Wireshark Lab: TCP

The Assignment

The TCP protocol is responsible for reliable transport of packets. In this lab we will be using Wireshark to see how TCP behaves. For this lab you are to download an existing trace file for analysis.

Instructions

First, download the trace file, `tcp_ssh_capture1.pcap`, and save it somewhere on your computer. Then, open Wireshark, click on File Open and load the saved ssh capture file. Follow the instructions below and answer the questions that follow.

Write your answers to each of the questions. Be sure to include your name in the document. Whenever necessary, when answering a question you should copy-and-paste (or screenshot of the relevant lines from the Wireshark tool) the packet(s) within the trace that you used to answer the question asked. Annotate the captured lines to explain your answer. Try to select the minimum amount of packet detail that you need to answer the question. Turn your answer document to Canvas by the due date.

Wireshark Settings and Viewing the Packets

1. Set a filter to view only tcp traffic, in the filter bar type, tcp (all lowercase).
2. Select Analyze and then the Enable Protocols menu option. Uncheck the SSH protocol, click OK. This allows SSH details to be displayed.
3. Begin looking at the packets in the trace.

Analyzing TCP using an SSH Session

Think about what ssh does. It is like Telnet in that you open a window to another computer and type commands and see the results displayed. So, you type something and what gets displayed are the results of what you typed. This trace file was created by Dr. Carol Taylor using the command: `ssh penguin.ewu.edu`. She then asked to see a directory listing and quit.

Questions

1. What is the IP address of the client and what is the IP address of the remote machine in this trace?
2. What port numbers are being used for the client and remote machine?
3. What packet numbers are involved in the initiation of the TCP ssh session? How can you tell TCP is starting a new session?
4. What are the sequence numbers of the client and remote machine in the beginning?
5. Is any data being sent during TCP initiation? How can you tell?

6. What is the Maximum Segment Size on both machines (MSS)? What is the meaning of the MSS?
7. How many bytes are in the TCP header?
8. What is the smallest window size during this entire connection? What is the meaning of the win field?
9. In this trace, packet 16 and on up has the PSH flag set. What does this flag mean? Why do you think it is set in this trace?
10. Can you see the ASCII (American Standard Code for Information Interchange) commands typed in this ssh session and the data returned? Why or why not?
11. 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?

A Different Look

Now, we can view some overall statistics for this trace. Click on Statistics, then Flow Graph. In the Flow Graph window, find the "Flow type:" pull down menu at the bottom; select TCP flow. This graph displays the flow of data and the sequence and acknowledgement numbers. Answer the next two questions from this graph.

12. From the first SYN packet until the last ACK of the final FIN packets, how long did this session last?
13. How much data was sent from the remote machine?

Finally, let us look at some other way to graph the TCP flow. Back in the main Wireshark window, click on Statistic and then TCP Stream Graph. Choose Round Trip Time Graph. Answer the question below.

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