Elevate Labs – Cyber Security Internship

NAME:Srinivas Atta

Task 5: Capture and Analyze Network Traffic Using Wireshark

By: Ministry of MSME, Govt. of India

Objective

Capture live network packets with Wireshark and identify basic protocols and traffic types for practical packet analysis experience.

Tools Required

- Wireshark (free, open-source network protocol analyzer)

Execution Steps / Guide

1. Install Wireshark
    - Download and install from the official website.
2. Start Packet Capture
    - Open Wireshark and choose your active network interface to begin capturing.
3. Generate Network Traffic
    - Browse a website, stream a video, or ping an external server to generate different types of traffic.
4. Stop Capture
    - After about one minute, stop the capture to ensure a manageable dataset.
5. Filter and Analyze Packets
    - Use protocol filters (e.g., `http`, `dns`, `tcp`, `udp`) in Wireshark's search bar to isolate relevant traffic.
6. Identify Protocols

    - Examine packet details to identify at least three protocols (e.g., HTTP, DNS, TCP).
7. Export Packet Capture
    - Save the captured data as a `.pcap` file for documentation and sharing.
8. Document Findings
    - Summarize identified protocols, typical packet details, and their purpose in the network.

Findings / Results

- Protocols Identified:
    - HTTP: Shows web traffic between browser and web server; request and response details visible.
    - DNS: Demonstrates domain name lookups from local host to DNS server; query/response packets evident.
    - TCP: Underlies reliable delivery for protocols like HTTP and DNS; seen in connection setup/teardown packets.
- Packet Details:
    - HTTP packet: Includes request headers, source and destination IPs/ports, visible URLs.
    - DNS packet: Shows query types (e.g., A record), queried domain, server responses.
    - TCP packet: Displays sequence and acknowledgment numbers, flags (SYN, ACK), connection details.
- Screenshots and Evidence:
  (Add screenshots from Wireshark – protocol filters, packet detail views, overview statistics.)

Security Analysis

Packet capture reveals the types of communications happening on a network. Visible HTTP and DNS traffic can expose sensitive browsing behavior or site access, while TCP flags show connection flows. Unencrypted traffic (like HTTP, DNS in clear text) is easily readable and poses privacy concerns. Encrypted protocols (HTTPS) are not viewable in full detail without keys.

Recommendations

- Prefer encrypted protocols (HTTPS, DNS over TLS) to protect sensitive information.
- Use Wireshark filters to focus analysis and troubleshooting.
- Regularly review network traffic for signs of malicious or abnormal patterns.
- Limit packet capture to test/troubleshoot to avoid collecting excessive private data.

Outcome

- Learned hands-on packet capturing and protocol identification with Wireshark.
- Understood the basic anatomy of network packets and popular protocols.
- Gained practical exposure to network troubleshooting and protocol filtering.

Key Concepts

- Packet capture
- Protocol analysis (HTTP, DNS, TCP/IP)
- Network troubleshooting
- Wireshark filtering
- Traffic visibility and security