

ASSIGNMENT - 11

Demonstrate data transmission using FTP and HTTP protocols and analyse the network traffic through Wireshark or tcpdump

FTP

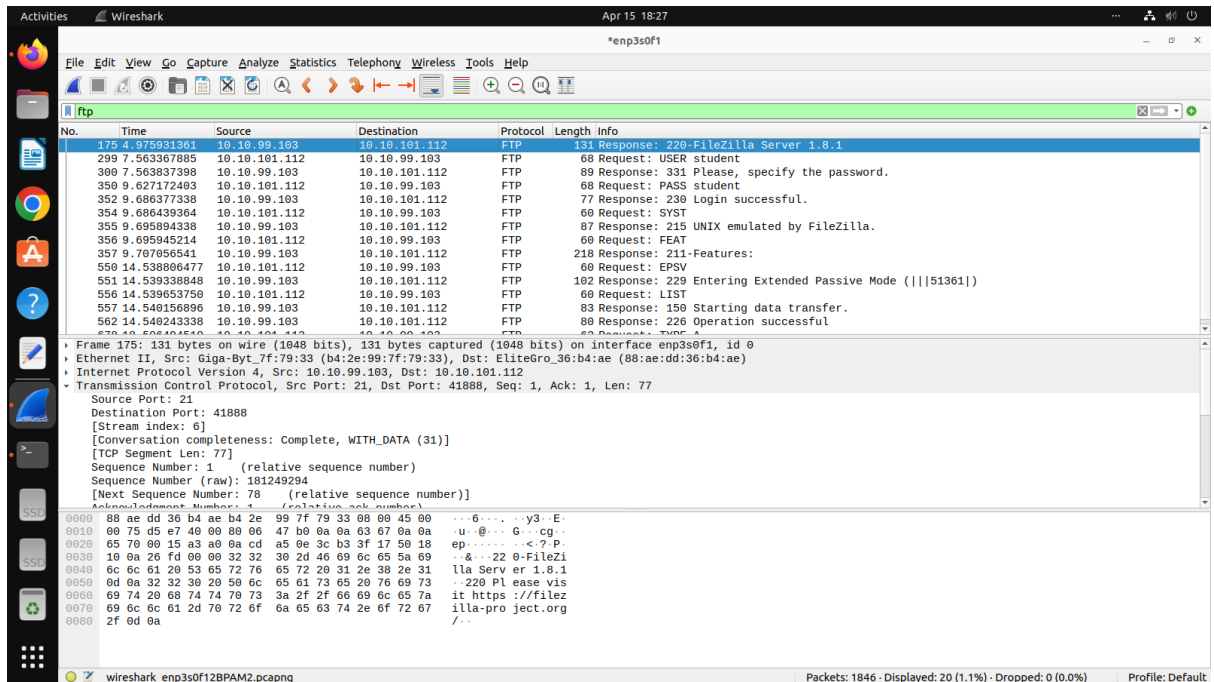
Terminal commands

```
Activities Terminal Apr 15 18:40 student@L08-C46: ~  
ftp> get  
(remote-file) UDP Socket Programming_2.pdf  
usage: get remote-file [local-file]  
ftp> close  
221 Goodbye.  
ftp> exit  
student@L08-C46:~$ ftp 10.10.99.103  
Connected to 10.10.99.103.  
220-FileZilla Server 1.8.1  
220 Please visit https://filezilla-project.org/  
Name (10.10.99.103:student): student  
331 Please, specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> dir  
229 Entering Extended Passive Mode (|||51361|)  
150 Starting data transfer.  
-rw-rw-rw- 1 ftp ftp 107914 Apr 15 05:53 UDP Socket Programming_2.pdf  
226 Operation successful  
ftp> ascii  
200 Type set to A  
ftp> binary  
200 Type set to I  
ftp> hash  
Hash mark printing on (1024 bytes/hash mark).  
ftp> get  
(remote-file) UDP Socket Programming_2.pdf  
usage: get remote-file [local-file]  
ftp> close  
221 Goodbye.  
ftp> exit  
student@L08-C46:~$
```

Tcpdump for FTP

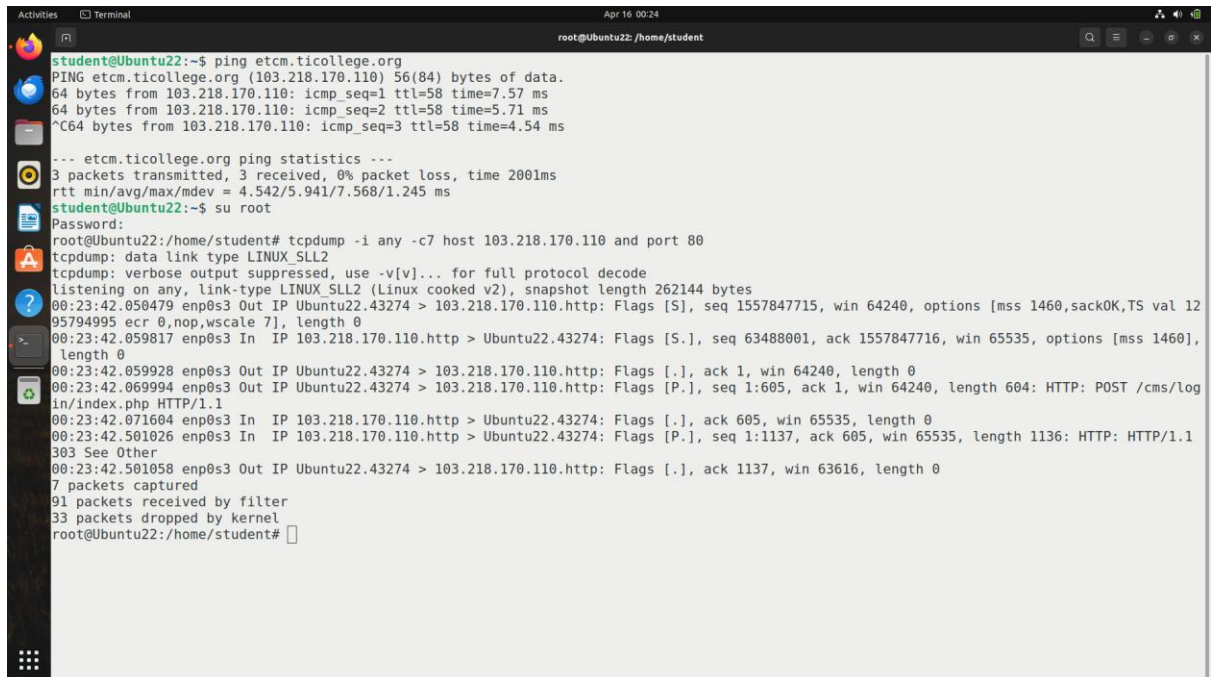
```
Activities Terminal Apr 16 01:10 root@Ubuntu22: /home/ftpuser/ftp  
root@Ubuntu22: /home/ftpuser/ftp# tcpdump -i any -c7 port 21  
tcpdump: data link type LINUX_SLL2  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes  
01:07:22.579359 lo In IP Ubuntu22.40728 > Ubuntu22.ftp: Flags [S], seq 3587127311, win 65535, options [mss 65495,sackOK,TS val 3375206872  
ecr 0,nop,wscale 2], length 0  
01:07:22.579379 lo In IP Ubuntu22.ftp > Ubuntu22.40728: Flags [S.], seq 4179266346, ack 3587127312, win 65483, options [mss 65495,sackOK,  
TS val 3375206872, ecr 3375206872, nop,wscale 7], length 0  
01:07:22.579393 lo In IP Ubuntu22.40728 > Ubuntu22.ftp: Flags [.], ack 1, win 16384, options [nop,nop,TS val 3375206872 ecr 3375206872],  
length 0  
01:07:22.582713 lo In IP Ubuntu22.ftp > Ubuntu22.40728: Flags [P.], seq 1:21, ack 1, win 512, options [nop,nop,TS val 3375206876 ecr 3375  
206872], length 20: FTP: 220 (vsFTPd 3.0.5)  
01:07:22.582800 lo In IP Ubuntu22.40728 > Ubuntu22.ftp: Flags [.], ack 21, win 16384, options [nop,nop,TS val 3375206876 ecr 3375206876],  
length 0  
01:07:27.067445 lo In IP Ubuntu22.40728 > Ubuntu22.ftp: Flags [P.], seq 1:15, ack 21, win 16384, options [nop,nop,TS val 3375211360 ecr 3  
375206876], length 14: FTP: USER ftpuser  
01:07:27.067462 lo In IP Ubuntu22.ftp > Ubuntu22.40728: Flags [.], ack 15, win 512, options [nop,nop,TS val 3375211360 ecr 3375211360], l  
ength 0  
7 packets captured  
18 packets received by filter  
0 packets dropped by kernel  
root@Ubuntu22: /home/ftpuser/ftp#
```

Wireshark for FTP



HTTP

Tcpdump for HTTP



Wireshark for HTTP

Wireshark interface showing an HTTP packet capture on interface enp3s0f1. The packet list displays several HTTP requests and responses. The selected packet (No. 796) is a POST request to /cms/login/index.php. The packet details pane shows the structure of the HTTP request, including the HTML Form URL Encoded body. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
796	15.693237724	10.10.101.112	10.10.100.3	HTTP	670	POST /cms/login/index.php HTTP/1.1 (application/x-www-form-urlencoded)
803	16.007409638	10.10.100.3	10.10.101.112	HTTP	1202	HTTP/1.1 303 See Other (text/html)
805	16.009070330	10.10.101.112	10.10.100.3	HTTP	544	GET /cms/login/index.php?testsession=11547 HTTP/1.1
809	16.103479873	10.10.100.3	10.10.101.112	HTTP	906	HTTP/1.1 303 See Other (text/html)
810	16.104547670	10.10.101.112	10.10.100.3	HTTP	511	GET /cms/ HTTP/1.1
926	16.545331210	10.10.100.3	10.10.101.112	HTTP	73	HTTP/1.1 200 OK (text/html)
1113	19.315830208	10.10.101.112	10.10.100.3	HTTP	533	GET /cms/course/view.php?id=697 HTTP/1.1
1192	19.644433915	10.10.100.3	10.10.101.112	HTTP	71	HTTP/1.1 200 OK (text/html)
1263	20.652223912	10.10.101.112	10.10.100.3	HTTP	500	GET /cms/mod/assign/view.php?id=3919 HTTP/1.1
1332	20.985224194	10.10.100.3	10.10.101.112	HTTP	71	HTTP/1.1 200 OK (text/html)
1350	21.030957091	10.10.101.112	10.10.100.3	HTTP	620	GET /cms/pluginfile.php/17999/assignsubmission_file/submission_files/190806/proc1.c?forc...
1359	22.111750905	10.10.100.3	10.10.101.112	HTTP	1464	HTTP/1.1 200 OK (text/plain)

Frame 796: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits) on interface enp3s0f1, id 0

- Ethernet II, Src: EliteGro_36:b4:ae (88:ae:dd:36:b4:ae), Dst: Ibm_d9:8d:33 (40:f2:e9:d9:8d:33)
- Internet Protocol Version 4, Src: 10.10.101.112, Dst: 10.10.100.3
- Transmission Control Protocol, Src Port: 50776, Dst Port: 80, Seq: 1, Ack: 1, Len: 604
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded

0000 40 f2 e9 d9 8d 33 88 ae dd 36 b4 ae 08 00 45 00 @...3...6...E-
0010 02 90 14 fd 40 00 40 06 45 e4 0a 0a 65 70 0a 0a ...@...E...ep..
0020 64 03 dd c8 00 50 b3 e2 b8 f9 ce bd 1a d9 80 18 d...P... ..
0030 01 f6 e0 09 00 00 01 08 0a a8 4d 02 46 02 22M.F..
0040 47 8b 50 4f 53 54 20 2f 03 6d 73 2f 6c 6f 67 69 G-POST / cms/logi
0050 6e 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 50 n/index.php HTTP
0060 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 74 63 6d /1.1-Host: etcm
0070 2e 74 69 63 6f 6c 6c 65 67 65 2e 6f 72 67 0d 0a .ticolle ge.org..
0080 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 0f 7a 69 User-Age nt: Mozi
0090 6c 6c 61 2f 35 2e 30 20 20 50 31 31 3b 20 55 62 lla/5.0 (X11; Ub
00a0 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f untu; Li nux x86_
00b0 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65 64; rv:1.09.0) Ge

Packets: 1506 · Displayed: 12 (0.8%) Profile: Default