Task 3: Networking Basics for Cyber Security

Objective

Tools Used

Wireshark
Operating System: Windows

Networking Concepts Observed

IP Address – Identifies devices on a network
MAC Address – Physical address of network interfaces
DNS – Resolves domain names to IP addresses
TCP – Reliable, connection-based protocol
UDP – Fast, connectionless protocol

Packet Capture Process

Wireshark was installed and live network traffic was captured for approximately 5 minutes. The capture included DNS queries, TCP connections, and HTTPS traffic. The file was saved as network_capture.pcapng.

Protocol Filtering

dns – DNS queries
tcp – TCP traffic
http – Unencrypted traffic
https – Encrypted traffic

TCP Three-Way Handshake

1. SYN – Client requests connection
2. SYN-ACK – Server responds
3. ACK – Connection established

Plain Text vs Encrypted Traffic

HTTP traffic was readable, while HTTPS traffic was encrypted, showing the importance of secure communication.

DNS Analysis

DNS queries were captured showing how domain names are translated into IP addresses.

Security Observations

Encrypted traffic protects sensitive data.
DNS traffic can reveal browsing activity.
Packet analysis helps detect suspicious behavior.

Conclusion

This task provided hands-on experience with networking basics and packet analysis using Wireshark.