CYBER SECURITY INTERNSHIP – TASK 3

Understanding Cyber Security Basics & Attack Surface

Name: Anshu Pratap Giri
Internship Domain: Cyber Security
Task: 3
Tools Used: Wireshark

🌐 Basic Networking Concepts

1️⃣ IP Address (Internet Protocol Address)

An **IP address** is a **logical address** assigned to each device connected to a network. It is used to **identify and locate devices** so data can reach the correct destination.

Types of IP Addresses:

- **IPv4:** 32-bit address
  Example: 192.168.1.1
- **IPv6:** 128-bit address
  Example: 2001:0db8::1

Example:

When you open google.com, your device uses an IP address to communicate with Google's server.

Importance in Cyber Security:

- Helps identify source and destination of traffic
- Used in firewall rules and network monitoring
- Attackers may hide or spoof IP addresses

2️⃣ MAC Address (Media Access Control Address)

A **MAC address** is a **physical hardware address** assigned to a network interface card (NIC) by the manufacturer.

Features:

- Unique for every device
- Fixed and hard-coded
- 48-bit address

Example:

00:1A:2B:3C:4D:5E

Difference from IP:

IP Address	MAC Address
Logical	Physical
Can change	Permanent
Works at Network Layer	Works at Data Link Layer

Cyber Security Importance:

- Used in device identification
- MAC filtering in networks
- Can be spoofed by attackers

3️⃣ DNS (Domain Name System)

DNS converts **human-readable domain names** into **IP addresses**.

Why DNS is Needed?

Humans remember names, computers understand numbers.

Example:

google.com → 142.250.182.14

How DNS Works:

1. User enters website name
2. DNS query is sent
3. DNS server responds with IP address
4. Browser connects to the IP

Cyber Security Risks:

- DNS spoofing
- DNS poisoning
- Phishing attacks

4️⃣ TCP (Transmission Control Protocol)

TCP is a **reliable, connection-oriented protocol** used for accurate data delivery.

Key Features:

- Uses **three-way handshake**
- Ensures data reaches correctly

- Error checking and retransmission

TCP Three-Way Handshake:

1. SYN
2. SYN-ACK
3. ACK

Examples:

- Web browsing (HTTPS)
- Email
- File transfer

Cyber Security Importance:

- Can be monitored for attacks
- Used in DoS/DDoS attacks

5️⃣ UDP (User Datagram Protocol)

UDP is a **connectionless and fast protocol** that does not guarantee delivery.

Key Features:

- No handshake
- Faster than TCP
- No error correction

Examples:

- Video streaming
- Online gaming
- Voice calls

Cyber Security Importance:

- Used in amplification attacks
- Harder to track due to no connection

🔄 TCP vs UDP (Quick Comparison)

Feature	TCP	UDP
Connection	Yes	No
Reliability	High	Low

Feature	TCP	UDP
Speed	Slower	Faster
Use Case	Web, Email	Streaming, Games