CSSE 490-- Network Security

Rose-Hulman Institute of Technology

Concept lab 2: Exploring TCP

Learning Objectives

At the end of this concept lab, you should be able to:

- Identify the steps involved in the `TCP` protocol.
- Expire the `TCP` session setup steps.
- Identify vulnerabilities in the `TCP` protocol.

Name: _____

Question	Points	Score
Question 1	5	
Question 2	5	
Question 3	5	
Question 4	5	
Question 5	5	
Question 6	5	
Question 7	5	
Question 8	5	
Question 9	5	
Question 10	5	
Question 11	5	
Question 12	5	
Question 13	5	
Question 14	5	
Question 15	5	
Question 16	5	
Question 17	5	
Question 18	5	
Question 19	5	
Question 20	5	
Question 21	5	
Question 22	5	
Question 23	5	
Question 24	5	
Question 25	5	
Question 26	5	
Question 27	5	
Question 28	15	
Total:	150	

1 Experiment I

The questions below refer to `experiment 1`.

Question 1. (5 points) How does a client initiate a connection request with the server?

Question 2. (5 points) If the server is ready to accept a connection, how does it tell the client so?

Question 3. (5 points) What does the client do when it receives the server's confirmation?

Question 4. (5 points) Open the `TCP` header fields, which part of the `TCP` header dictate the type of the packet?

Question 5. (5 points) Why do you think the server expects the client to respond back to confirm the connection's establishment (i.e., why do we need a third packet)?

2 Experiment II

The questions below refer to `experiment 2`.

Question 6. (5 points) What does the server container do when it receives a connection request for a service that it does not normally provide?

Question 7. (5 points) What happens at the client when it receives that information?

Question 8. (5 points) Do you notice any potential problems with this particular option in the `TCP` protocol?

3 Experiment III

The questions below refer to `experiment 3`.

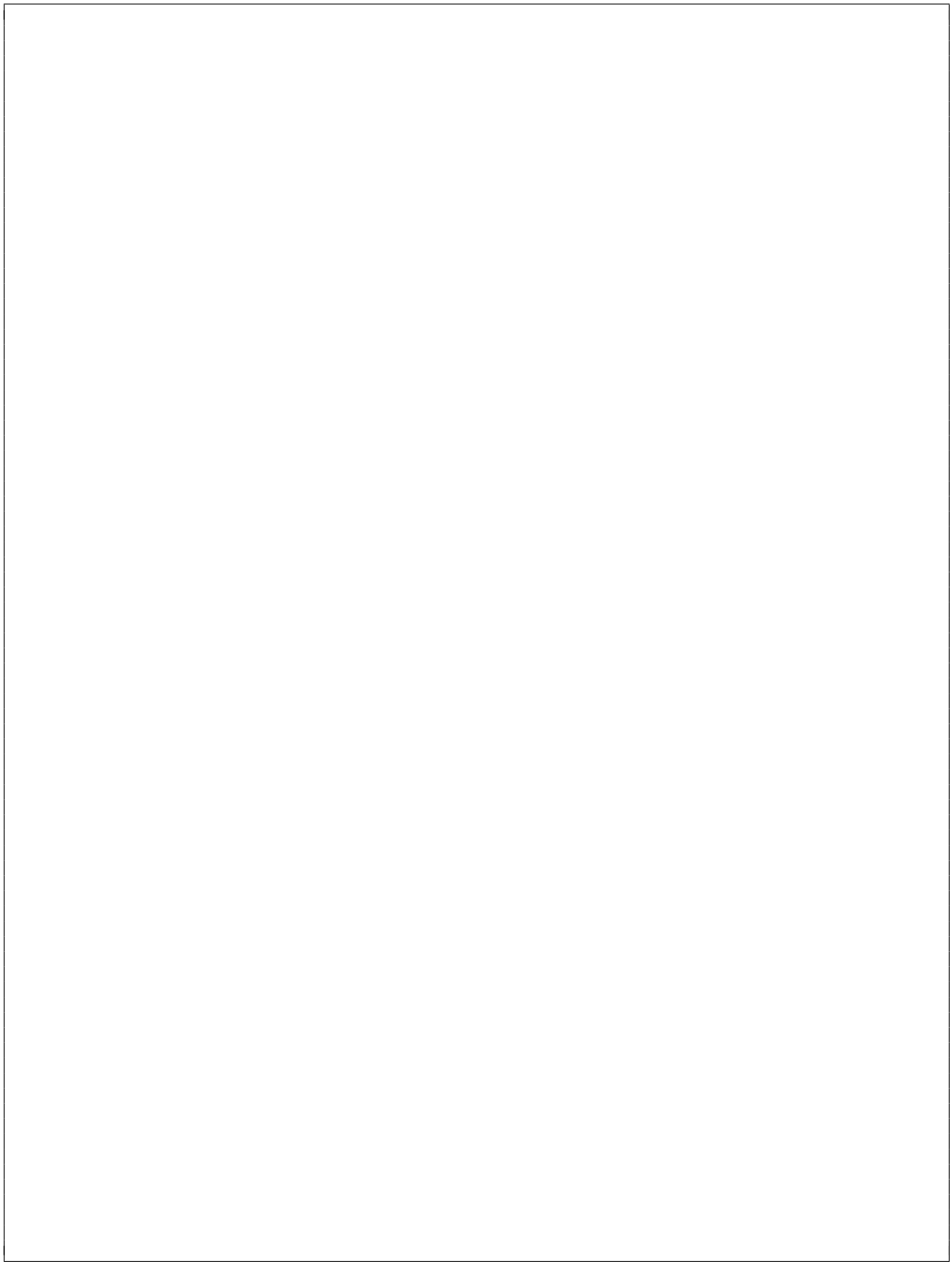
Question 9. (5 points) By default, what does the client do when it does not hear a response from the server to its `SYN` packets?

Question 10. (5 points) How many times does the client try to connect before giving up (in addition to the first one)?

Question 11. (5 points) On the client machine, check out the value in `cat /proc/sys/net/ipv4/tcp_syn_retries`, what do you notice?

Question 12. (5 points) Observe the timestamps at which the packets are sent, what can you say about the intervals between packet retries (approximately)?

Question 13. (5 points) Based on the above three experiments, draw a finite state machine diagram that represents the `TCP` connection establishment phase. We refer to this phase as the `TCP` three-way-handshake.



4 Experiment IV

The questions below refer to `experiment 4`. After the connection has been established using the regular three-way-handshake that we discussed before, the connection is terminated by the client. Observe the packet capture and answer the following questions.

Question 14. (5 points) How does the client signal to the server that it wishes to end the connection?

Question 15. (5 points) What does the server do when it receives a connection termination request from the client?

Question 16. (5 points) Why do you think the server waits for the client to confirm that it has received its acknowledgment of connection termination request?

Question 17. (5 points) Assume that the server did not receive the client's acknowledgment, what do you think it will do at that point?

5 Experiment V

The questions below refer to `experiment 5`.

Question 18. (5 points) What flags are set in the packets that contain data in `netcat`?

Question 19. (5 points) What does the server do when it receives a data packet from the client?

Question 20. (5 points) For the packets between the connection establishment and tear-down, fill out the following table with the following fields.

- The `sequence number` that you can obtain from the `TCP` header (use the relative number printed out by `Wireshark`).
- The `acknowledgment number` that you can obtain from the `TCP` header (also use the relative one shown by `Wireshark`).
- The `TCP` segment length that you can find in the `TCP` header or in the packet summary in `Wireshark`.
- In the table, `C` $\rightarrow$ `S` represents a packet sent from the client to the server, while `S` $\rightarrow$ `C` represents a packet sent from the server to the client.
- If you have less packets than the rows here, that's okay, fill out the ones you have.

Packet Number	Sequence Number	Acknowledgment Number	TCP Segment Len
4 `C` $\rightarrow$ `S`			
5 `S` $\rightarrow$ `C`			
6 `C` $\rightarrow$ `S`			
7 `S` $\rightarrow$ `C`			
8 `C` $\rightarrow$ `S`			
9 `S` $\rightarrow$ `C`			
10 `C` $\rightarrow$ `S`			
11 `S` $\rightarrow$ `C`			
12 `C` $\rightarrow$ `S`			
13 `S` $\rightarrow$ `C`			
14 `C` $\rightarrow$ `S`			
15 `S` $\rightarrow$ `C`			

Question 21. (5 points) Based on the content of the table above, what is the relationship between the **sequence number**, the **acknowledgment number**, and the **segment length**?

Question 22. (5 points) Assume now that we have a network that is very unstable, where packets can be delayed in the way, or even lost. How can the client and the server use the sequence and acknowledgment numbers to still communicate even if the medium of communication is unreliable?

Question 23. (5 points) Examine any packet containing data, you can see that `Wireshark` is printing a relative sequence number, while the real sequence number starts off at a very weird random value. Why do you think we need the sequence number to start at a very weird random location?

6 Experiment VI

The questions below refer to `experiment 6`.

Question 24. (5 points) How does the client send its username to the server?

Question 25. (5 points) How does the server respond to each packet sent by the client when entering the username? Who does the acknowledgment?

Question 26. (5 points) How does sending the password differ (in terms of the communication) between the client and the server?

Question 27. (5 points) How are commands sent from the client to the server?

Question 28. (15 points) In the box below, please summarize what you have learned about the TCP protocol. Make sure to mention who connections are established, how they are terminated, and how is data arranged.

When it comes to the `Telnet` protocol, list out any potential vulnerabilities you might think of if you were able to sit in the middle between the server and the client.