CAPTURING AND ANALYZING NETWORK TRAFFIC USING A SNIFFER

ETHICAL HACKING & LAB 3

Student Info
Name:SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

Executive Summary

Highlights

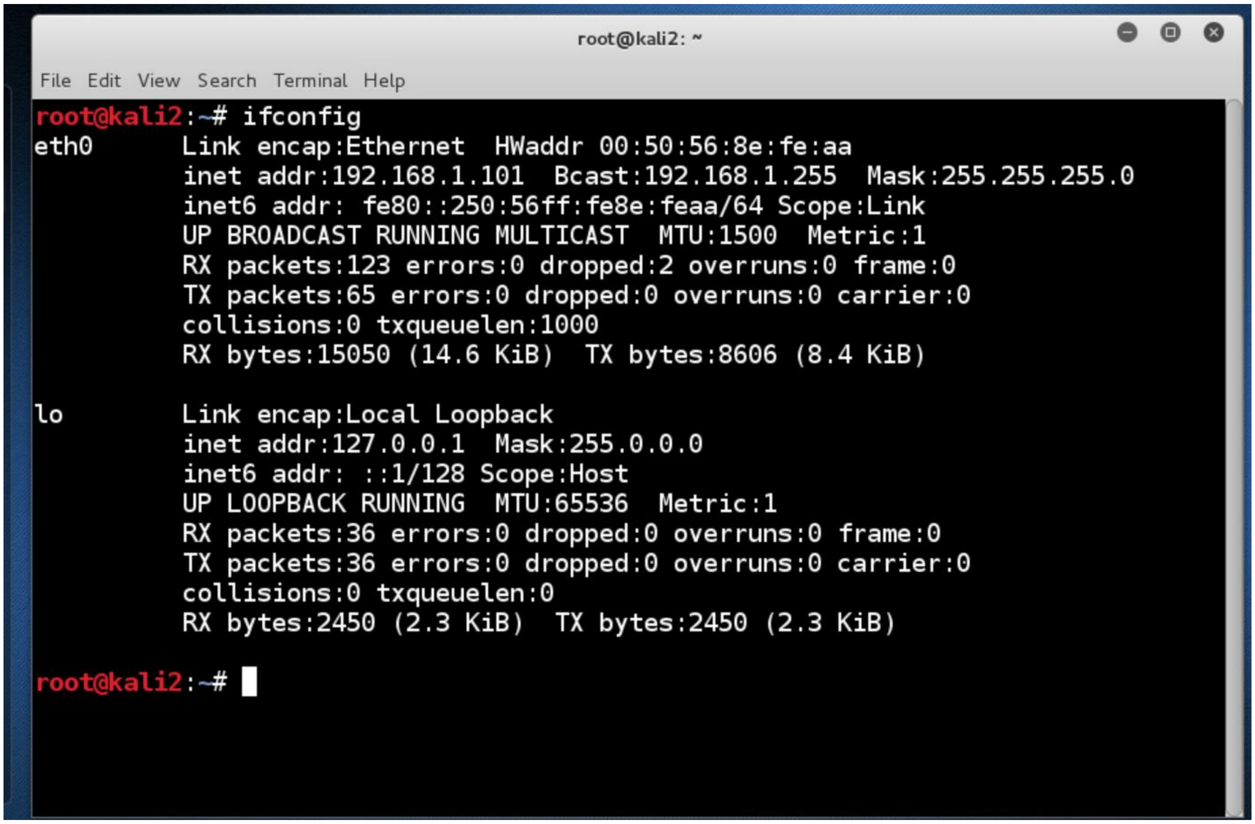
In this lab, I will use Wireshark to capture and analyze network traffic. I will configure the network interface, generate traffic using FTP, Telnet, and Mail protocols, and then analyze the captured traffic.

Objectives

The objective of this lab is to configure a sniffer to capture live network traffic and analyze the data using Wireshark to understand the protocols and traffic patterns within the network.

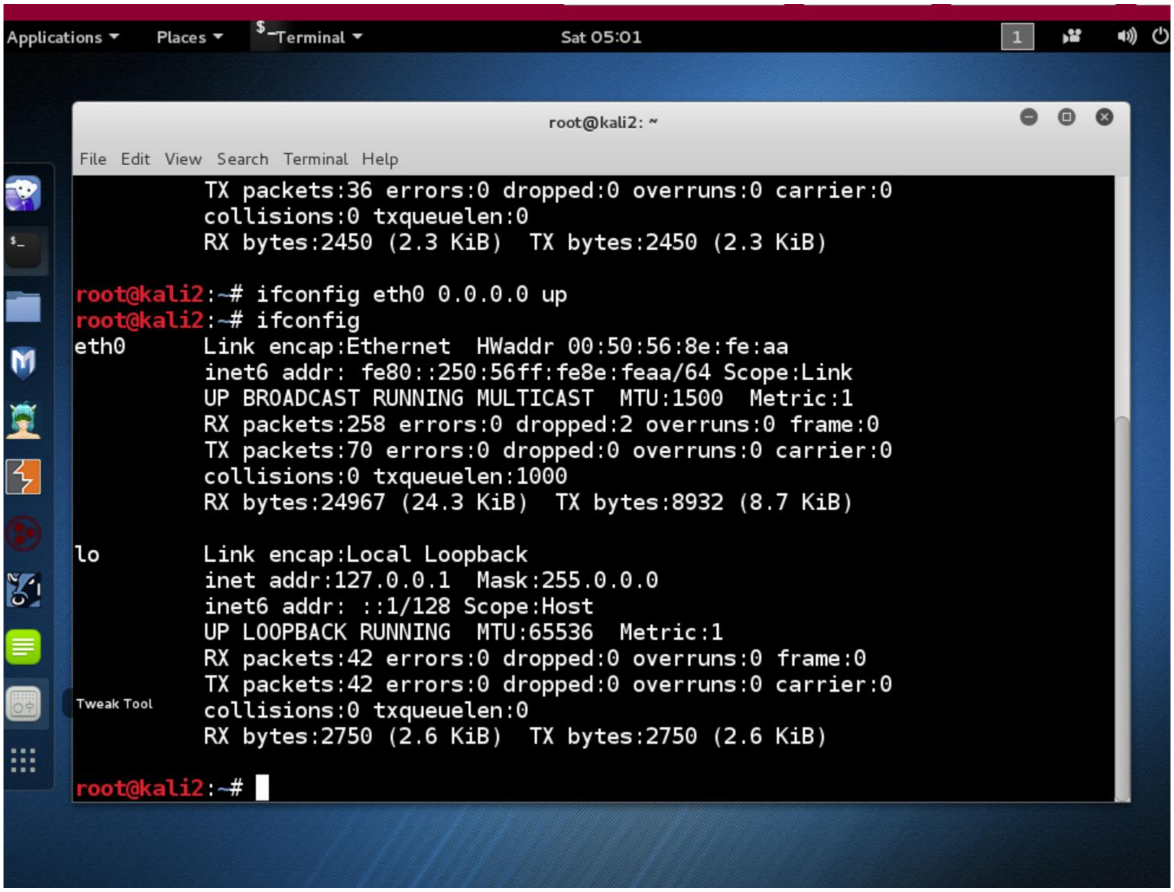
Lab Description Details

The kali linux machine configuration had been checked and the ethernet had been setup.



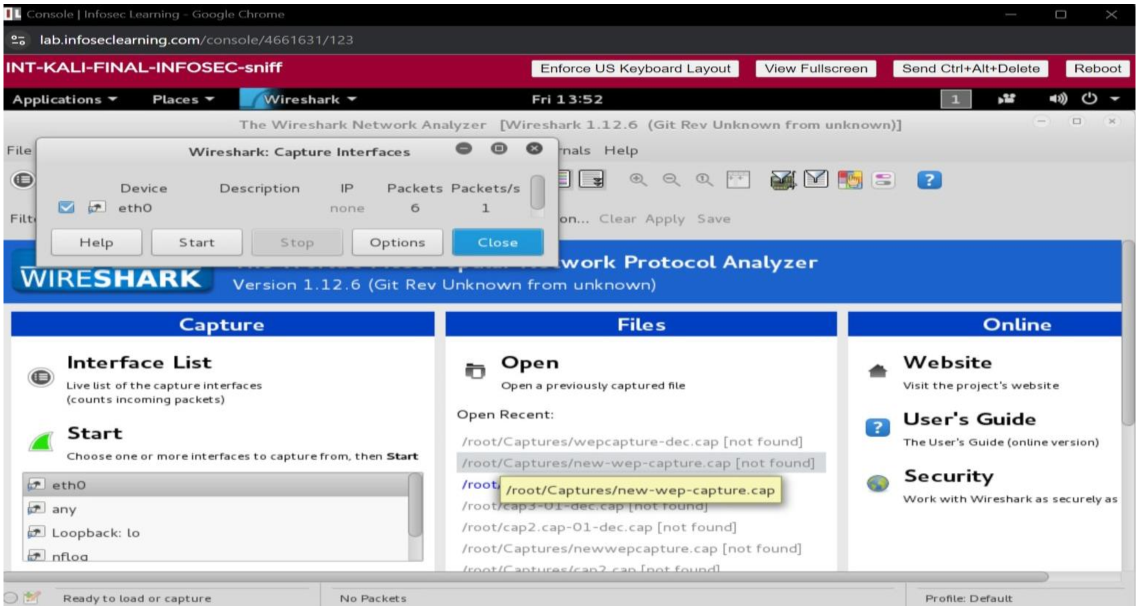
```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:8e:fe:aa
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8e:feaa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:123 errors:0 dropped:2 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15050 (14.6 KiB)  TX bytes:8606 (8.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2450 (2.3 KiB)  TX bytes:2450 (2.3 KiB)

root@kali2:~# 
```

The ip address had been configured by setting up ethernet(eth0)



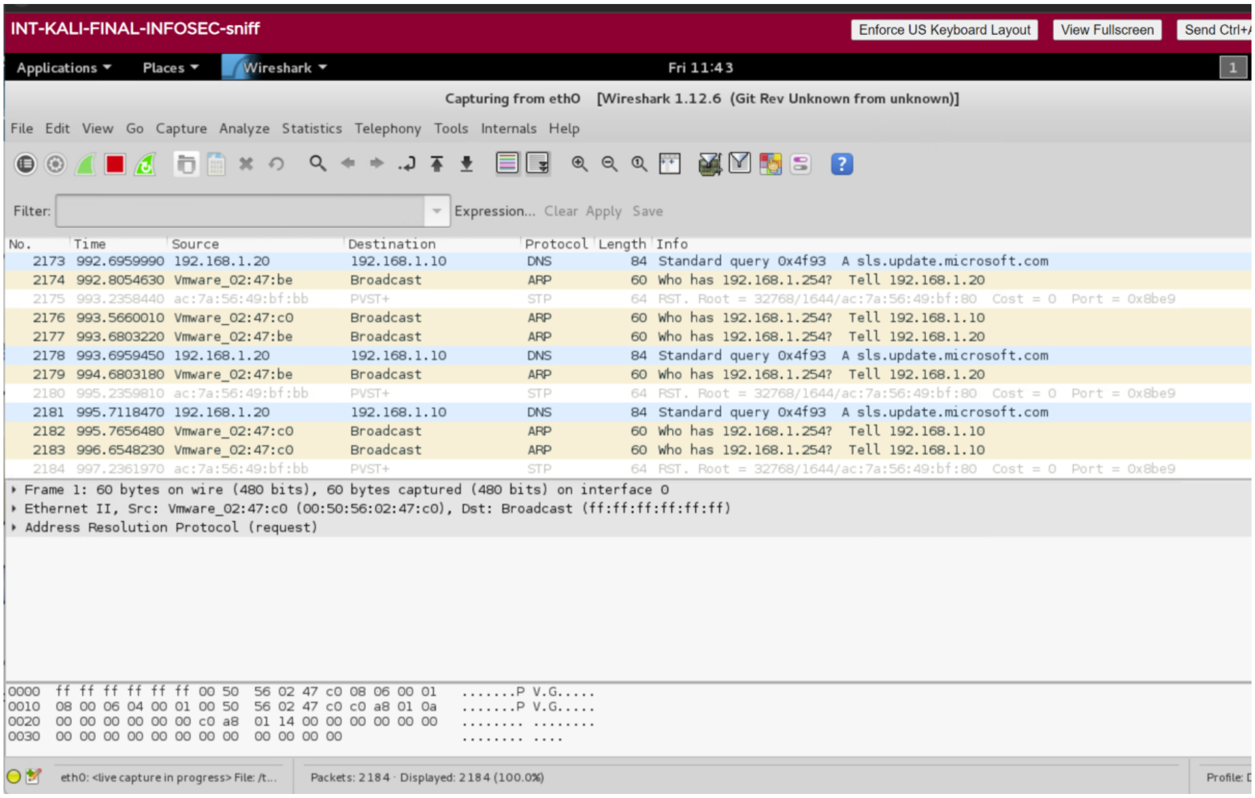
```
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2450 (2.3 KiB)  TX bytes:2450 (2.3 KiB)

root@kali2:~# ifconfig eth0 0.0.0.0 up
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:8e:fe:aa
          inet6 addr: fe80::250:56ff:fe8e:feaa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:258 errors:0 dropped:2 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24967 (24.3 KiB)  TX bytes:8932 (8.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2750 (2.6 KiB)  TX bytes:2750 (2.6 KiB)

root@kali2:~# 
```

Wireshark had been started to capture interfaces


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4661631/123
INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Wireshark
Fri 13:52
The Wireshark Network Analyzer [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File
nals Help
Filt
on... Clear Apply Save
Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close
WIRESHARK
work Protocol Analyzer
Version 1.12.6 (Git Rev Unknown from unknown)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
any
Loopback: lo
nflog
Files
Open
Open a previously captured file
Open Recent:
/root/Captures/wepcapture-dec.cap [not found]
/root/Captures/new-wep-capture.cap [not found]
/root/Captures/new-wep-capture.cap
/root/cap3-01-dec.cap [not found]
/root/cap2.cap-01-dec.cap [not found]
/root/Captures/newwepcapture.cap [not found]
/root/Captures/cap2.cap [not found]
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as
Ready to load or capture
No Packets
Profile: Default

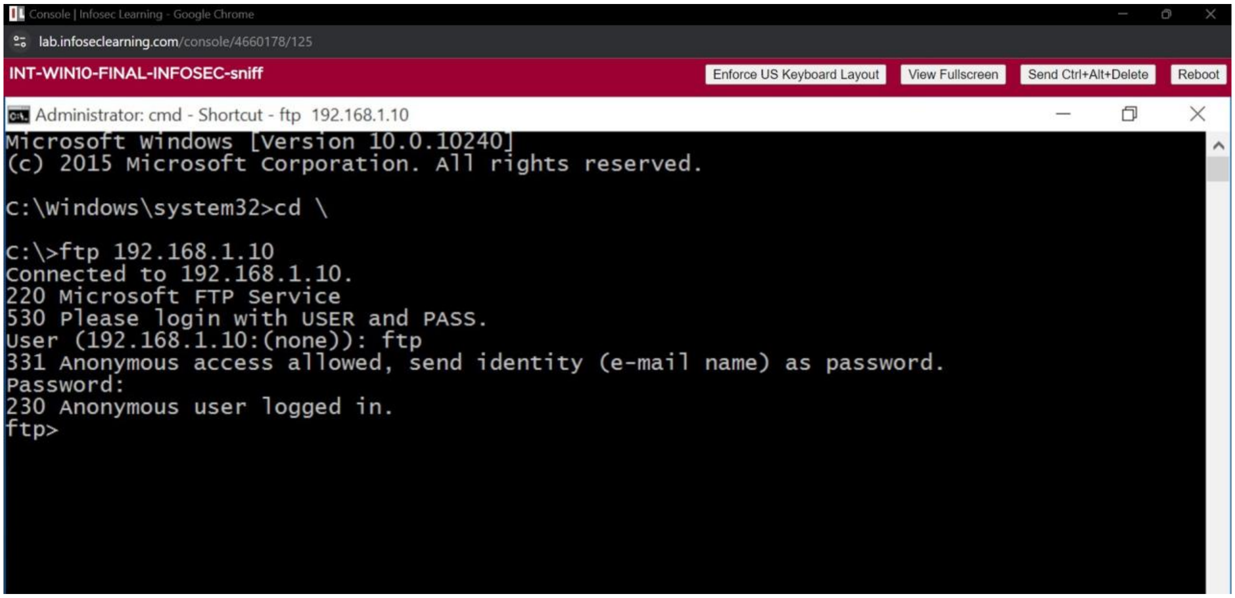
	Device	Description	IP	Packets	Packets/s
☑	eth0		none	6	1

The Traffic is getting captured in the wireshark


INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+A
Applications
Places
Wireshark
Fri 11:43
1
Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

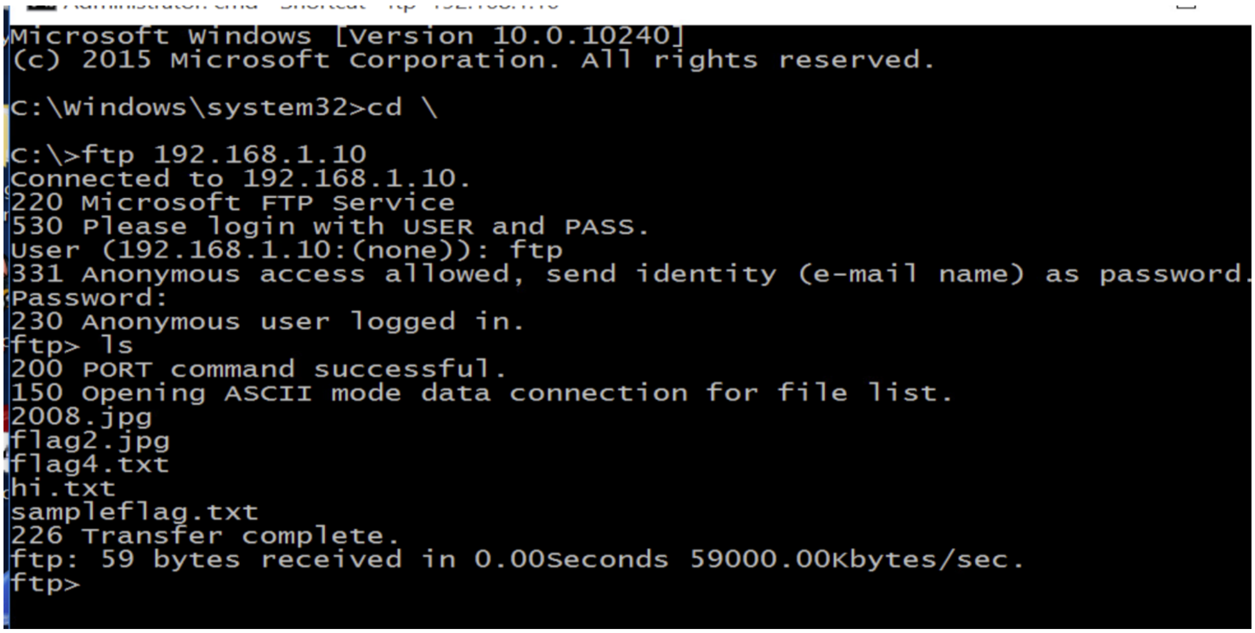
```
No.   Time         Source              Destination    Protocol Length Info
 2173 992.6959990  192.168.1.20        192.168.1.10   DNS         84 Standard query 0x4f93  A sls.update.microsoft.com
 2174 992.8054630  Vmware_02:47:be     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.20
 2175 993.2358440  ac:7a:56:49:bf:bb   PVST+          STP         64 RST. Root = 32768/1644/ac:7a:56:49:bf:80  Cost = 0  Port = 0x8be9
 2176 993.5660010  Vmware_02:47:c0     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.10
 2177 993.6803220  Vmware_02:47:be     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.20
 2178 993.6959450  192.168.1.20        192.168.1.10   DNS         84 Standard query 0x4f93  A sls.update.microsoft.com
 2179 994.6803180  Vmware_02:47:be     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.20
 2180 995.2359810  ac:7a:56:49:bf:bb   PVST+          STP         64 RST. Root = 32768/1644/ac:7a:56:49:bf:80  Cost = 0  Port = 0x8be9
 2181 995.7118470  192.168.1.20        192.168.1.10   DNS         84 Standard query 0x4f93  A sls.update.microsoft.com
 2182 995.7656480  Vmware_02:47:c0     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.10
 2183 996.6548230  Vmware_02:47:c0     Broadcast      ARP         60 Who has 192.168.1.254?  Tell 192.168.1.10
 2184 997.2361970  ac:7a:56:49:bf:bb   PVST+          STP         64 RST. Root = 32768/1644/ac:7a:56:49:bf:80  Cost = 0  Port = 0x8be9

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_02:47:c0 (00:50:56:02:47:c0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 50  56 02 47 c0 08 06 00 01   .......P V.G.....
0010  08 00 06 04 00 01 00 50  56 02 47 c0 c0 a8 01 0a   .......P V.G.....
0020  00 00 00 00 00 00 c0 a8  01 14 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

eth0: <live capture in progress> File: /t...    Packets: 2184 · Displayed: 2184 (100.0%)    Profile: D
```

Ftp Login has been done in the windows machine


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660178/125
INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Administrator: cmd - Shortcut - ftp 192.168.1.10

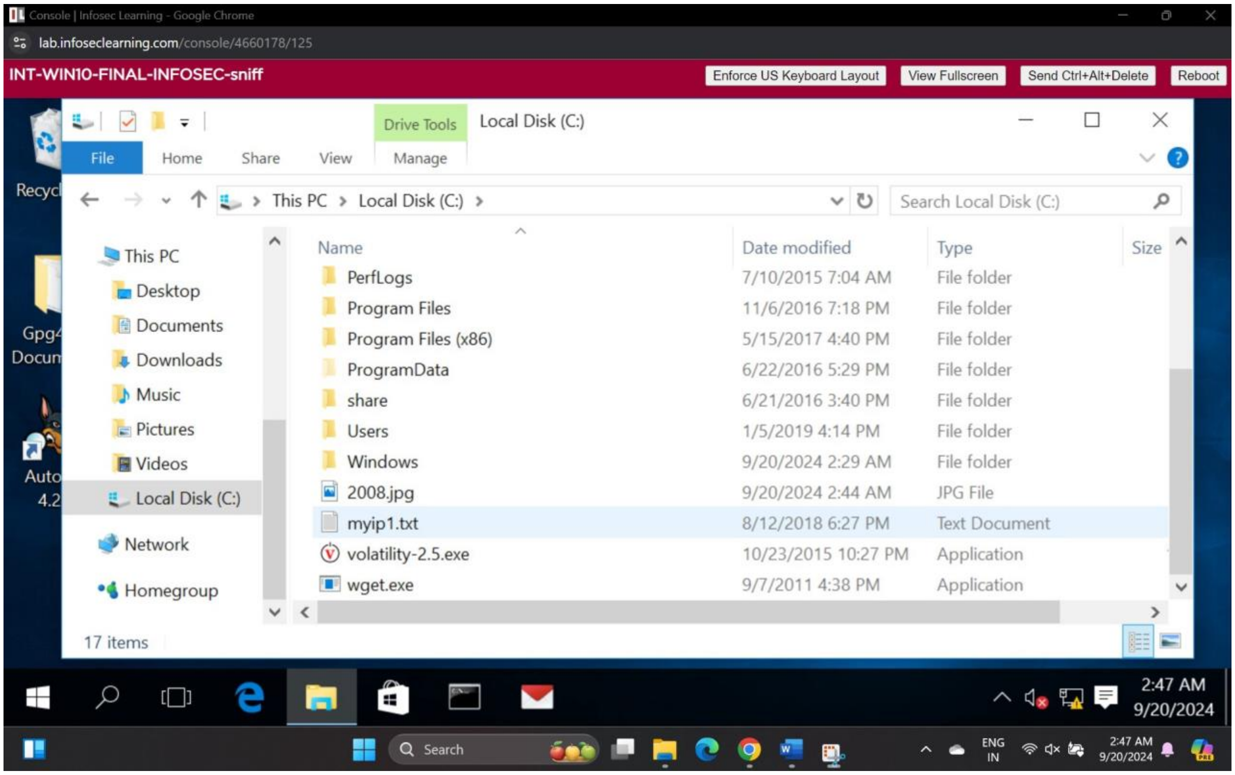
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \

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)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

After logging in Anonymously we got to know more details about 2008.jpg by entering command get 2008.jpg



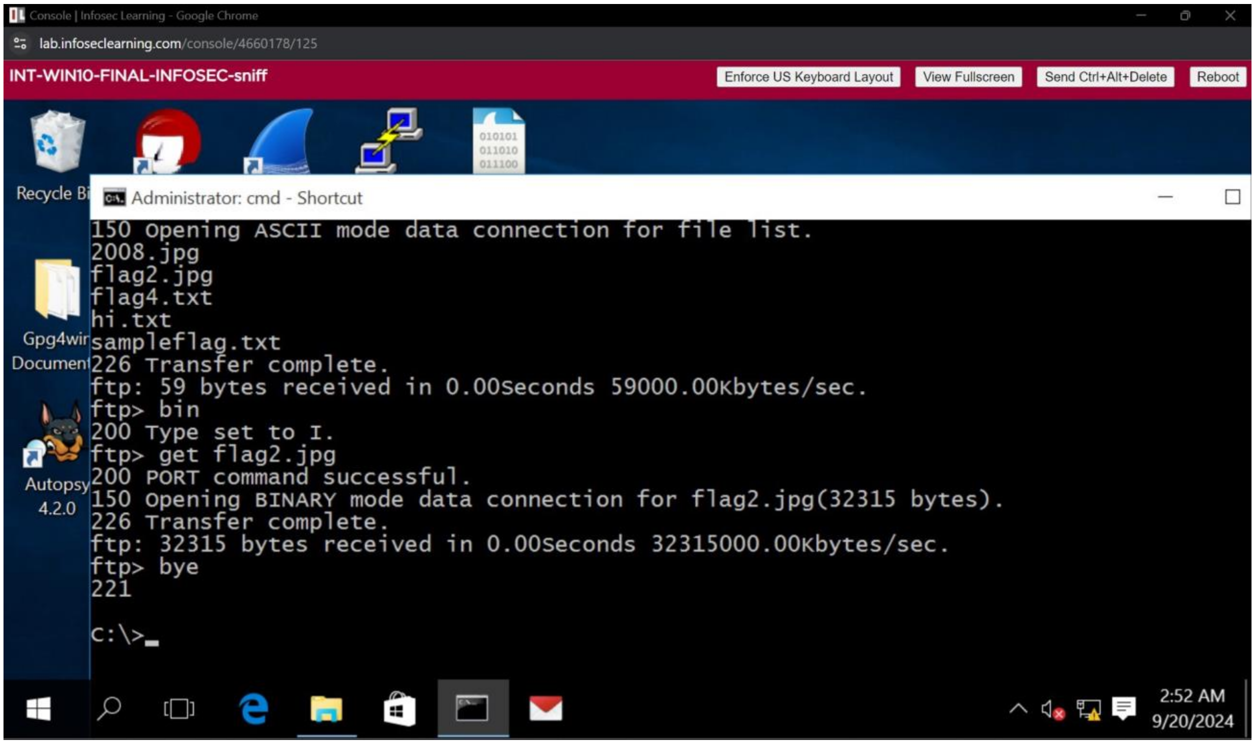
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \

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)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
2008.jpg
flag2.jpg
flag4.txt
hi.txt
sampleflag.txt
226 Transfer complete.
ftp: 59 bytes received in 0.00Seconds 59000.00Kbytes/sec.
ftp>
```

In the local disk the 2008.jpg got popped up. And the sample challenge got completed by opening the jpg file.



Name	Date modified	Type	Size
PerfLogs	7/10/2015 7:04 AM	File folder	
Program Files	11/6/2016 7:18 PM	File folder	
Program Files (x86)	5/15/2017 4:40 PM	File folder	
ProgramData	6/22/2016 5:29 PM	File folder	
share	6/21/2016 3:40 PM	File folder	
Users	1/5/2019 4:14 PM	File folder	
Windows	9/20/2024 2:29 AM	File folder	
2008.jpg	9/20/2024 2:44 AM	JPG File	
myip1.txt	8/12/2018 6:27 PM	Text Document	
volatility-2.5.exe	10/23/2015 10:27 PM	Application	
wget.exe	9/7/2011 4:38 PM	Application	

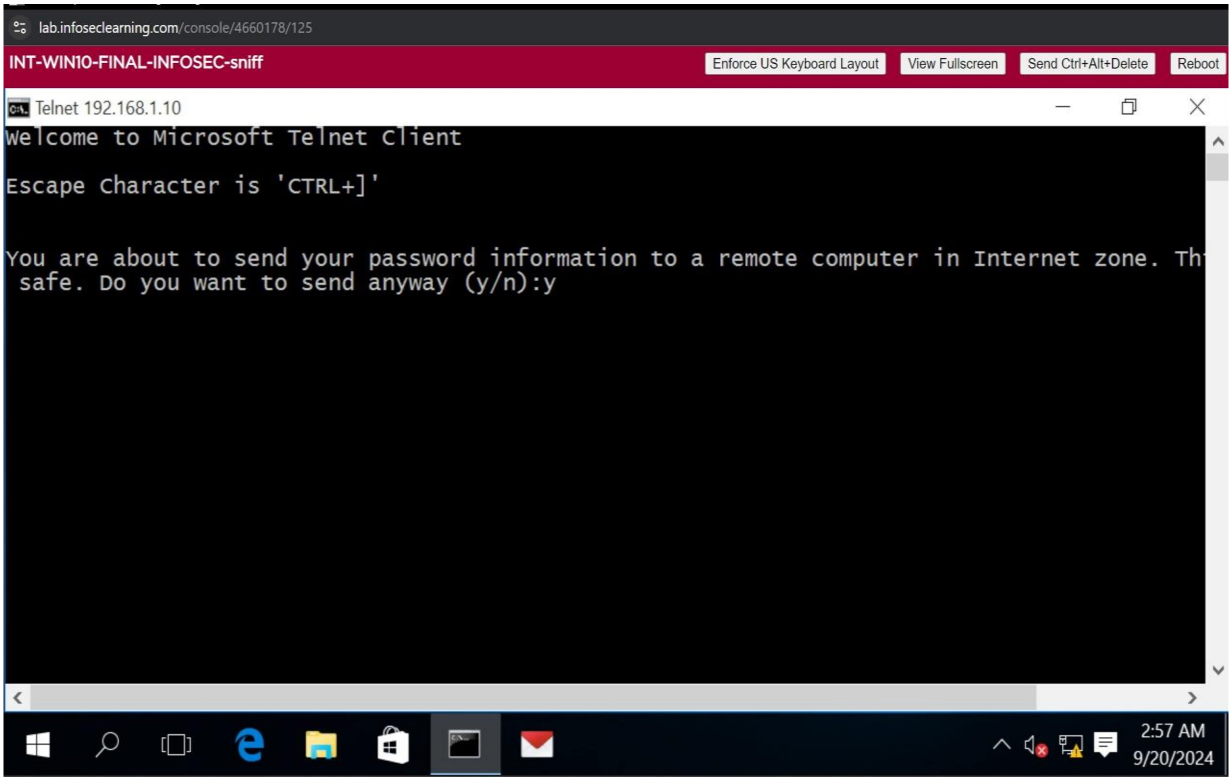
Similarly I performed same steps for flag2.jpg



Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660178/125
INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Recycle Bi
Gpg4wir
Documen
Autopsy
4.2.0
Administrator: cmd - Shortcut
2:52 AM
9/20/2024

```
150 Opening ASCII mode data connection for file list.
2008.jpg
flag2.jpg
flag4.txt
hi.txt
sampleflag.txt
226 Transfer complete.
ftp: 59 bytes received in 0.00Seconds 59000.00Kbytes/sec.
ftp> bin
200 Type set to I.
ftp> get flag2.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for flag2.jpg(32315 bytes).
226 Transfer complete.
ftp: 32315 bytes received in 0.00Seconds 32315000.00Kbytes/sec.
ftp> bye
221

C:\>_
```

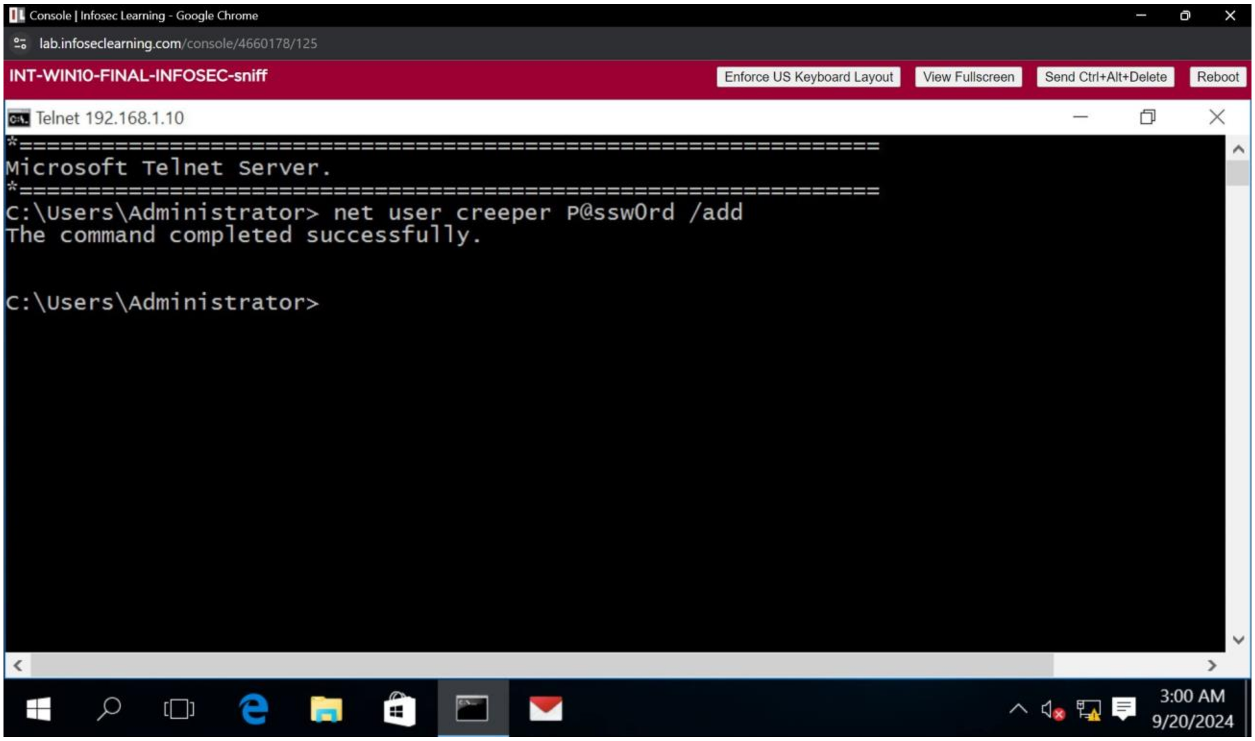
In the windows machine command prompt we are starting telnet .



lab.infoseclearning.com/console/4660178/125
INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Telnet 192.168.1.10
2:57 AM
9/20/2024

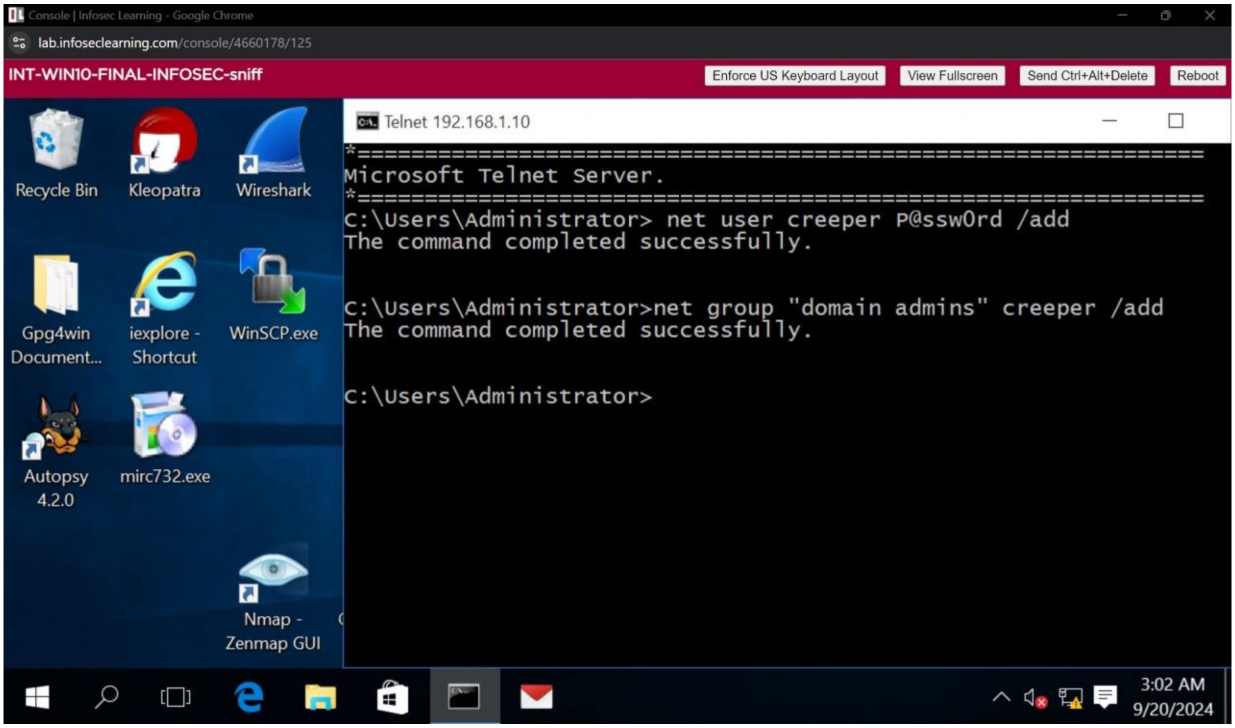
```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'


You are about to send your password information to a remote computer in Internet zone. Th
 safe. Do you want to send anyway (y/n):y
```

Opened the command prompt by administrator rights and entered into telnet service by entering telnet 192.168.1.10

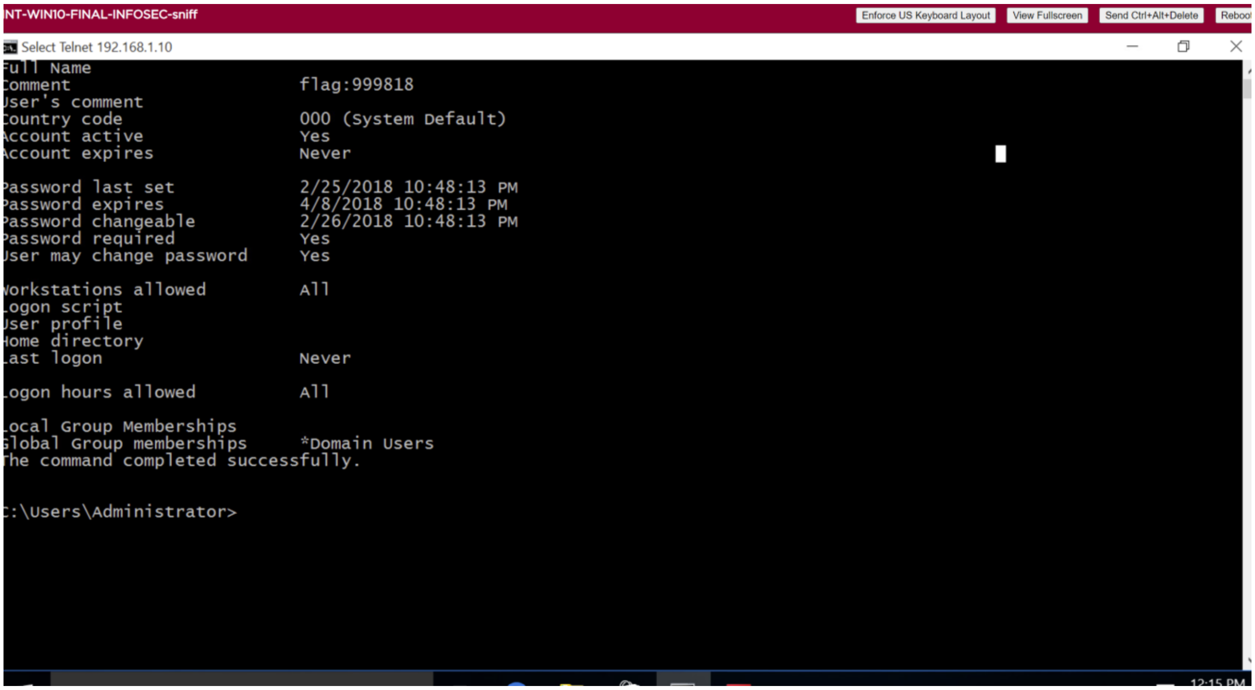

Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660178/125
INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Telnet 192.168.1.10
3:00 AM
9/20/2024

```
*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator> net user creeper P@ssw0rd /add
The command completed successfully.


C:\Users\Administrator>
```

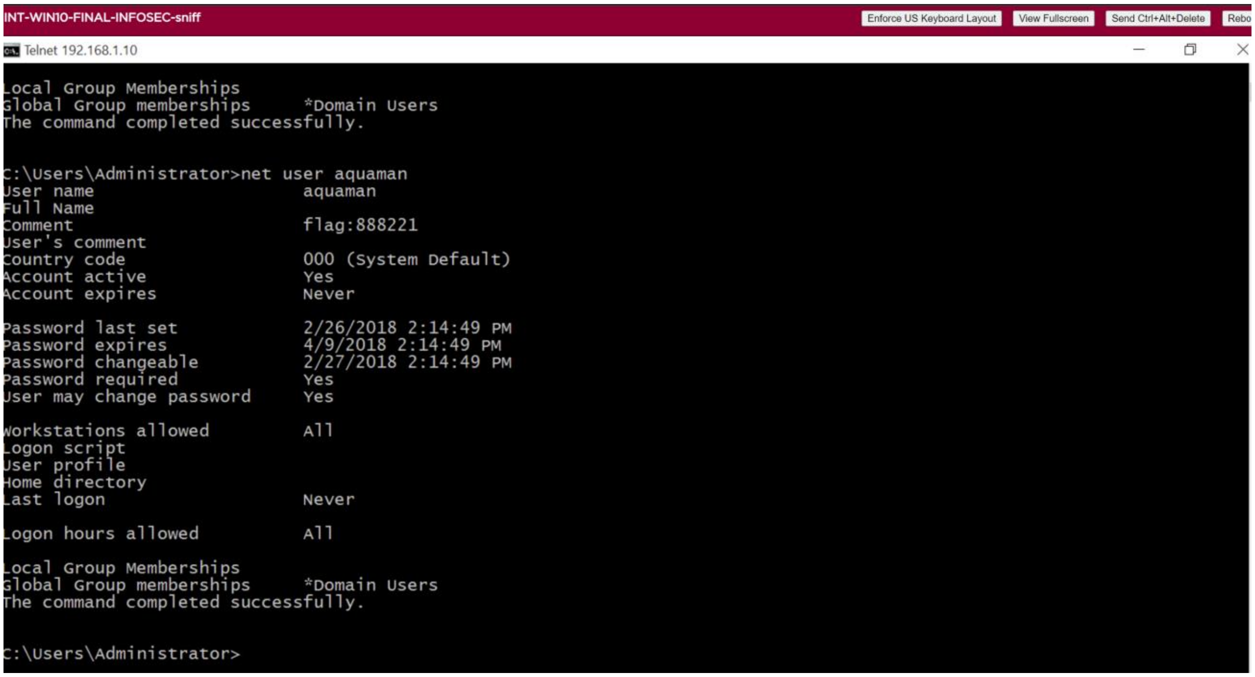
created creeper and added and created the domain admins group



```
*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator> net user creeper P@ssw0rd /add
The command completed successfully.


C:\Users\Administrator>net group "domain admins" creeper /add
The command completed successfully.


C:\Users\Administrator>
```


INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Select Telnet 192.168.1.10
12:15 PM

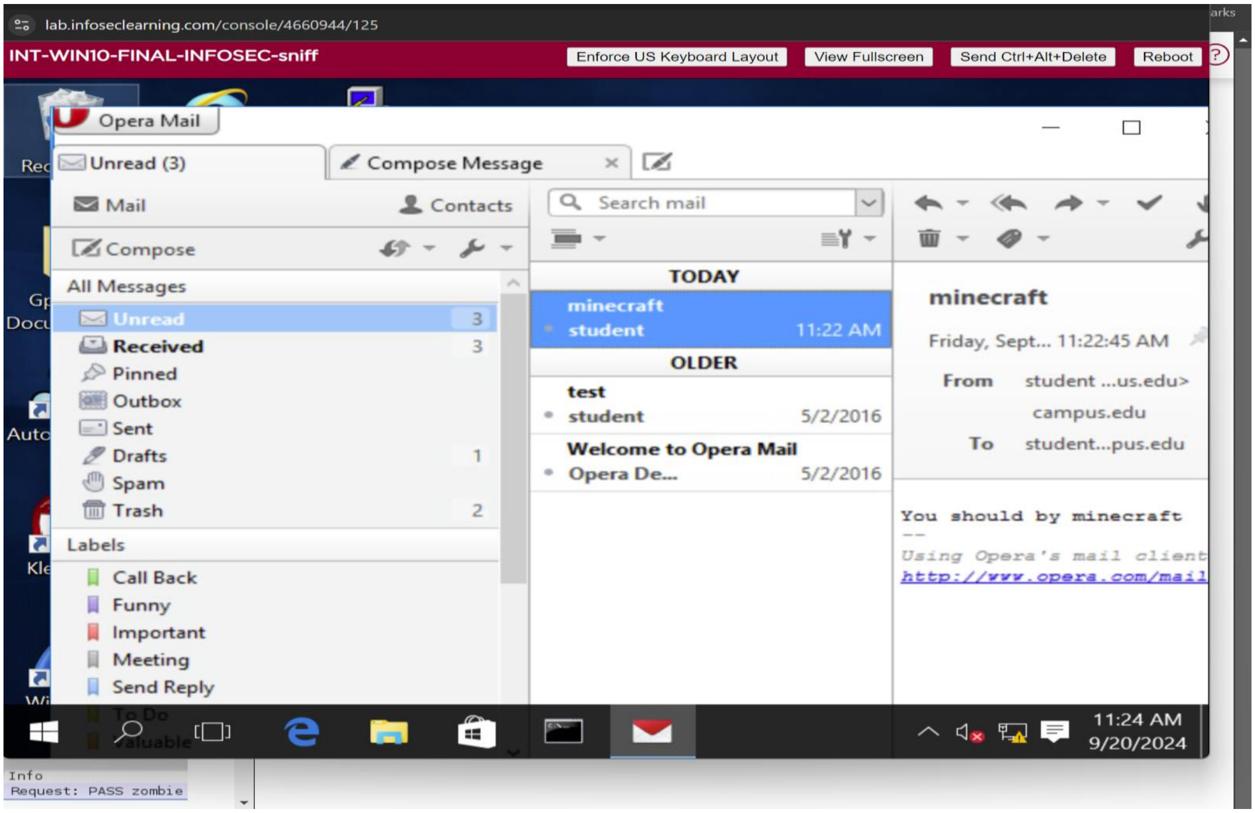
```
Full Name
Comment                      flag:999818
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/25/2018 10:48:13 PM
Password expires             4/8/2018 10:48:13 PM
Password changeable          2/26/2018 10:48:13 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


C:\Users\Administrator>
```



```
Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


C:\Users\Administrator>net user aquaman
User name                    aquaman
Full Name
Comment                      flag:888221
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/26/2018 2:14:49 PM
Password expires             4/9/2018 2:14:49 PM
Password changeable          2/27/2018 2:14:49 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


C:\Users\Administrator>
```

We opened the opera mail in the windows machine and composed a mail to student@campus.edu as entering the subject as Minecraft and entering the body of mail as “You should buy Minecraft”. And We had sent it.

By checking the opera mail and checked all mail we’ll find the mail which we sent.



minecraft
student 11:22 AM

test
student 5/2/2016

Welcome to Opera Mail
Opera De... 5/2/2016

minecraft

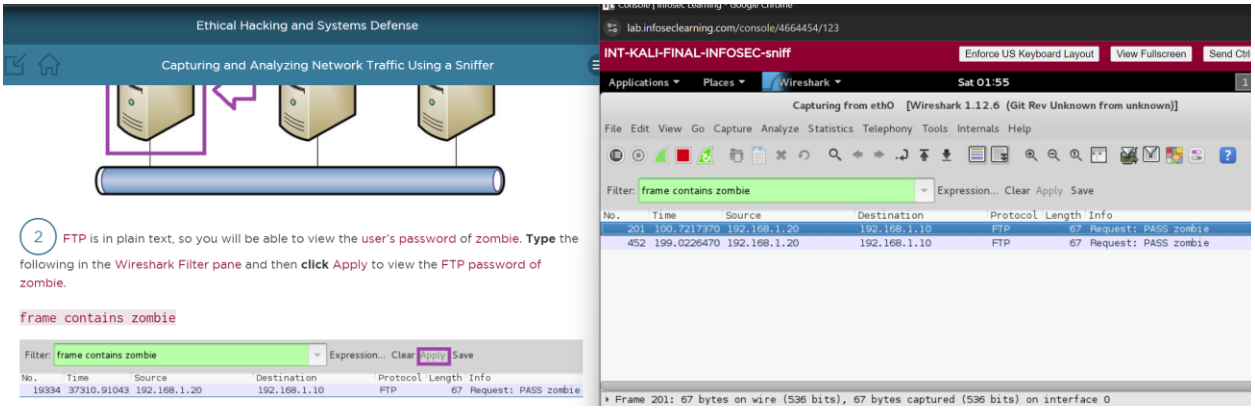
Friday, Sept... 11:22:45 AM

From student ...us.edu>
campus.edu
To student...pus.edu

```
You should by minecraft
--
Using Opera's mail client
http://www.opera.com/mail
```

```
Info
Request: PASS zombie
```

Coming back to the linux machine where wireshark had been running we gonna check the “frame contains zombie”, ”pop”, ”frame contains buy”.

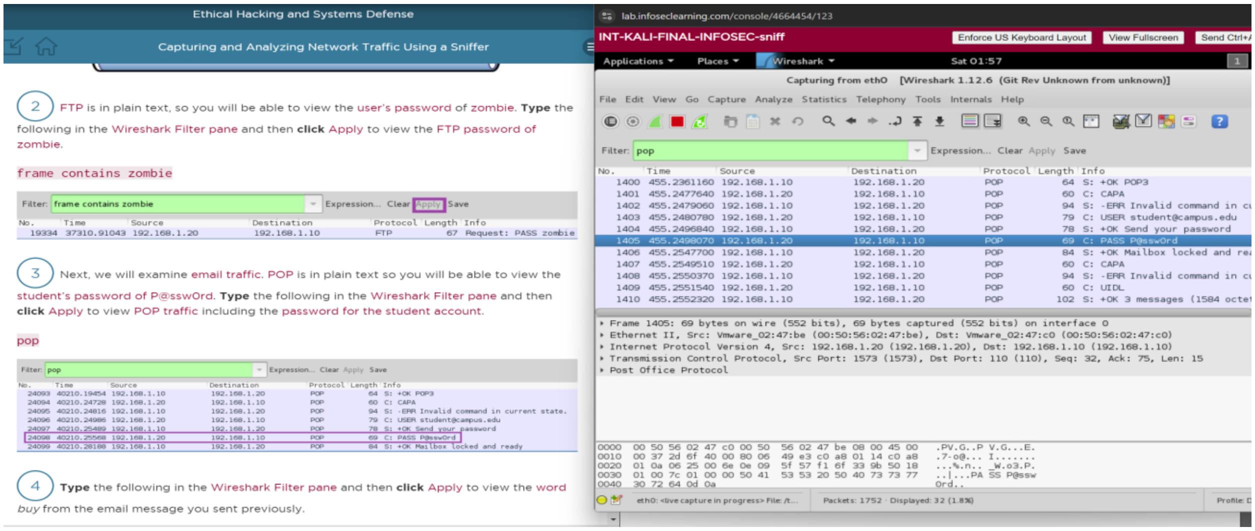

Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
lab.infoseclearning.com/console/4664454/123
INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl
Applications
Places
Wireshark
Sat 01:55
Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

2 FTP is in plain text, so you will be able to view the user's password of zombie. **Type** the following in the Wireshark Filter pane and then **click** Apply to view the FTP password of zombie.

`frame contains zombie`

```
Filter: frame contains zombie
No.    Time         Source        Destination   Protocol Length Info
 19334 37310.91043  192.168.1.20  192.168.1.10  FTP          67 Request: PASS zombie
```

```
Filter: frame contains zombie
No.   Time         Source        Destination   Protocol Length Info
  201 100.7217370  192.168.1.20  192.168.1.10  FTP          67 Request: PASS zombie
  452 199.0226470  192.168.1.20  192.168.1.10  FTP          67 Request: PASS zombie

▸ Frame 201: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
```


Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a Sniffer
lab.infoseclearning.com/console/4664454/123
INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+A
Applications
Places
Wireshark
Sat 01:57
Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

2 FTP is in plain text, so you will be able to view the user's password of zombie. **Type** the following in the Wireshark Filter pane and then **click** Apply to view the FTP password of zombie.

`frame contains zombie`

```
Filter: frame contains zombie
No.    Time         Source        Destination   Protocol Length Info
 19334 37310.91043  192.168.1.20  192.168.1.10  FTP          67 Request: PASS zombie
```

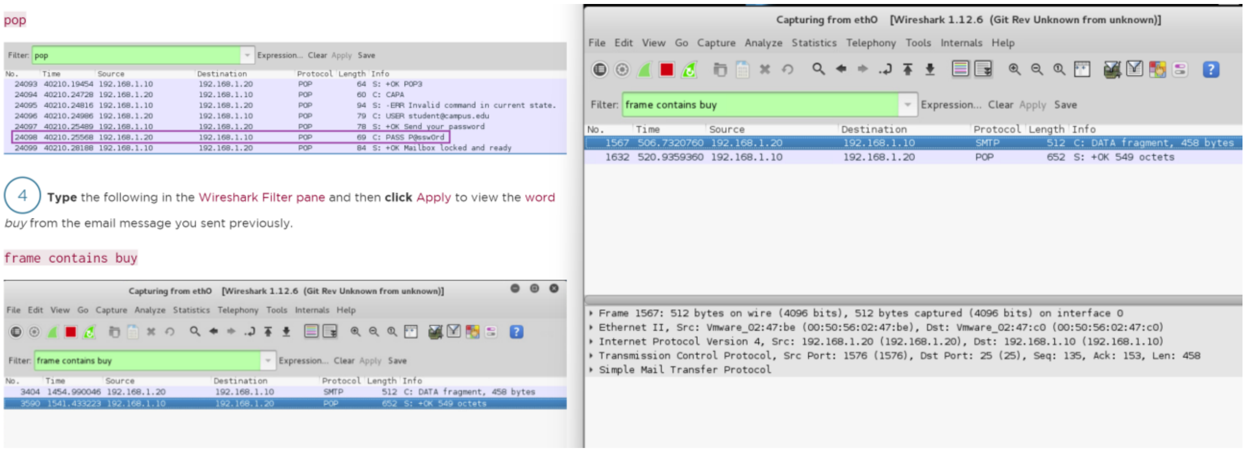
3 Next, we will examine email traffic. POP is in plain text so you will be able to view the student's password of P@sswOrd. **Type** the following in the Wireshark Filter pane and then **click** Apply to view POP traffic including the password for the student account.

`pop`

```
Filter: pop
No.    Time         Source        Destination   Protocol Length Info
 24093 40210.19454  192.168.1.10  192.168.1.20  POP          64 S: +OK POP3
 24094 40210.24728  192.168.1.20  192.168.1.10  POP          60 C: CAPA
 24095 40210.24816  192.168.1.10  192.168.1.20  POP          94 S: -ERR Invalid command in current state.
 24096 40210.24986  192.168.1.20  192.168.1.10  POP          79 C: USER student@campus.edu
 24097 40210.25489  192.168.1.10  192.168.1.20  POP          78 S: +OK Send your password
 24098 40210.25568  192.168.1.20  192.168.1.10  POP          69 C: PASS P@sswOrd
 24099 40210.28188  192.168.1.10  192.168.1.20  POP          84 S: +OK Mailbox locked and ready
```

4 **Type** the following in the Wireshark Filter pane and then **click** Apply to view the word *buy* from the email message you sent previously.

```
Filter: pop
No.   Time         Source        Destination   Protocol Length Info
 1400 455.2361160  192.168.1.10  192.168.1.20  POP          64 S: +OK POP3
 1401 455.2477640  192.168.1.20  192.168.1.10  POP          60 C: CAPA
 1402 455.2479060  192.168.1.10  192.168.1.20  POP          94 S: -ERR Invalid command in cu
 1403 455.2480780  192.168.1.20  192.168.1.10  POP          79 C: USER student@campus.edu
 1404 455.2496840  192.168.1.10  192.168.1.20  POP          78 S: +OK Send your password
 1405 455.2498070  192.168.1.20  192.168.1.10  POP          69 C: PASS P@sswOrd
 1406 455.2547700  192.168.1.10  192.168.1.20  POP          84 S: +OK Mailbox locked and rea
 1407 455.2549510  192.168.1.20  192.168.1.10  POP          60 C: CAPA
 1408 455.2550370  192.168.1.10  192.168.1.20  POP          94 S: -ERR Invalid command in cu
 1409 455.2551540  192.168.1.20  192.168.1.10  POP          60 C: UIDL
 1410 455.2552320  192.168.1.10  192.168.1.20  POP         102 S: +OK 3 messages (1584 octet

▸ Frame 1405: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
▸ Ethernet II, Src: Vmware_02:47:be (00:50:56:02:47:be), Dst: Vmware_02:47:c0 (00:50:56:02:47:c0)
▸ Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.10 (192.168.1.10)
▸ Transmission Control Protocol, Src Port: 1573 (1573), Dst Port: 110 (110), Seq: 32, Ack: 75, Len: 15
▸ Post Office Protocol

0000  00 50 56 02 47 c0 00 50  56 02 47 be 08 00 45 00   .PV.G..P V.G...E.
0010  00 37 2d 6f 40 00 80 06  49 e3 c0 a8 01 14 c0 a8   .7-o@... I.......
0020  01 0a 06 25 00 6e 0e 09  5f 57 f1 6f 33 9b 50 18   ...%.n.. _W.o3.P.
0030  01 00 7c 01 00 00 50 41  53 53 20 50 40 73 73 77   ..|...PA SS P@ssw
0040  30 72 64 0d 0a                                     0rd..

eth0: <live capture in progress> File: /t...   Packets: 1752 · Displayed: 32 (1.8%)   Profile: D
```


Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

`pop`

```
Filter: pop
No.    Time         Source        Destination   Protocol Length Info
 24093 40210.19454  192.168.1.10  192.168.1.20  POP          64 S: +OK POP3
 24094 40210.24728  192.168.1.20  192.168.1.10  POP          60 C: CAPA
 24095 40210.24816  192.168.1.10  192.168.1.20  POP          94 S: -ERR Invalid command in current state.
 24096 40210.24986  192.168.1.20  192.168.1.10  POP          79 C: USER student@campus.edu
 24097 40210.25489  192.168.1.10  192.168.1.20  POP          78 S: +OK Send your password
 24098 40210.25568  192.168.1.20  192.168.1.10  POP          69 C: PASS P@sswOrd
 24099 40210.28188  192.168.1.10  192.168.1.20  POP          84 S: +OK Mailbox locked and ready
```

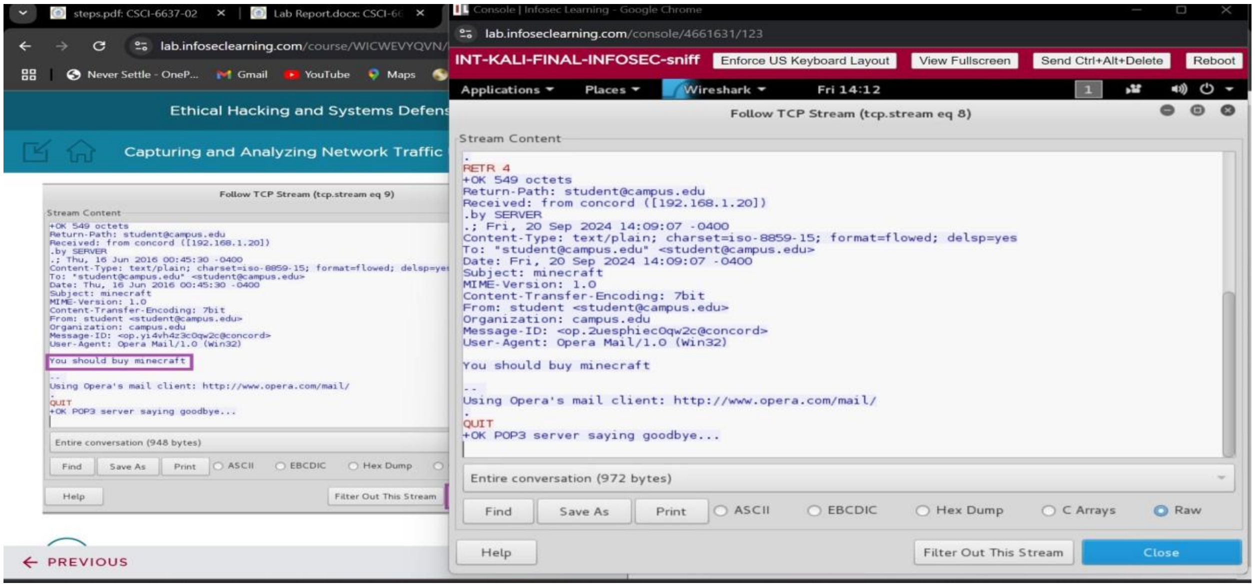
4 **Type** the following in the Wireshark Filter pane and then **click** Apply to view the word *buy* from the email message you sent previously.

`frame contains buy`

```
Filter: frame contains buy
No.   Time          Source        Destination   Protocol Length Info
 3404 1454.990046   192.168.1.20  192.168.1.10  SMTP        512 C: DATA fragment, 458 bytes
 3590 1541.433223   192.168.1.10  192.168.1.20  POP         652 S: +OK 549 octets
```

```
Filter: frame contains buy
No.   Time         Source        Destination   Protocol Length Info
 1567 506.7320760  192.168.1.20  192.168.1.10  SMTP        512 C: DATA fragment, 458 bytes
 1632 520.9359360  192.168.1.10  192.168.1.20  POP         652 S: +OK 549 octets

▸ Frame 1567: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface 0
▸ Ethernet II, Src: Vmware_02:47:be (00:50:56:02:47:be), Dst: Vmware_02:47:c0 (00:50:56:02:47:c0)
▸ Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.10 (192.168.1.10)
▸ Transmission Control Protocol, Src Port: 1576 (1576), Dst Port: 25 (25), Seq: 135, Ack: 153, Len: 458
▸ Simple Mail Transfer Protocol
```

We checked TCP stream for pop as we can see “You should buy Minecraft” in it.



Follow TCP Stream (tcp.stream eq 9)

Stream Content

```
+OK 549 octets
Return-Path: student@campus.edu
Received: from concord ([192.168.1.20])
.by SERVER
.; Thu, 16 Jun 2016 00:45:30 -0400
Content-Type: text/plain; charset=iso-8859-15; format=flowed; delsp=yes
To: "student@campus.edu" <student@campus.edu>
Date: Thu, 16 Jun 2016 00:45:30 -0400
Subject: minecraft
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
From: student <student@campus.edu>
Organization: campus.edu
Message-ID: <op.yi4vh4z3c0qw2c@concord>
User-Agent: Opera Mail/1.0 (Win32)

You should buy minecraft

--
Using Opera's mail client: http://www.opera.com/mail/
.
QUIT
+OK POP3 server saying goodbye...
```

Entire conversation (948 bytes)

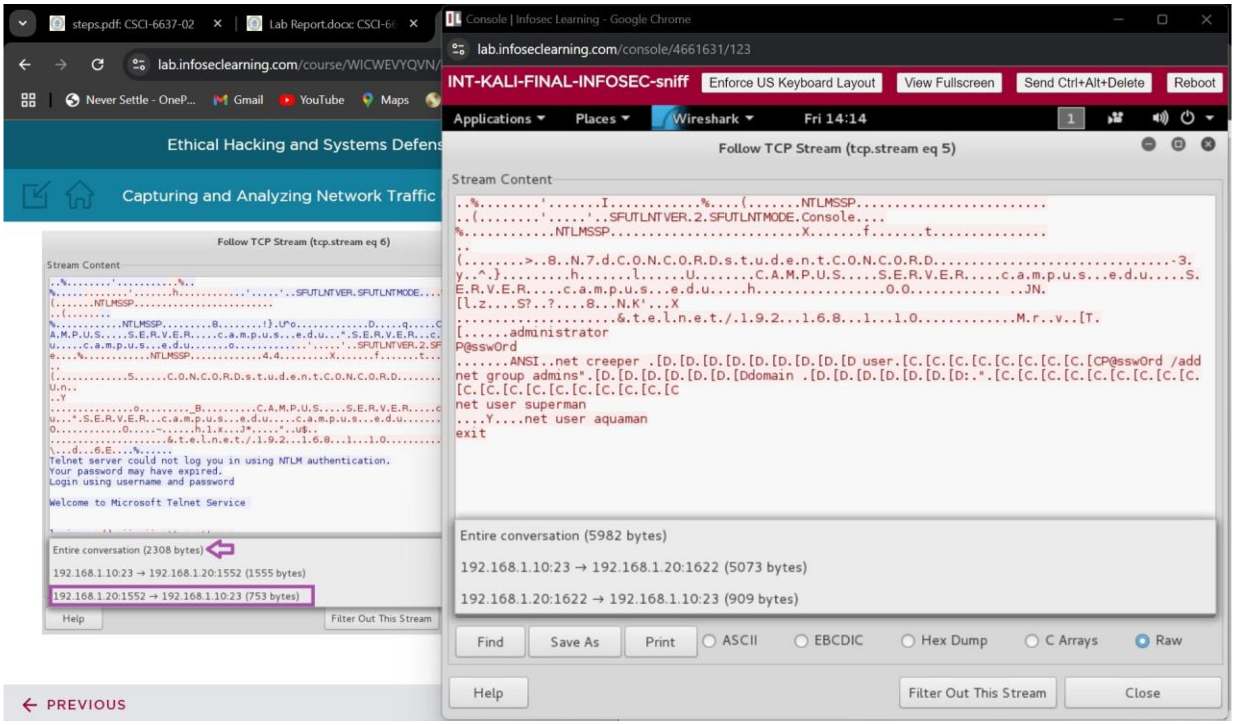
Follow TCP Stream (tcp.stream eq 8)

Stream Content

```
.
RETR 4
+OK 549 octets
Return-Path: student@campus.edu
Received: from concord ([192.168.1.20])
.by SERVER
.; Fri, 20 Sep 2024 14:09:07 -0400
Content-Type: text/plain; charset=iso-8859-15; format=flowed; delsp=yes
To: "student@campus.edu" <student@campus.edu>
Date: Fri, 20 Sep 2024 14:09:07 -0400
Subject: minecraft
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
From: student <student@campus.edu>
Organization: campus.edu
Message-ID: <op.2uesphiec0qw2c@concord>
User-Agent: Opera Mail/1.0 (Win32)

You should buy minecraft

--
Using Opera's mail client: http://www.opera.com/mail/
.
QUIT
+OK POP3 server saying goodbye...
```

Entire conversation (972 bytes)

We had found the P@ssw0rd creeper and found both the users Superman and Aquaman in the group.



Follow TCP Stream (tcp.stream eq 6)

Stream Content

```
..%........'..........%..
%.............'.......h...........'.....'..SFUTLNTVER.SFUTLNTMODE....
(.......NTLMSSP........................
..(........
%............NTLMSSP.........8........!}.U^o.............D.....q.....C
A.M.P.U.S.....S.E.R.V.E.R.....c.a.m.p.u.s...e.d.u...".S.E.R.V.E.R...c.
u.....c.a.m.p.u.s...e.d.u.......o.............'.....'..SFUTLNTVER.2.SF
e....%............NTLMSSP.............4.4.........X.......f.......t...
..
(............5......C.O.N.C.O.R.D.s.t.u.d.e.n.t.C.O.N.C.O.R.D.......
U.n..
..Y
...............o.........B..........C.A.M.P.U.S.....S.E.R.V.E.R.....c
u...".S.E.R.V.E.R...c.a.m.p.u.s...e.d.u.....c.a.m.p.u.s...e.d.u.......
0............0.....~......h.l.x...J*......"..u$..
.......................&.t.e.l.n.e.t./.1.9.2...1.6.8...1...1.0.........
\...d...6.E....%......
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service
```

Entire conversation (2308 bytes)

192.168.1.10:23 → 192.168.1.20:1552 (1555 bytes)

192.168.1.20:1552 → 192.168.1.10:23 (753 bytes)

Follow TCP Stream (tcp.stream eq 5)

Stream Content

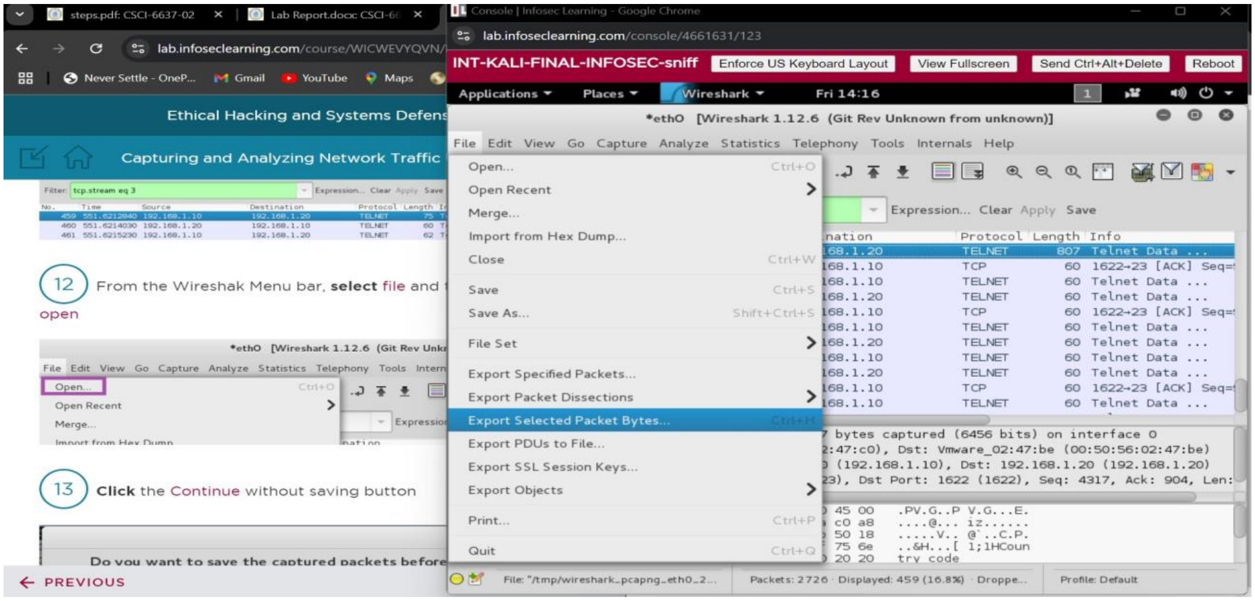
```
..%........'.......I............%....(.......NTLMSSP.........................
..(........'.....'..SFUTLNTVER.2.SFUTLNTMODE.Console....
%............NTLMSSP........................X.......f.......t...............
..
(........>..8..N.7.d.C.O.N.C.O.R.D.s.t.u.d.e.n.t.C.O.N.C.O.R.D................................-3.
y..^.}.........h.......l.......U........C.A.M.P.U.S.....S.E.R.V.E.R.....c.a.m.p.u.s...e.d.u.....S.
E.R.V.E.R.....c.a.m.p.u.s...e.d.u.....h.................0.0............ ..JN.
[l.z....S?..?....8...N.K'...X
.....................&.t.e.l.n.e.t./.1.9.2...1.6.8...1...1.0.............M.r..v..[T.
[......administrator
P@ssw0rd
.......ANSI..net creeper .[D.[D.[D.[D.[D.[D.[D.[D.[D user.[C.[C.[C.[C.[C.[C.[C.[C.[CP@ssw0rd /add
net group admins".[D.[D.[D.[D.[D.[D.[Ddomain .[D.[D.[D.[D.[D.[D.[D:.".[C.[C.[C.[C.[C.[C.[C.[C.[C.
[C.[C.[C.[C.[C.[C.[C.[C.[C.[C
net user superman
....Y....net user aquaman
exit
```

Entire conversation (5982 bytes)

192.168.1.10:23 → 192.168.1.20:1622 (5073 bytes)

192.168.1.20:1622 → 192.168.1.10:23 (909 bytes)

Telnet we opened the new file by stopping the capture .



steps.pdf: CSCI-6637-02
Lab Report.docx: CSCI-66
lab.infoseclearning.com/course/WICWEVYQVN/
Never Settle - OneP...
Gmail
YouTube
Maps
Ethical Hacking and Systems Defens
Capturing and Analyzing Network Traffic
PREVIOUS
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4661631/123
INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Wireshark
Fri 14:16
*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Expression... Clear Apply Save

Filter: tcp.stream eq 3

```
No.  Time         Source        Destination   Protocol Length
459  551.6212840  192.168.1.10  192.168.1.20  TELNET   75
460  551.6214030  192.168.1.20  192.168.1.10  TELNET   60
461  551.6215230  192.168.1.10  192.168.1.20  TELNET   62
```

12 From the Wireshak Menu bar, **select** file and
open

*eth0 [Wireshark 1.12.6 (Git Rev Unkr

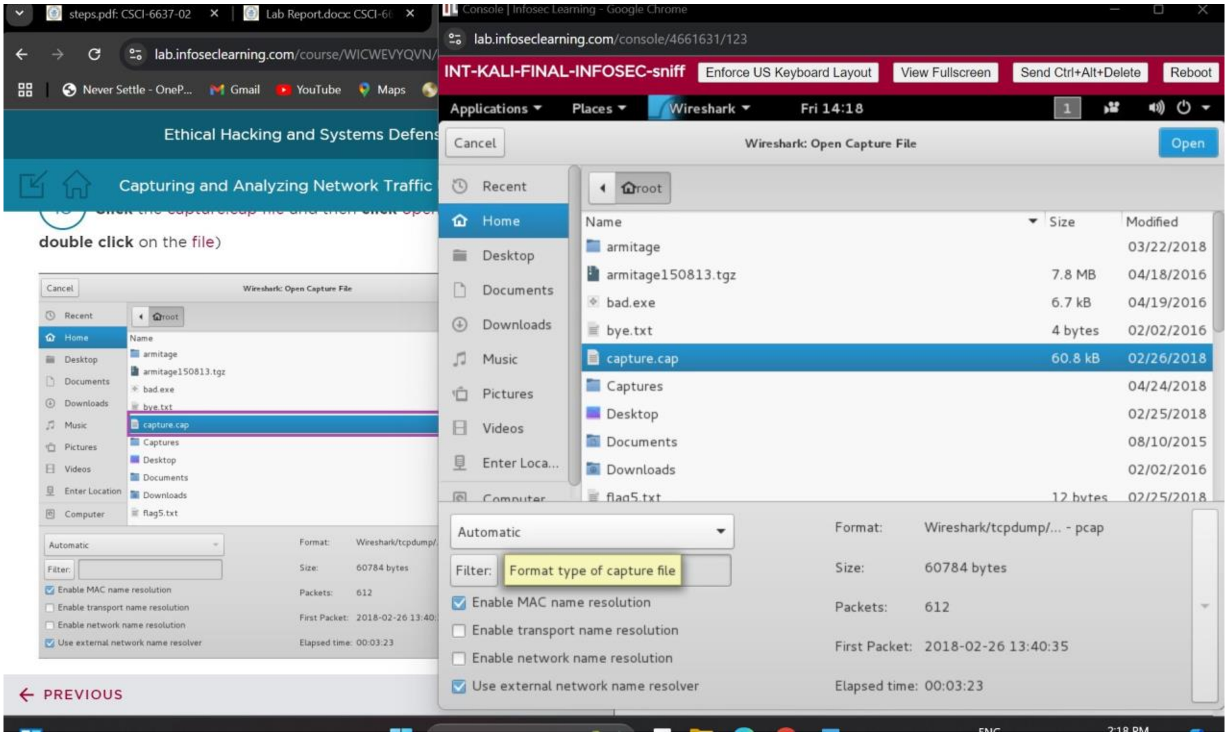
13 **Click** the Continue without saving button

Do you want to save the captured packets before

```
nation     Protocol Length Info
168.1.20   TELNET   807  Telnet Data ...
168.1.10   TCP       60  1622→23 [ACK] Seq=
168.1.10   TELNET    60  Telnet Data ...
168.1.20   TELNET    60  Telnet Data ...
168.1.10   TCP       60  1622→23 [ACK] Seq=
168.1.10   TELNET    60  Telnet Data ...
168.1.20   TELNET    60  Telnet Data ...
168.1.10   TELNET    60  Telnet Data ...
168.1.20   TELNET    60  Telnet Data ...
168.1.10   TCP       60  1622→23 [ACK] Seq=
168.1.10   TELNET    60  Telnet Data ...

7 bytes captured (6456 bits) on interface 0
2:47:c0), Dst: Vmware_02:47:be (00:50:56:02:47:be)
) (192.168.1.10), Dst: 192.168.1.20 (192.168.1.20)
23), Dst Port: 1622 (1622), Seq: 4317, Ack: 904, Len:

) 45 00   .PV.G..P V.G...E.
 c0 a8   ....@... iz......
 50 18   .....V.. @`..C.P.
 75 6e   ..&H...[ 1;1HCoun
) 20 20   try code
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 2726 · Displayed: 459 (16.8%) · Droppe... Profile: Default

We now open the capture.cap file in the home



steps.pdf: CSCI-6637-02
Lab Report.docx: CSCI-66
lab.infoseclearning.com/course/WICWEVYQVN/
Never Settle - OneP...
Gmail
YouTube
Maps
Ethical Hacking and Systems Defens
Capturing and Analyzing Network Traffic
PREVIOUS
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4661631/123
INT-KALI-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Wireshark
Fri 14:18
Cancel
Wireshark: Open Capture File
Open
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Enter Loca...
Computer
root
Filter:
Format type of capture file

double click on the file)

Name	Size	Modified
armitage		03/22/2018
armitage150813.tgz	7.8 MB	04/18/2016
bad.exe	6.7 kB	04/19/2016
bye.txt	4 bytes	02/02/2016
capture.cap	60.8 kB	02/26/2018
Captures		04/24/2018
Desktop		02/25/2018
Documents		08/10/2015
Downloads		02/02/2016
flag5.txt	12 bytes	02/25/2018

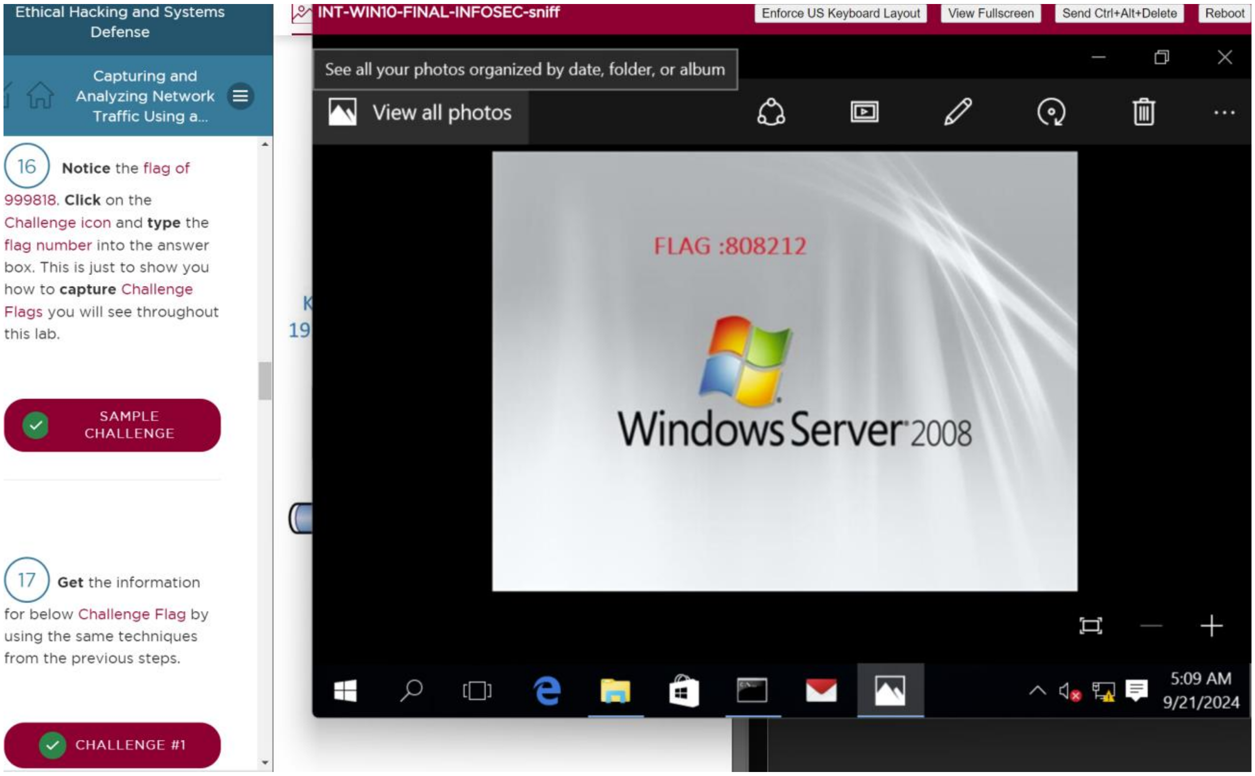
Automatic

☑ Enable MAC name resolution
□ Enable transport name resolution
□ Enable network name resolution
☑ Use external network name resolver

Format: Wireshark/tcpdump/... - pcap
Size: 60784 bytes
Packets: 612
First Packet: 2018-02-26 13:40:35
Elapsed time: 00:03:23

Supporting Evidence

These are the screenshots of challenges that were encountered while performing the lab

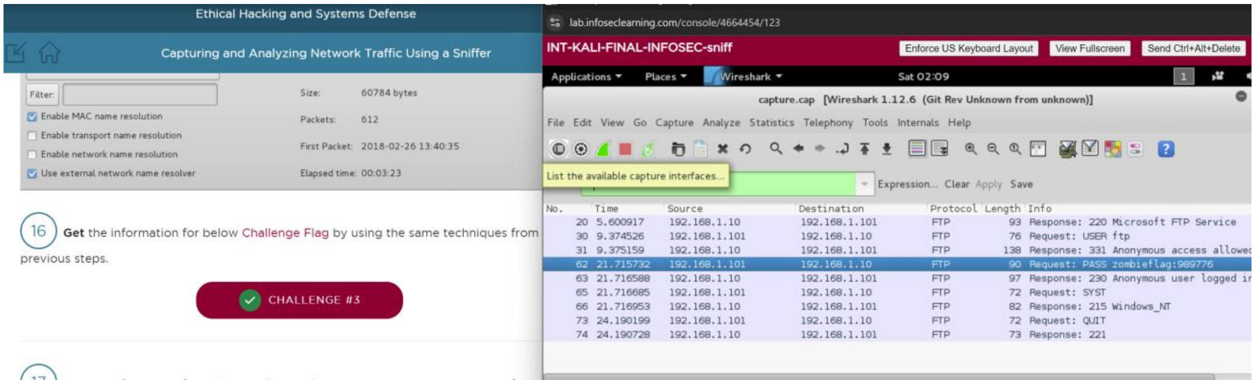


Ethical Hacking and Systems Defense
Capturing and Analyzing Network Traffic Using a...
INT-WIN10-FINAL-INFOSEC-sniff
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
See all your photos organized by date, folder, or album
View all photos
Windows Server 2008
SAMPLE CHALLENGE
CHALLENGE #1
5:09 AM
9/21/2024

16 **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the answer box. This is just to show you how to **capture** Challenge Flags you will see throughout this lab.

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

FLAG :808212



Ethical Hacking and Systems Defense

Capturing and Analyzing Network Traffic Using a Sniffer

Filter:

☑ Enable MAC name resolution
☐ Enable transport name resolution
☐ Enable network name resolution
☑ Use external network name resolver

Size: 60784 bytes
Packets: 612
First Packet: 2018-02-26 13:40:35
Elapsed time: 00:03:23

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

✓ CHALLENGE #3

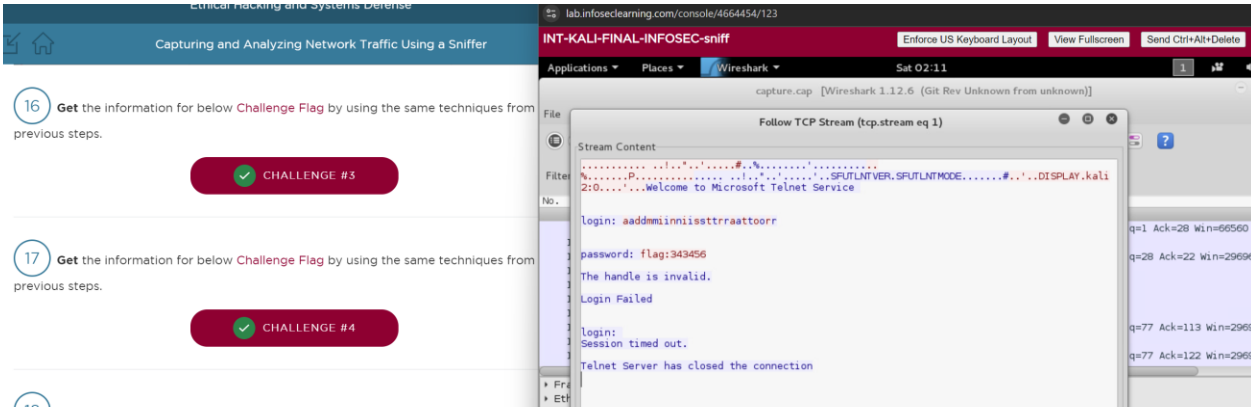
lab.infoseclearning.com/console/4664454/123

INT-KALI-FINAL-INFOSEC-sniff

Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Wireshark
Sat 02:09
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
List the available capture interfaces...
Expression... Clear Apply Save

capture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

```
No.  Time       Source         Destination    Protocol Length Info
  20 5.600917   192.168.1.10   192.168.1.101  FTP        93 Response: 220 Microsoft FTP Service
  30 9.374526   192.168.1.101  192.168.1.10   FTP        76 Request: USER ftp
  31 9.375159   192.168.1.10   192.168.1.101  FTP       138 Response: 331 Anonymous access allowe
  62 21.715732  192.168.1.101  192.168.1.10   FTP        90 Request: PASS zombieflag:989776
  63 21.716588  192.168.1.10   192.168.1.101  FTP        97 Response: 230 Anonymous user logged ir
  65 21.716685  192.168.1.101  192.168.1.10   FTP        72 Request: SYST
  66 21.716953  192.168.1.10   192.168.1.101  FTP        82 Response: 215 Windows_NT
  73 24.190199  192.168.1.101  192.168.1.10   FTP        72 Request: QUIT
  74 24.190728  192.168.1.10   192.168.1.101  FTP        73 Response: 221
```



Ethical Hacking and Systems Defense

Capturing and Analyzing Network Traffic Using a Sniffer

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

✓ CHALLENGE #3

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

✓ CHALLENGE #4

lab.infoseclearning.com/console/4664454/123

INT-KALI-FINAL-INFOSEC-sniff

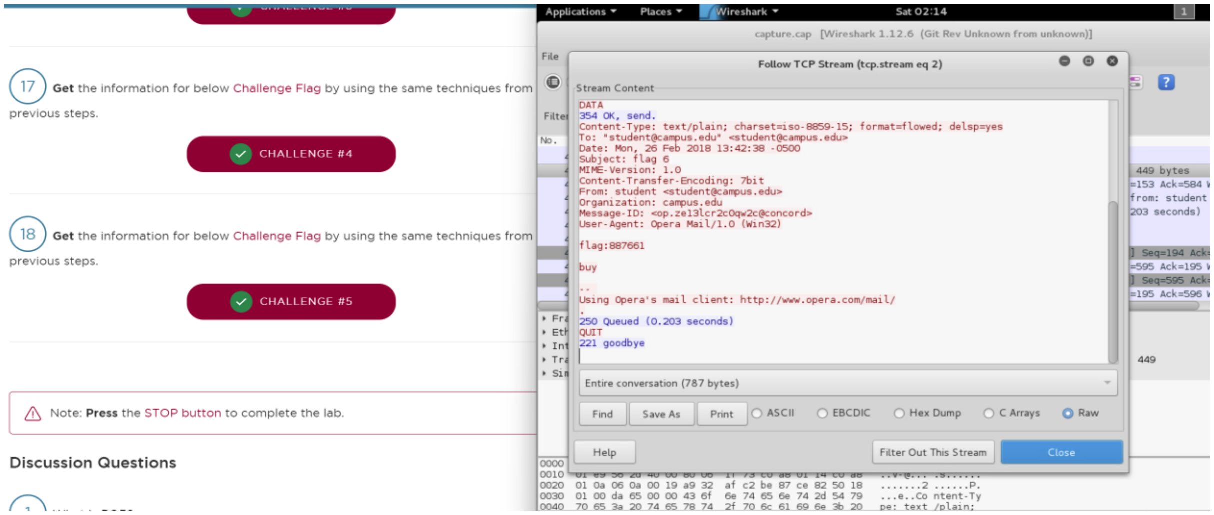
capture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Follow TCP Stream (tcp.stream eq 1)

Stream Content

```
........... ..!..".."......#..%........'..........
%.......P............. ..!.."..'.....'..SFUTLNTVER.SFUTLNTMODE.......#..'..DISPLAY.kali
2:0....'...Welcome to Microsoft Telnet Service


login: aaddmmiinniissttrraattoorr


password: flag:343456

The handle is invalid.

Login Failed


login:
Session timed out.

Telnet Server has closed the connection
```

```
q=1 Ack=28 Win=66560
q=28 Ack=22 Win=2969
q=77 Ack=113 Win=296
q=77 Ack=122 Win=296
```



✓ CHALLENGE #3

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

✓ CHALLENGE #4

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

✓ CHALLENGE #5

⚠ Note: **Press** the STOP button to complete the lab.

Discussion Questions

capture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Follow TCP Stream (tcp.stream eq 2)

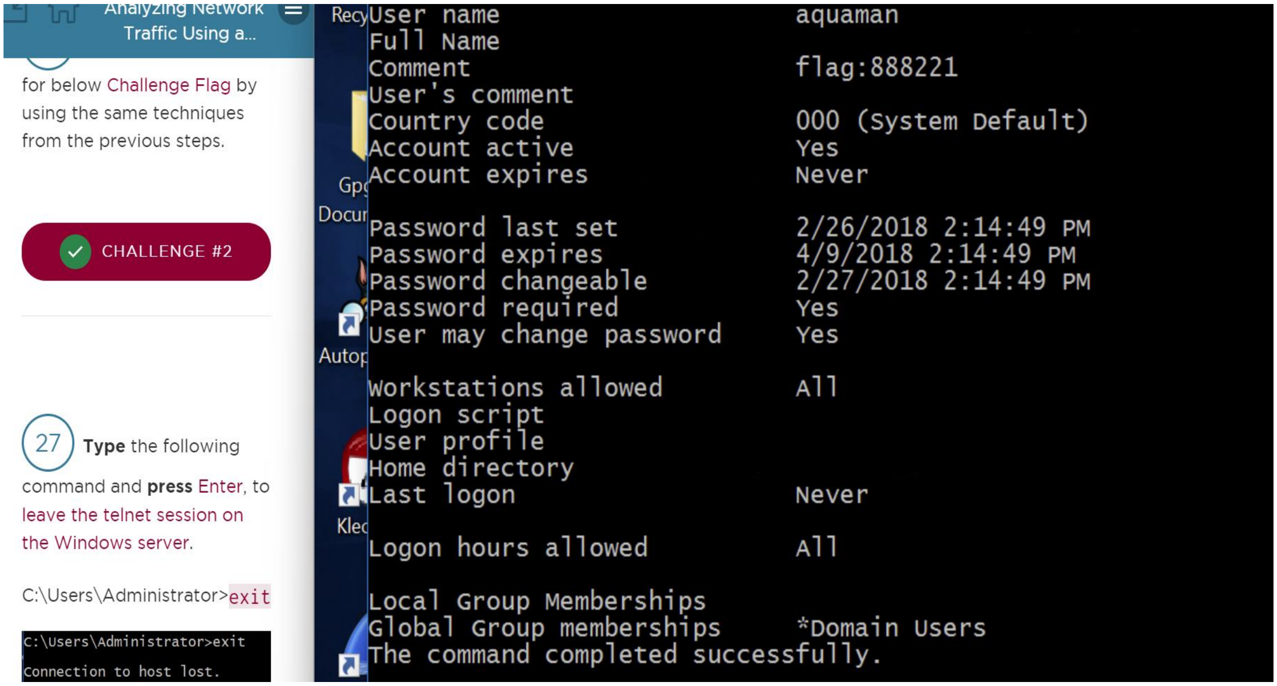
Stream Content

```
DATA
354 OK, send.
Content-Type: text/plain; charset=iso-8859-15; format=flowed; delsp=yes
To: "student@campus.edu" <student@campus.edu>
Date: Mon, 26 Feb 2018 13:42:38 -0500
Subject: flag 6
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
From: student <student@campus.edu>
Organization: campus.edu
Message-ID: <op.ze13lcr2c0qw2c@concord>
User-Agent: Opera Mail/1.0 (Win32)

flag:887661

buy

..
Using Opera's mail client: http://www.opera.com/mail/
.
250 Queued (0.203 seconds)
QUIT
221 goodbye
```

Entire conversation (787 bytes)

```
449 bytes
=153 Ack=584
from: student
203 seconds)
] Seq=194 Ack
=595 Ack=195
] Seq=595 Ack
=195 Ack=596
449
```

```
0000
0010
0020  01 0a 06 0a 00 19 a9 32  af c2 be 87 ce 82 50 18   .......2 ......P.
0030  01 00 da 65 00 00 43 6f  6e 74 65 6e 74 2d 54 79   ...e..Co ntent-Ty
0040  70 65 3a 20 74 65 78 74  2f 70 6c 61 69 6e 3b 20   pe: text /plain;
```



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

✓ CHALLENGE #2

27 **Type** the following command and **press** Enter, to leave the telnet session on the Windows server.

C:\Users\Administrator>`exit`

```
C:\Users\Administrator>exit

Connection to host lost.
```

```
User name                    aquaman
Full Name
Comment                      flag:888221
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/26/2018 2:14:49 PM
Password expires             4/9/2018 2:14:49 PM
Password changeable          2/27/2018 2:14:49 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I observed that Wireshark successfully captured network traffic from various protocols, including FTP, Telnet, and Mail. By configuring the network interface to operate in promiscuous mode, I was able to capture all the packets transmitted on the network. The captured traffic clearly displayed the expected patterns and data, helping me understand the flow of information and how different protocols behave in a live network environment.

Identified risks
A key risk identified during this lab is the vulnerability of unencrypted protocols such as FTP and Telnet. Sensitive data, such as usernames and passwords, are sent in plain text, making them easily accessible to anyone monitoring the network. This opens up the possibility of interception and misuse by malicious actors. Additionally, the generation of excessive traffic can lead to network congestion, potentially disrupting normal operations and slowing down services for other users.

Suggested recommendations

To mitigate the risks observed, I recommend switching to encrypted protocols like SFTP and SSH, which provide secure data transmission and prevent the exposure of sensitive information. It's also important to configure and monitor SPAN ports regularly to ensure they are set up correctly, as improper configuration can result in incomplete packet capture or disruptions in the network. This practice will help maintain both security and network efficiency.

Your successes & failures

I successfully generated network traffic using various protocols and analyzed it in Wireshark. The capture of traffic was thorough once the network interface was correctly configured, and I was able to filter and analyze specific protocol data effectively. However, my initial attempt to capture traffic failed due to a misconfiguration of the network interface, leading to missed packets. Once I identified and corrected this issue, the capture proceeded as expected, highlighting the importance of correct interface setup.

Challenges

One of the main challenges I faced was configuring the network interface to capture all packets in promiscuous mode. It took some trial and error to get it right. Additionally, analyzing the captured data in Wireshark was a bit overwhelming at first due to the large amount of data and different protocols involved. Lastly, generating consistent traffic patterns across multiple protocols (FTP, Telnet, Mail) required careful planning to ensure meaningful analysis. Despite these challenges, I gained valuable hands-on experience in network traffic analysis and troubleshooting.