CYBER SECURITY INTERNSHIP

Task 3: Networking Basics for Cyber Security

Networking knowledge is a core requirement in cybersecurity because most attacks and defenses occur over networks. In this task, I studied basic networking concepts and used Wireshark to capture and analyze real network traffic. The aim was to understand how data flows across a network and how insecure communication can expose sensitive information.

1. Basic Networking Concepts

I learned fundamental networking concepts such as IP address, MAC address, DNS, TCP, and UDP. IP addresses identify devices on a network, MAC addresses identify network interfaces, DNS resolves domain names to IP addresses, and TCP/UDP are used to transmit data between systems.

2. Packet Capturing Using Wireshark

Wireshark was installed to capture live network traffic. By selecting the active network interface, I observed packets being transmitted in real time, including DNS queries, TCP connections, and encrypted HTTPS traffic.

3. Packet Filtering and Protocol Analysis

Filters such as http, dns, and tcp were applied to focus on specific protocols. Filtering helped reduce noise and made packet analysis more effective and manageable.

4. TCP Three-Way Handshake

The TCP three-way handshake was identified using SYN, SYN-ACK, and ACK packets. This process ensures a reliable connection is established before data transmission.

5. Plain-text vs Encrypted Traffic

Plain-text traffic such as HTTP allows packet contents to be read directly, while HTTPS traffic is encrypted and unreadable. This clearly shows why encrypted protocols are essential for security.

6. DNS Traffic Analysis

DNS packets were captured to analyze how domain names are resolved into IP addresses. This demonstrated how attackers could gain useful information from DNS traffic if it is not protected.

Observations

- Normal browsing generates a large amount of network traffic.
- Packet filtering is essential for clear analysis.
- Unencrypted traffic exposes sensitive data.
- DNS traffic reveals metadata about user activity.
- Encrypted protocols significantly improve security.

Final Outcome

This task improved my ability to analyze network traffic using packet capture tools. I gained hands-on experience with Wireshark and developed a stronger understanding of how networking knowledge is applied in cybersecurity monitoring and analysis.