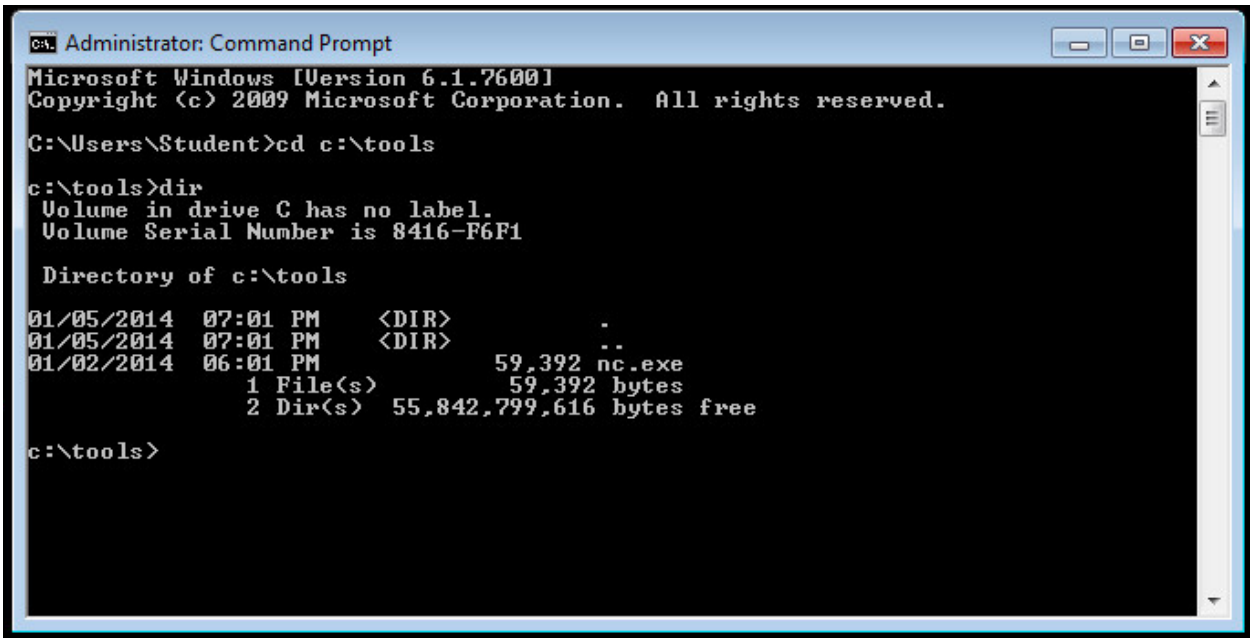
Lab 06 Report

Report by Joynal Abedin

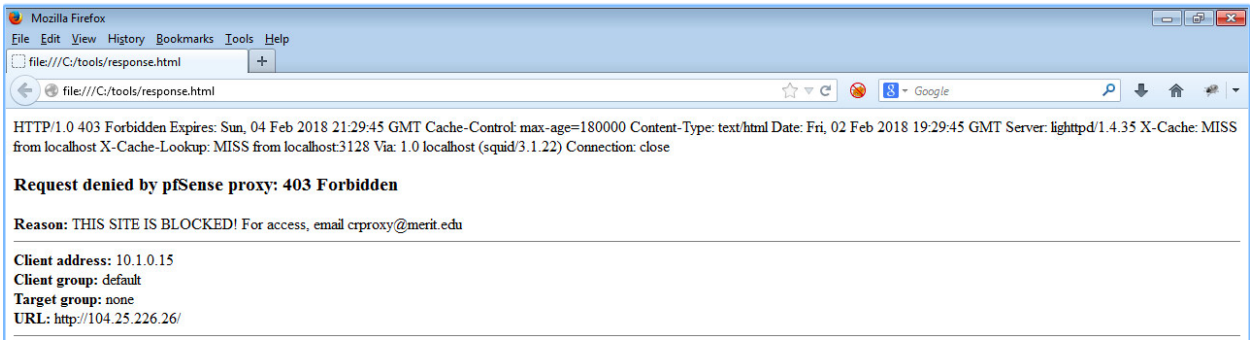
Documentation

NETCAT




```
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>
```

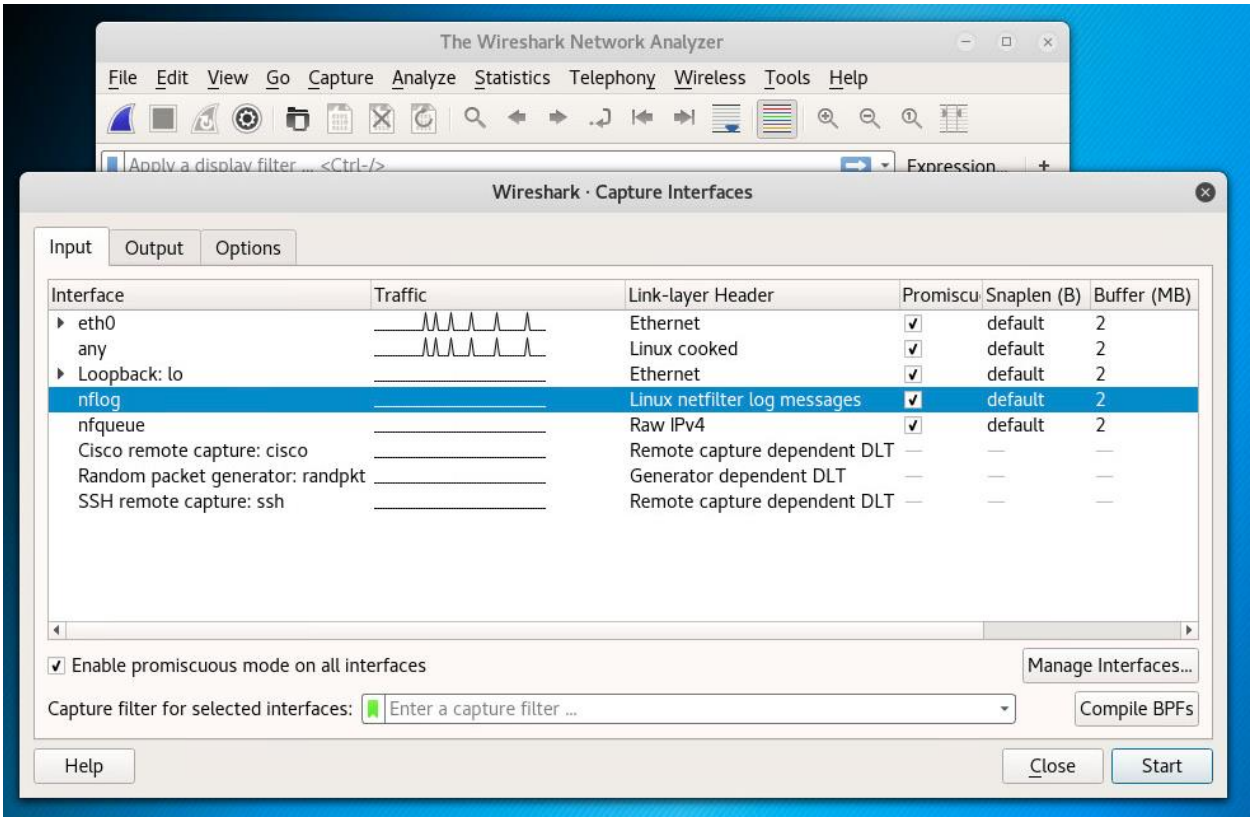
Lab 06 Report



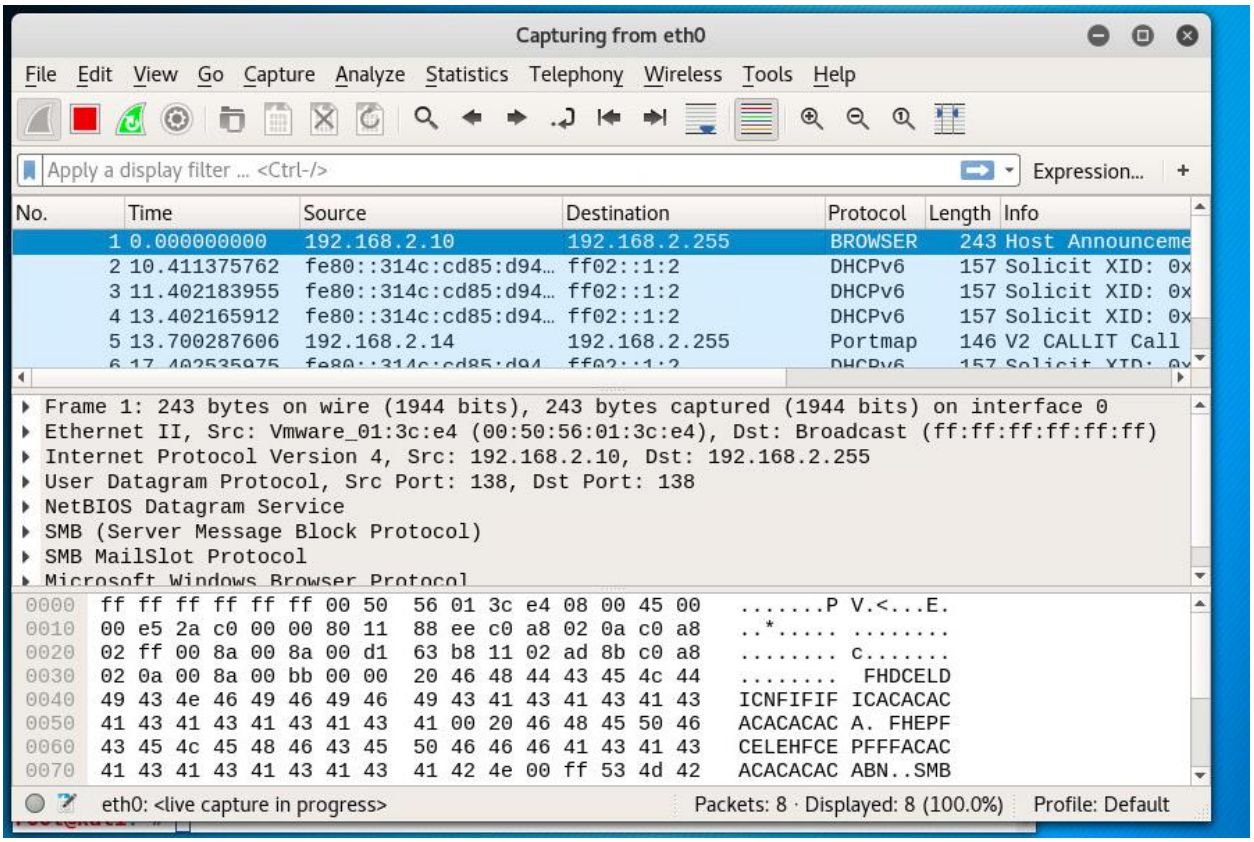

```
c:\tools>nc -help
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -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>_
```

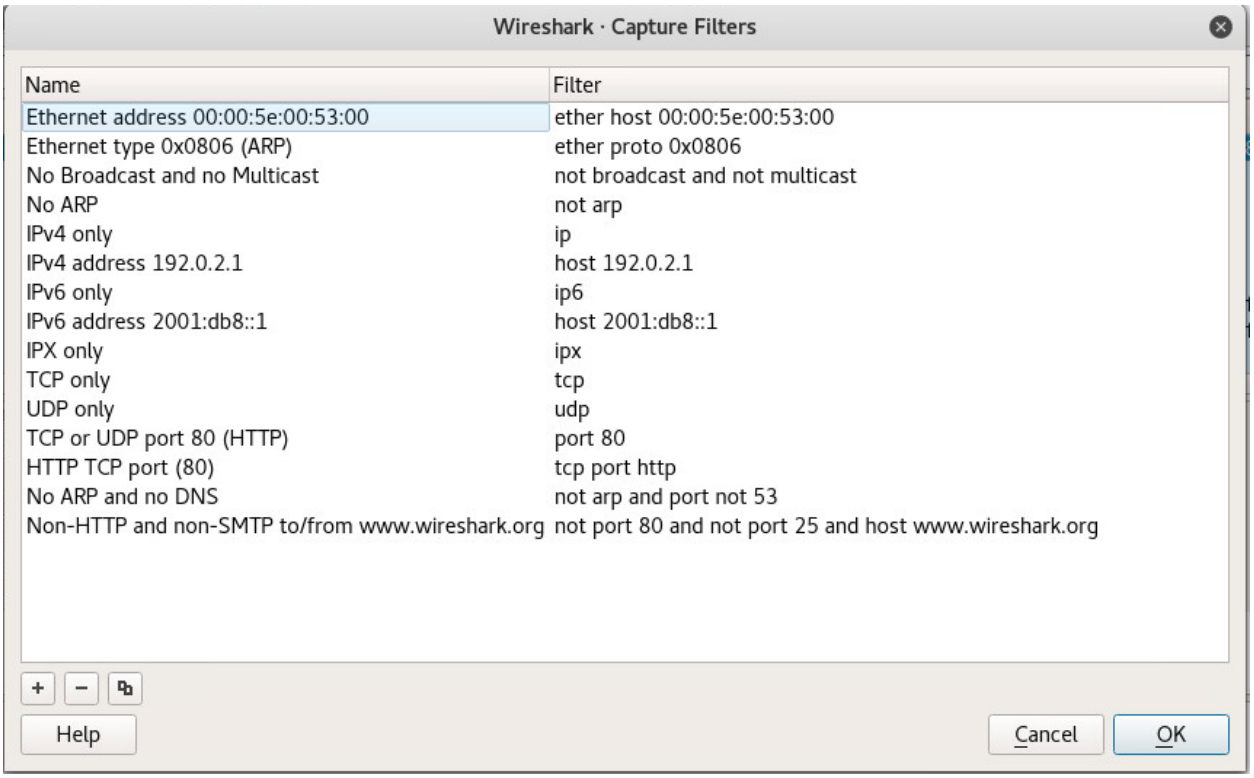
```
root@kali:~# nc 192.168.2.12 1234
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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>
```

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-/>

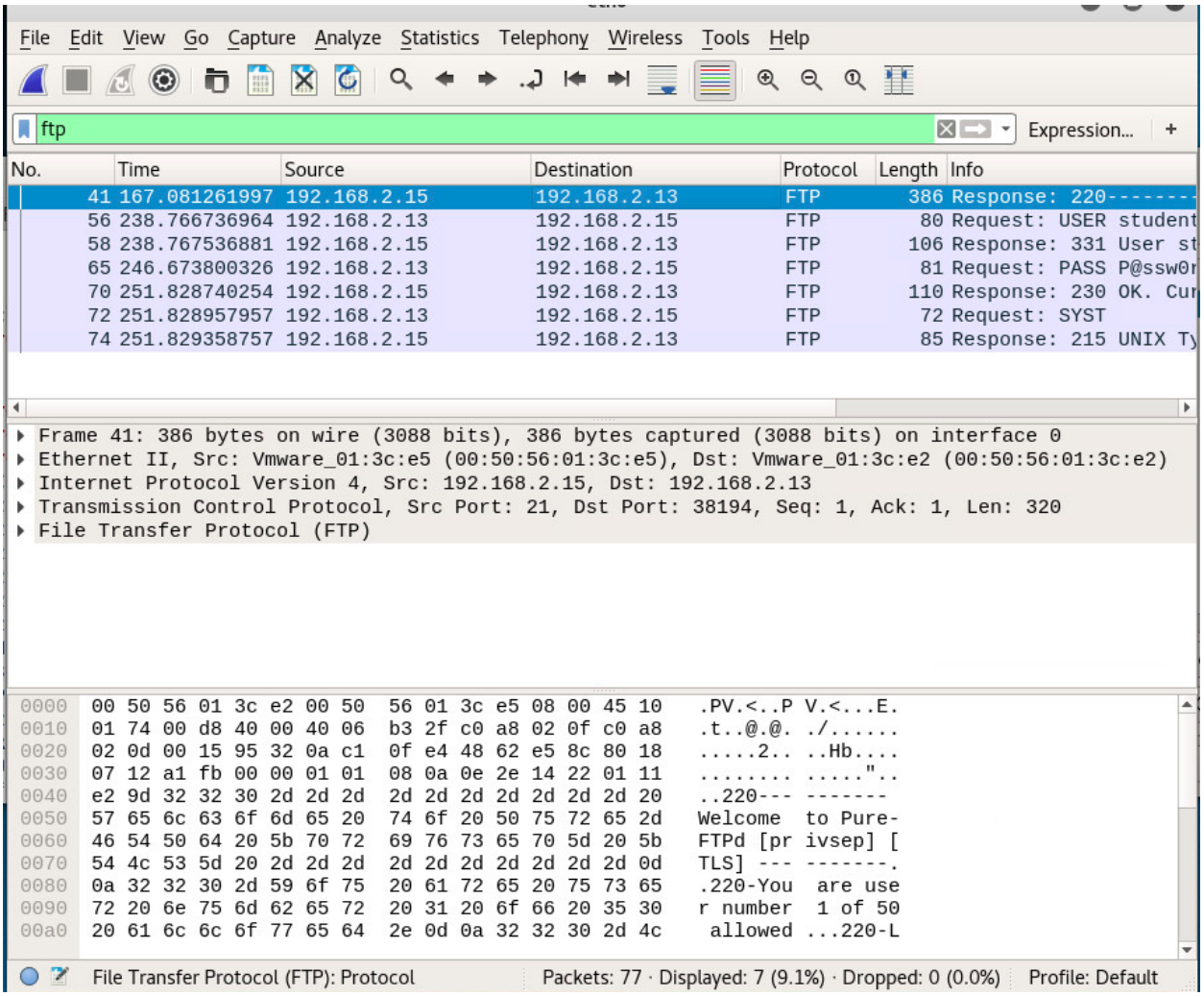
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.11	192.168.2.255	BROWSER	243	Host Announcement W2K3-XXX, Works
2	4.780859103	192.168.2.14	192.168.2.255	Portmap	146	V2 CALLIT Call
3	8.785035549	192.168.2.14	192.168.2.255	Portmap	146	[RPC retransmission of #2]V2 CALL
4	14.789296511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

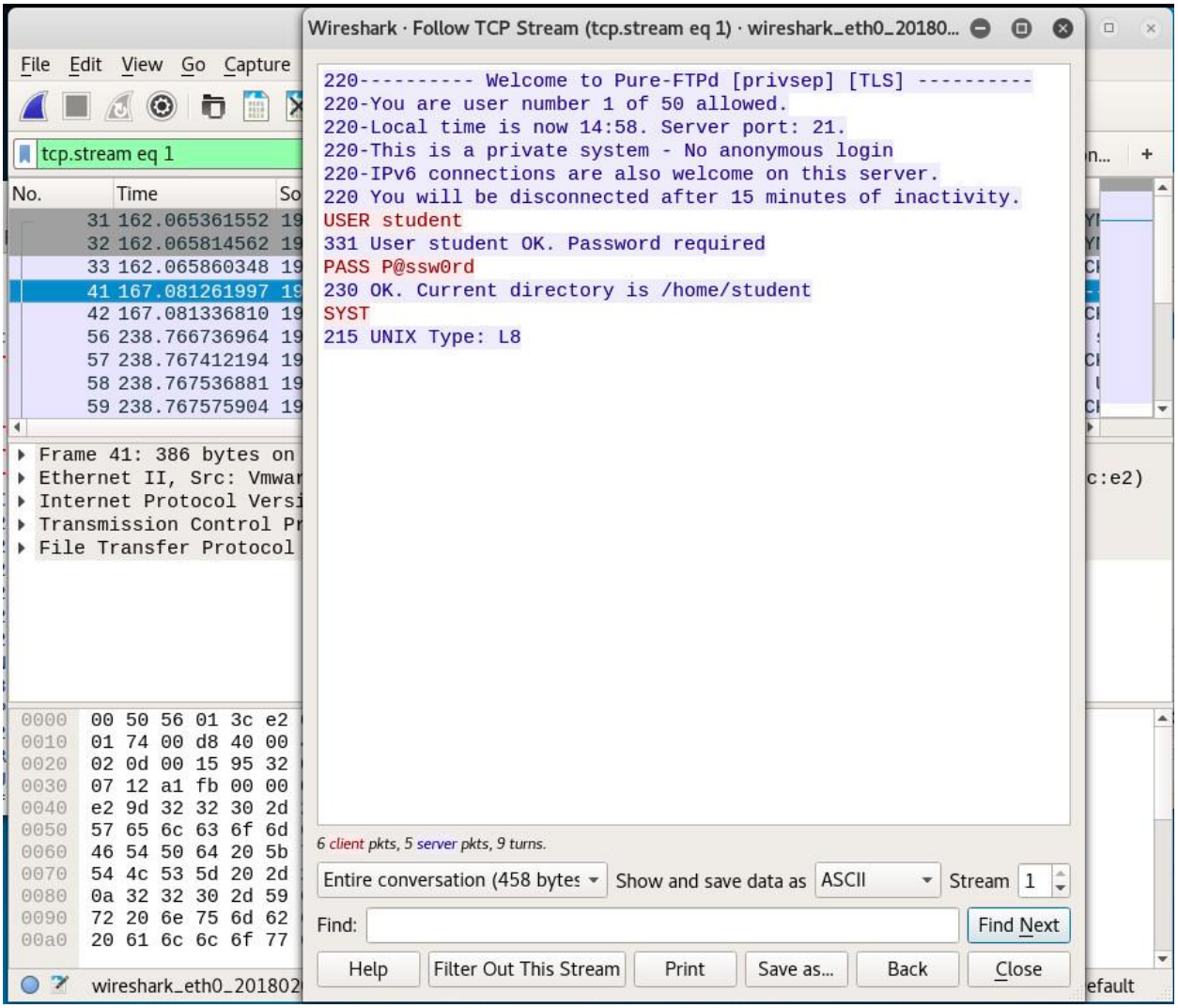
```
▸ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
▸ Ethernet II, Src: Vmware_01:37:30 (00:50:56:01:37:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 192.168.2.11, Dst: 192.168.2.255
▸ User Datagram Protocol, Src Port: 138, Dst Port: 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




Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_eth0_20180...
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
6 client pkts, 5 server pkts, 9 turns.
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
File Edit View Go Capture
tcp.stream eq 1
No. Time
Frame 41: 386 bytes on
Ethernet II, Src: Vmwar
Internet Protocol Versi
Transmission Control Pr
File Transfer Protocol
wireshark_eth0_201802

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.