**Lab-4**

**Lab Statement 1: Capturing FTP packets using Wireshark**

1. **FTP uses two port numbers: 20 and 21. Apply tcp.port==20 and tcp.port==21. Analyze the result and write down the purposes of these two ports for FTP.**

**Answer:** Port numbers 21 and 20 are used for FTP. Port 21 is used to establish and manage the connection between the 2 computers (or hosts) and port 20 is used to transfer data (via the Data channel).

1. **Filter out each packet using either FTP or FTP-DATA Protocol (using ftp || ftp-data filter). Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt (screenshot show above). Also look for Response Code and Response Arg in the FTP Header for each packet**

**Answer:**

Packet 89 - Response: 220 spftp/1.0.0000 Server [195.89.6.167]

Packet 94 - Request: USER anonymous

Packet 96 - Response: 331 Password required for USER.

Packet 99 - Request: PASS

Packet 100 - Response: 230-

Packet 104 - Request: PORT 192,168,1,2,63,213

Packet 105 - Response: 200 PORT command successful.

Packet 106 - Request: NLST

Packet 107 - Response: 150 Opening ASCII mode data connection for /.

Packet 125 - Response: 226 Transfer Complete

Packet 127 - FTP Data: 125 bytes (PORT) (NLST)

Packet 151 - Request: PORT 192,168,1,2,63,214

Packet 152 - Response: 200 PORT command successful.

Packet 153 - Request: RETR legal.txt

Packet 155 - Response: 150 Opening ASCII mode data connection for legal.txt (1415 bytes).

Packet 160 - Response: 226 Transfer Complete

Packet 161 - FTP Data: 1415 bytes (PORT) (RETR legal.txt)

Packet 173 - Request: QUIT

Packet 175 - Response: 221 Goodbye.

**Lab Statement 3: Analyzing ICMP Packets using Wireshark**

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

**Answer:** None

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

**Answer:** Source: (60:67:20:55:7b:ac)

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

**Answer:** Echo (ping) request is sent.

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

**Answer:** 4 echo (ping) requests are sent.

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

**Answer:** Source IP: 192.168.33.110 Destination IP: 172.217.27.36

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

**Answer:** The ICMP packet does not have source and destination port numbers because it is designed to communicate network-layer information between hosts and routers, not between application layer processes.

1. **What values in the ICMP request message differentiate this message from the ICMP reply message?**

**Answer:** Type field in the ICMP request message has a value of 8 whereas type field in the ICMP reply message has a value of 0.

1. **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?**

**Answer:** Type: 8, Code: 0. Other fields are Checksum, Identifier and Sequence Number. Checksum, sequence number and identifier fields are 2 bytes each.

1. **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?**

**Answer:** Type: 0, Code: 0. Other fields are Checksum, Identifier and Sequence Number. Checksum, sequence number and identifier fields are 2 bytes each.

1. **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?**

**Answer:** Type: 3, Code: 3. The IP and TCP headers of the original packet that caused the ICMP message are included in the ICMP payload. This inclusion serves an essential purpose and provides important context to the sender.