OSI Model Lab

Jacob Berger

4/9/20

Statement of Objective

The objective of this lab is to investigate the capabilities of Wireshark and further analyze the OSI model and determine which functions and protocols belong in each of the layers.

Procedure

The remote machine was started and a Wireshark capture was examined. The interface was examined in detail, such as the packet window and the types of information gathered. The key contents of an HTTP packet were investigated and response messages were explained. The three-way handshake used in a TCP connection was then looked at and the SYN and ACK messages were introduced and explained. The Internet Protocol Version information was then expanded upon. The Network and Sharing Center was then opened and the machine's MAC address was altered, then the change was verified using command prompt. We then took a closer look at the hexadecimal contents that actually make up the packets. Another WS capture was opened and TCP and UDP packets were followed to see more information on the exchanges.

Data Analysis

The network layer uses IP addresses to forward packets towards their destination networks.

The MAC address can be filtered or changed on the client.

The data link layer uses the MAC address for data between clients on the same network.

Wireshark allows the user to follow TCP and UDP streams.

Discussion of Results

The network layer of the OSI model is where IP addresses come into play and there is a lot of information even just under the IP section in WS. Changing a client's MAC address could allow for MAC-filtered networks to possibly be compromised if a good address is known. Changing the MAC address was also very simple to do. WS's built-in packet following option is also very helpful and easy to use.

Conclusions

Along with understanding the lower layers of the OSI model, this lab was very eye-opening with regard to what Wireshark can do. This will come in handy later, as it's much easier to understand this information in WS. In addition to this, I feel I better understand what each layer of the OSI model is responsible for.