Cyber Security Internship – Task 3

Networking Basics for Cyber Security

---

1. Introduction

Networking plays a very important role in cyber security because most attacks happen over networks. Understanding how data travels between devices helps in identifying suspicious or malicious activity. In this task, I learned basic networking concepts and analyzed network traffic using Wireshark.

---

2. Basic Networking Concepts

IP Address

An IP address is a unique identifier assigned to a device on a network. It helps devices communicate with each other over the internet or a local network.

MAC Address

A MAC address is a hardware address assigned to a network interface. It is used for communication within a local network.

DNS (Domain Name System)

DNS converts human-readable domain names like google.com into IP addresses so that computers can locate servers.

TCP (Transmission Control Protocol)

TCP is a reliable protocol that ensures data is delivered correctly and in order.

UDP (User Datagram Protocol)

UDP is a faster but unreliable protocol that does not guarantee delivery. It is commonly used for streaming and online games.

---

3. Packet Sniffing Using Wireshark

Wireshark is a network packet analyzer used to capture and inspect network traffic in real time. It allows visibility into what data is being transmitted over the network.

Using Wireshark, I captured live network traffic and observed different types of packets such as TCP, DNS, and HTTP.

---

4. Filtering Network Traffic

Wireshark provides filters to analyze specific protocols:

- tcp → Shows TCP packets
- udp → Shows UDP packets
- dns → Shows DNS queries
- http → Shows HTTP traffic

Filtering helps focus on relevant packets and makes analysis easier.

---

5. TCP Three-Way Handshake

The TCP connection process follows a three-step handshake:

1. **SYN** – Client requests a connection
2. **SYN-ACK** – Server acknowledges the request
3. **ACK** – Client confirms the connection

This handshake ensures a reliable connection before data transfer begins.

---

6. Plain Text vs Encrypted Traffic

- **HTTP traffic** sends data in plain text, meaning it can be easily read by attackers.
- **HTTPS traffic** encrypts data, making it unreadable even if intercepted.

While observing packets, encrypted HTTPS traffic appeared unreadable, showing the importance of encryption.

---

7. DNS Traffic Analysis

DNS queries were captured to observe how domain names are resolved into IP addresses. Each DNS request and response showed communication between the client and DNS server.

DNS analysis helps in detecting suspicious or malicious domain requests.

---

8. Saving Packet Captures

Captured network traffic was saved as a packet capture file (.pcap) for later analysis. Saving captures allows deeper inspection and sharing evidence if required.

---

9. Summary

This task helped me understand basic networking concepts and how network traffic can be analyzed using Wireshark. Observing protocols like TCP, DNS, and HTTP provided practical insight into how data flows across networks and how encryption helps protect information.