Name:Sownthari R P

Week 2 Assignment

1.Among A and B, select which one is the software layer and which one is the hardware layer in the Open Systems Interconnection Model.

A. **Application layer**
   Presentation layer
   Session layer

B. **Network layer**
   Datalink layer
   Physical layer

In the Open Systems Interconnection (OSI) model:

A: Software Layer

B: Hardware Layer

2. HTTPS uses which protocol for security?

HTTPS (Hypertext Transfer Protocol Secure) uses the Transport Layer Security (TLS) protocol to provide encrypted communication and secure identification of a network web server. TLS ensures the privacy and data integrity between the client (e.g., a web browser) and the server by encrypting the data transmitted, protecting it from eavesdropping and tampering.

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

A VPN (Virtual Private Network) is a technology that creates a secure, encrypted connection over a less secure network, such as the internet. It allows users to send and receive data as if their devices were directly connected to a private network, providing privacy and security.

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.

In addition to digital signatures, other methods of authentication commonly used over networks include:

1. **Password Authentication:** Using usernames and passwords to verify identity.
2. **Two-Factor Authentication (2FA):** Combining something you know (password) with something you have (e.g., a smartphone app or SMS code) for added security.
3. **Biometric Authentication:** Using physical characteristics such as fingerprints, facial recognition, or iris scans.
4. **OAuth Tokens:** Used in many web services to grant access without sharing passwords, often through a third-party authentication service.
5. **Security Certificates:** Certificates like those used in HTTPS to verify the authenticity of websites.

These methods help ensure secure access and verify identities in various online interactions.

5. After the authentication is successful, authorization **(Authorization/Communication) can be used to determine what resources is the user allowed to access and the operations that can be performed.**

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

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

- If the source IP is 192.168.21.0, Rule 1 denies the action regardless of other conditions.
- Rule 4 allows the connection from the source IP 192.168.21.0 only if the destination port is greater than 1023.

Since Rule 1 is a broader rule and explicitly denies traffic from 192.168.21.0, it takes precedence over Rule 4.

7. Application Layer Firewall, software Firewall and Hardware Firewall allows only destined and avoids malicious data.

If these firewalls are not installed, your application may receive **malicious** data (malicious / all Secured) data.

8.When a bigger network is divided into smaller networks, in order to maintain security and to maintain smaller networks easier using routing table, we go for Subnetting **(Subnetting/Firewall)**

9. Move A and B to the corresponding IP assignment.

Static IP Address	**Dynamic IP address**
It is provided by ISP(Internet Service Provider).	**While it is provided by DHCP (Dynamic Host Configuration Protocol).**
This IP address does not change at IP any time, which means if a IP address is provided then it can't be changed or modified and is easily traceable.	These addresses changes at any time and not easily traced.

10. List any two difference between MAC address , IP address and Network Address.

Layer of Operation and Scope:

- MAC Address: Operates at the Data Link Layer (Layer 2) of the OSI model and is used within a local network segment to uniquely identify devices.
- IP Address: Operates at the Network Layer (Layer 3) of the OSI model and is used to identify devices across different networks for routing purposes.
- Network Address: A broader term that can encompass both MAC addresses and IP addresses, referring to any identifier used to route or identify a device or node on a network.

Type and Nature of Address:

- MAC Address: A permanent, physical address assigned to the network interface card (NIC) by the hardware manufacturer, unique to each network device.
- IP Address: A logical address assigned by the network, which can be static (fixed) or dynamic (changing), used specifically for routing packets across networks.

- Network Address: Can be either a permanent (e.g., MAC address) or a temporary (e.g., dynamic IP address) identifier, encompassing any address used for routing or identification within a network.

11. Match numbers with letters according to 7 layers roles.

Application Layer - Message format, Human-Machine interfaces, HTTP, FTP, Data

Presentation Layer - Coding into 1s and 0s, encryption, compression, JPG, HTTPS, SSL, TSL, ASCII, Data

Session Layer - Authentication, Permission, connection between two hosts, NetBIOS, PPTP, RPC, API, Data

Transport Layer - End-to-End Error Control, TCP, UDP, Segment

Network Layer - Routing, switching, IPV4, IPV6, IPSec, Packet

Data Link Layer - MAC Address, Flow control, Frames, switches, ARP

Physical Layer - 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.

Domain: amazon

IP address:

Pinging amazon.com [64:ff9b::345e:ecf8] with 32 bytes of data:

Reply from 64:ff9b::345e:ecf8: time=300ms

Reply from 64:ff9b::345e:ecf8: time=448ms

Reply from 64:ff9b::345e:ecf8: time=297ms

Reply from 64:ff9b::345e:ecf8: time=250ms

Ping statistics for 64:ff9b::345e:ecf8:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 250ms, Maximum = 448ms, Average = 323ms

13. Consider below network address and subnetID.

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: 1.

Network ID	**Subnet Mask**	**Interface**
200.1.2.0	**255.255.255.192**	**A**
172.16.0.0	**255.255.255.193**	**B**

Given that the network ID 172.16.0.0 matches with the subnet mask 255.255.255.193, the correct interface to choose is **B**.