Data Communications Laboratory
TCP & FTP

Your Name:

Your Student ID:

Documentation Task 1.

1. What is the name and IP address of the FTP server contacted? In which packets can this information be found (hint: you will need to clear the filter and examine the packets just before the first packets on port 21)?

Name: ftp.ftpplanet.com

IP Address (src address of ftp Response): 156.21.1.54

2. What is the port used on the server?

There are 2 connections.

Port 21 is used for credentials and the LIST reply to the client.

Port 20 is used for the file transfer (send).

3. What port is being used on the client?

There are 2 connections.

Port 2011 is used for credentials and the LIST request to the server.

Port 5001 is used for the file transfer (receive).

4. Identify the three-way handshake that established the TCP connection between the client and server. Which packet numbers does the three-way handshake appear in?

There appears to be 2 handshakes happening.

The first occurs in packets 79, 83 and 84. This is establishing a connection with the server and is used to communicate our credentials and LIST request.

The second occurs in packets 161, 162, 172. This is establishing a connection with the server and is used to send the ftp response from the server to client.

5. The TCP connection is set by a SYN message from the FTP client, a SYN/ACK from the FTP server and an ACK from the client. What is happening in each of these messages?

Let's start with first packet:

There is a SYN packet sent from the client to the server. This packet includes a sequence number which is used in request messages from client to server to help the server identify the order of completion of packets being received.

The second packet:

There is a SYN / ACK packet sent from the server to the client. This packet also includes a similar SYN message that the client sent to the server but with the server's own sequence number. This part of the messages acts the exact same. The ACK part of the message is the acknowledgement of the first SYN packet from the client.

The third packet:

There is a final ACK packet from the client to the server, acknowledging that the client received the SYN packed from the server's SYN ACK packet.

6. Once the connection is established the FTP server sends a message saying it is ready. What packet carries this message?

There is a Response 220 Packet that tells the client that the server is ready.

7. What information in the packet makes you think you have the correct packet?

In Wireshark, inside of the FTP layer, the 220 has a descriptor that says "Service ready for new user (220)"

8. The user then types a user ID and a password. What packet numbers are involved in this exchange? Are the characters in the user ID sent individually or in a single packet? What is the username?

The packet numbers involved in this exchange are 124, 126, 149, 152.

The characters for this user ID (I am assuming this means the USER request command) are all sent in 1 packet. There is a separate packet for the password.

The username is anonymous.

9. Can you see the password? If so, what is it?

We can see the password. The password is apassword.

10. What is your conclusion about the security of FTP? Isn't packet sniffing fun?

FTP is not secure as messages are sent in plain text. This means that if anyone captured these packets, they would be able to identify the username, password and any communication or files transferred easily.

11. Find the single FTP command issued to the server. What is it and what message is it in?

The FTP command issued to the server is a LIST command and is in message 160.

12. In what packet(s) is the actual data sent from the server in response to that command? NOTE: that this will be in the FTP-DATA packets sent from the server on port 20.

The FTP-DATA packets are sent in messages 173 and 175 on port 20.

13. Why do FTP and other protocols use a separate channel for command and data communications?

There are 2 channels so that the client and server can identify what is a communication packet and what is a data packet. This also ensures that the command channel is not flooded and can also allow for easier communication to provide commands during data packets being transferred.

14. In what packet does the client say it wants to end the FTP session?

The client sends a QUIT request to the server in message 302 to tell the server it wants to end the FTP session.

15. Which flag is set in this packet?

The ACK and PSH flags are set in the TCP layer and the QUIT command is set in the FTP layer.

16. In what packet does the server respond?

The server responds in packets 303.

17. What messages are used to close the TCP connection?

There is a FIN / ACK message sent from the server to the client to signal that the server is closing (finishing) the connection. The client sends an ACK packet back to the server, acknowledging the closure of the connection.

18. Which end – client or server – actually terminates the TCP connection?

The server terminates the TCP connection after receiving the ACK message from the client for the servers FIN message.

We can identify this, because after the ACK message from the client is sent, the client sends a RESET ACK message to the server, of which the server never responds.

19. What are the sequence numbers used in these messages?

The sequence numbers used in these messages is 182 and 71.

20. Compare the sequence numbers displayed in Wireshark's analysis against the actual values shown in the raw packet in the bottom pane – are they the same? Can you suggest why?

They are VERY different.

This is because Wireshark is being smart, and the sequence is relative to the first RAW sequence from the connection. This helps us puny humans identify which message is being sent.

The RAW sequence number is the actual number that the server and the client are using the confirm order and packet size communication between each other.

21. Select the first message in the command (port 21) conversation. Use the "Follow TCP Stream" option in the Wireshark Analyze Menu to see a summary of the information that is exchanged between the client and server. Does the result show the password?

Yes, the password results is shown.

22. Select the first message on the data port (20). Display it as a stream – what data is being transferred?

This shows all files that were downloaded.

23. Identify the three-way handshake for this connection – which end is initiating the connection: the client or the server?

The server is initiating this connection with the client. This connection is the data port to being transferring the files.

24. Find the PORT command issued by the FTP client. How does the FTP server know where to send the data from this message?

In this PORT request packet from the client to the server, there is an “Active Port” section that lets the server know which port the client is listening for data. This is a 5001 in this packet.

25. In packets 174 and 178, the server sends two messages to the client (“125 Transferring directory” and “226 Transfer complete”) but there is only one ACK message from the client following both of these. Explain why two messages can have only one ACK.

I am assuming that because the data is being transferred on a different port, only an acknowledgment is required for the transfer complete message.