TASK 3

What is TCP handshake?

The TCP handshake is a three-step process used to establish a reliable connection between two devices before data transfer begins. First, the client sends a request to start communication. The server responds by acknowledging this request. Finally, the client confirms the acknowledgment. This process ensures that both devices are ready to communicate and agree on connection parameters.

Difference between TCP and UDP?

TCP and UDP are transport layer protocols, but they work differently. TCP is connection-oriented and ensures reliable, ordered, and error-checked data delivery, making it suitable for applications like web browsing and email. UDP is connectionless and does not guarantee delivery or order, but it is faster and used in applications like video streaming, online gaming, and DNS.

What is DNS?

DNS (Domain Name System) is a system that translates domain names into IP addresses so that computers can locate each other on the internet. Instead of remembering numeric IP addresses, users can simply type website names, and DNS handles the conversion automatically.

What is packet sniffing?

Packet sniffing is the practice of capturing and examining data packets as they travel across a network. It is commonly used by network administrators to monitor traffic and troubleshoot problems. However, it can also be misused by attackers to intercept sensitive information if the data is not encrypted.

Why is HTTPS more secure than HTTP?

HTTPS is more secure than HTTP because it uses SSL/TLS encryption to protect data transmitted between the user and the server. This encryption prevents unauthorized parties from reading or altering the data. HTTPS also verifies the identity of websites, ensuring secure and trustworthy communication.