Cybersecurity Internship

Task 5: Network Traffic Analysis

Objective

- The objective of this task is to capture, inspect, and analyze network traffic using Wireshark and other tools. The analysis focuses on DNS, TCP, and ICMP protocols, along with HTTP(S) traffic such as Facebook login activity.

Tools Used

- Wireshark – for packet capture and protocol analysis
- Web Browser – to generate HTTP(S) traffic
- Ping Utility – for ICMP traffic generation

Steps Performed

1. Opened the provided PCAP file in Wireshark.
2. Inspected DNS traffic to identify domain resolution requests and responses.
3. Analyzed TCP sessions to verify handshake and data exchange.
4. Reviewed ICMP packets to confirm connectivity to external hosts.
5. Observed HTTP(S) activity related to Facebook login attempts.
6. Documented findings with screenshots for each protocol type.

Findings

- ✓ DNS – Successfully resolved domains such as facebook.com.
- ✓ TCP – Connection established using the three-way handshake on port 443 (HTTPS).
- ✓ ICMP – Successful ping to google.com with replies received.
- ✓ HTTP(S) – Captured browser session accessing Facebook login page.

Conclusion

- The network traffic captured and analyzed indicates normal network behavior with DNS resolution, secure TCP connections, and ICMP connectivity. The Facebook login capture demonstrates application-layer activity within the observed session.