Ethan Tuning
5/25/2017
CSCD330 Lab#5

What is the IP address of the client and what is the IP address of the remote machine in this trace?

 src: 192.168.0.197 dest: 146.187.134.7

What port numbers are being used for the client and remote machine?

 src: 42988 dest: 22

What packet numbers are involved in the initiation of the TCP ssh session (the three-way handshake)?

 13, 14, and 15

How can you tell TCP is starting a new session?

 [SYN] [SYN, ACK] [ACK]

What are the sequence numbers of the client and remote machine in the beginning?

 0, 0, and 1

Is any data being sent during TCP initiation? How can you tell?

 No, there is no "data" entry in the TCP header.

What's the Maximum Segment Size on both machines (MSS)? What is the meaning of the MSS?

 src: 1460 dest: 1380

How many bytes are in the TCP header?

 74

What is the smallest window size during this entire connection? What is the meaning of the win field?

66 bytes. Win field is the window size.

In this trace, packet 16 and on up has the PSH flag set. What does this flag mean? Why do you think its set in this trace?

PSH is a push flag. Its set so that It is here to immediately push the data to the application.

Can you see the ascii commands typed in this ssh session and the data returned? Why or why not?

No, its encrypted.

View the last few packets of this trace file. Which side sent the first Fin packet? Does the Fin packet seem to be counted as data? How can you tell?

The client sent the first. No its not data. No data entry in header.

From the first Syn packet until the last Ack of the final Fin packets, how long did this session last?

24.669631

How much data was sent from the remote machine?

7142 bytes

Does it appear that the packets are being sent at a constant rate? What is the average RTT?

No, average RTT was 77.7-ish

Are there any patterns in port numbers in your connections?

Just back and forth between client and server.

Notice any patterns in sequence numbers?

No not really, they start out super spread out and then condense towards the end.