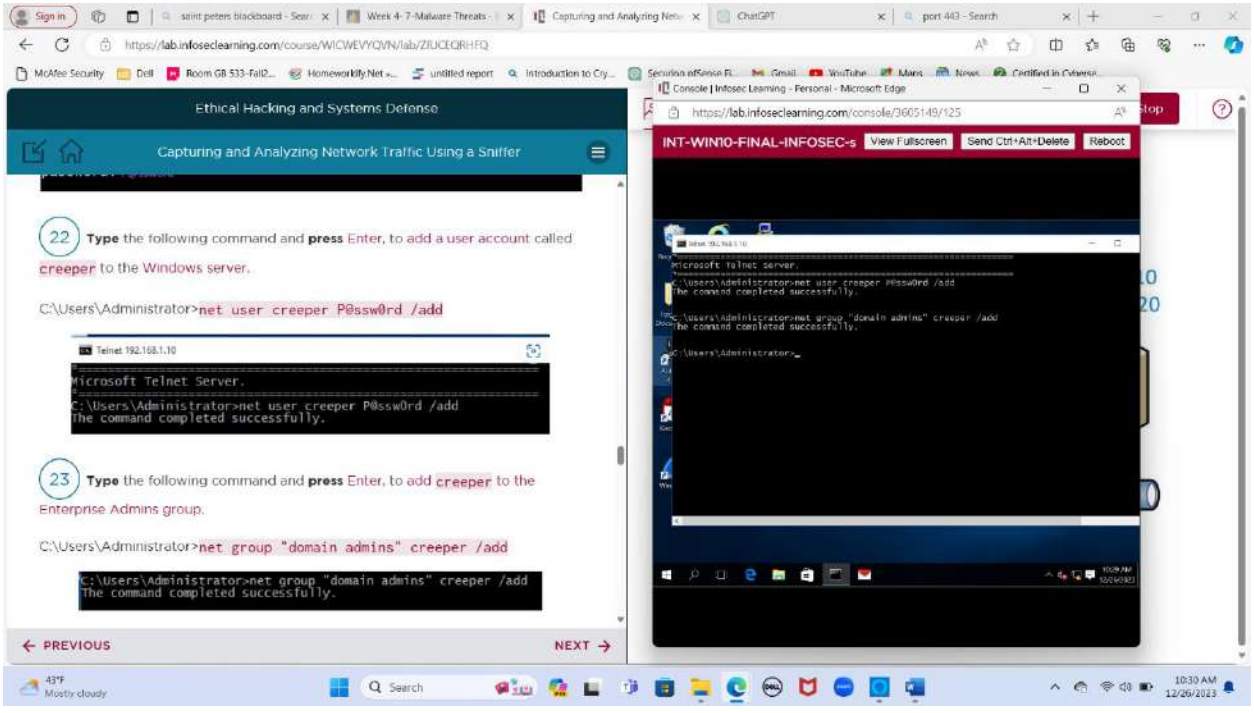

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
ftp> get 2008.jpg
ftp> get 2008.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for 2008.jpg(18144 bytes).
226 Transfer complete.
ftp: 18144 bytes received in 0.00Seconds 18144000.00Kbytes/sec.
ftp>
9 Type the following command and press Enter, to leave the ftp session and exit the ftp sub-prompt.
ftp> bye
ftp> bye
221
C:\>
10 Type the following command and press Enter, to leave the Command Prompt session.
C:\> exit
PREVIOUS
NEXT
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

TELNET

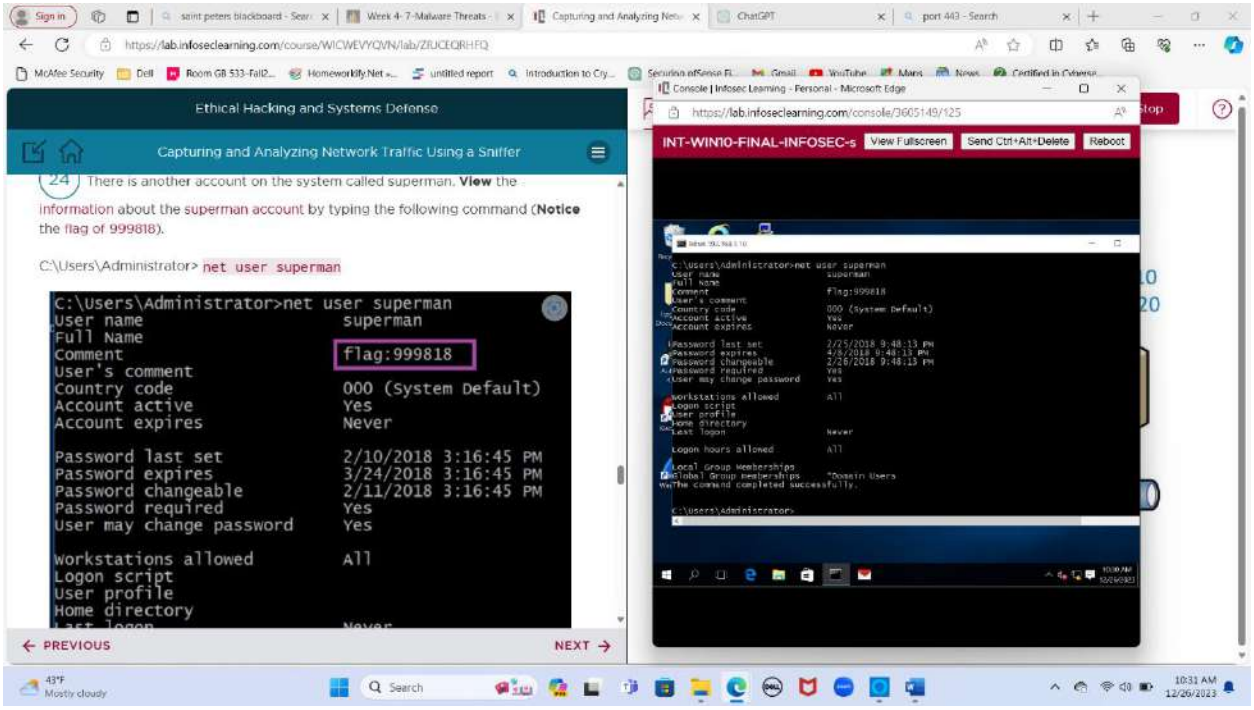

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
19 Type the following command and press Enter, to connect to the Windows server using telnet.
C:\Users\student>telnet 192.168.1.10
cmd - Shortcut
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\student>telnet 192.168.1.10
20 Type y when asked about sending your password information to a remote computer. Then press Enter.
Telnet 192.168.1.10
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'
PREVIOUS
NEXT
INT-WIN10-FINAL-INFOSEC-s
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

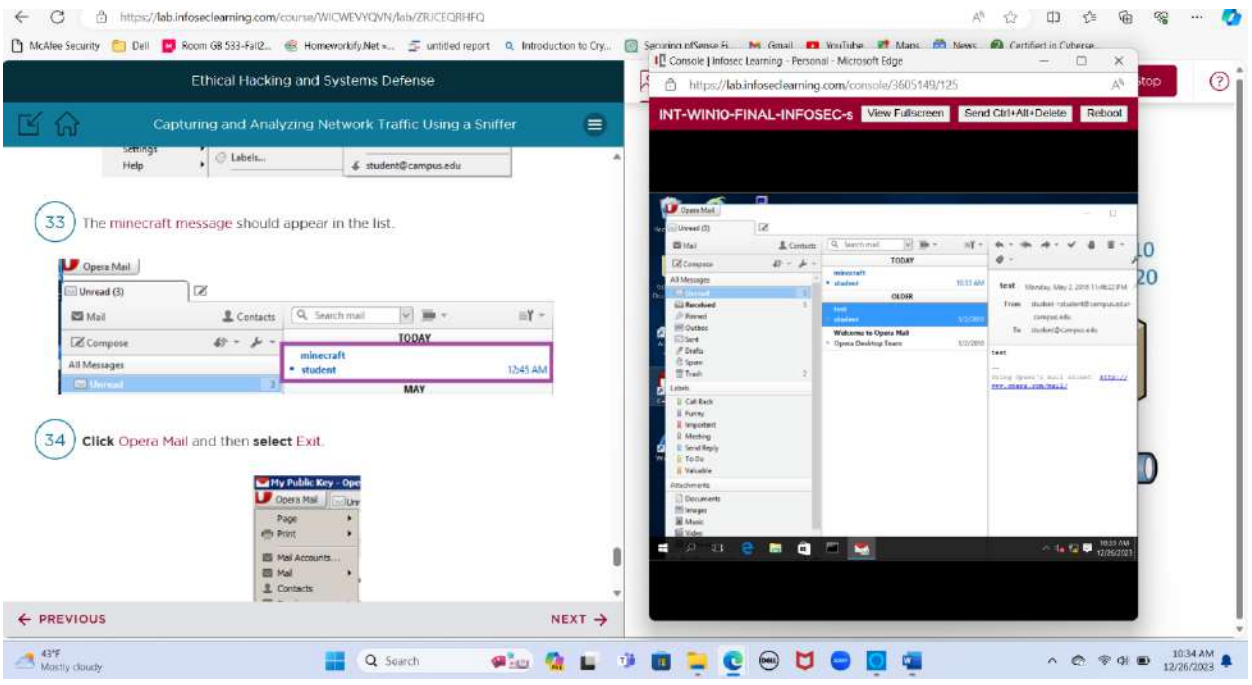


Adding a User

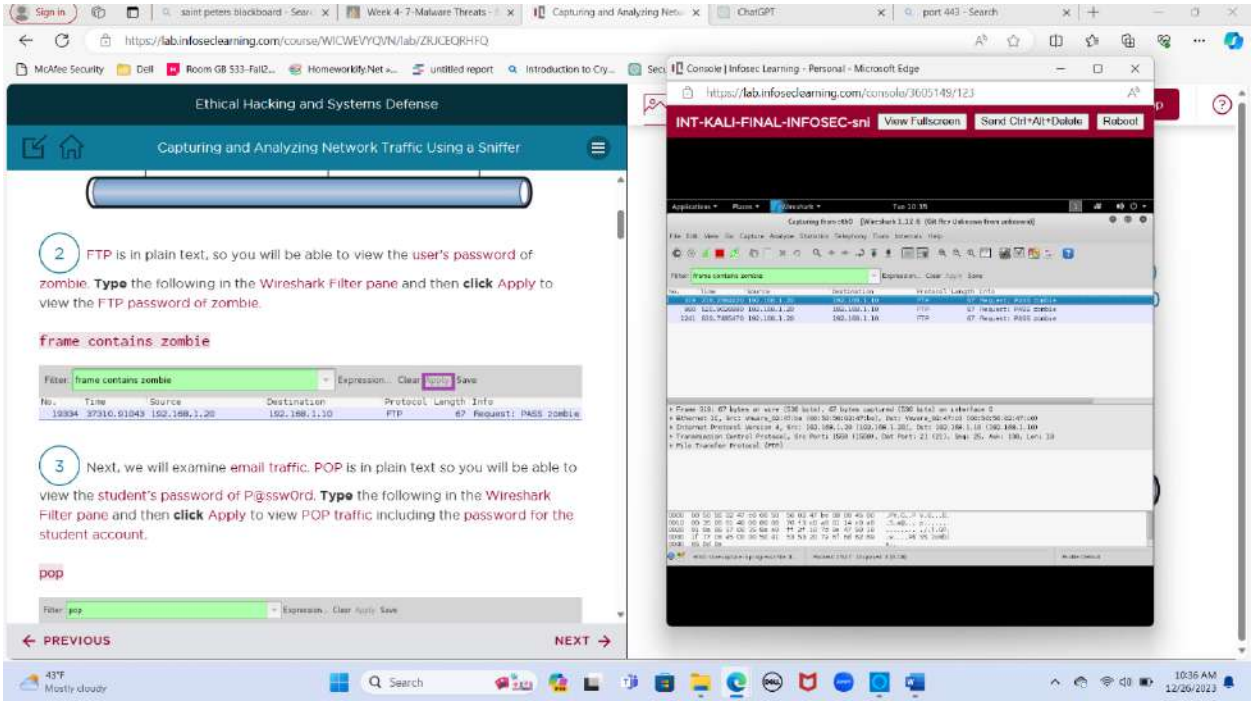


Viewing accounts

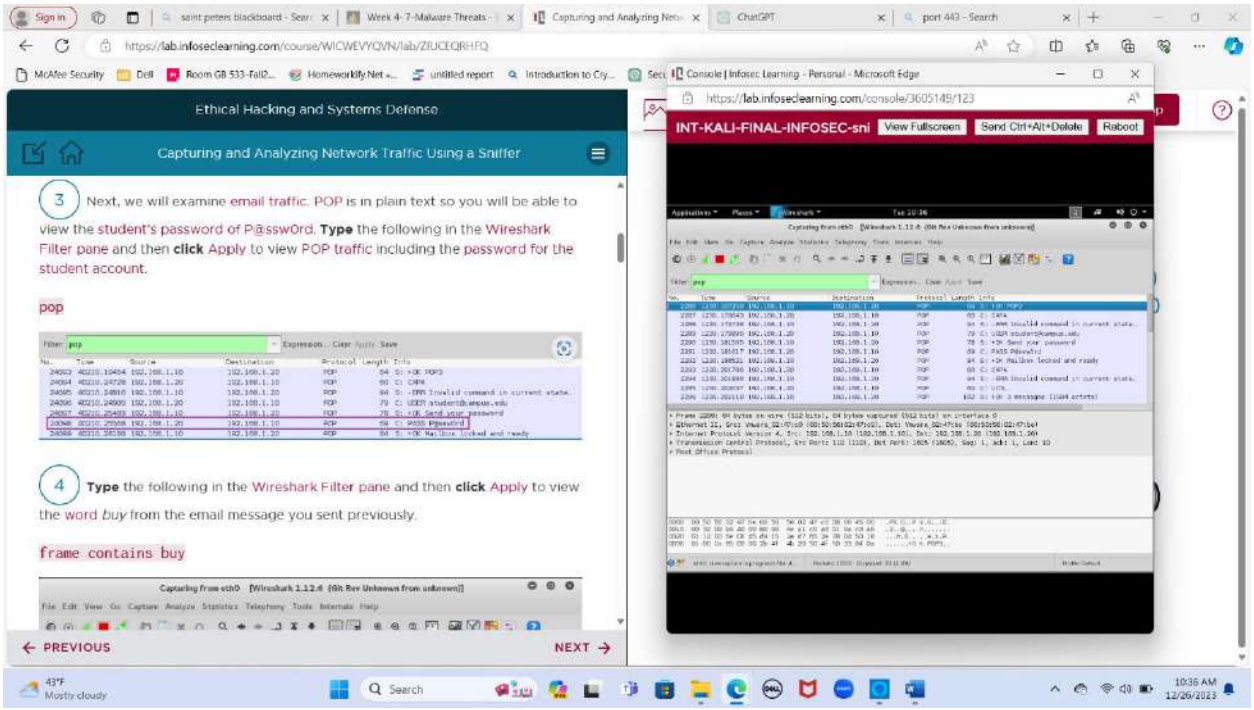




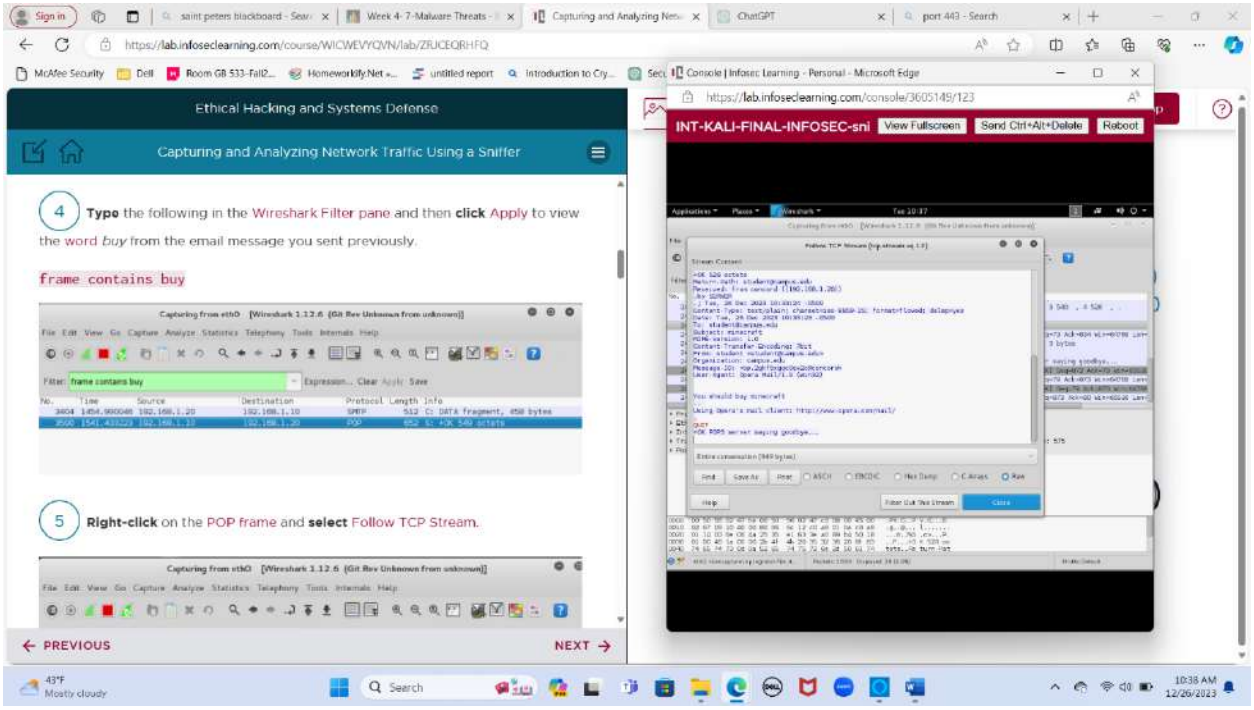
Frame contains zombie



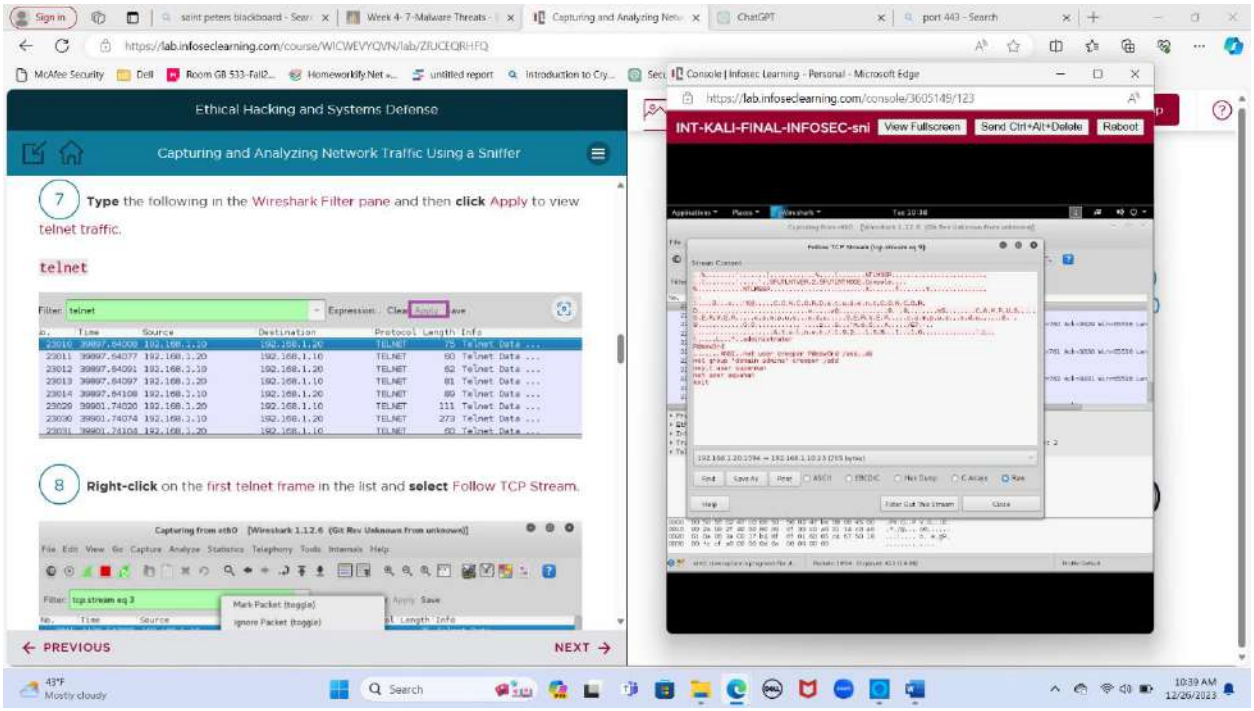
pop



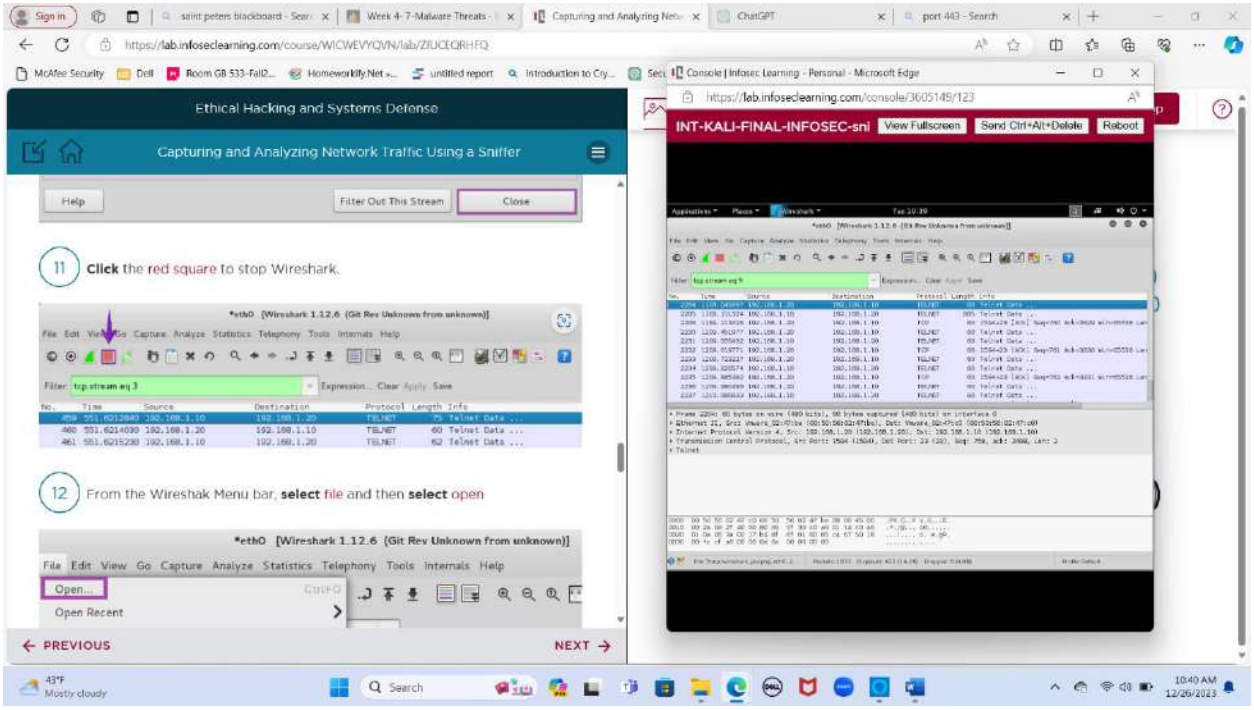
Frame contains buy



Telnet



Stopping Wireshark



This is the last screen before the end of this lab.