Project 1 - Application Protocols

1. Wireshark - Collect and Filter Network Traffic

Collect

Start Wireshark. Visit http://synprint.com/ece303/project1/login.html. Log into the webpage using your Cooper email and a fake password. Stop Wireshark. Keep page open for Step 3.

Filter

Create a wireshark filter that reduces the number of network packets to the ones that matter. In this case, we care about all DNS traffic as well as all HTTP traffic with the synprint.com server (IP address: 192.241.168.54). You will need to use the following filter keywords: ip.addr, dns, http, or, and, 192.241.168.54, and parentheses. Once you've created the filter, "export the specified bytes/packets" as a .pcap file using the format <last name>_<date>.pcap. The file should then be uploaded to https://drive.google.com/drive/u/0/folders/1kp47Y7Exmh5EbmhCgRchJHihuw-YzFQJ.

2. Protocol Analysis

Use the following template (below) to describe the protocol observed in the pcap file you just generated. Only include the DNS request/response for synprint.com. Only include HTTP requests with the synprint.com server (IP address: 192.241.168.54).

```
------------------------------------------------------------------------------------------------
Client                                                                                    Server
------------------------------------------------------------------------------------------------
DNS Request; Query: <query> →
                                                       ← DNS Response; Answer: <address>
------------------------------------------------------------------------------------------------
HTTP <Request Method> Request; <URI> →
                                 ← HTTP <Status Code> Response; Content-Type: <content-type>
------------------------------------------------------------------------------------------------
Repeat as necessary...
------------------------------------------------------------------------------------------------
```

3. Browser Cookies

When visiting http://synprint.com/ece303/project1/main.php, a cookie is sent to the client from the server. The cookie is then loaded and stored in the browser. The cookie's name is "secret". Find the value of the "secret" cookie. Use "Developer Tools" built into Chrome and Firefox browsers to discover this value.

Secret=________________________________

4. Packet Capture Automation

Install a program called tcpdump. Use this to save a packet capture from command line. Make sure you use the correct options to save a .pcap file. While it is running, visit cnn.com and weather.com. After visiting both pages, ctrl-c out of tcpdump. You should have a .pcap file in your local directory. Tcpdump is a useful tool to quickly run a packet capture from command line.

Install a program called tshark. Tshark is a useful tool to analyze, filter and parse packet captures from command line. Read a tutorial and get familiar with the tool. It has filter capabilities just like Wireshark but it can be used to perform more automated tasks. Use tshark to analyze the file generated above from tcpdump. Perform the following:

- Use the pcap generated from tcpdump as the input
- Use a filter that only allows packets that are TLS Client Hellos
- Print out the Source IP, Destination IP, and Server Name found in each TLS Client Hello
- Save the output to a file

Hint: If you need help finding out pcap filters, open the pcap file in Wireshark, navigate to the field you are interested in filtering, and the filter should show up at the bottom of the Wireshark window, like a tooltip.
Now write a script (any language such as Python) that runs the above tshark command and parses the resulting output. The script should remove duplicates. For each Destination IP, perform a “whois” command and retrieve the “Organization” from the response.
The resulting output should contain multiple lines with the following format: source IP, destination IP, server name, and organization\n
Cut and paste the script code and the resulting output below:

5. User-Agent Spoofing

Download and install Burp Suite (free version). Read a tutorial on this tool to understand how you can perform a basic man-in-the-middle attack on yourself. You will use a web browser to connect to http://synprint.com/ece303/project1/login.html. During your GET request for main.php, use Burp to catch the request and change the following values:

- Change the User-Agent string to a mobile device (Android or iPhone). You can Google search to find a valid mobile device User-Agent to use.
- Change the URI to main_spoof.php from main.php

Allow the packet to be sent. Cut and paste the contents of the resulting webpage from the browser below: