Network Traffic Analysis Report

Eleyate Cyber Security Internship - Task 5

Prepared by: Sujay Vegi

Date: June 02, 2025

1. Introduction

This report documents the process of capturing and analyzing network traffic using Wireshark as part of Task 5 for the Eleyate Cyber Security Internship. The objective was to identify various protocols from live traffic and understand the structure and behavior of captured packets.

2. Methodology

1. Wireshark was installed and launched.
2. Capture was started on the active network interface.
3. Regular internet activity like browsing and pinging was done to generate traffic.
4. The capture was stopped after 1 minute.
5. Filters were applied to isolate protocols like HTTP, DNS, and TCP.
6. Packet details were analyzed and the .pcap file was saved.

3. Protocols Identified

- HTTP: Observed in website access packets.
- DNS: Detected when resolving domain names.
- TCP: Used for connection-oriented communications including HTTP and DNS queries.

Additional protocols like ARP and TLS were also captured.

4. Packet Analysis Summary

The packet capture revealed how different protocols work together in typical web browsing. DNS queries were followed by HTTP requests. TCP three-way handshakes were seen at the start of connections, and ARP packets showed device discovery in the local network.

5. Interview Questions and Answers

1. What is Wireshark used for?

Wireshark is a network protocol analyzer used to capture and inspect network packets in real-time.

2. What is a packet?

A packet is a formatted unit of data carried by a network. It includes headers and the actual data payload.

3. How to filter packets in Wireshark?

Use display filters like 'http', 'dns', or 'tcp.port==80' in the filter bar.

4. What is the difference between TCP and UDP?

TCP is connection-oriented and reliable, while UDP is connectionless and faster but less reliable.

5. What is a DNS query packet?

It is a request sent by a client to a DNS server to resolve a domain name to an IP address.

6. How can packet capture help in troubleshooting?

It helps identify network issues, unauthorized traffic, and performance bottlenecks.

7. What is a protocol?

A protocol defines rules for data exchange between devices on a network.

8. Can Wireshark decrypt encrypted traffic?

Yes, but only if the session keys or private certificates are available. TLS traffic is encrypted by default.