

Task 03 – Networking Basics for Cyber Security

Introduction

In this task, I learned the basics of computer networking and how networking concepts are important in cyber security. I explored how data travels through a network and how attackers can analyze network traffic.

Tools Used

Wireshark was used to capture and analyze live network traffic on my system.

What I Did

I installed Wireshark and started capturing live network packets. I observed DNS queries, TCP connections, and HTTP/HTTPS traffic. I applied filters such as DNS, TCP, and HTTP to analyze packets clearly. I studied the TCP three-way handshake (SYN, SYN-ACK, ACK).

Observations

DNS packets show how domain names are resolved to IP addresses. TCP provides reliable communication, while UDP is faster but unreliable. HTTP traffic can be read in plain text, whereas HTTPS is encrypted and secure.

Learning Outcome

This task helped me understand packet sniffing, network protocols, and how attackers analyze traffic.