Task 3: Networking Basics for Cyber Security

Objective

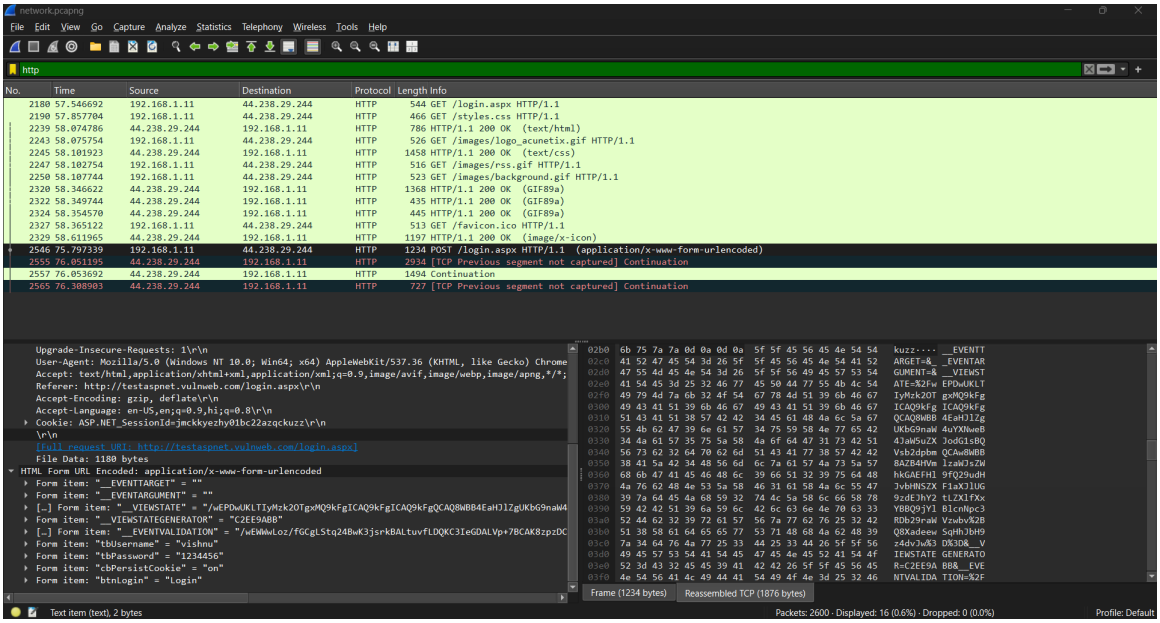
The objective of this task is to understand fundamental networking concepts and analyze live network traffic using Wireshark. This task focuses on identifying different protocols, observing TCP handshakes, analyzing DNS queries, and distinguishing between plain-text and encrypted traffic, which are essential skills for a SOC Analyst.

Tools & Environment

- Tool Used: Wireshark
- Capture File Format: PCAPNG
- Network Type: Live network traffic capture
- Protocols Analyzed: HTTP, TCP, DNS, TLS/HTTPS

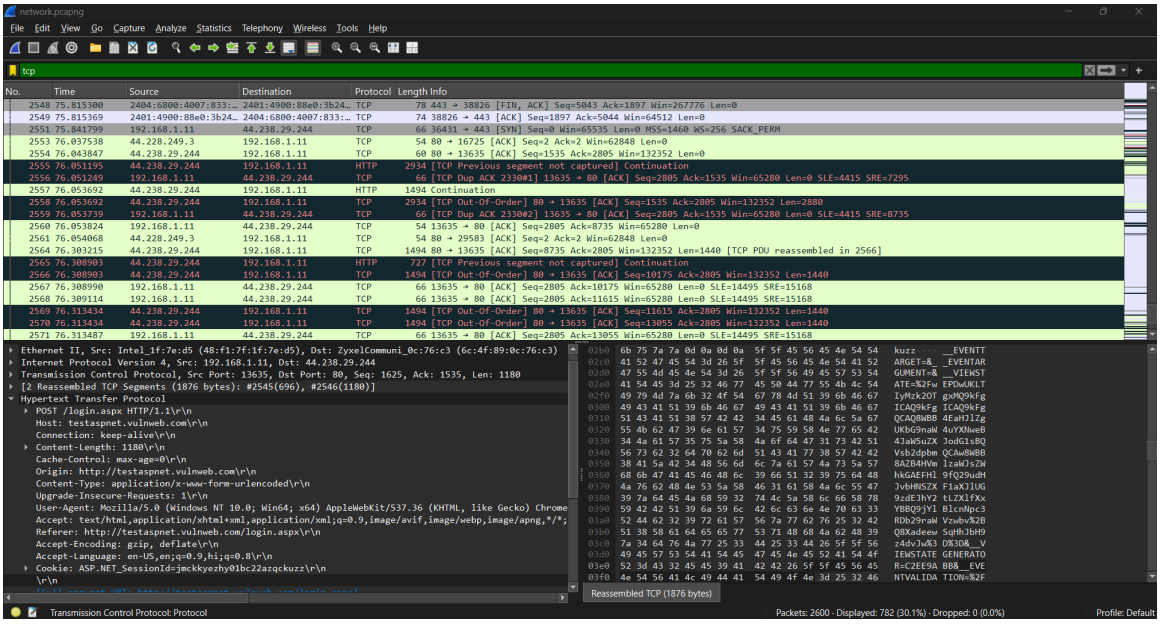
1. HTTP Traffic Analysis (Plain Text)

The HTTP filter was applied to analyze unencrypted web traffic. The captured packets show HTTP GET and POST requests. Login credentials were transmitted in plain text, demonstrating why HTTP is insecure and vulnerable to packet sniffing attacks.



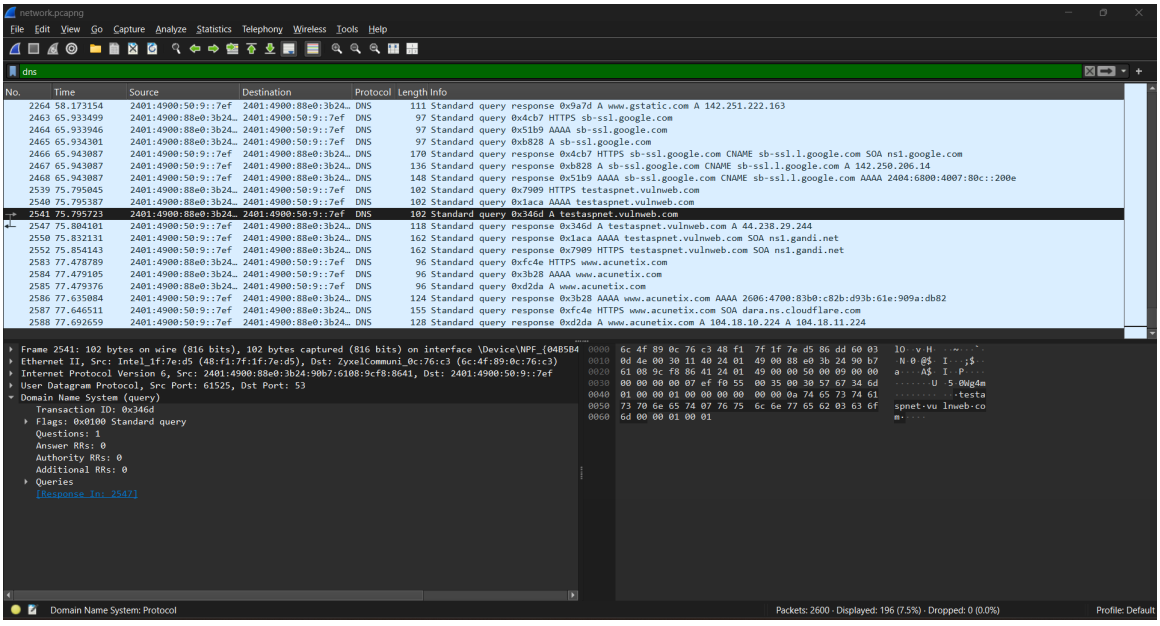
2. TCP Traffic & Session Analysis

TCP packets were analyzed to observe reliable communication between client and server. Reassembled TCP segments and acknowledgment packets confirm ordered and reliable delivery of data.



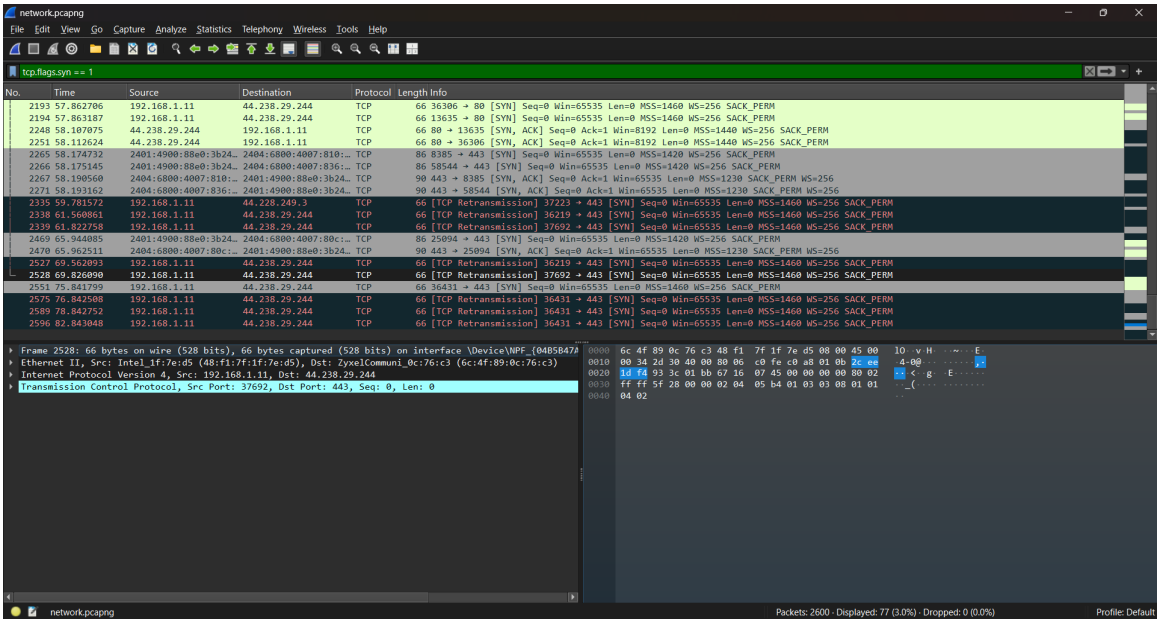
3. DNS Query Analysis

DNS traffic was captured to observe domain name resolution. Queries for domains such as testaspnet.vulnweb.com were resolved into IP addresses. DNS analysis is critical in SOC operations to detect malicious or suspicious domain activity.



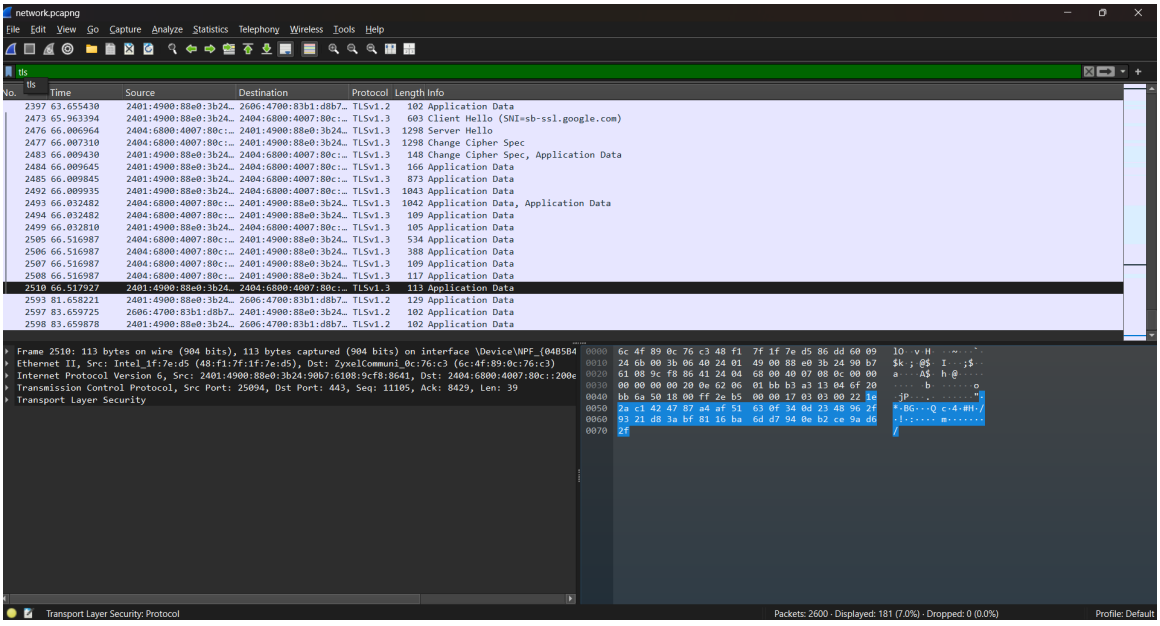
4. TCP Three-Way Handshake Observation

The TCP three-way handshake was identified using SYN, SYN-ACK, and ACK flags. This confirms how TCP establishes a connection before data transmission. Multiple SYN retransmissions were also observed, which could indicate latency or packet loss.



5. Encrypted Traffic (HTTPS / TLS)

TLS traffic was analyzed to identify encrypted communication. Unlike HTTP, the application data is unreadable, confirming encryption. TLS Client Hello and Server Hello packets were observed, demonstrating secure session establishment.



Key Observations

- HTTP traffic exposes sensitive data in plain text.
- TCP ensures reliable and ordered data transmission.
- DNS reveals domain-to-IP resolution information.
- TCP handshake confirms connection establishment.

• HTTPS encrypts data, preventing credential leakage.

Conclusion

This task provided hands-on experience in capturing and analyzing network traffic using Wireshark. Understanding protocol behavior, identifying insecure traffic, and analyzing encrypted communication are critical SOC Analyst skills. The analysis demonstrates the ability to investigate real-world network activity and identify potential security risks.