Question 1: **Skipped**

What is the well-known port for SMTP?

○ **443**

○ **25** **(Correct)**

○ **22**

○ **80**

Explanation

Port 25 is the well-known port used by the SMTP protocol for sending email.

Question 2: **Skipped**

What is the range of well-known ports? (★)

○ **1024-49151**

○ **0-1023** **(Correct)**

○ **none of the above**

○ **49152-65535**

Explanation

Well-known ports are related to the common protocols that are at the core of the TCP/IP model and fall in the range of 0-1023.

Question 3: **Skipped**

A company has noticed that their network performance has been slow lately. After investigating, they discover that their router is not configured properly, leading to network congestion. Which OSI layer is most likely affected by this issue?

○ **Data Link Layer**

○ **Transport Layer**

○ **Network Layer** **(Correct)**

○ **Application Layer**

Explanation

The network layer deals with routing and logical addressingwhich is crucial for efficient data transmission and avoiding network congestion.

Question 4: **Skipped**

A user reports that they are unable to access a specific website. Which OSI layer is most likely affected by this issue?

○ **Network Layer**

○ **Application Layer** **(Correct)**

○ **Data Link Layer**

○ **Transport Layer**

Explanation

The application layer deals with end-user applications and protocolssuch as HTTP used for websites.

Question 5: **Skipped**

What layer of the OSI model is the target of a ping flood attack?

○ **Layer 6**

○ **Layer 5**

○ **Layer 4**

○ **Layer 3** **(Correct)**

Explanation

A ping flood attack is a type of DoS attack that targets the network layer (Layer 3) of the OSI model by flooding the target server with a large number of ICMP Echo Request (ping) packets.

Question 6: **Skipped**

What protocol is associated with port 80?

○ **Telnet**

○ **FTP**

○ **HTTP** **(Correct)**

○ **SSH**

Explanation

Port 80 is the default port used by the HTTP protocol for web traffic.

Question 7: **Skipped**

Your organization is concerned about network security and wants to prevent unauthorized access to its resources by implementing a security model where the network has no trusted space. Which type of security model is this?

○ **Zero-trust** **(Correct)**

○ **Trusted computing**

○ **Trusted platform module**

○ **Trusted execution environment**

Explanation

A zero-trust security model is one where the network has no trusted space and security is managed at each possible levelrepresenting the most granular asset.

Question 8: **Skipped**

A hacker uses a distributed denial of service (DDoS) attack to flood a company's network with traffic, rendering it unable to function properly. Which OSI layer is being attacked?

○ **Data link layer**

○ **Network layer** **(Correct)**

○ **Physical layer**

○ **Transport layer**

Explanation

The network layer is responsible for routing network traffic and providing logical addressing. In this scenariothe hacker is flooding the network with trafficwhich is an attack on the network layer.

Question 9: **Skipped**

What is the range of dynamic or private ports?

○ **49152-65535** **(Correct)**

○ **1024-49151**

○ **none of the above**

○ **0-1023**

Explanation

Dynamic or private ports fall in the range of 49152-65535 and are used whenever a service is requested that is associated with well-known or registered ports.

Question 10: **Skipped**

Your organization is looking to outsource its computing infrastructure to a third-party provider. Which type of cloud computing model would be the best fit for this purpose?

○ **Hybrid cloud**

○ **PaaS**

○ **SaaS**

○ **IaaS** **(Correct)**

Explanation

IaaS (Infrastructure as a Service) is the provider of the core computingstorage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. It is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.

Question 11: **Skipped**

Who is responsible for securing the data in Software as a Service (SaaS)?

○ **Cloud Service Provider (CSP)**

○ **Cloud Service Customer (CSC)**

○ **Both CSP and CSC** **(Correct)**

○ **None of the above**

Explanation

In SaaSboth the CSP and CSC are responsible for securing the data. The CSP is responsible for securing the infrastructure and the CSC is responsible for securing their data and access control.

Question 12: **Skipped**

What is the purpose of the Ethernet standard?

○ **To define wired connections of networked devices** **(Correct)**

○ **To define the way data is formatted over the air**

○ **To define wireless connections of networked**

devices

○ **To define the way data is formatted over the wire**

Explanation

Ethernet (IEEE 802.3) is a standard that defines wired connections of networked devices. It defines the way data is formatted over the wire to ensure disparate devices can communicate over the same cables.

Question 13: **Skipped**

Which type of malware encrypts a user's files and demands payment in exchange for the decryption key?

○ **Trojan**

○ **Virus**

○ **Worm**

○ **Ransomware** **(Correct)**

Explanation

Ransomware is a type of malware that encrypts a user's files and demands payment in exchange for the decryption key.

Question 14: **Skipped**

Which port is used by the FTP protocol?

○ **21** **(Correct)**

○ **22**

○ **80**

○ **23**

Explanation

Port 21 is the default port used by the FTP protocol for file transfers.

Question 15: **Skipped**

Your organization is experiencing network congestion and is looking to implement a mechanism that can handle a high volume of network traffic without slowing down the system. Which mechanism is this?

○ **VLAN**

○ **Load balancing** **(Correct)**

○ **MPLS**

○ **DNS**

Explanation

Load balancing is a mechanism used to distribute network traffic across multiple servers to handle a high volume of network traffic without slowing down the system.

Question 16: **Skipped**

Which device is used to control traffic flow on networks

○ **hub**

○ **router**

○ **switch** **(Correct)**

○ **Firewalls**

Explanation

Switches are wired devices that know the addresses of the devices connected to them and route traffic to that port/device rather than retransmitting to all devices. They're smarter than hubsbut not as smart as routers.

Question 17: **Skipped**

What are registered ports used for?

○ **Proprietary applications from vendors and developers** (Correct)

○ **Used for inhouse or opensource applications**

○ **Used for Web servers**

○ **Common protocols at the core of TCP/IP model**

Explanation

Registered ports are often associated with proprietary applications from vendors and developers and fall in the range of 1024-49151.

Question 18: **Skipped**

A hacker sends a specially crafted email with a malicious attachment to an employee of a company. Once the employee downloads and opens the attachment, malware is installed on the computer. Which TCP layer is being attacked?

○ **Network layer**

○ **Application layer** **(Correct)**

○ **Transport layer**

○ **Physical layer**

Explanation

The application layer is responsible for providing applications with access to the network. In this scenariothe hacker is using an email as a vector to attack the application layer of the employee's computer.

Question 19: **Skipped**

Which protocol is used for secure email?

○ **IMAPS**

○ **POP3S**

○ **SMTPS**

○ **All of the above** **(Correct)**

Explanation

Secure email can be achieved using SMTPSIMAPSor POP3S protocolswhich encrypt email traffic to provide security for sensitive information.

Question 20: **Skipped**

A user receives an email that appears to be from their bank, requesting their login credentials. This is an example of what type of attack?

○ **Spoofing**

○ **Virus**

○ **Phishing** **(Correct)**

○ **DOS/DDOS**

Explanation

The attacker is attempting to trick the user into giving away sensitive information by pretending to be a trusted entity.

Question 21: **Skipped**

What layer of the OSI model is the target of a buffer overflow attack?

○ **Layer 5**

○ **Layer 7** **(Correct)**

○ **Layer 6**

○ **Layer 8**

Explanation

A buffer overflow attack is a type of attack that targets the application layer (Layer 7) of the OSI model by sending more data to a program or service than it can handlecausing it to crash or execute arbitrary code.

Question 22: **Skipped**

Which of the following is NOT a function of an Intrusion Prevention System (IPS)? (★)

○ **To detect and prevent attacks**

○ **To filter network traffic**

○ **To monitor network traffic**

○ **To encrypt network traffic** **(Correct)**

Explanation

While an IPS can inspect network traffic for malicious activity and take action to stop itit is not designed to encrypt network traffic.

Question 23: **Skipped**

Which of the following is an example of a registered port?

○ **SMB and MySQL**

○ **LDAP and FTP**

○ **HTTP and HTTPS**

○ **Microsoft SQL Server and RADIUS authentication** **(Correct)**

Explanation

Examples of registered ports include Microsoft SQL Server (1433/1434) and RADIUS authentication (1812).

Further, HTTP and HTTPS are well-known ports. MySQL is registered, but SMB is well known. And LDAP and FTP both are well-known.

Question 24: **Skipped**

What is the cloud service model where the provider offers hardware infrastructure to the customer to build, install, and manage their own applications?

○ Infrastructure as a Service (IaaS) (Correct)

○ Software as a Service (SaaS)

○ None of the above

○ Platform as a Service (PaaS)

Explanation

IaaS provides the customer with infrastructure components such as serversstorageand network resources to buildinstalland manage their own applications.

Question 25: **Skipped**

What layer of the OSI model is the target of a MAC flooding attack?

○ **Layer 4**

○ **Layer 2** **(Correct)**

○ **Layer 3**

○ **Layer 7**

Explanation

A MAC flooding attack is a type of attack that targets the data link layer (Layer 2) of the OSI model by flooding a switch's MAC address table with fake MAC addressescausing the switch to broadcast traffic to all portsallowing an attacker to intercept traffic.

Question 26: **Skipped**

At which layer of the TCP/IP protocol stack does a firewall operate?

○ **Layer 3**

○ **Layer 2**

○ **Layer 4** **(Correct)**

○ **Layer 1**

Explanation

Firewalls operate at the transport layer (Layer 4) of the TCP/IP protocol stack, which is responsible for managing the communication between applications running on different hosts. The transport layer protocols, such as TCP and UDP, provide reliable and efficient communication services to the upper layer protocols.

Question 27: **Skipped**

What type of fire suppression system is more friendly to electronics?

○ **Water-based**

○ **Chemical-based**

○ **Foam-based**

○ **Carbon dioxide-based** **(Correct)**

Explanation

Gas-based fire suppression systems are more friendly to the electronicsbut can be toxic to humans.

Question 28: **Skipped**

A user receives an email with a link to a fake login page that appears to be from their bank. When they enter their credentials, the attacker now has access to their account. This is an example of what type of attack?

○ **DOS/DDOS**

○ **Virus**

○ **Phishing** **(Correct)**

○ **Spoofing**

Explanation

The attacker is using social engineering to trick the user into entering their credentials into a fake website.

Question 29: **Skipped**

What is the potential impact of an IPSec replay attack?

○ **Modification of network traffic**

○ **Unauthorized access to network resources**

○ **Disruption of network communication**

○ **All of the above** **(Correct)**

Explanation

An IPSec replay attack can have a range of impacts on a networkincluding unauthorized accessdisruption of communicationand modification of traffic.

Question 30: **Skipped**

What layer of the OSI model is the target of a port scanning attack?

○ **Layer 4** **(Correct)**

○ **Layer 2**

○ **Layer 3**

○ **Layer 1**

Explanation

A port scanning attack is a type of reconnaissance attack that targets the transport layer (Layer 4) of the OSI model by scanning a target host's ports to identify open services and potential vulnerabilities.

Question 31: **Skipped**

What layer of the OSI model is the target of a SYN flood attack?

○ **Layer 6**

○ **Layer 7**

○ **Layer 4** **(Correct)**

○ **Layer 5**

Explanation

A SYN flood attack is a type of denial-of-service (DoS) attack that targets the transport layer (Layer 4) of the OSI model by flooding the target server with a large number of SYN requests.

Question 32: **Skipped**

Which port is used by the SSH protocol for secure file transfers?

○ **SFTP** **(Correct)**

○ **SCP**

○ **FTPS**

○ **TFTP**

Explanation

SSH File Transfer Protocol (SFTP) uses the SSH protocol and typically uses port 22 for secure file transfers.

Question 33: **Skipped**

How does subnetting help to improve network performance?

○ **By increasing network bandwidth**

○ **By simplifying network management**

○ **By improving network security**

○ **By reducing network congestion** **(Correct)**

Explanation

Subnetting can help to reduce network congestion by dividing a larger network into smaller, more manageable subnets. This can improve network performance by reducing the amount of broadcast traffic on the network and limiting the scope of network issues.

Question 34: **Skipped**

What is an IPSec replay attack?

○ **An attack where an attacker modifies packets in transit**

○ **An attack where an attacker eavesdrops on network traffic**

○ **An attack where an attacker overloads a network with traffic**

○ **An attack where an attacker attempts to inject packets into an existing session** (Correct)

Explanation

In an IPSec replay attackan attacker intercepts and retransmits packets to try and gain unauthorized access to a network or to disrupt network communication.

Question 35: **Skipped**

What layer of the OSI model is the target of a man-in-the-middle (MITM) attack?

○ **Layer 4**

○ **Layer 7**

○ **Layer 3** **(Correct)**

○ **Layer 2**

Explanation

A MITM attack is a type of attack that targets the network layer (Layer 3) of the OSI model by intercepting and modifying network traffic between two communicating hosts.

Question 36: **Skipped**

Who is responsible for securing the data in Infrastructure as a Service (IaaS)?

○ **Cloud Service Customer (CSC)** **(Correct)**

○ **Both CSP and CSC**

○ **Cloud Service Provider (CSP)**

○ **None of the above**

Explanation

In IaaSthe CSC is responsible for securing the dataas they have full control over the operating systemmiddlewareand applications. The CSP is responsible for securing the infrastructure.

Question 37: **Skipped**

What is the recommended fire suppression system for server rooms?

○ **Foam-based**

○ **Powder-based**

○ **Water-based**

○ **Gas-based** **(Correct)**

Explanation

Water-based fire suppression systems can cause more harm to servers and other electronic components.

Question 38: **Skipped**

What security feature is commonly used with HTTPS?

○ **SSL/TLS** **(Correct)**

○ **VPN**

○ **IPsec**

○ **SSH**

Explanation

HTTPS uses the SSL/TLS protocol to encrypt web traffic and provide security for sensitive information such as login credentials and financial transactions.

Question 39: **Skipped**

An attacker intercepts traffic between a user and a server in order to eavesdrop on sensitive information being transmitted. This is an example of what type of attack?

○ **Phishing**

○ **Side-channel**

○ **On-path Attack** **(Correct)**

○ **Spoofing**

Explanation

The attacker is "on the path" between the user and the serverallowing them to intercept and view the traffic being transmitted.

Question 40: **Skipped**

Which of the following would be considered an endpoint

○ **Router**

○ **Software task**

○ **Laptop** **(Correct)**

○ **Firewall**

Explanation

An endpoint device is a computing device that is connected to a network and has an IP address. Examples of endpoint devices include desktop computers, laptops, tablets, smartphones, and IoT devices. Endpoint devices are often the target of cyber attacks, and security measures such as antivirus software and firewalls are used to protect them.

Question 41: **Skipped**

What protocol is associated with port 53?

○ **HTTPS**

○ **SMTP**

○ **DNS** **(Correct)**

○ **HTTP**

Explanation

Port 53 is associated with the Domain Name Service (DNS) protocol.

Question 42: **Skipped**

What is an IPv4 address?

○ A 32-bit address used to uniquely identify devices on a network. (Correct)

○ A 128-bit address used to uniquely identify devices on a network.

○ An address used for documentation purposes only.

○ An address used for internal network use only.

Explanation

IPv4 addresses are 32-bit addresses used to uniquely identify devices on a network.

Question 43: **Skipped**

A hacker uses a man-in-the-middle attack to intercept network traffic between two nodes and injects malicious code into the data stream. Which TCP layer is being attacked? (★)

○ **Network layer**

○ **Application layer**

○ **Transport layer** **(Correct)**

○ **Data link layer**

Explanation

The transport layer is responsible for providing reliable data transfer services to the upper layers. In this scenariothe hacker is intercepting network traffic and injecting malicious codewhich is an attack on the transport layer.

Question 44: **Skipped**

Which of the following is an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing specific terms to set the quality of the cloud services delivered?

○ **Service-Level Agreement (SLA)** **(Correct)**

○ **Open Authorization (OAuth)**

○ **Simple Object Access Protocol (SOAP)**

○ **Security Assertion Markup Language (SAML)**

Explanation

The passage defines Service-Level Agreement (SLA) as an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing-specific terms to set the quality of the cloud services delivered.

Question 45: **Skipped**

Which device is used to connect WAN to LAN? (★)

○ **Router** **(Correct)**

○ **Hub**

○ **Switch**

○ **Firewalls**

Explanation

Routers are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between them. They're smarter than hubs and switchesand determine the most efficient "route" for the traffic to flow across the network.

Question 46: **Skipped**

What is the difference between a hub and a switch? (★)

○ **A hub can connect more devices than a switch.**

○ **A switch broadcasts data to all devices on the network, while a hub sends data only to the intended device.**

○ **A switch is a passive device, while a hub is an active device.**

○ **A switch sends data only to the intended device, while a hub broadcasts data to all devices on the network.** **(Correct)**

Explanation

A switch sends data only to the intended device, while a hub broadcasts data to all devices on the network. This means that a switch is able to route traffic more efficiently than a hub, which can lead to improved network performance. Switches are commonly used in networks to segment traffic and reduce network congestion.

Question 47: **Skipped**

Which layer of the OSI model is responsible for assigning MAC addresses to network devices?

○ **Data Link layer** **(Correct)**

○ **Transport layer**

○ **Network layer**

○ **Physical layer**

Explanation

The Data Link layer of the OSI model is responsible for the physical addressing of devices on the network. MAC addresses are assigned at this layer, and are used to identify network devices at the physical layer.

Question 48: **Skipped**

Which type of attack involves exploiting weaknesses in a network or system over an extended period of time to gain access and steal data?

○ **DOS/DDOS**

○ **Spoofing**

○ **Advanced Persistent Threat (APT)** **(Correct)**

○ **Phishing**

Explanation

APT attacks involve a slow and deliberate approach to infiltrating a systemoften using multiple attack vectors and exploiting vulnerabilities over an extended period of time.

Question 49: **Skipped**

What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

○ **64°F to 81°F** **(Correct)**

○ **62°F to 69°F**

○ **91°F to 100°F**

○ **82°F to 90°F**

Explanation

The recommended range for optimized maximum uptime and hardware life is from 64° to 81°F (18° to 27°C).

Question 50: **Skipped**

A hacker uses a DNS spoofing attack to redirect a user to a fake website that looks like a legitimate one. Once the user enters their login credentials, the hacker steals the information. Which OSI layer is being attacked?

○ **Application layer** **(Correct)**

○ **Data link layer**

○ **Network layer**

○ **Physical layer**

Explanation

The application layer is responsible for providing end-user services such as web browsing. In this scenariothe hacker is using a DNS spoofing attack to redirect the user to a fake websitewhich is an attack on the application layer.

Question 51: **Skipped**

How does IPSec protect against replay attacks?

○ **By using digital signatures**

○ **By limiting access to the network**

○ **By encrypting all network traffic**

○ **By using sequence numbers** **(Correct)**

Explanation

IPSec uses sequence numbers to prevent replay attacks. Sequence numbers are assigned to packets and checked by the receiver to ensure that they are in the correct order and that no packets have been duplicated or delayed.

Question 52: **Skipped**

A user clicks on an attachment in an email that they believe is from a friend, which then installs malicious software on their computer. This is an example of what type of malware?

○ **Trojan** **(Correct)**

○ **Worm**

○ **Ransomware**

○ **Virus**

Explanation

A Trojan is a type of malware that disguises itself as a legitimate program in order to trick the user into downloading and installing it.

Question 53: **Skipped**

Which port is commonly used for HTTPS?

○ **80**

○ **443** **(Correct)**

○ **22**

○ **21**

Explanation

Port 443 is the default port used by the HTTPS protocol for secure web traffic.

Question 54: **Skipped**

Your organization is concerned about network security and wants to prevent unauthorized access to its resources by authenticating the identity of users and devices before granting access. Which type of security mechanism is this?

○ **Firewalls**

○ **Identity and access management** **(Correct)**

○ **Intrusion detection systems**

○ **Encryption**

Explanation

Identity and access management (IAM) is a security mechanism used to authenticate the identity of users and devices before granting access to resources. It includes authenticationauthorizationand accounting (AAA) mechanisms.

Question 55: **Skipped**

An organization is experiencing issues with their VPN connection, causing frequent disconnects. Which OSI layer is most likely affected by this issue?

○ **Network Layer**

○ **Physical Layer**

○ **Application Layer**

○ **Transport Layer** **(Correct)**

Explanation

The transport layer is responsible for reliable data transfer between hostswhich is crucial for maintaining a stable VPN connection.

Question 56: **Skipped**

Which type of attack involves flooding a network or server with traffic, rendering it unavailable to legitimate users?

○ **Phishing**

○ **DOS/DDOS** **(Correct)**

○ **Spoofing**

○ **Virus**

Explanation

The attack is aimed at disrupting services and making them unavailable to users.

Question 57: **Skipped**

What is an IP address?

○ **An address that denotes the vendor or manufacturer of the physical network interface**

○ **A physical address used to connect multiple devices**

in a network

○ **A logical address associated with a unique network interface within the network** (Correct)

○ **An address that represents the network interface within the network**

Explanation

While MAC addresses are generally assigned in the firmware of the interfaceIP hosts associate that address with a unique logical address. This logical IP address represents the network interface within the network and can be useful to maintain communications when a physical device is swapped with new hardware.

Question 58: **Skipped**

A company has been experiencing network connectivity issues that have been traced to a problem with the cabling. Which OSI layer is affected by this issue?

○ **Application Layer**

○ **Physical Layer** **(Correct)**

○ **Transport Layer**

○ **Network Layer**

Explanation

The physical layer of the OSI model deals with the transmission of data over the physical mediumsuch as cables.

Question 59: **Skipped**

A hacker gains access to a company's network and begins to intercept network traffic in order to steal login credentials. Which OSI layer is being attacked?

○ **Network layer**

○ **Application layer**

○ **Physical layer**

○ **Data link layer** **(Correct)**

Explanation

The data link layer is responsible for the logical transmission of data between network nodes and error detection. Intercepting network traffic in order to steal login credentials is an attack on this layer.

Question 60: **Skipped**

Which port is commonly used for SSH?

○ **22** **(Correct)**

○ **443**

○ **80**

○ **23**

Explanation

Port 22 is the default port used by the SSH protocol for secure remote access to a server.