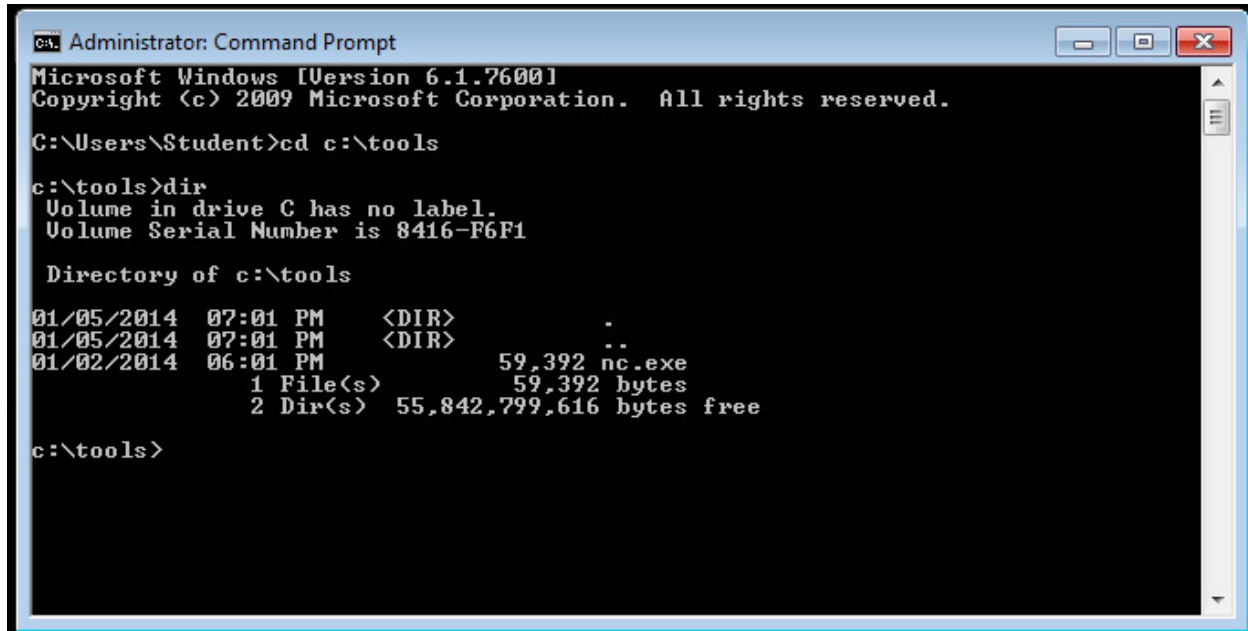


# Lab 06 Report

Report by Joynal Abedin

## Documentation

### NETCAT



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Student>cd c:\tools

c:\tools>dir
Volume in drive C has no label.
Volume Serial Number is 8416-F6F1

Directory of c:\tools

01/05/2014  07:01 PM    <DIR>          .
01/05/2014  07:01 PM    <DIR>          ..
01/02/2014  06:01 PM                59,392 nc.exe
               1 File(s)                59,392 bytes
               2 Dir(s)  55,842,799,616 bytes free

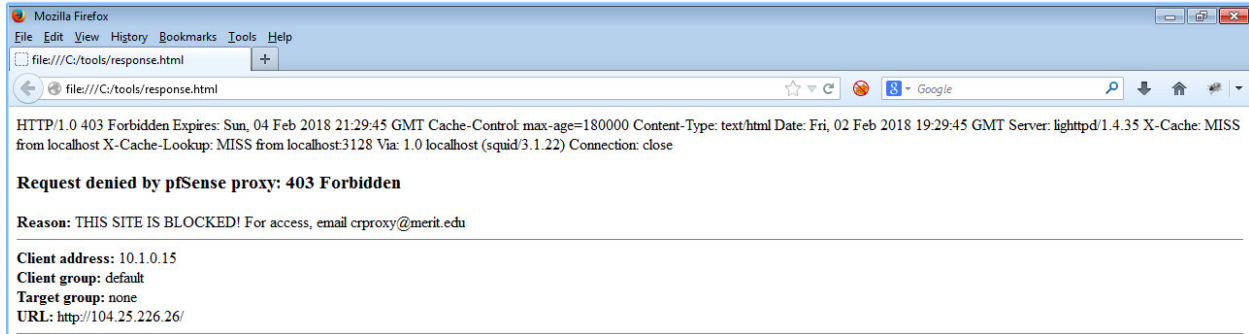
c:\tools>
```

```
c:\tools>nc www.mile2.com 80
GET / HTTP/1.0

HTTP/1.0 403 Forbidden
Expires: Sun, 04 Feb 2018 20:44:02 GMT
Cache-Control: max-age=180000
Content-Type: text/html
Date: Fri, 02 Feb 2018 18:44:02 GMT
Server: lighttpd/1.4.35
X-Cache: MISS from localhost
X-Cache-Lookup: MISS from localhost:3128
Via: 1.0 localhost (squid/3.1.22)
Connection: close

<html>
<body>
<h3>Request denied by pfSense proxy: 403 Forbidden</h3>
<b> Reason: </b> THIS SITE IS BLOCKED! For access, email crproxy@merit.edu
<hr size="1" noshade>
<b> Client address: </b> 10.1.0.15 <br>
<b> Client group: </b> default <br>
<b> Target group: </b> none <br>
<b> URL: </b> http://104.25.226.26/ <br>
<hr size="1" noshade>
</body>
</html>
c:\tools>
```

# Lab 06 Report



```
c:\tools>nc -help
[v1.10 NT]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:  nc -l -p port [options] [hostname] [port]
options:
    -d                detach from console, stealth mode
    -e prog           inbound program to exec [dangerous!!]
    -g gateway        source-routing hop point[s], up to 8
    -G num            source-routing pointer: 4, 8, 12, ...
    -h                this cruft
    -i secs           delay interval for lines sent, ports scanned
    -l                listen mode, for inbound connects
    -L                listen harder, re-listen on socket close
    -n                numeric-only IP addresses, no DNS
    -o file           hex dump of traffic
    -p port           local port number
    -r                randomize local and remote ports
    -s addr           local source address
    -t                answer TELNET negotiation
    -u                UDP mode
    -v                verbose [use twice to be more verbose]
    -w secs           timeout for connects and final net reads
    -z                zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
c:\tools>_
```

## Lab 06 Report

```
root@kali:~# nc 192.168.2.12 1234
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
c:\tools>ipconfig
ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::314c:cd85:d944:8414%14
IPv4 Address. . . . . : 192.168.2.12
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
```

Tunnel adapter isatap.{9DE4404D-973F-4C91-A4F1-0D9E55F73994}:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

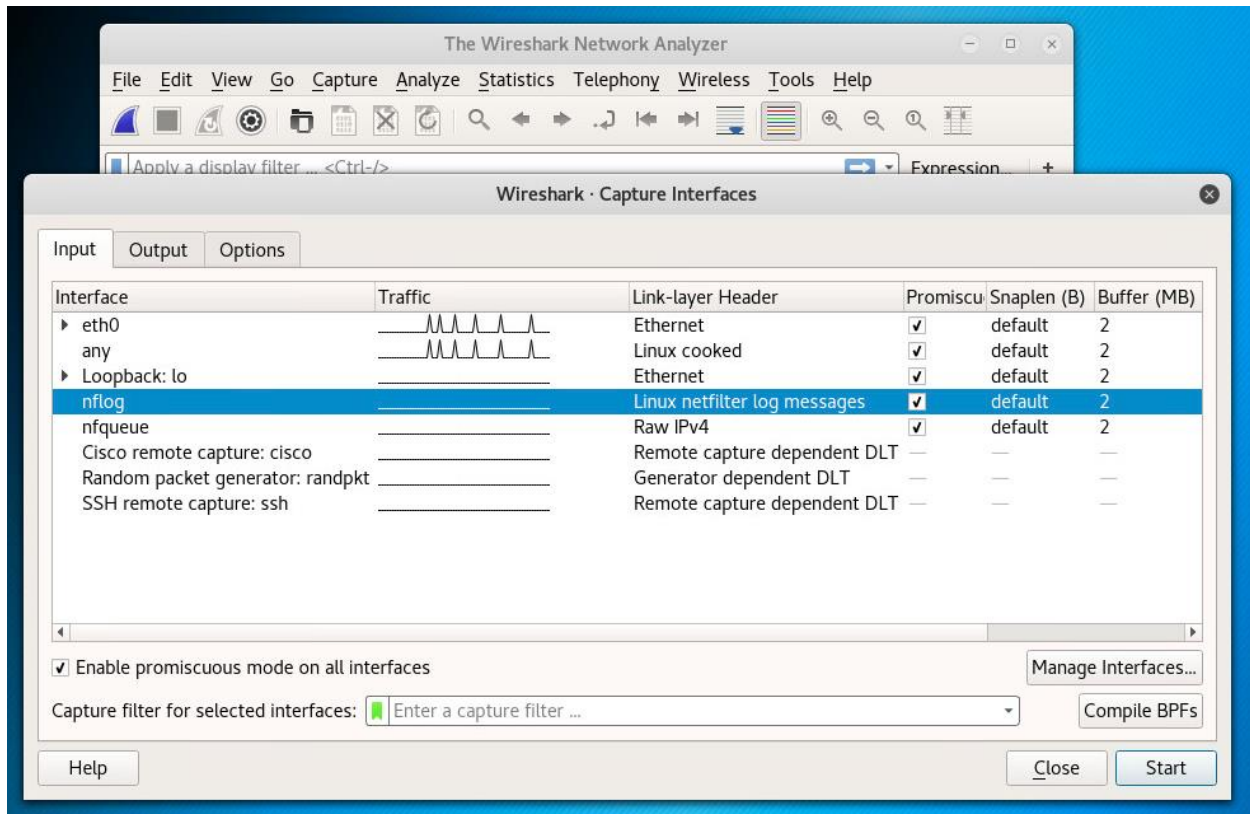
Tunnel adapter Teredo Tunneling Pseudo-Interface:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

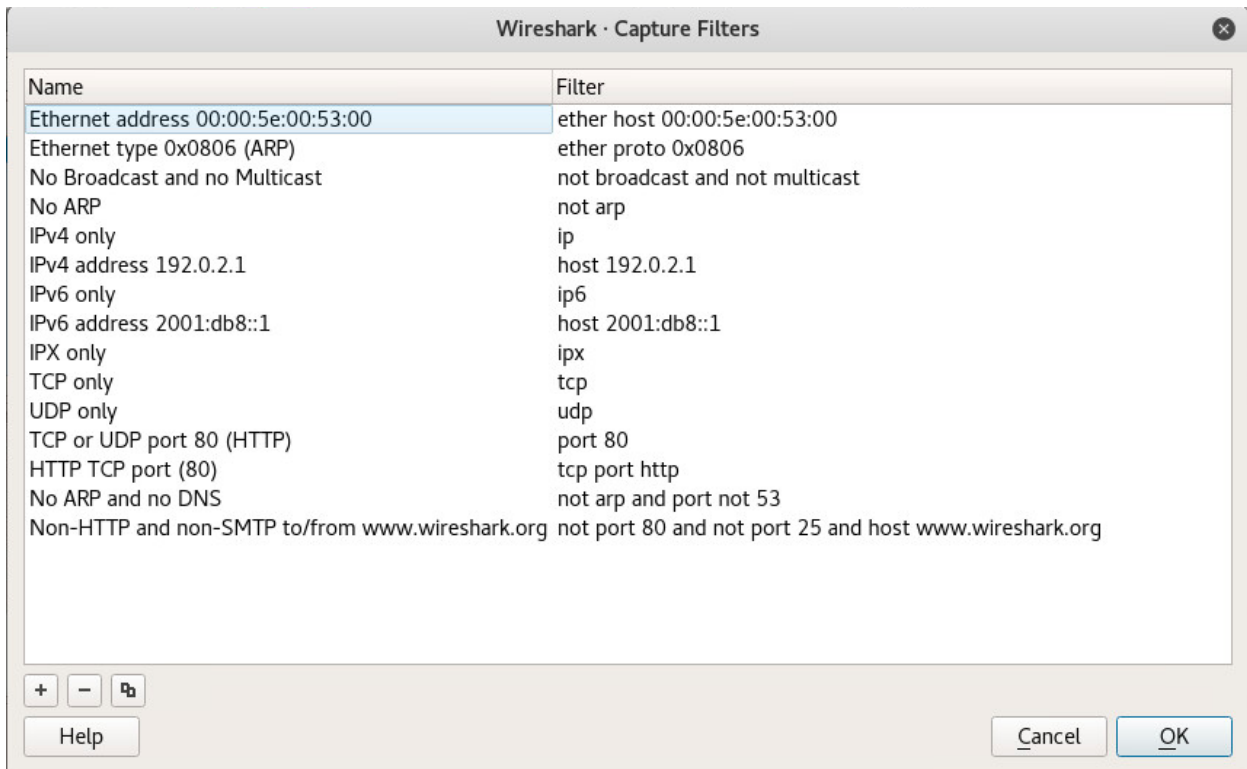
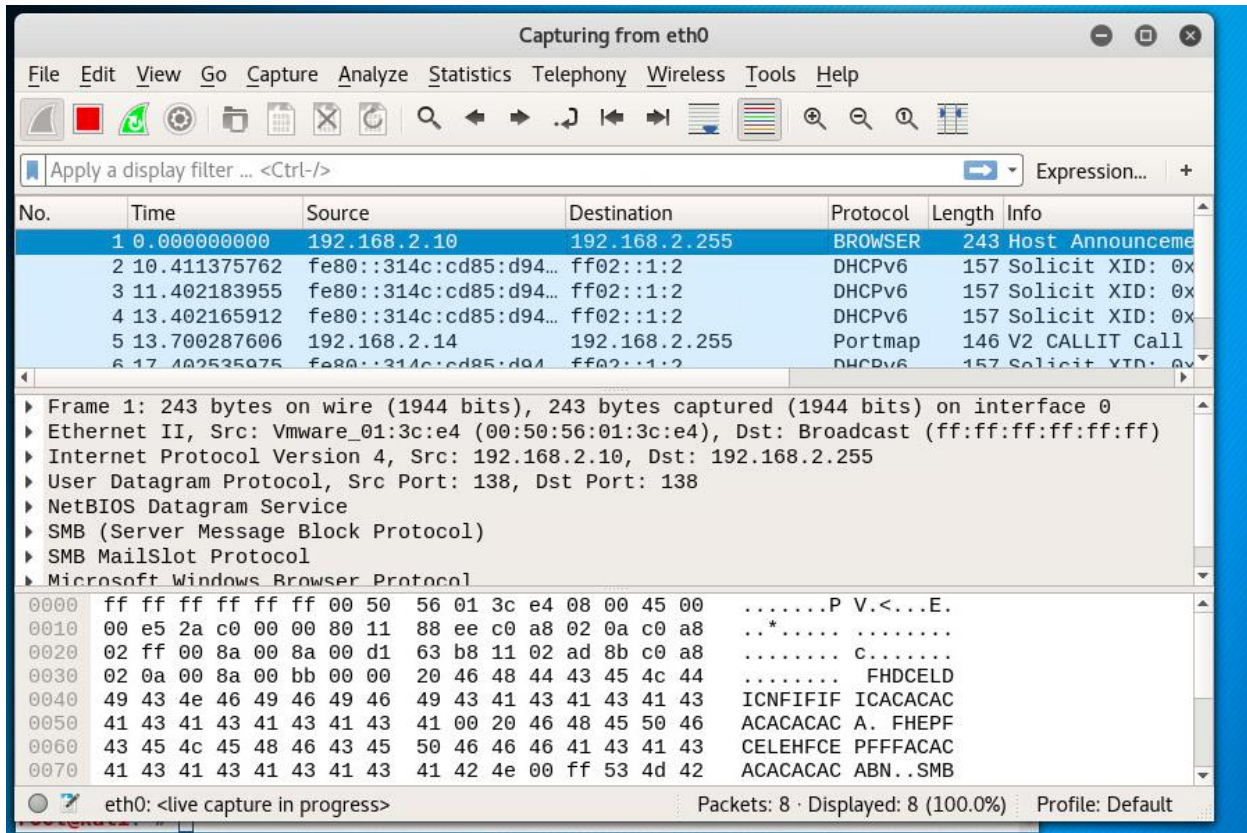
```
c:\tools>
```

# Lab 06 Report

## Capture FTP Traffic



## Lab 06 Report





# Lab 06 Report


## CPEH-LinuxAttack

English (US)  

Applications ▾ Places ▾ Wireshark ▾ Fri 14:55

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.11	192.168.2.255	BROWSER	243	Host Announcement W2K3-XXX, Works
2	4.780859103	192.168.2.14	192.168.2.255	Portmap	146	V2 CALLIT Call
3	8.785035549	192.168.2.14	192.168.2.255	Portmap	146	[RPC retransmission of #2]V2 CALL
4	14.789296511	192.168.2.14	192.168.2.255	Portmap	146	[RPC retransmission of #2]V2 CALL
5	22.797487727	192.168.2.14	192.168.2.255	Portmap	146	[RPC retransmission of #2]V2 CALL

▶ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0  
▶ Ethernet II, Src: Vmware\_01:37:30 (00:50:56:01:37:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
▶ Internet Protocol Version 4, Src: 192.168.2.11, Dst: 192.168.2.255  
▶ User Datagram Protocol, Src Port: 138, Dst Port: 138  
▶ NetBIOS Datagram Service  
▶ SMB (Server Message Block Protocol)  
▶ SMB MailSlot Protocol  
▶ Microsoft Windows Browser Protocol

0000	ff ff ff ff ff ff 00 50	56 01 37 30 08 00 45 00	.....P V.70..E.
0010	00 e5 98 0d 00 00 80 11	1b a0 c0 a8 02 0b c0 a8	.....
0020	02 ff 00 8a 00 8a 00 d1	79 b5 11 02 8f 8e c0 a8	.....y.....
0030	02 0b 00 8a 00 bb 00 00	20 46 48 44 43 45 4c 44	.....FHDCELD
0040	44 43 4e 46 49 46 49 46	49 43 41 43 41 43 41 43	DCNFIFIF ICACACAC
0050	41 43 41 43 41 43 41 43	41 00 20 46 48 45 50 46	ACACACAC A. FHEPF
0060	43 45 4c 45 48 46 43 45	50 46 46 46 41 43 41 43	CELEHFCE PFFFACAC
0070	41 43 41 43 41 43 41 43	41 42 4e 00 ff 53 4d 42	ACACACAC ABN SMB

```
root@kali:~# ftp 192.168.2.15
Connected to 192.168.2.15.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 14:58. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.2.15:root): student
331 User student OK. Password required
Password:
230 OK. Current directory is /home/student
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

# Lab 06 Report

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp Expression...

No.	Time	Source	Destination	Protocol	Length	Info
41	167.081261997	192.168.2.15	192.168.2.13	FTP	386	Response: 220-----
56	238.766736964	192.168.2.13	192.168.2.15	FTP	80	Request: USER student
58	238.767536881	192.168.2.15	192.168.2.13	FTP	106	Response: 331 User st
65	246.673800326	192.168.2.13	192.168.2.15	FTP	81	Request: PASS P@ssw0r
70	251.828740254	192.168.2.15	192.168.2.13	FTP	110	Response: 230 OK. Cur
72	251.828957957	192.168.2.13	192.168.2.15	FTP	72	Request: SYST
74	251.829358757	192.168.2.15	192.168.2.13	FTP	85	Response: 215 UNIX Ty

Frame 41: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

Ethernet II, Src: Vmware\_01:3c:e5 (00:50:56:01:3c:e5), Dst: Vmware\_01:3c:e2 (00:50:56:01:3c:e2)

Internet Protocol Version 4, Src: 192.168.2.15, Dst: 192.168.2.13

Transmission Control Protocol, Src Port: 21, Dst Port: 38194, Seq: 1, Ack: 1, Len: 320

File Transfer Protocol (FTP)

```

0000 00 50 56 01 3c e2 00 50 56 01 3c e5 08 00 45 10 .PV.<..P V.<...E.
0010 01 74 00 d8 40 00 40 06 b3 2f c0 a8 02 0f c0 a8 .t..@.@. ./.....
0020 02 0d 00 15 95 32 0a c1 0f e4 48 62 e5 8c 80 18 .....2.. ..Hb....
0030 07 12 a1 fb 00 00 01 01 08 0a 0e 2e 14 22 01 11 ..... ....."..
0040 e2 9d 32 32 30 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 ..220--- .....
0050 57 65 6c 63 6f 6d 65 20 74 6f 20 50 75 72 65 2d Welcome to Pure-
0060 46 54 50 64 20 5b 70 72 69 76 73 65 70 5d 20 5b FTPd [pr ivsep] [
0070 54 4c 53 5d 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d TLS] --- .....
0080 0a 32 32 30 2d 59 6f 75 20 61 72 65 20 75 73 65 .220-You are use
0090 72 20 6e 75 6d 62 65 72 20 31 20 6f 66 20 35 30 r number 1 of 50
00a0 20 61 6c 6c 6f 77 65 64 2e 0d 0a 32 32 30 2d 4c allowed ...220-L

```

File Transfer Protocol (FTP): Protocol Packets: 77 · Displayed: 7 (9.1%) · Dropped: 0 (0.0%) Profile: Default

## Lab 06 Report

The image shows a Wireshark window titled "Follow TCP Stream (tcp.stream eq 1) · wireshark\_eth0\_20180...". The left pane shows a packet list with the following entries:

No.	Time	Source
31	162.065361552	192.168.1.1
32	162.065814562	192.168.1.1
33	162.065860348	192.168.1.1
41	167.081261997	192.168.1.1
42	167.081336810	192.168.1.1
56	238.766736964	192.168.1.1
57	238.767412194	192.168.1.1
58	238.767536881	192.168.1.1
59	238.767575904	192.168.1.1

The right pane shows the packet details for the selected packet (Frame 41):

- Frame 41: 386 bytes on wire (3088 bytes captured) on interface eth0
- Ethernet II, Src: Vmware, Dst: 192.168.1.1
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
- Transmission Control Protocol, Seq: 311111111, Len: 458
- File Transfer Protocol

The bottom pane shows the raw packet data in hexadecimal and ASCII:

```
0000 00 50 56 01 3c e2 00 00 00 00 00 00 00 00 00 00
0010 01 74 00 d8 40 00 00 00 00 00 00 00 00 00 00 00
0020 02 0d 00 15 95 32 00 00 00 00 00 00 00 00 00 00
0030 07 12 a1 fb 00 00 00 00 00 00 00 00 00 00 00 00
0040 e2 9d 32 32 30 2d 00 00 00 00 00 00 00 00 00 00
0050 57 65 6c 63 6f 6d 00 00 00 00 00 00 00 00 00 00
0060 46 54 50 64 20 5b 00 00 00 00 00 00 00 00 00 00
0070 54 4c 53 5d 20 2d 00 00 00 00 00 00 00 00 00 00
0080 0a 32 32 30 2d 59 00 00 00 00 00 00 00 00 00 00
0090 72 20 6e 75 6d 62 00 00 00 00 00 00 00 00 00 00
00a0 20 61 6c 6c 6f 77 00 00 00 00 00 00 00 00 00 00
```

The main pane displays the ASCII representation of the TCP stream:

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 14:58. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER student
331 User student OK. Password required
PASS P@ssw0rd
230 OK. Current directory is /home/student
SYST
215 UNIX Type: L8
```

The bottom status bar shows: 6 client pkts, 5 server pkts, 9 turns. The bottom right pane shows: Entire conversation (458 bytes) Show and save data as ASCII Stream 1 Find: Find Next Help Filter Out This Stream Print Save as... Back Close



# Lab 06 Report

## Vulnerabilities

### Vulnerability 01

#### Description

The FTP is a TCP/IP protocol that allows files transfers between FTP servers and clients. FTP has a drawback while doing authentication, the data will transfer in plain text, which can be read by anyone who's sniffing into the traffic to capture a few username or password for bad intention.

#### Relative Risk (High, Medium, Low)

- Medium
  - Approximately 10 times more expensive than a "low" risk
  - additional budget request may be required

#### Mitigation

One way to mitigate this kind of vulnerability is to choose SFTP (secure) and enable Anti-hacking feature on a FTP server. Also, limit the number of password attempts one can make before locked out.

While FTP is sometimes a requirement because it's easy and cost-effective for file transferring, however, it is always best to check your security protocol regularly to stay up to date.