Packet Sniffing and Analysis with Wireshark

Wireshark Packet Sniffing Report

Name: Chandima Kavishka

Date: June 21, 2025

Course: Vulnerability Assessment and Penetration Testing - II

Packet Sniffing and Analysis with Wireshark

1. Introduction

Packet sniffing is a technique used to monitor and capture network traffic. This project uses Wireshark,
a free and powerful packet analysis tool, to capture and analyze real-time network traffic. The goal is to identify protocols,
detect security issues, and understand how data is transmitted over a network.

2. Tools and Setup

- Wireshark (Version: Latest)
- Operating System: Windows 10
- Browser: Chrome
- Test Network: Home Wi-Fi
- Captured File: my_capture.pcapng

3. Methodology

1. Launched Wireshark and selected active network interface (Wi-Fi).
2. Started packet capture.
3. Opened websites like example.com and google.com.
4. Applied filters: dns, http, tcp.port == 443.
5. Stopped capture and saved file as .pcapng.
6. Analyzed specific packets and extracted data.

4. Analysis & Results

- Protocols found: Ethernet, IP, TCP, UDP, DNS, HTTP
- IPs observed: 192.168.x.x (local), 142.250.x.x (Google), 8.8.8.8 (DNS)
- DNS Queries: example.com, google.com
- HTTP requests include GET/POST methods.
- Unsecured login data found via HTTP (plaintext credentials).

5. Security Observations

- HTTP traffic is unencrypted and reveals sensitive data.
- Some POST requests may include usernames/passwords in plain text.
- Reinforces need for HTTPS and secure protocols.
- Attackers on same network could capture this data easily.

6. Conclusion

This project demonstrated how packet sniffing can expose network vulnerabilities. Tools like Wireshark help understand how data flows and uncover risks. Key takeaways include the importance of encrypted communication (HTTPS),
protocol awareness, and safe network practices.

7. References

- https://www.wireshark.org
- https://en.wikipedia.org/wiki/Wireshark
- Course materials on Network Security and VA/PT