**22L\_7925**

**Faizan Saleh**

**BSE-6C1**

**CN-LAB**

Q1:

**Ftp.mcaffe doesn’t work anymore so I will skip Step 1-4**

**Step 5:**

**1.**

By analyzing port 20 and port 21

**Port 20:** Meant for data transfer over FTP

**Port 21:** Meant for request and responses for FTP

#### **FTP Communication(Port 21)**

1. **(Packet 86)** Client initiates a connection
2. **(Packet 87)** Server acknowledges the request.
3. **(Packet 88)** Client completes the handshake: Connection is established on port 21.
4. **(Packet 89)** 220 spftp/1.0.0000 Server [195.89.6.167]
5. **(Packets 94-100)** Client logs in with USER and PASS commands
6. **(Packet 104-105)** Client sends the PORT command
7. **(Packet 106-107)** Client requests a directory listing (NLST)

#### **FTP Data Transfer (Port 20)**

1. **(Packet 108)** Server initiates a data connection
2. **(Packet 122)** Client acknowledges
3. **(Packet 125-127)** Server sends data
4. **(Packet 128-131)** Connection closes after data transfer

**FTP Communication (Port 21)**

1. **(Packet 151-152)** Client requests another data connection
2. **(Packet 153)** Client requests file retrieval
3. **(Packet 155)** Server prepares to send
4. **(Packet 156-157)** Data connection setup
5. **(Packet 161)** FTP Data transfer
6. **(Packets 162-165)** Data connection closes.

**2.**

**(Packet 89)** Server greets the client: 220 spftp/1.0.0000 Server [195.89.6.167]

**(Packet 94)** Client requests login: USER anonymous

**(Packet 96)** Server asks for a password: 331 Password required for USER.

**(Packet 99)** Client sends password: PASS

**(Packet 100)** Server grants access: 230-

**(Packet 104)** Client sets up data connection: PORT 192,168,1,2,63,213

**(Packet 105)** Server confirms data connection: 200 PORT command successful.

**(Packet 106)** Client requests file listing: NLST

**(Packet 107)** Server opens data connection for listing: 150 Opening ASCII mode data connection for /.

**(Packet 125)** Server completes transfer: 226 Transfer Complete

**(Packet 127)** FTP data transfer occurs (directory listing): 125 bytes (PORT) (NLST)

**(Packet 151)** Client requests another data connection: PORT 192,168,1,2,63,214

**(Packet 152)** Server confirms: 200 PORT command successful.

**(Packet 153)** Client requests file download: RETR legal.txt

**(Packet 155)** Server prepares file transfer: 150 Opening ASCII mode data

**(Packet 160)** Server completes file transfer: 226 Transfer Complete

**(Packet 161)** FTP data transfer occurs

**(Packet 173)** Client requests to disconnect: QUIT

**(Packet 175)** Server acknowledges and ends session: 221 Goodbye.

**Q2:**

**1.Are ICMP messages sent over UDP or TCP?**

No, because ICMP is itself a protocol.

**2. What is the link-layer (e.g., Ethernet) address of the host?**

Source: TpLinkTechno\_87:05:fe (c0:4a:00:87:05:fe)

**3. Which kind of request is sent through these ICMP packets?**

Echo pings requests are made 4 times

**4. How many requests are sent through the host?**

4 as I said earlier

**5. What is the IP address of your host? What is the IP address of the destination host?**

**IP address of host:** 92.168.33.110

**IP of Destination:** 172.217.27.36

**6. Why is it that an ICMP packet does not have source and destination port numbers?**

Because Ports doesn’t exist on network layer and ICMP is a network layer protocol unlike TCP and UDP at transport layer.

**7. What values in the ICMP request message differentiate this message from the**

**ICMP reply message?**

Type value is 8 in request and 0 in reply.

**8. Examine one of the ping request packets sent by your host. What are the ICMP**

**type and code numbers? What other fields does this ICMP packet have? How**

**many bytes are the checksum, sequence number and identifier fields?**

**Type**: 8 (Echo (ping) request) (**1 byte**)

**Code**: 0 (**1 bytes**)

**Checksum**: 0x4d38 [correct] (**2 bytes**)

**Identifier** (BE): 1 (0x0001) (**2 bytes**)

**Sequence Number** (BE): 35 (0x0023) (**2 bytes**)

**Data** , (Random size) for now its 32 bytes)

**9. Examine the corresponding ping reply packet. What are the ICMP type and code**

**numbers? What other fields does this ICMP packet have? How many bytes are the**

**checksum, sequence number and identifier fields?**

**Type**: 0 (Echo (ping) reply) (**1 byte**)

**Code**: 0 (**1 bytes**)

**Checksum**: 0x5538 [correct] (**2 bytes**)

**Identifier** (BE): 1 (0x0001) (**2 bytes**)

**Sequence Number** (BE): 35 (0x0023) (**2 bytes**)

**Data** , (Random size) for now its 32 bytes)

**10. Examine the packet no 56. What are the ICMP type and code numbers? Why is the**

**IP and TCP Header included in the ICMP Header? What does these headers**

**Depict?**

Type: 3 (Destination unreachable)

Code: 3 (Port unreachable)

IP and TCP headers are included so that we can find original packet that caused the error

It will help identify which request failed