Lab 3: wireshark

Due 3/13/2020

Network protocols can interact in ways that are difficult to anticipate, understand, and debug, especially when systems are functioning in an unanticipated or undesired manner. Wireshark is a powerful tool that enables users to "drill down" to interpret the interaction of layered protocols.

A key aspect of wireshark is a timestamped packet capture (pcap) trace containing a sequential list of frame data. Wireshark incorporates features that allows users to obtain and analyze trace data.

Simple Trace Analysis

The first part of this lab focuses on analysis of data captured in a trace. Towards that end, we provide a trace of network traffic generated when a web client obtained a simple web page stored in PCAP Next Generation Dump Format (PCAPNG) named *simple.pcapng*.

Your task is to use wireshark to examine the traffic within this trace.

Wireshark is well documented free software published at https://www.wireshark.org/ and is supported on many platforms. It's included in the 3432 virtual machine. (It may be easier for you to install and use it on your desktop/laptop.)

There is copious documentation on wireshark including many tutorials and videos (on youtube and elsewhere), but you should initially need to read very little (if any) of it. Just

- start wireshark (it has a graphical user interface),
- tell it to open the packet capture file,
- select the conveniently numbered frames from the upper window,
- and browse their contents in the lower window.
    - Clicking on the left-edge triangles in the lower window lets you "drill down".

The trace includes arp, dns, and http requests and responses.

Your task is to answer the following:

- The ARP traffic
    - Which frame numbers contain the request and response?
    - What is the IP address being requested?
    - What protocol layers are involved (and why)?
    - Why was only one ARP request required when there are multiple hosts?
- The DNS traffic
    - Explain what information is contained in each frame (just summarize at a very high level - a few words are fine).
    - What is the hostname being looked up and its IP address?
    - What protocol layers are involved (and why)?
- The HTTP traffic
    - What URL is being requested?

- What protocol layers are involved (and why)?
- Which frames contain messages related to establishing and closing the connection used for the HTTP traffic?
- What is the server's IP address and port?
- What is the server's ISN?
- What is the client's IP address and port?
- What is the client's ISN?
- Which frames contain
  - The HTTP request
  - HTTP ACK
  - HTTP headers
  - HTTP response

Part 2

Use wireshark to capture the interaction between your browser and the result of clicking on the "course schedule" tab of http://www.cs.utep.edu/cs/ web page. Examine this trace. Explain how HTTP is encapsulated within TCP and IP.

Was the trace that you captured more difficult to analyze than the provided one? Why?

What to turn in

Answers to the questions in part 1.
The trace with explanations of the interactions in part 2.