Liliane Owens
U00846594
Undergraduate
Meilin Liu
4/18/2025

CEG 4424/6624 Security Attacks and Defenses
Lab/Project 3 (60 Points)

1. The objective
   The objective of this lab is to use an existing tool to perform packet/traffic analysis.

2. Submission
   A team can have up to 3 students. All students in the same team will receive the same grade.
   a. Each team only submits one report or a copy of answers/files on Pilot under dropbox. (See the section of tasks).
   b. **Each team member needs to submit the list of the names of all team members** on Pilot under dropbox.

3. Tools:
   Wireshark: Please download and install Wireshark (https://www.wireshark.org). The installation process is self-explanatory under windows systems. If you do not have access to a personal computer, please go to the CS department public lab, to use the computers in the lab to work on the project.

4. Tasks:
   (1) Download and install Wireshark.
   (2) Download the pcap file for this project from Pilot, and analyze it using wireshark, i.e., open the provided pcap file for this project using wireshark, analyze it to answer the following questions in your project report.

Questions:

What is the first TCP session that is successfully established? Please offer the information for the first 3 packets in this TCP session (e.g., the SYN, SYN-ACK, and ACK packets). (60 points)

- Timestamp (Seconds since first captured packet):1.186820
- Source MAC address: f8:1e:df: e5:84:3a
- Destination MAC address: 00:1f: f3:3c: e1:13
- Source IP address: 172.16.11.12
- Destination IP address: 216.34.181.45
- Source Port: 64581

- Destination Port: 80
- Sequence Number (absolute value): 3904319675
- Acknowledge Number (absolute value): 0
- SYN Flag: 1
- ACK Flag: 0
- RST Flag: 0

- Timestamp (Seconds since first captured packet): 1.281879
- Source MAC address: 00:1f: f3:3c: e1:13
- Destination MAC address: f8:1e:df: e5:84:3a
- Source IP address: 216.34.181.45
- Destination IP address: 172.16.11.12
- Source Port: 80
- Destination Port: 64581
- Sequence Number (absolute value): 3971588985
- Acknowledge Number (absolute value): 3904319676
- SYN Flag: 1
- ACK Flag: 1
- RST Flag: 0

- Timestamp (Seconds since first captured packet): 1.281937
- Source MAC address: f8:1e:df: e5:84:3a
- Destination MAC address: 00:1f: f3:3c: e1:13
- Source IP address: 172.16.11.12
- Destination IP address: 216.34.181.45
- Source Port: 64581
- Destination Port: 80
- Sequence Number (absolute value): 3904319676
- Acknowledge Number (absolute value): 3971588986
- SYN Flag: 0
- ACK Flag: 1
- RST Flag: 0