Lab 6: Introduction to Networking

This lab is intended to give you hands on experience with the network tools and processes we will be using in Project 3.

Introduction

EECS 388 is in trouble! An attacker has stolen some valuable information from our servers, and has hidden the data on a remote server. Only you can help us retrieve what was taken from us! Your mission, should you choose to accept it, is as follows...

The Mission

1. Our intel has found a program used by the attackers. Download the file "send.py" from https://github.com/debug12/eecs388ia/tree/master/lab6, and run it from the command line using

   ```
   $ python send.py
   ```

   While the file looks obfuscated and appears to do nothing, our intel believes that it is making network connections to a remote host. The best way to look into this is to create a packet capture file (pcap) that we can analyze with the network analysis tool Wireshark.

2. First, determine which of your network interfaces are active. You can do this by running the following from the command line and checking the "status" attribute of each interface.

   ```
   $ ifconfig
   ```

3. Pick the name of the active wireless interface that your machine is using to make the network connections (likely begins with an "en"). From there, enter the following command

   ```
   $ tcpdump -i <network_interface> -v
   ```

   And you can observe the network traffic! Now, with the "send.py" file running, execute the following command to save the dump to a file called "labdump.pcap"

   ```
   $ tcpdump -i <network_interface> -v -w labdump.pcap
   ```

   and let tcpdump run for a few minutes to capture a good amount of network traffic.

4. Now that we've captured a few packets, we can use a program like Wireshark to analyze them. Use Wireshark to open the "labdump.pcap" file, and observe the network trace. Do you see anything that might be useful?

5. If given an IP address, you might like to know if there are any ports open to network connections. For example, a server can be running network services like ssh, http, ftp, smtp, etc. To determine what ports are open to connections, we can use the following command:

   ```
   $ nmap <ip_addr>
   ```

   You might find this command useful in returning our data.

   Best of luck!