2 – WEEK – TASK (03-08-2024 TO 04-08-2024)

1. 1. Among A and B, select which one is software layer and which one is hardware layer in Open Systems Interconnection Model.
   A. Application layer, Presentation layer, Session layer
   B. Network layer, Datalink layer, Physical layer

   Software Layers: Application layer, Presentation layer, Session layer

   Hardware Layers: Network layer, Data Link layer, Physical layer

2. HTTPS uses which protocol for security?
   HTTPS uses TLS (Transport Layer Security) for security.

3. Apart from LAN, VAN and MAN, what do you understand by VPN?
   A VPN (Virtual Private Network) creates a secure, encrypted connection over a public network, allowing users to access a private network remotely and safely.

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.
   Two-Factor Authentication (2FA) - Adds a second layer of security by requiring a second form of verification, like a code sent to your phone.
   Password Hashing - Encrypts passwords before storing them, ensuring that the actual password is not exposed.
   Biometric Authentication - Uses fingerprints, facial recognition, or other biometric data to verify identity.
   Secure Sockets Layer (SSL)/Transport Layer Security (TLS) - Encrypts data transmitted between your browser and websites to secure communication.
   Public Key Infrastructure (PKI) - Uses a pair of cryptographic keys (public and private) for secure communications and authentication.

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

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. IIs the Action allowed, as per above table firewall rule? (Allow/Deny)

Deny

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 _____ data (malicious / all Secured) data.

Malicious

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/Firewall)

Subnetting

9. Move A and B to corresponding IP assignment.

S NO	Static IP Address	Dynamic IP address
1	It is provided by ISP (Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2	**A) This IP address does not change at IP any time, which means if an Ip address is provided then it can't be changed or modified and is easily traceable.**	**B) These addresses changes at any time and not easily traced.**

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

Identification Scope:

MAC Address:

- **Scope:** Identifies a specific network interface card (NIC) on a local network segment.
- **Example:** `00:1A:2B:3C:4D:5E` uniquely identifies a hardware device on the same local network.
- **Changeability:** Generally fixed and assigned by the hardware manufacturer; not easily changed.
- **Example:** A MAC address like `00:1A:2B:3C:4D:5E` remains constant for a specific NIC.

IP Address:

- **Scope:** Identifies a device on a network, which can be local or remote, and is used for routing data across different networks.
- **Example:** `192.168.1.10` identifies a specific device within a network, enabling communication across different networks.
- **Changeability:** Can be dynamically assigned or manually configured; may change based on network configuration or DHCP settings.
- **Example:** An IP address like `192.168.1.10` can change if assigned by DHCP or manually reconfigured.

Network Address:

- **Scope:** Identifies an entire network or subnet, used for routing and managing IP addresses within that network.
- **Example:** `192.168.1.0/24` represents all devices within the subnet `192.168.1.0` with a subnet mask of `/24`.
- **Changeability:** Represents a network range and typically changes if the network design or subnetting is altered.
- **Example:** A network address like `192.168.1.0/24` may change if the network is restructured or subnetted differently.

11. Match numbers with letters according to 7 layers 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

1 : G
2 : C
3 : D
4 : E
5 : F
6 : B
7 : A

12. DNS is a host name to IP address translation service. Use ping amazon.com and share IP address.
    Domain: amazon.com
    amazon IP address: 205.251.242.103

    Pinging amazon.com [205.251.242.103] with 32 bytes of data:
    Reply from 205.251.242.103: bytes=32 time=273ms TTL=241
    Reply from 205.251.242.103: bytes=32 time=271ms TTL=241
    Reply from 205.251.242.103: bytes=32 time=330ms TTL=241
    Reply from 205.251.242.103: bytes=32 time=263ms TTL=241

    Ping statistics for 205.251.242.103:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 263ms, Maximum = 330ms, Average = 284ms

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

network ID “172.16.0.0“is **Interface B**.