CYBER SECURITY INTERNSHIP – Task 3

Networking Basics for Cyber Security

This document explains networking fundamentals and packet analysis using Wireshark.

Introduction

Networking is essential for cybersecurity professionals to analyze and secure data transmission.

Basic Networking Concepts

IP Address identifies devices.
MAC Address identifies network interfaces.
DNS converts domain names into IP addresses.
TCP is reliable and connection-oriented.
UDP is fast and connectionless.

Packet Capture Using Wireshark

Wireshark was used to capture live network traffic for analysis.

Filtering Network Traffic

Traffic was filtered using protocols such as HTTP, DNS, TCP, and UDP.

TCP Three-Way Handshake

TCP establishes a connection using SYN, SYN-ACK, and ACK packets.

Plain-text vs Encrypted Traffic

HTTP traffic is readable in packet captures, while HTTPS traffic is encrypted.

DNS Analysis

DNS queries and responses were captured and analyzed.

Observations

Multiple protocols are present in network traffic.
DNS resolves domain names.
HTTPS protects sensitive information.

Interview Questions

What is TCP handshake?
Difference between TCP and UDP?
What is DNS?
What is packet sniffing?
Why is HTTPS more secure than HTTP?

Final Outcome

Ability to capture and analyze network traffic effectively.