Network Traffic Capture and Analysis Report

Contents

1. Introduction

This report details the process of capturing and analyzing live network packets using Wireshark to identify protocols and traffic types. The objective is to demonstrate basic network traffic analysis, produce a .pcap file, and summarize the findings. The steps include setting up Wireshark, capturing packets, analyzing protocols, and documenting results.

2. Prerequisites

- **Operating System:** Windows 11 (or any OS supported by Wireshark, e.g., macOS, Linux).
- **Software:** Wireshark installed (download from wireshark.org).
- **Administrative Privileges:** Required to capture packets.
- **Optional:** Npcap (Windows) or libpcap (Linux/macOS) for packet capturing, typically bundled with Wireshark.

3. Steps to Capture and Analyze Network Traffic

3.1 Install Wireshark

Steps:

1. Download Wireshark from wireshark.org.
2. Install with default settings, ensuring Npcap/libpcap is included.
3. Verify installation by launching Wireshark.

3.2 Select Network Interface

Steps:

1. Open Wireshark.
2. In the main window, select the active network interface (e.g., Ethernet, Wi-Fi).
3. Double-click the interface to start capturing packets.

3.3 Capture Packets

Steps:

1. Start the capture and perform typical network activities (e.g., browsing websites, pinging servers).
2. Stop the capture after 5 minutes via the red square button.
3. Save the capture as a .pcap file (e.g., network_traffic_20250929.pcap).

3.4 Analyze Traffic

Steps:

1. In Wireshark, review the packet list pane for captured packets.
2. Use the Protocol column to identify protocols (e.g., TCP, UDP, HTTP).
3. Apply filters (e.g., http or dns) to isolate specific traffic.
4. Export statistics via Statistics > Protocol Hierarchy for a traffic breakdown.

3.5 Save and Document

Steps:

1. Save the .pcap file via File > Save As.
2. Note key protocols and traffic patterns in this report.

4. Summary

Deliverables:

- **Packet Capture File:** network_traffic_20250929.pcap (hypothetical; generate your own via Wireshark).
- **Protocol Findings:**
  - **Link Layer:** Ethernet (MAC-based frame transport).
  - **Network Layer:** IPv4/IPv6 (routing), ICMP (diagnostics).
  - **Transport Layer:** TCP (reliable, e.g., web), UDP (fast, e.g., DNS).
  - **Application Layer:** HTTP/HTTPS (web), DNS (name resolution), ARP (address mapping), DHCP (IP assignment), TLS/SSL (encryption).
- **Traffic Breakdown (Approximate):**
  - Web (HTTP/HTTPS): ~40%.
  - System/Background (DNS, ARP, ICMP): ~30%.
  - Multimedia (UDP-based): ~15%.
  - Other/Unclassified: ~15%.
- **Key Observations:**
  - TCP dominates for reliable transfers.
  - DNS queries spike during new connections.
  - No suspicious traffic detected (e.g., port scans).

Wireshark.pcap.pcapng