Cybersecurity Lab - DNS, Ping, Traceroute, Nmap & Wireshark

Name: Aasmi Joshi
Date: March 22, 2025

Included Screenshots and Descriptions:

1. DNS Resolution (nslookup)
- I used the nslookup command on my EUID domain 1166937.com which returned an NXDOMAIN error, as expected.
- I also queried unt.edu and successfully resolved it to the IP address 10.157.0.4.

2. Ping and Traceroute
- I used ping to test connectivity to 10.157.0.4 (from unt.edu).
- I also used traceroute to observe the path taken by packets to reach 10.157.0.4.

3. Nmap Scanning
- I performed a basic Nmap scan on my local machine’s IP address 10.0.2.15 to identify open ports and services.
- The scan showed closed ports (which is expected for a secured system).

4. Wireshark – UDP Filter
- Captured packets using Wireshark while browsing the internet.
- Applied a udp filter and captured DNS traffic to location.services.mozilla.com.

5. Wireshark – QUIC Filter
- Applied a quic filter and captured QUIC handshake traffic with IP 34.117.188.166.
- Verified encrypted QUIC payloads and session details.

Tools Used:
- Terminal commands: nslookup, ping, traceroute, nmap, ip a, history
- Wireshark: Packet capture, filtering for udp and quic protocols