Wireshark Network Traffic Analysis Lab – Portfolio Overview

Objective

The goal of this lab was to gain hands-on experience using Wireshark, an industry-standard network protocol analyzer, to explore and analyze captured network traffic. The exercise simulated a real-world cybersecurity workflow — from inspecting raw packet data to filtering and identifying specific network communications.

Tools & Environment

• Tool Used: Wireshark
• File Type Analyzed: .pcap (packet capture file)
• Operating System: Windows
• Protocols Observed: ICMP, TCP, UDP, HTTP, DNS, and Ethernet II

Key Learning Outcomes

1. Open and navigate Wireshark packet capture files to examine live network data.
2. Apply display filters (ip.addr, ip.src, ip.dst, eth.addr, udp.port, tcp.port, etc.) to isolate specific network traffic.
3. Analyze network layers and protocols, including Ethernet, IPv4, TCP, UDP, and ICMP.
4. Inspect DNS queries and responses, identifying how domain names (like opensource.google.com) resolve to IP addresses.
5. Investigate TCP communications by examining ports, sequence numbers, flags, and payloads.
6. Use payload searches (e.g., tcp contains 'curl') to locate specific requests embedded within packet data.
7. Interpret frame, header, and protocol details such as Time To Live (TTL), source/destination MAC & IP addresses, and protocol types.

Technical Highlights

• Discovered ICMP Echo (ping) requests to confirm network connectivity.
• Used IP and MAC address filtering to isolate device-specific communication.
• Explored DNS traffic on UDP port 53 to understand query/response structure.
• Examined HTTP requests on TCP port 80, observing how web traffic is transmitted.
• Identified TCP destination port 80 as a key communication channel for HTTP data.
• Practiced interpreting hexadecimal and ASCII representations of packet payloads.

Cybersecurity Relevance

This exercise reinforced the importance of network visibility and packet-level inspection in identifying anomalies, investigating incidents, and validating network behavior. Understanding how to capture, filter, and interpret packets is a foundational skill for:

- Incident Response
- Network Forensics
- Threat Hunting
- Security Monitoring

Key Takeaway

By completing this lab, I strengthened my ability to analyze network traffic systematically, use Wireshark filters efficiently, and correlate network activity with protocol behavior — a critical competency for any cybersecurity analyst or network defender.