CSSE 341 -- Network Security

Rose-Hulman Institute of Technology

Lab 8.5: TCP Primer

Learning Objectives

At the end of this 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: ______________________________

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) What flags are set in the packets that contain data in `netcat`?

Question 10. (5 points) What does the server do when it receives a data packet from the client?

Question 11. (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` → `S` represents a packet sent from the client to the server, while `S` → `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` → `S`			
5 `S` → `C`			
6 `C` → `S`			
7 `S` → `C`			
8 `C` → `S`			
9 `S` → `C`			
10 `C` → `S`			
11 `S` → `C`			
12 `C` → `S`			
13 `S` → `C`			
14 `C` → `S`			
15 `S` → `C`			

Question 12. (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 13. (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 14. (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?

4 Experiment IV

The questions below refer to `experiment 4`.

Question 15. (5 points) How does the client send its username to the server?

Question 16. (5 points) How does the server respond to each packet sent by the client when entering the username? Who does the acknowledgment?

Question 17. (5 points) How does sending the password differ (in terms of the communication) between the client and the server?

Question 18. (5 points) How are commands sent from the client to the server?