Task 3: Networking Basics for Cyber Security (Wireshark)

This report documents basic networking concepts and packet analysis observations using Wireshark. The objective is to understand how network traffic flows and how attackers can analyze data in transit.

1. Basic Networking Concepts

1. **IP Address:** Logical address used to identify devices on a network
2. **MAC Address:** Physical hardware address of a network interface
3. **DNS:** Translates domain names into IP addresses
4. **TCP:** Reliable, connection-oriented protocol
5. **UDP:** Fast, connectionless protocol

2. Wireshark Installation & Traffic Capture

Wireshark was installed and live network traffic was captured by selecting the active network interface. Packet capture was started and allowed to run during normal browsing activity.

3. Packet Filtering by Protocol

1. HTTP filter used to view unencrypted web traffic
2. DNS filter used to observe domain name queries
3. TCP filter used to analyze connection-based communication

4. TCP Three-Way Handshake Observation

The TCP handshake consists of SYN, SYN-ACK, and ACK packets. This process establishes a reliable connection between client and server before data transmission.

5. Plain-text vs Encrypted Traffic

HTTP traffic was visible in plain text, exposing request and response data. HTTPS traffic appeared encrypted, preventing readable content from being viewed.

6. DNS Query Analysis

DNS packets revealed domain names being queried by the system. This demonstrates how attackers can monitor browsing behavior through DNS traffic.

7. Saving Packet Captures

Captured traffic was saved as a .pcap file for offline analysis and future reference.

8. Observations (Simple Language)

1. Network traffic contains sensitive information if not encrypted
2. DNS requests reveal visited websites
3. TCP ensures reliable data delivery
4. Wireshark helps visualize and understand network behavior

9. Summary

Analyzing network traffic is a critical cyber security skill. Wireshark allows security professionals to detect insecure communication, troubleshoot issues, and identify suspicious activity on a network.