

Task 3 – Networking Basics for Cyber Security

Objective

The goal of this task was to understand basic networking concepts and analyze live network traffic using Wireshark. This included identifying encrypted and plain-text traffic, observing TCP handshake, and capturing DNS queries.

Tools Used

- Wireshark

Procedure

1. Captured live traffic using Wireshark.
2. Applied protocol filters such as HTTP, TLS, DNS, TCP.
3. Observed TCP three-way handshake.
4. Identified encrypted and plain-text traffic.
5. Captured and analyzed DNS queries.

TCP Three-Way Handshake

SYN -> SYN-ACK -> ACK

Plain-text vs Encrypted Traffic

HTTP shows readable data.

HTTPS shows encrypted data.

DNS Analysis

Captured domain queries and IP responses.

Observations

- HTTP exposes data.
- HTTPS secures communication.
- DNS resolves domain names.
- TCP ensures reliable connection.

Conclusion

This task improved understanding of real-time network traffic analysis using Wireshark.