ECS 152A: HW1 Part 1a

Nghi Dao (921147615), Bian Lee (920763430)

November 2024

Link to ChatGPT conversation: Here. The GPT generated code can also be found in `1a_analysis_chatgpt.py`, which we referred to when polishing our final code found in `1a_analysis_Bian_Lee_920763430_Nghi_Dao_921147615.py`

1. Application Layer Protocols and Their Counts for Each Activity

- **Activity 1 (`Activity_1.pcap`):** Pinging Google.com uses ICMP (Internet Control Message Protocol), which is NOT an application layer protocol.
- **Activity 2 (`Activity_2.pcap`):** 24 instances of port 443 (HTTPS).
- **Activity 3 (`Activity_3.pcap`):** 8 instances of port 80 (HTTP) and 12 instances of port 443 (HTTPS).
- **Activity 4 (`Activity_4.pcap`):** 6 instances of port 80 (HTTP), 6125 instances of port 443 (HTTPS), and 1900 instances of SSDP.
- **Activity 5 (`Activity_5.pcap`):** 8 instances of port 443 (HTTPS) and 22 instances of FTP.
- **Activity 6 (`Activity_6.pcap`):** 86 instances of port 443 (HTTPS). When SSH'ing into the CSIF machine, ESP is used given the access through the VPN.

2. Recorded Packet Counts for Selected Activities

- **Activity 2 (`Activity_2.pcap`):** Recorded 24 HTTPS packets.
- **Activity 3 (`Activity_3.pcap`):** Recorded 8 HTTP packets and 12 HTTPS packets.

3. IP addresses

- The text output dump can be found in `question_3_log.txt`

4. Browser Used

- Activities 2, and 4, in which HTTPS connection is used, we are unable to determine which browser was used given that HTTP encrypts the payload and headers meaning the User-Agent detail is hidden. On the other hand, for activity 3, HTTP is used and the User-Agent header is sent in plaintext, from which we were able to determine that Firefox was used as the browser (which is indeed the correct answer).