Task 3: Networking Basics for Cyber Security

Networking is very important in cyber security because all data travels through networks. If we understand how data moves from one system to another, it becomes easier to detect attacks, data leaks, and suspicious activity.

1. Basic Networking Concepts
Before analyzing traffic, it is important to understand some basic networking terms.
An IP address is like the home address of a device on a network. It helps data reach the correct system.
MAC address is a unique physical address of a network device and is mostly used inside local networks.
DNS is like the internet's phone book. It converts website names like google.com into IP addresses.
TCP is a reliable protocol that ensures data reaches correctly and in order.
UDP is faster but does not guarantee delivery, and is used for streaming and online games.

2. Capturing Live Network Traffic Using Wireshark
Wireshark is a tool used to capture and analyze network traffic. After installing Wireshark, I selected the active network interface and started capturing packets. While browsing websites and using apps, Wireshark showed live data packets moving across the network.

3. Filtering Packets by Protocol
Wireshark captures a lot of data, so filters are used to view specific traffic.
By using filters like http, dns, or tcp, I was able to see only the packets related to those protocols. This made analysis much easier and clearer.

4. Observing the TCP Three-Way Handshake
The TCP connection starts with a three-way handshake.
First, the client sends a SYN packet to the server.
Then the server replies with SYN-ACK.
Finally, the client sends ACK, and the connection is established.
This process ensures that both systems are ready to communicate.

5. Plain-Text Traffic vs Encrypted Traffic
While observing packets, I noticed that HTTP traffic shows data in readable plain text. This means usernames or messages can be seen easily.
On the other hand, HTTPS traffic is encrypted, so the data is not readable. This shows why encryption is very important for security.

6. Capturing and Analyzing DNS Queries
When a website is opened, a DNS query is sent to find the IP address of that website.
In Wireshark, I captured DNS packets and observed domain names being requested. This helped me understand how systems resolve website names before connecting to them.

7. Saving Packet Captures
Wireshark allows saving captured packets as files.
These saved files can be opened later for analysis or shared with others. This is useful in investigations and learning purposes.

8. Observations and Learning
By using Wireshark, I understood how data travels in a network. I learned how to filter traffic, identify protocols, observe handshakes, and understand the difference between secure and insecure communication. This practical experience helped me understand real network behavior.

Interview Questions:

1. What is TCP handshake?
TCP handshake is the process used to create a reliable connection between two devices before data transfer starts.
It happens in three steps. First, the client sends a request to start communication. Then the server replies that it is ready. Finally, the client confirms it. After this, both sides can safely exchange data.

2*. Difference between TCP and UDP?*
TCP is a reliable protocol. It makes sure data reaches the destination correctly and in the right order. If something is missing, it is sent again. This is why TCP is used in emails, web browsing, and file transfer.
UDP is a faster protocol but it is not reliable. It does not check whether data reaches or not. Because of this, it is used in video streaming, online games, and voice calls where speed is more important than accuracy.

3*. What is DNS?*
DNS stands for Domain Name System. It works like the internet's contact list.
When we type a website name like google.com, DNS converts it into an IP address so the system knows where to connect.

4. *What is packet sniffing?*
Packet sniffing is the process of capturing and analyzing network data packets as they travel through a network.
Tools like Wireshark are used for this. It is useful for troubleshooting and security analysis, but attackers can also misuse it to steal information if data is not encrypted.

5. *Why is HTTPS more secure than HTTP?*
HTTPS is more secure because it encrypts data before sending it over the internet.

This means even if someone captures the data, they cannot read it. HTTP sends data in plain text, which can be easily seen by attackers. HTTPS protects sensitive information like passwords and personal details.