1. Report Header

Utilization of Wireshark in the Review of Several OSI Models
Austin Hall
4/10/20

2. Statement of Objective

The primary objective of this lab was to investigate how the network protocol analyzer Wireshark can be used to capture and interactively browse the traffic running on a computer network. Several other objectives include: identifying the different layers of the open systems interconnection (OSI) model; identify how these layers interact with one another and the system they run on; and measure the data contained within each layer.

3. Procedure

To conduct this experiment, I started up the provided virtual machine and opened a Wireshark trace file that contains a previously acquired capture of traffic along a network. During the beginning portion of the lab, I navigated the Wireshark interface, selecting different packets and identifying various data contained within each. The next several segments of the experiment pertained to identifying the different layers of the OSI, the data they contain, and how they interact with other layers. I began by analyzing the captured packets that used the application, presentation, and session layers of the OSI. To do this, I selected packets that were of the protocol HTTP and navigated the middle pane of the capture window to investigate the different data held in the packet, clicking and expanding different sections and subsections of the packet (mainly the HTTP part). The experiment continued in a similar manner to this, but for the other OSI layers. In each packet there are sections for TCP, IP, and ethernet, each of which I navigated and investigated the data within.

4. Data Analysis

During the experiment, I used Wireshark to obtain data transmitted over a network that was contained in the packets captured. The first flag had the value 999818 and was found by filtering the packets by the protocol UDP and another filter to display only those that contained “sampleflag” in the frame. The objective of this flag was to investigate the way the filter works. The objective of the second flag, with the value 223344, is the same as the first and was also found in the info section of the packet viewer. The third flag had the value 833821, and was found the same way. The fourth flag had the value 444333, and was a little harder to find. This flag, I began by filtering

the packets for UDP and TFTP.block. Then, I selected the first packet and followed the UDP stream to the answer. The objective of this flag is to show how a UDP stream can be followed. The fifth flag had the value 775661 and was found by filtering the packets by FTP and looking at the info box for each one, where it was in the last. The final flag had the value 363661. This was the most difficult to find because I first had to filter http and the frame containing sampleflag6, then select the one packet and follow the tcp stream, then scan the file until I found the flag.

5. Discussion of Results

The data contained in the flags weren't necessarily useful and didn't tell me much since they were just random numbers. But the procedures used in acquiring the flags will translate into practical behavior in the real world. The flags themselves didn't tell me anything, but they showed me how to filter packets by the protocol and data contained in the frames to find useful information. They also showed me that Wireshark is capable of following TCP and UDP streams to discover where data flows to.

6. Conclusion

The objective of investigating how to navigate Wireshark was explored in capturing the flags and other sections of this experiment. I navigated the interface and captured the flags by selecting the correct section of captured packets. The experiment focused on exploring the different OSI layers which satisfied the objectives of identifying and understanding these layers. Understanding these layers, the way they interact with each other, and interpreting the information contained within them, are critical components of being efficient at network management and analysis.