Network Traffic Analysis Report

Name: Aditya Aryan

Roll: 2301MC58

Introduction

This report summarizes the findings from a network traffic analysis exercise conducted using Wireshark. The objective was to capture live network data during common internet activities, such as web browsing and using the *ping* utility, and then to filter and analyze the captured packets to understand the underlying communication protocols and patterns. The capture file *Task1.pcap* forms the basis of this analysis.

Most Active Protocols

An analysis of the captured traffic was performed using Wireshark's "Protocol Hierarchy" tool. The results, shown in the screenshot provided, clearly indicate the dominant protocols used during the session.

The most active protocols, ranked by the percentage of total bytes transferred, were:

- **Transport Layer Security (TLSv1.3 & TLSv1.2)**: This was by far the most dominant protocol, accounting for the vast majority of the data transferred. This is expected, as modern web browsing to sites like *wikipedia.org* uses HTTPS, which encrypts the application data (HTTP) using the TLS protocol for security.
- **Transmission Control Protocol (TCP)**: TCP was the most common transport protocol, making up a significant portion of the total packets. It serves as the reliable foundation for TLS and other protocols, managing the connection setup, data transfer, and teardown for web browsing.
- **Domain Name System (DNS)**: This protocol was frequently observed. Before the browser could connect to any website, it had to send DNS queries over UDP to resolve the domain names (e.g.,*example.com*) into their corresponding IP addresses.
- **User Datagram Protocol (UDP)**: This protocol was active primarily as the transport mechanism for DNS queries.

Analysis of Traffic and Communication Patterns

A detailed review of the captured packets was conducted. No suspicious or malicious activity was detected. The traffic patterns observed were consistent with the actions performed (web browsing and network diagnostics).

Key Insights and Communication Flow

The capture provided several key insights into standard network communication:

1. **Web Browsing Flow (HTTPS)**: The process of visiting a website like *https://wikipedia.org* is not a single request but a multi-step conversation:

    - **Step 1: DNS Query:** The session begins with the computer sending a **DNS query** over UDP to find the IP address for *wikipedia.org*.
    - **Step 2: TCP Handshake:** Once the IP is known, the computer initiates a **TCP three-way handshake** (SYN, SYN-ACK, ACK) with the web server to establish a reliable connection.
    - **Step 3: TLS Handshake:** Immediately following the TCP setup, a **TLS handshake** occurs. This involves an exchange of certificates and cryptographic information to create a secure, encrypted channel.
    - **Step 4: Encrypted Data Transfer:** All subsequent HTTP traffic is encapsulated within TLS records, appearing as "Application Data" in Wireshark. This is why TLS, and not HTTP, dominates the traffic statistics.
2. **Network Diagnostics (ICMP)**: The *ping 8.8.8.8* command generated **Internet Control Message Protocol (ICMP)** traffic. This involved a straightforward exchange of *Echo (ping) request* packets sent from the source machine and corresponding *Echo (ping) reply* packets received from the destination server (*8.8.8.8*), confirming network connectivity.
3. **The Importance of Filtering:** The exercise highlighted the necessity of display filters. A raw capture contains thousands of packets from various applications. Using filters like *icmp*, *dns*, and the custom filter *ip.src == <your_IP> && (tcp.port == 80 || tcp.port == 443)* was essential to isolate specific conversations and perform meaningful analysis.

Conclusion

This lab exercise successfully demonstrated the power of Wireshark as a tool for network analysis. By capturing and dissecting live traffic, it was possible to observe the layered nature of network protocols in action. The analysis confirmed the standard communication flows for secure web browsing and network diagnostics, showing how protocols like DNS, TCP, TLS, and ICMP work together to facilitate modern internet communication. The traffic was found to be normal, and the patterns observed provided valuable practical insight into theoretical network concepts.