CYBER SECURITY INTERNSHIP – TASK 3

Networking plays a crucial role in cyber security as data is constantly transferred between devices over networks. Understanding how data packets move and how they can be analyzed helps in detecting security issues and threats. This task focuses on capturing and analyzing network traffic using Wireshark.

Tools Used

- Wireshark
- Wi-Fi Network
- Windows Operating System

Basic Networking Concepts

IP Address

An IP address is a unique identifier assigned to each device on a network.

MAC Address

A MAC address is a physical address assigned to a network interface card.

TCP

Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol.

UDP

User Datagram Protocol (UDP) is faster but does not guarantee delivery.

DNS

Domain Name System (DNS) converts domain names into IP addresses.

Packet Capture Process

Wireshark was used to capture live network traffic over a Wi-Fi connection. During the capture, various websites were accessed to generate network traffic. The capture was stopped after sufficient packets were collected for analysis.

Packet Analysis and Observations

DNS Traffic Analysis

A DNS query was observed where the client device requested the IP address for the domain `realtime.chatgpt.com`. This shows how DNS resolves domain names before communication begins.

Encrypted Traffic Analysis (HTTPS)

After DNS resolution, encrypted traffic using TLSv1.2 was observed between the client system and the server. The packets contained application data, indicating secure communication.

TCP Communication

TCP packets were observed, demonstrating reliable communication using the TCP three-way handshake.

Plain Text vs Encrypted Traffic

- **HTTP:** Data is transmitted in plain text and is not secure.
- **HTTPS:** Data is encrypted using TLS, making communication secure.