

Cyber Security Internship – Task 3

Networking Basics for Cyber Security

Objective

To understand basic networking concepts and analyze network traffic for cyber security purposes.

Basic Networking Concepts

IP Address identifies devices on a network. MAC Address is a unique hardware address. DNS converts domain names into IP addresses.

TCP and UDP

TCP is connection-oriented and reliable. UDP is connectionless and faster but less reliable.

TCP Three-Way Handshake

The TCP handshake includes SYN, SYN-ACK, and ACK steps to establish a reliable connection.

Packet Sniffing

Packet sniffing is the process of capturing and analyzing network packets using tools like Wireshark.

HTTP vs HTTPS

HTTP sends data in plain text, while HTTPS encrypts data, making it more secure.

DNS Analysis

DNS queries resolve website names into IP addresses so browsers can connect to servers.

Observations

Network traffic analysis helps identify protocols, detect insecure communication, and understand data flow.

Final Outcome

Improved understanding of networking fundamentals and packet analysis for cyber security.