Cyber Security Internship – Task 3

Networking Basics for Cyber Security

1. Introduction

Networking is a core part of cyber security. Understanding how data travels across a network helps identify security risks and malicious activities. In this task, Wireshark was used to capture and analyze network traffic.

2. Basic Networking Concepts

- **IP Address:** Every device on a network has an IP address which helps identify it.
- **MAC Address:** A unique physical address assigned to a network interface.
- **DNS:** Converts website names (like google.com) into IP addresses.
- **TCP:** A reliable protocol that ensures data is delivered correctly.
- **UDP:** A faster protocol that does not guarantee delivery.

3. Live Network Traffic Capture

Wireshark was installed and used to capture live network traffic. Traffic was captured while browsing websites using a web browser. Various packets were visible in real time.

4. Packet Filtering by Protocol

Filters such as `http`, `dns`, and `tcp` were applied in Wireshark.
This helped in viewing only specific types of network packets instead of all traffic.

5. TCP Three-Way Handshake

The TCP handshake was observed using TCP packets.
It includes:

1. **SYN** – Client requests connection
2. **SYN-ACK** – Server responds
3. **ACK** – Connection is established

This ensures reliable communication between devices.

6. Plain-Text vs Encrypted Traffic

- **HTTP traffic:** Data is visible in plain text and can be read.
- **HTTPS traffic:** Data is encrypted and cannot be read easily.

Most websites now use HTTPS for better security.

7. DNS Query Analysis

DNS packets were observed when accessing websites.
DNS requests were sent to resolve domain names into IP addresses before loading the website.

8. Saving Packet Captures

The captured network traffic was saved as a `.pcapng` file.
This allows further analysis of network activity at any time.

9. Overall Observation

This task helped in understanding how network communication works and how tools like Wireshark can be used to monitor traffic, identify protocols, and analyze security-related information.

10. Conclusion

This task helped me understand basic networking concepts and how to analyze network traffic using Wireshark. It improved my ability to identify protocols, DNS queries, and encrypted traffic.