Tcpdump Beginner Project: HTTP Packet Analysis (YouTube)

Overview

This project demonstrates how to capture and analyze basic HTTP traffic using tcpdump. It focuses on identifying and understanding the TCP 3-way handshake when accessing YouTube.

Tools Used

- tcpdump
- macOS terminal (or Linux shell)
- GitHub for documentation and project sharing

Steps

1. Installed tcpdump on the system.
2. Identified the active network interface using 'tcpdump -D'.
3. Captured 10 HTTP packets with:
sudo tcpdump -i en0 tcp port 80 -c 10 -w http_traffic.pcap
4. Visited youtube.com in a browser while capturing traffic.
5. Read the packets with 'tcpdump -r http_traffic.pcap' and observed the TCP 3-way handshake.

Findings

The captured packets revealed the TCP 3-way handshake:
- SYN: The client requested a connection.
- SYN-ACK: The server acknowledged the request.
- ACK: The client confirmed, establishing the connection.
This demonstrated how tcpdump can be used to analyze basic HTTP traffic.

Key Takeaways

- Learned how to capture live traffic using tcpdump.
- Understood the TCP 3-way handshake process.
- Practiced filtering traffic by port (HTTP on port 80).