Lamar Roulhac

FTP Traffic Analysis and Security Assessment

Objectives of the lab- The objectives of this lab were to practice command-line packet tracing on a Windows machine using Wireshark to analyze network traffic, and capture FTP packets to see the security vulnerabilities of an unencrypted FTP session.

Background- Packet analysis is a technique in networking and cybersecurity that allows professionals to monitor, troubleshoot, and secure network communications. FTP is an early internet protocol used for transferring files between a client and a server. It is insecure as it transmits credentials and data in plaintext rather than it being encrypted.

Procedures

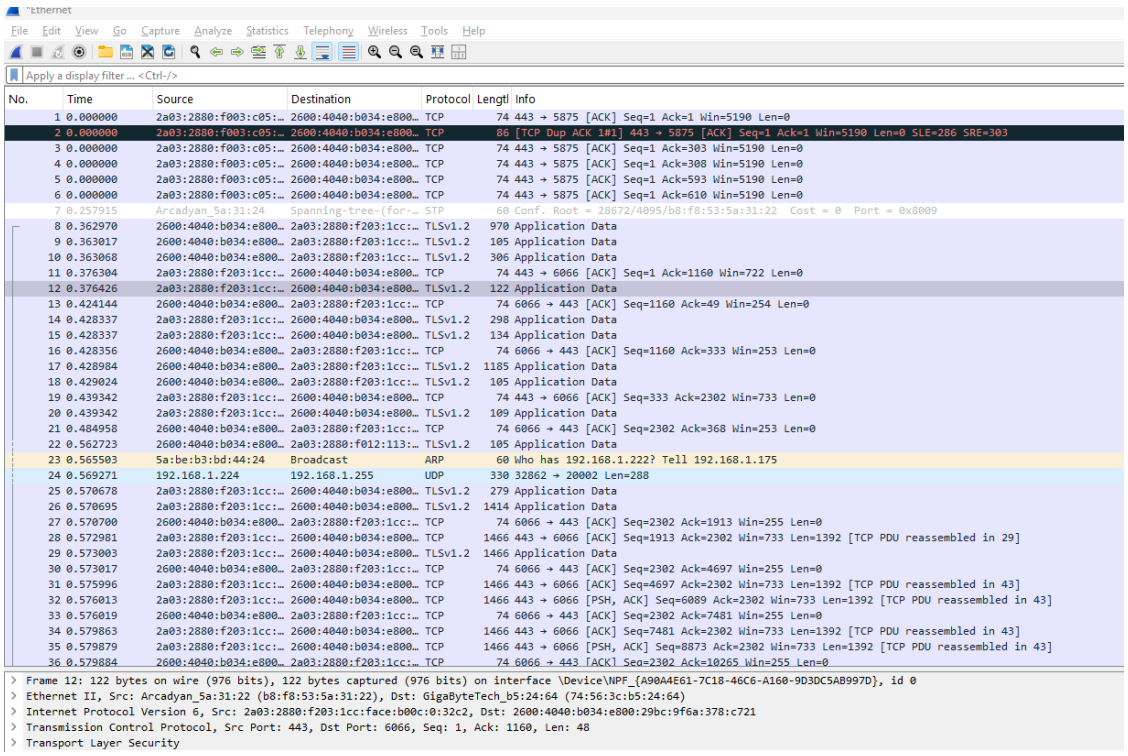
Part 1: Environment Setup and Initial Packet Capture

Task 1:

First i opened Wireshark and started a packet capture on the ens33 traffic, i then used the second VM to ping amazon to generate ICMP packets with the following command.

```
ping www.amazon.com -t
```

After 10 seconds I stopped the capture and took a screenshot of the network interface information as seen in **Figure 1**.

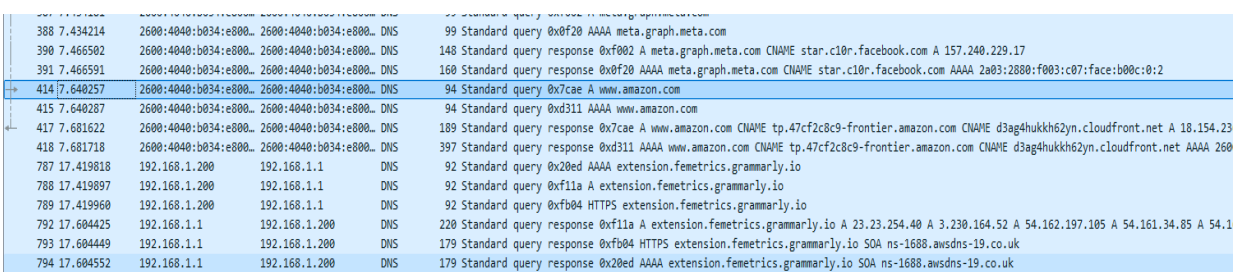


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	74	443 → 5875 [ACK] Seq=1 Ack=1 Win=5190 Len=0
2	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	86	[TCP Dup ACK 1#1] 443 → 5875 [ACK] Seq=1 Ack=1 Win=5190 Len=0 SLE=286 SRE=303
3	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	74	443 → 5875 [ACK] Seq=1 Ack=303 Win=5190 Len=0
4	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	74	443 → 5875 [ACK] Seq=1 Ack=308 Win=5190 Len=0
5	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	74	443 → 5875 [ACK] Seq=1 Ack=593 Win=5190 Len=0
6	0.000000	2a03:2880:f003:c05:…	2600:4040:b034:e800…	TCP	74	443 → 5875 [ACK] Seq=1 Ack=610 Win=5190 Len=0
7	0.257915	Arcadyan_5a:31:24	Spanning-tree-(for-…	STP	60	Conf. Root = 28672/4095/b8:f8:53:5a:31:22 Cost = 0 Port = 0x8009
8	0.362970	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TLSv1.2	970	Application Data
9	0.363017	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TLSv1.2	105	Application Data
10	0.363068	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TLSv1.2	306	Application Data
11	0.376304	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	74	443 → 6066 [ACK] Seq=1 Ack=1160 Win=722 Len=0
12	0.376426	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	122	Application Data
13	0.424144	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=1160 Ack=49 Win=254 Len=0
14	0.428337	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	298	Application Data
15	0.428337	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	134	Application Data
16	0.428356	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=1160 Ack=333 Win=253 Len=0
17	0.428984	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TLSv1.2	1185	Application Data
18	0.429024	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TLSv1.2	105	Application Data
19	0.439342	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	74	443 → 6066 [ACK] Seq=333 Ack=2302 Win=733 Len=0
20	0.439342	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	109	Application Data
21	0.484958	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=2302 Ack=368 Win=253 Len=0
22	0.562723	2600:4040:b034:e800…	2a03:2880:f012:113:…	TLSv1.2	105	Application Data
23	0.565503	5a:be:b3:bd:44:24	Broadcast	ARP	60	Who has 192.168.1.222? Tell 192.168.1.175
24	0.569271	192.168.1.224	192.168.1.255	UDP	330	32862 → 20002 Len=288
25	0.570678	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	279	Application Data
26	0.570695	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	1414	Application Data
27	0.570700	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=2302 Ack=1913 Win=255 Len=0
28	0.572981	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	1466	443 → 6066 [ACK] Seq=1913 Ack=2302 Win=733 Len=1392 [TCP PDU reassembled in 29]
29	0.573003	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TLSv1.2	1466	Application Data
30	0.573017	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=2302 Ack=4697 Win=255 Len=0
31	0.575996	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	1466	443 → 6066 [ACK] Seq=4697 Ack=2302 Win=733 Len=1392 [TCP PDU reassembled in 43]
32	0.576013	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	1466	443 → 6066 [PSH, ACK] Seq=6089 Ack=2302 Win=733 Len=1392 [TCP PDU reassembled in 43]
33	0.576019	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=2302 Ack=7481 Win=255 Len=0
34	0.579863	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	1466	443 → 6066 [ACK] Seq=7481 Ack=2302 Win=733 Len=1392 [TCP PDU reassembled in 43]
35	0.579879	2a03:2880:f203:1cc:…	2600:4040:b034:e800…	TCP	1466	443 → 6066 [PSH, ACK] Seq=8873 Ack=2302 Win=733 Len=1392 [TCP PDU reassembled in 43]
36	0.579884	2600:4040:b034:e800…	2a03:2880:f203:1cc:…	TCP	74	6066 → 443 [ACK] Seq=2302 Ack=10265 Win=255 Len=0

```
> Frame 12: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{A90A4E61-7C18-46C6-A160-9D3DC5AB997D}, id 0
> Ethernet II, Src: Arcadyan_5a:31:22 (b8:f8:53:5a:31:22), Dst: GigaByteTech_b5:24:64 (74:56:3c:b5:24:64)
> Internet Protocol Version 6, Src: 2a03:2880:f203:1cc:face:b00c:0:32c2, Dst: 2600:4040:b034:e800:29bc:9f6a:378:c721
> Transmission Control Protocol, Src Port: 443, Dst Port: 6066, Seq: 1, Ack: 1160, Len: 48
> Transport Layer Security
```

Figure 1: Ping ICMP Traffic

I then located the first packet related to the ping command **(Figure 2)** which also showed its source and destination IP addresses seen in **Figure 3** in **Figure 4** you can see my machine's Ip to prove this is the first packet that came from my machine., and found the DNS reply packet **(Figure 5)**.



388	7.434214	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	99	Standard query 0x0f20 AAAA meta.graph.meta.com
390	7.466502	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	148	Standard query response 0xf002 A meta.graph.meta.com CNAME star.c10r.facebook.com A 157.240.229.17
391	7.466591	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	160	Standard query response 0x0f20 AAAA meta.graph.meta.com CNAME star.c10r.facebook.com AAAA 2a03:2880:f003:c07:face:b00c:0:2
414	7.640257	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	94	Standard query 0x7cae A www.amazon.com
415	7.640287	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	94	Standard query 0xd311 AAAA www.amazon.com
417	7.681622	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	189	Standard query response 0x7cae A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net A 18.154.23
418	7.681718	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	397	Standard query response 0xd311 AAAA www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net AAAA 260
787	17.419818	192.168.1.200	192.168.1.1	DNS	92	Standard query 0x20ed AAAA extension.femetrics.grammarly.io
788	17.419897	192.168.1.200	192.168.1.1	DNS	92	Standard query 0xf11a A extension.femetrics.grammarly.io
789	17.419960	192.168.1.200	192.168.1.1	DNS	92	Standard query 0xfb04 HTTPS extension.femetrics.grammarly.io
792	17.604425	192.168.1.1	192.168.1.200	DNS	220	Standard query response 0xf11a A extension.femetrics.grammarly.io A 23.23.254.40 A 3.230.164.52 A 54.162.197.105 A 54.161.34.85 A 54.1
793	17.604449	192.168.1.1	192.168.1.200	DNS	179	Standard query response 0xfb04 HTTPS extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
794	17.604552	192.168.1.1	192.168.1.200	DNS	179	Standard query response 0x20ed AAAA extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk

Figure 2: First Packet Related to Ping

```
> Frame 414: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{A90A4E61-7C18-46C6-A160-9D3DC5AB997D}, id 0
> Ethernet II, Src: GigaByteTech_b5:24:64 (74:56:3c:b5:24:64), Dst: Arcadyan_5a:31:22 (b8:f8:53:5a:31:22)
> Internet Protocol Version 6, Src: 2600:4040:b034:e800:29bc:9f6a:378:c721, Dst: 2600:4040:b034:e800::1
> User Datagram Protocol, Src Port: 49572, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7cae
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.amazon.com: type A, class IN
    [Response In: 417]
```

Figure 3: Source and Destination IP

```
Connection-specific DNS Suffix  . : mynetworksettings.com
IPv6 Address. . . . . . . . . . . : 2600:4040:b034:e800:88d5:232b:d563:49c5
Temporary IPv6 Address. . . . . . : 2600:4040:b034:e800:183:f5c:a38:ceed
Temporary IPv6 Address. . . . . . : 2600:4040:b034:e800:29bc:9f6a:378:c721
Link-local IPv6 Address . . . . . : fe80::ca95:3f1:5055:e42d%15
IPv4 Address. . . . . . . . . . . : 192.168.1.200
```

Figure 4: My Machine's IP

390	7.466502	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	148	Standard query response 0xf002 A meta.graph.meta.com CNAME star.c10r.facebook.com A 157.240.229.17
391	7.466591	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	160	Standard query response 0x0f20 AAAA meta.graph.meta.com CNAME star.c10r.facebook.com AAAA 2a03:2880:f003:c07:face:b00c:0:2
414	7.640257	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	94	Standard query 0x7cae A www.amazon.com
415	7.640287	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	94	Standard query 0xd311 AAAA www.amazon.com
417	7.681622	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	189	Standard query response 0x7cae A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net A 18.154.236.231
418	7.681718	2600:4040:b034:e800…	2600:4040:b034:e800…	DNS	397	Standard query response 0xd311 AAAA www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net AAAA 2600:9000:2501:c400:7:
787	17.419818	192.168.1.200	192.168.1.1	DNS	92	Standard query 0x20ed AAAA extension.femetrics.grammarly.io
788	17.419897	192.168.1.200	192.168.1.1	DNS	92	Standard query 0xf11a A extension.femetrics.grammarly.io
789	17.419960	192.168.1.200	192.168.1.1	DNS	92	Standard query 0xfb04 HTTPS extension.femetrics.grammarly.io
792	17.604425	192.168.1.1	192.168.1.200	DNS	220	Standard query response 0xf11a A extension.femetrics.grammarly.io A 23.23.254.40 A 3.230.164.52 A 54.162.197.105 A 54.161.34.85 A 54.163.141.145 A 52.205
793	17.604449	192.168.1.1	192.168.1.200	DNS	179	Standard query response 0xfb04 HTTPS extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
794	17.604552	192.168.1.1	192.168.1.200	DNS	179	Standard query response 0x20ed AAAA extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk

Figure 5: DNS Reply Packet

Part 2: Virtualized Environment and FTP Analysis

Task 3: Install and Configure an Insecure FTP Server on Ubuntu

1. First, I Installed vsftpd since I didn't have it installed then I checked to see if the program was running using the command:

   `ps -ef | grep "ftp"`

   I then edited the `vsftpd.conf` file to enable write permissions by uncommenting the following line: write_enable=YES.

Task 4: Capture FTP Traffic

I then started Wireshark on the FTP server machine and began capturing packets and used the second Linux VM to connect to the FTP server using the command

```
ftp 192.168.192.128
```

After that i got a prompt to login to the server and logged in with the same username and password as the host machine. I then executed the help command to see available FTP commands and then exited the session.

I stopped the Wireshark capture and located the FTP login packets by filtering for FTP on the top search. As seen in **Figure 6** the username and password are seen in Wireshark in plaintext.

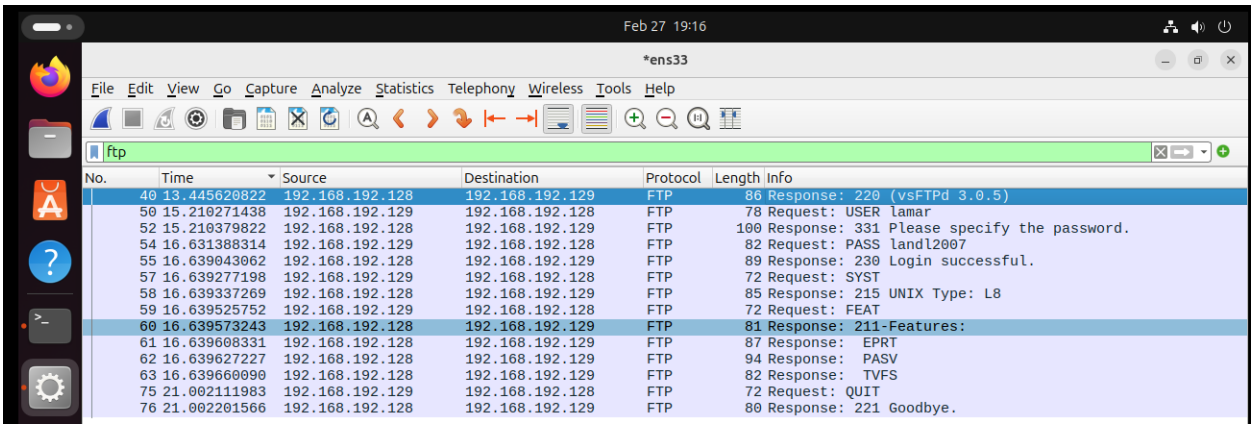


Figure 6: FTP Traffic

Analysis Questions

1. **Observations About Password Capture:** The FTP login information was sent in plaintext, which is dangerous because it can lead to a malicious person taking advantage of that vulnerability.
2. **Securing FTP:** To reduce the security risks of FTP some solutions are:
    a. Using SFTP or FTPS instead of the standard FTP. It's like using http rather than using https.
    b. Added firewall rules to limit access to trusted IP addresses.
    c. Using encryption, such as VPNs, to secure data in transit.

In conclusion this lab shows us the security risks that come with FTP by capturing unencrypted credentials using Wireshark. Also, showing why encryption is important in network communications. Without encryption we risk vulnerability in our systems.