WEEK-01

Cloud Infra and Security

Name **: Divya Shivnath Khedkar**

College Name **: MITAOE**
Task -03

- **<u>Prepare R&D Document working of TCP & UDP Protocols, working of HTTP, HTTPs & ICMP Protocol</u>**

    - **Introduction**
      In computer networks, different protocols handle data in their own ways to make communication smooth, safe, and reliable. This document explains how five important Internet protocols work:

- **TCP -** Transmission Control Protocol
- **UDP -** User Datagram Protocol
- **HTTP -** Hypertext Transfer Protocol
- **HTTPS -** HTTP Secure
- **ICMP -** Internet Control Message Protocol

<u>1. Transmission Control Protocol (TCP)</u>

- **Where it works:** Transport Layer
- **What it does:**
  TCP makes sure data is sent correctly and in the right order between devices. It creates a reliable connection for communication.
- **How it works:**
    - First, TCP sets up a connection using a three-step handshake (SYN, SYN-ACK, ACK).
    - It breaks data into smaller parts called segments, numbers them, and checks that all arrive safely.
    - If errors happen, it asks for the data to be sent again.
    - TCP controls the data flow so the network doesn't get overwhelmed.
    - When finished, it closes the connection with a four-step process.
- **Where it's used:**
  Email services, web browsing, and file transfers.

---

2. User Datagram Protocol (UDP)

- **Where it works:** Transport Layer
- **What it does:**
  UDP sends data quickly without setting up a connection first. It's great for apps that need speed over accuracy.
- **How it works:**
  - No handshake or connection setup is done.
  - Data is sent as separate packets called datagrams.
  - The sender doesn't wait for confirmation, so packets may get lost or arrive out of order.
  - It can optionally check for errors with a simple checksum.
- **Where it's used:**
  Streaming videos, online games, and DNS lookups.

🔹 3. Hypertext Transfer Protocol (HTTP)

- **Where it works:** Application Layer
- **What it does:**
  HTTP is used by browsers and servers to request and deliver web pages. It's stateless, meaning each request is independent.
- **How it works:**
  - The browser sends a request (like GET or POST) to the server.
  - The server replies with the requested data and a status code (like 200 OK).
  - Communication happens over TCP, usually on port 80.
  - Cookies or tokens are used to maintain user sessions across requests.
- **Where it's used:**
  Loading websites and web-based APIs.

🔹 4. HTTP Secure (HTTPS)

- **Where it works:** Application Layer
- **What it does:**
  HTTPS is like HTTP but with security added through encryption to keep data private and safe.
- **How it works:**
  - It starts with a TCP handshake.
  - Then, a TLS handshake happens where keys and certificates are exchanged to create a secure channel.
  - After that, all data transferred is encrypted.
  - Certificates are checked and verified by trusted authorities.

- **Where it's used:**
  Online banking, login pages, and any site requiring secure data transfer.

🔹 5. Internet Control Message Protocol (ICMP)

- **Where it works:** Network Layer
- **What it does:**
  ICMP is used mainly for network troubleshooting and sending error messages, not for transferring regular data.
- **How it works:**
  - Routers and devices send ICMP messages when problems occur (like unreachable destinations).
  - It is also used by tools like ping to check if a device is reachable.
  - Unlike TCP or UDP, it doesn't use ports and does not carry user data.
- **Where it's used:**
  Ping commands, traceroute, and network diagnostics.

Protocol	Layer	Reliable	Connection-Based	Encrypted	Main Use
TCP	Transport	Yes	Yes	No	File transfers, emails
UDP	Transport	No	No	No	Streaming, gaming
HTTP	Application	Reliable via TCP	Yes (TCP)	No	Web browsing, APIs
HTTPS	Application	Reliable via TCP	Yes (TCP)	Yes	Secure browsing, payments
ICMP	Network	No	N/A	No	Network tests and errors
