Wireshark Layer 4 Lab

Kaleb Alstott

11/29/2019

In this lab, students will use Wireshark to inspect the content of layer 4 segments traveling between different hosts. This one is formatted a little differently from the previous labs. All of the questions are at the end. Students will perform two Wireshark captures. The first captures uses ssh. The second one uses http. Once you save a Wireshark capture, it can be re-opened simply by double-clicking on the file in the Ubuntu GUI.

**Part 1 – TCP Connections**

1.Start Wireshark by running **sudo wireshark** in a terminal window.

2.Start a capture session on interface ens32

3.Open another terminal window ssh to kosh.nku.edu. Upon receiving a login prompt, terminate the ssh session by entering ctrl-C. You do not need to log into kosh. Answer “yes” if prompted with a question about the ssh key.

The command to ssh to kosh is

ssh kosh.nku.edu

4.Stop your Wireshark capture session. Save your capture session using the file name “ssh.pcap”. Remember where you save this file so that you can submit it on Canvas.

**Part 2 – DNS and UDP**

In this portion of the lab, you will start a new Wireshark capture and inspect the frames resulting from navigating to http://example.com from a web browser.

1.Open a web browser.

2.Start a capture session on the Ethernet port for your laptop

3.In your browser, navigate to **http://example.com.** This will return a very simple web page.

4.Stop your Wireshark capture session. Save your capture session using the file name “http.pcap”. Remember where you save this file so that you can submit it on Canvas.

**Questions**

Using what you learned about TCP connections and your ssh.pcap capture file, answer the following questions.

1.Identify the frames in your Wireshark capture that are part of the ssh connection establishment sequence. If you want to reduce the frames captured that are unrelated to your ssh connection, you can use the Wireshark filter and filter only for “tcp”. Answer the following questions:

1. What are the Wireshark frame numbers of the frames used in the TCP connection establishment sequence.
   1. **505 ,508, and 509**
2. Provide a brief description of each of the frames you identified in terms of their role in establishing the TCP connection.
   1. **The 505 frame which is the SYN (Synchronise sequence numbers), this is you sending information or a request to the server. In the next frame in 508 we can see the SYN ACK, saying that the server has received the request acknowledging what was sent. We then see In frame 509 we have ACK, which is us acknowledging the server has received our request and starts the establishment.**

2.What is the server port number being used by this TCP connection?

**22**

3.What is the client port number being used by this TCP connection?

**47652**

4.Identify the frames in your Wireshark capture file that are part of the ssh connection termination sequence and answer the following questions (you should see 3 frames):

1. What are the Wireshark frame numbers of the frames used in the TCP connection termination sequence?
   1. **801-803**

5.Somewhere between the establishment and termination, choose any TCP ACK frame that is sent from the SSH server to the client and answer the following questions:

1. What frame number did you choose?
   1. **553**
2. What is next sequence number that the SSH server expects the client to send? How did you determine this?
   1. **1574 is the next sequence number we can expect the client to send. This was determined by looking transmission control protocol, while also using the next ACK frame which is found on 555.**
3. In which subsequent frame number is that next sequence number sent from the client to the server?
   1. **555**

For the remainder of the questions, refer to your http.pcap capture file.

7.Now locate the HTTP GET request for example.com and the response from the HTTP server in your capture file and answer the following questions:

1. What is the frame number of the GET request?
   1. **274**
2. What is the frame number of the response?
   1. **277**
3. What is the source port number of the GET request?
   1. **46250**
4. What is the destination port number of the GET request?
   1. **80**
5. Which port number is a well-known port number? Explain.
   1. **80 is a well-known port number. This is the most common point for web servers. Specifically port 80 is used for http traffic on web servers.**
6. What frame numbers were involved in establishing the TCP connection prior to the HTTP GET request?
   1. **75-77**
7. What is the initial window size established during the connection handshake?
   1. **29200**
8. What is the status code in the HTTP response?
   1. **200**
9. What is the version of HTTP used in the get request?
   1. **1.1**
10. What is the frame number of the ACK to the get request?
    1. **276**

Submit your answers to the questions and upload your Wireshark files on Canvas.