Infosec Lab 1

Jacob Berger

4/8/20

Objective

The objective of this lab is to become familiar with network utilities and investigate what Wireshark can do. We will also take a look at what is inside different packets, how they differ, and what they are used for.

Procedure

Command prompt was first opened and commands such as ipconfig, dir, and more were used to become familiar with the machine and to ensure connections between machines are working properly. Wireshark was then setup for logging ARP traffic to and from the machine, command prompt was used to delete the stored ARP records, then the external machine was pinged. The captured packets were viewed in Wireshark where the type of request and more information was visible. Internet Explorer was then opened and navigated to http://www.isp.com/. Wireshark was then configured to filter only UDP packets and the header was again examined.

Data Analysis

ARP request opcode = 1, reply opcode = 2.

ARP requests/replies contain both the sender's and receiver's address in the handshake.

ARP destination is initially 00:00:00:00:00:00

TCP traffic includes web browsing information.

Discussion of Results

ipconfig will show information about the computer's network addresses.

ping will show if the target is running.

arp with options will allow you to see and clear your ARP table.

Conclusions

These commands, along with Wireshark, will be essential for understanding the layout of a network.