Austin Hall 04/07/2020

Review of Internetwork and Transport Layer Protocols

One objective of this lab was to investigate the interconnectedness of a network and compare the derived values (such as IP and MAC addresses) of the network to other networks. Another objective was to parse specific network protocols and analyze this data when connected to a network.

To complete the first objective of the lab, I pinged the IP address of my host machine, a connected internal system, and a connected external system to verify the network layer connectivity. I then ran ifconfig commands to determine basic network information. The second objective of this lab required the use of wireshark. I filtered ARP, then TCP, then UDP network traffic to individually analyze each protocol.

In this lab, the majority of the time spent was not in capturing flags. The flags captured where trivially hidden in easily accessible files through the command prompt and with the use of “dir” and “more”. The bulk of the data that was captured came from the wireshark portion of the lab when I filtered the separate protocol segments. During the lab, there was no data analyzed, I simply opened random segments and looked over the protocol information with no interpretation.

The flags in this assignment had nothing to tell us, they were random 6 digit numbers. The first flags were found in the command prompt window by opening a file in the directory, then next flags were found in a text file on the desktop, and the final flag was found in the header of a website. The ARP, TCP, and UDP data segments contained some data, but the objective of this lab wasn’t to interpret that data, only to observe it. This will be useful in future lab assignments because I will have a better understanding of how to navigate the wireshark interface.

In conclusion, the objectives of this lab were met. I was able to investigate the interconnectedness of a network and compare network values using a windows system. I also learned windows command line commands which will be beneficial. After this lab, I am more comfortable with navigating wireshark and targeting specific network protocols to be analyzed, as well as, where to find the data to be analyzed.