Weekly Assignment

1. Among A and B, identify which are software layers and which are hardware layers in the OSI Model.

A

• Application layer

• Presentation layer

• Session layer

B

• Network layer

• Datalink layer

• Physical layer

Answer:

In the Open Systems Interconnection (OSI) Model the below are the software layers and hardware layers

A (Software Layers):

- Application layer
- Presentation layer
- Session layer

B (Hardware Layers):

- Network layer
- Data Link layer
- Physical layer

2. HTTPS utilizes which protocol for security?

Answer:-

HTTPS (HyperText Transfer Protocol Secure) leverages Transport Layer Security (TLS) to ensure encryption, authentication, and data integrity for secure network communication.

Detailed breakdown of TLS in HTTPS:

1. **Encryption**: TLS employs both asymmetric and symmetric encryption to secure data. Initially, during the handshake, asymmetric encryption (public and private keys) is used to exchange a symmetric key, which then encrypts data for the session.
2. **Authentication**: The server provides a digital certificate from a trusted Certificate Authority (CA), which the client verifies to confirm the server's identity, thwarting man-in-the-middle attacks.
3. **Data Integrity**: Message Authentication Codes (MACs) in TLS ensure that the data has not been altered during transmission.

TLS Handshake Process:

- **Client Hello**: The client sends a request including supported TLS versions, encryption algorithms, and a random number.
- **Server Hello**: The server responds with its supported TLS version, chosen encryption algorithm, digital certificate, and another random number.
- **Key Exchange**: The client and server exchange keys. The client encrypts a session key with the server's public key, which only the server can decrypt with its private key.
- **Session Key Generation**: The session key creates a secure, encrypted communication channel.
- **Secure Communication**: Data between the client and server is encrypted using the session key.

3. Apart from LAN, VAN and MAN, what do you understand by VPN?

Answer:-

A VPN (Virtual Private Network) establishes a secure and encrypted connection over a public network, offering:

1. **Security**: Encrypts data to protect it from unauthorized access.
2. **Privacy**: Masks the user's IP address to enhance anonymity.
3. **Remote Access**: Enables secure connection to a private network from a remote location.
4. **Bypassing Geo-Restrictions**: Allows access to region-restricted content by routing traffic through servers in different locations.
5. **Data Integrity**: Ensures that data remains unaltered during transmission.

How VPN Works:

- **Client Software**: User installs VPN client software on their device.

- **Connection Establishment**: The client connects to a VPN server, creating an encrypted tunnel for data transmission.
- **Data Encryption**: Data is encrypted before transmission and decrypted by the VPN server.
- **Secure Communication**: Reverses the process for received data, ensuring secure communication.

Types of VPNs:

- **Remote Access VPN**: For individuals to securely connect to a private network remotely.
- **Site-to-Site VPN**: Connects entire networks securely over the internet.
- **Personal VPN**: For privacy, security, and accessing restricted content.

4. Digital Signatures, As the name sounds are the new alternative to signing a document digitally. What other authenticity you have used over network in regular life?

Answer:-

1. **Two-Factor Authentication (2FA)**: Requires two forms of verification (e.g., password and a verification code on a mobile device).
2. **Biometric Authentication**: Uses unique biological traits (e.g., fingerprints, facial recognition) for identity verification.
3. **Public Key Infrastructure (PKI)**: Utilizes a pair of keys (public and private) and digital certificates to authenticate identities.
4. **SSL/TLS Certificates**: Authenticate website identity and establish encrypted connections.
5. **OAuth**: An open standard for access delegation, allowing limited access without exposing passwords.
6. **CAPTCHA**: Verifies that the user is human and not an automated bot.
7. **Email Verification**: Sends a verification link or code to confirm identity.
8. **SMS Verification**: Sends a one-time password (OTP) to a mobile phone for identity verification.
9. **Blockchain Verification**: Uses blockchain technology for secure and tamper-proof records.
10. **Access Tokens**: Provide secure API access without repeatedly sharing credentials.
11. **MAC Address Filtering**: Restricts network access based on device hardware addresses.
12. **Security Questions**: Uses pre-set questions for identity verification, often in account recovery.

5. After successful authentication, *authorization* determines the resources a user can access and the actions they can perform.

6. A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic, and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

Consider above Packet firewall rule. Now Network IP: 192.168.21.0, Trying to connect to your machine and want to send data. Ils the Action allowed, as per above table firewall rule? (Allow/Deny)

Answer:-

Given the firewall rules and the network IP: 192.168.21.0 trying to connect:

- Incoming packets from network 192.168.21.0 are blocked.
- Incoming packets to the internal TELNET server (port 23) are blocked.
- Incoming packets to host 192.168.21.3 are blocked.
- All well-known services to network 192.168.21.0 are allowed.

Action: Deny

7. *Firewalls* (application layer, software, hardware) prevent malicious data from reaching applications. Without them, applications are vulnerable to malicious data.

8. *Subnetting* divides a larger network into smaller, manageable sub-networks to enhance security and simplify routing table management.

9. Move A and B to corresponding IP assignment?

Answer:-

Static IP Address:

- **A)** This IP address does not change and remains constant, provided by an ISP. It is easily traceable.

Dynamic IP Address:

- **B)** These addresses change and are assigned by DHCP, making them harder to trace.

10. Differences between MAC address, IP address, and Network address?

Answer:-

1. **Purpose and Scope**:
    - **MAC Address**: Uniquely identifies a network interface card (NIC) on a local network (Layer 2).
    - **IP Address**: Identifies a device on a network and routes data between networks (Layer 3).
    - **Network Address**: Represents an entire network or subnet, aiding in routing between networks.
2. **Permanence and Assignment**:
    - **MAC Address**: Fixed, hard-coded into the NIC, and typically static.
    - **IP Address**: Can be static or dynamic, assigned by DHCP or manually configured.
    - **Network Address**: Defined by network administrators, typically stable unless the network changes.

11. Match numbers with letters according to OSI layer roles:

1.Application Layer:

2.Presentation Layer:

3.Session Layer:

4.Transport Layer

5.Network Layer

6.Data Link Layer

7.Physical Layer

A. Bit Stream, physical medium, Cable, Connectors

B. MAc Address, Flow control, Frames, switches, ARP

C. Coding into 1s and 0s, encryption, compression, JPG, HTTPS, SSL,TSL, ASCII, Data

D. Authentication, Permission, connection between two hosts, NetBIOS, PPTP, RPC, API, Data

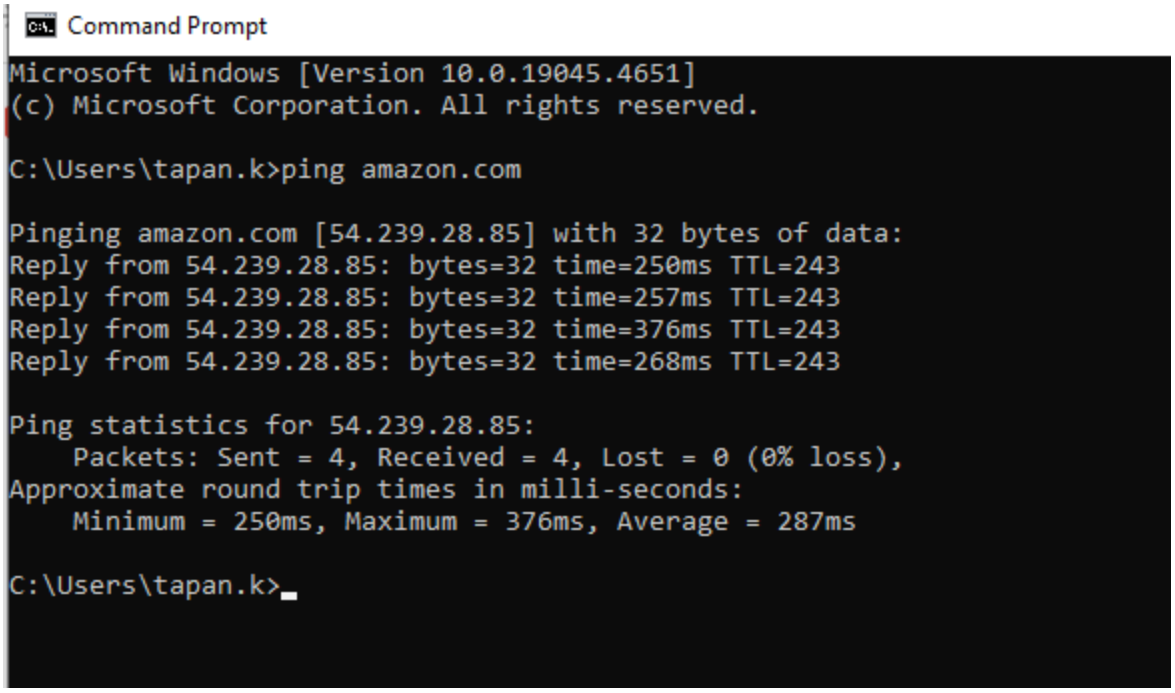
E. End-to-End Error Control, TCP, UDP, Segment F. Routing , switching, IPV4,IPV6, IPSec, Packet

G. Message format, Human-Machine interfaces, HTTP, FTP, Data

Answer:-

1. **Application Layer**:
    - **G)** Message format, Human-Machine interfaces, HTTP, FTP, Data
2. **Presentation Layer**:
    - **C)** Coding into 1s and 0s, encryption, compression, JPG, HTTPS, SSL, TLS, ASCII, Data
3. **Session Layer**:
    - **D)** Authentication, Permission, connection between two hosts, NetBIOS, PPTP, RPC, API, Data
4. **Transport Layer**:
    - **E)** End-to-End Error Control, TCP, UDP, Segment
5. **Network Layer**:
    - **F)** Routing, switching, IPv4, IPv6, IPSec, Packet
6. **Data Link Layer**:
    - **B)** MAC Address, Flow control, Frames, switches, ARP
7. **Physical Layer**:
    - **A)** Bit Stream, physical medium, Cable, Connectors

12.DNS is a host name to IP address translation service. Use ping amazon.com and share IP address.



13.Consider below network address and subnetID.
1. Network Address: 172.16.0.0
2. Subnet ID: 172.16.0.0/16
From the routing table, which Interface should be choosen for Network ID 172.16.0.0: (A/B)
Routing Table:
Network ID Subnet Mask Interface
200.1.2.0 255.255.255.192 A
172.16.0.0 255.255.255.193 B

Answer:-

Network Details:

- Subnet ID: 172.16.0.0/16
- Subnet Mask: 255.255.0.0

Routing Table:

- Network ID: 200.1.2.0, Subnet Mask: 255.255.255.192, Interface: A
- Network ID: 172.16.0.0, Subnet Mask: 255.255.255.193, Interface: B

Analysis:

1. **Subnet Mask Comparison:**
    - The given Subnet ID 172.16.0.0/16 has a subnet mask of 255.255.0.0.
    - The routing table entry for 172.16.0.0 has a subnet mask of 255.255.255.193, which is incorrect for a /16 network.
2. **Longest Prefix Match:**
    - In routing, the longest prefix match rule is used to determine the best route. However, the subnet mask 255.255.255.193 is not a standard subnet mask and does not correctly represent a /16 network.

Correction: If the subnet mask 255.255.255.193 in the routing table is a typo and was intended to be 255.255.0.0, then:

- Interface B should be used because it matches the network 172.16.0.0 directly.

Conclusion:

- If the subnet mask 255.255.255.193 is incorrect and should be 255.255.0.0, then **Interface B** is the correct choice.
- If the subnet mask 255.255.255.193 is correct and you need to select an interface based on the given routing table, it indicates a potential routing issue.

Therefore, considering standard practices and assuming the subnet mask was meant to be 255.255.0.0:

The correct interface to use is Interface B.