DUMPSBOSS.

ISSAP Information Systems Security Architecture Professional

ISC2 ISSAP

Version Demo

Total Demo Questions: 27

Total Premium Questions: 278

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Architecture Modeling	24
Topic 2, Infrastructure Security Architecture	142
Topic 3, Identity and Access Management Architecture	61
Topic 4, Security Operations Architecture	36
Topic 5, Architecture for Application Security	11
Topic 6, Security Architecture for the Cloud	1
Topic 7, Mix Questions	3
Total	278

QUESTION NO: 1

Which of the following types of ciphers are included in the historical ciphers? Each correct answer represents a complete solution. Choose two.

A. Block ciphers

B. Transposition ciphers

C. Stream ciphers

D. Substitution ciphers

ANSWER: B D

Explanation:

Historical, or classical, cryptography is commonly organized around substitution and transposition techniques. **Substitution ciphers** protect a message by replacing a plaintext letter, symbol, or group of symbols with a different symbol or group. Classical examples include Caesar-style shifts, monoalphabetic substitution, and polyalphabetic systems such as Vigenère. The essential characteristic is that the message symbols are changed while their positions in the message are generally retained.

Transposition ciphers protect a message by rearranging the positions of plaintext symbols according to a defined pattern or key. The original symbols remain present, but their ordering changes. Classical route and columnar transposition methods illustrate this approach. These two families are foundational historical cipher designs, and they were also frequently combined in more complex classical systems to provide both symbol transformation and positional rearrangement.

This classification is useful in security architecture because it distinguishes early manual cryptographic mechanisms from modern cryptographic constructions and helps explain the basic confidentiality properties that later algorithms build upon. Britannica describes cryptography's classical substitution and transposition approaches in its classic cryptography overview; additional historical context is available from the National Cryptologic Museum.

QUESTION NO: 2

Which of the following are the centralized administration technologies? Each correct answer represents a complete solution. Choose all that apply.

A. RADIUS

B. TACACS+

C. Media Access control

D. Peer-to-Peer

ANSWER: A B

Explanation:

RADIUS and TACACS+ are centralized administration technologies because they enable network devices and services to delegate authentication and, depending on the deployment, authorization and accounting functions to a centrally managed AAA server. This gives administrators a consistent way to manage user identities, access rules, credentials, and audit records across many routers, switches, wireless controllers, VPN gateways, and other systems rather than maintaining separate local user databases on each device.

RADIUS is widely used for centralized network-access authentication, particularly for remote access and network access control scenarios. It supports the exchange of authentication, authorization, and accounting information between a network access server and a RADIUS server. TACACS+ is commonly used for centralized administrative access to network infrastructure. Its design separates authentication, authorization, and accounting functions, allowing granular control over the commands an authenticated administrator may execute and producing useful accountability records.

Both technologies therefore support the security-architecture objective of centralized identity and access administration, including consistent policy enforcement and improved auditing. Cisco's overview of TACACS+ configuration describes its AAA role, while RFC 2865 defines the Remote Authentication Dial In User Service (RADIUS) protocol.

QUESTION NO: 3

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Non-repudiation

C. Integrity

D. Confidentiality

ANSWER: D

Explanation:

Confidentiality is the cryptographic security service that protects information from disclosure to unauthorized persons. On a local network, data can be exposed while traversing shared infrastructure or when it is accessible to systems and users that are not authorized to view it. Cryptographic mechanisms such as encryption transform plaintext into ciphertext, so that intercepted or otherwise accessed data remains unintelligible without the appropriate decryption key. Effective confidentiality therefore depends not only on using strong encryption, but also on ensuring that encryption keys are generated, distributed, stored, rotated, and revoked appropriately. In networked environments, confidentiality protections commonly include encrypted transport protocols and secure network tunnels, which protect data in transit from unauthorized observation. The NIST glossary defines confidentiality as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. This directly matches the requirement that information not be disclosed to unauthorized people. See the NIST definition of confidentiality and NIST's FIPS 199 security objectives for the foundational confidentiality, integrity, and availability model.

QUESTION NO: 4

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Discretionary Access Control (DAC)

B. Role Based Access Control (RBAC)

C. Mandatory Access Control (MAC)

D. Access Control List (ACL)

ANSWER: C

Explanation:

Mandatory Access Control (MAC) is correct because access decisions are centrally enforced according to security labels and a subject's clearance or authorization, rather than being delegated to the individual user who received or owns an object. In a MAC system, an object classified as secret retains its classification, and access to it is governed by the organization's mandatory security policy. A recipient cannot independently grant another user permission to view a copy simply because the recipient can view it; the prospective recipient must also satisfy the required authorization conditions for the secret classification.

This model is designed to protect information whose sensitivity must be controlled consistently across the enterprise, including government and military-style classified information. The security authority defines classifications, clearances, and the rules for information flow, while system mechanisms enforce those rules. This prevents users from changing permissions

in a manner that could bypass classification requirements. NIST describes mandatory access control as enforcing access based on information labels and formal authorization, and its glossary further distinguishes these centrally imposed controls from owner-directed permissions. See the NIST definition of mandatory access control and NIST SP 800-162 on attribute-based access control concepts.

QUESTION NO: 5

You work as a Chief Security Officer for Tech Perfect Inc. You have configured IPSec and ISAKMP protocol in the company's network in order to establish a secure communication infrastructure. ccording to the Internet RFC 2408, which of the following services does the ISAKMP protocol offer to the network? Each correct answer represents a part of the solution. Choose all that apply.

A. It relies upon a system of security associations.

B. It provides key generation mechanisms.

C. It authenticates communicating peers.

D. It protects against threats, such as DoS attack, replay attack, etc.

ANSWER: B C D

Explanation:

ISAKMP provides a framework and message formats for security-association management and key-management activities, while allowing the specific key-exchange method and security-domain interpretation to be supplied separately. “It provides key generation mechanisms” is correct because ISAKMP includes key-exchange payload processing that enables peers to establish shared secret material and derive keys used to protect subsequent exchanges or associated security services. “It authenticates communicating peers” is also correct: peer authentication is a core ISAKMP objective, ensuring that the entities negotiating security parameters can establish the claimed identities before relying on the resulting security relationship.

“It protects against threats, such as DoS attack, replay attack, etc.” is correct because RFC 2408 explicitly identifies resistance to replay and denial-of-service attacks as security goals. ISAKMP incorporates mechanisms such as cookies to help a responder avoid committing substantial state or computational resources before validating that an initiator can receive replies, which mitigates certain denial-of-service conditions. Exchange protections and negotiated cryptographic services also support detection or prevention of replayed protocol messages where applicable. The authoritative specification is RFC 2408, Internet Security Association and Key Management Protocol. For context on the later IKEv2 key-management protocol that superseded the original IKE approach, see RFC 7296.

QUESTION NO: 6

Which of the following should the administrator ensure during the test of a disaster recovery plan?

A. Ensure that the plan works properly

B. Ensure that all the servers in the organization are shut down.

C. Ensure that each member of the disaster recovery team is aware of their responsibility.

D. Ensure that all client computers in the organization are shut down.

ANSWER: A C

Explanation:

During a disaster recovery plan test, the administrator should ensure that the plan works properly and that each member of the disaster recovery team is aware of their responsibility. A recovery plan is operationally useful only when its documented recovery procedures can be performed successfully under realistic test conditions. Testing validates that recovery resources, dependencies, communications paths, recovery-site arrangements, restoration procedures, and recovery time objectives can

support the organization's required recovery capability. Test results should be recorded so the plan can be updated to address identified gaps.

Equally, disaster recovery depends on coordinated human action. Team members need clearly assigned roles, authority, contact information, escalation paths, and an understanding of the actions they must take during the exercise and an actual disruption. Personnel participation in testing confirms that responsibilities are understood and that coordination and communications work in practice. NIST contingency-planning guidance identifies testing, training, and exercises as essential for validating contingency capabilities and preparing personnel. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and the CISA exercises guidance.

QUESTION NO: 7

Which of the following are types of asymmetric encryption algorithms? Each correct answer represents a complete solution. Choose two.

A. RSA

B. AES

C. ECC

D. DES

ANSWER: A C

Explanation:

RSA and ECC are asymmetric, or public-key, cryptographic algorithm families. Asymmetric cryptography uses a mathematically related key pair: a public key that may be distributed and a private key that must remain under the key owner's control. The key pair supports security services such as encryption/decryption, digital signatures, and key establishment, depending on the specific scheme and protocol implementation.

RSA is a public-key algorithm whose security is based on the practical difficulty of factoring the product of large prime numbers. It is commonly used for digital signatures and key transport or key encapsulation in appropriately designed systems. ECC, or elliptic-curve cryptography, is a family of public-key techniques based on mathematical operations on elliptic curves over finite fields. ECC can provide comparable public-key security with substantially smaller key sizes than traditional RSA, which is particularly useful where bandwidth, storage, or computational capacity is constrained.

NIST identifies both RSA and elliptic-curve methods among approved public-key cryptographic techniques and provides implementation guidance for their use. See NIST FIPS 186-5, Digital Signature Standard and NIST SP 800-56A Rev. 3, Pair-Wise Key Establishment Using Discrete Logarithm Cryptography.

QUESTION NO: 8

Which of the following are natural environmental threats that an organization faces? Each correct answer represents a complete solution. Choose two.

A. Strikes

B. Floods

C. Accidents

D. Storms

ANSWER: B D

Explanation:

Floods and storms are natural environmental threats because they arise from naturally occurring weather and hydrological events and can directly affect an organization's people, facilities, technology, utilities, and operations. Flooding may damage

buildings, data centers, cabling, power equipment, and physical records; it can also prevent personnel from reaching a site and disrupt transportation or local infrastructure. Storms—including severe windstorms, thunderstorms, hurricanes, tornadoes, snowstorms, and related events—can create similar impacts through wind damage, water intrusion, lightning, utility outages, and communications disruptions. From a security-architecture and resilience perspective, these threats should be considered during risk assessment, site selection, facility design, business continuity planning, and disaster recovery planning. Appropriate safeguards can include locating critical facilities outside identified flood-prone areas, using environmental monitoring and drainage controls, protecting equipment from water exposure, providing resilient power and communications, and maintaining tested continuity procedures. NIST identifies natural disasters and severe weather among events that can disrupt organizational operations and that should be addressed through contingency planning. FEMA also provides authoritative guidance and flood-risk information relevant to organizational preparedness. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and FEMA Flood Maps.

QUESTION NO: 9

Which of the following cables provides maximum security against electronic eavesdropping on a network?

A. Fibre optic cable

B. STP cable

C. UTP cable

D. NTP cable

ANSWER: A

Explanation:

Fibre optic cable provides the greatest security against electronic eavesdropping because it transmits information as pulses of light rather than electrical signals. Unlike copper cabling, it does not produce electromagnetic emissions that can be intercepted remotely with radio-frequency or induction-based monitoring equipment. Accessing traffic on a fibre requires physical access to the cable and specialized optical tapping equipment; such tapping commonly alters the optical signal enough to create measurable attenuation or other link anomalies. This makes passive, undetected interception substantially more difficult than with conventional copper network media.

Fibre also provides strong resistance to electromagnetic interference, which supports both reliable communications and reduced exposure to signal leakage. Although fibre is not inherently immune to every possible physical attack, proper physical protections, link monitoring, and encryption make it an especially robust choice where protection against cable-based interception is important. NIST describes fibre-optic cable as a transmission medium using light and notes its immunity to electromagnetic interference; its physical and signaling characteristics make it the best selection among the listed media for minimizing electronic eavesdropping risk. See NIST Telecommunications Security Guidelines and CISA guidance on network cable protection.

QUESTION NO: 10

Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

A. Social engineering attack

B. Cross site scripting attack

C. Mail bombing

D. Password guessing attack

ANSWER: A

Explanation:

Social engineering attack is correct because it targets the people who operate, administer, and use systems rather than attempting to defeat a technical control directly. Even mature physical safeguards, authentication mechanisms, network controls, and monitoring can be undermined when an attacker persuades, deceives, or pressures an authorized person into granting access, revealing credentials, approving a request, or bypassing an established procedure. Examples include impersonating a trusted employee or supplier, using a pretext to obtain sensitive information, and persuading someone to allow unauthorized physical entry. Security architecture must therefore treat personnel as a critical part of the security boundary and apply administrative and procedural safeguards alongside technical controls. Effective defenses include recurring security-awareness training, clearly defined verification and escalation procedures, least privilege, separation of duties, phishing-resistant authentication, and a culture in which personnel are empowered to challenge unusual requests. The U.S. Cybersecurity and Infrastructure Security Agency describes social engineering as manipulation intended to cause individuals to divulge confidential information or take an action that benefits the attacker. The NIST security-awareness and training control family likewise recognizes training as an essential safeguard for reducing human-related security risk. See CISA: Social Engineering and NIST SP 800-53: Awareness and Training.

QUESTION NO: 11

Which of the following statements are true about Public-key cryptography? Each correct answer represents a complete solution. Choose two.

A. Data encrypted with the secret key can only be decrypted by another secret key.

B. The secret key can encrypt a message, and anyone with the public key can decrypt it.

C. Data encrypted by the public key can only be decrypted by the secret key.

ANSWER: B C

Explanation:

Public-key cryptography uses a mathematically related key pair: a public key that can be distributed and a private (secret) key that must remain under the owner's control. For confidentiality, a sender encrypts data using the recipient's public key; only the corresponding private key can perform the required decryption operation. This lets a sender protect information without first sharing a symmetric secret with the recipient. The National Institute of Standards and Technology describes public-key techniques as using related public and private keys, with the private key retained as confidential keying material. See NIST SP 800-57 Part 1 Rev. 5.

The reverse private-key operation supports digital-signature functionality. A signer applies the private key to create a signature, and any party with the corresponding public key can verify it. In simplified cryptography questions this is often described as the secret key "encrypting" a message and the public key decrypting it; operationally, modern signature schemes sign a message or its hash rather than encrypting an ordinary plaintext. This property provides public verifiability and supports authentication and integrity. NIST's FIPS 186-5 Digital Signature Standard specifies digital signatures as being generated with a private key and verified with the associated public key.

QUESTION NO: 12

John works as a Network Administrator for NetPerfect Inc. The company has a Windows-based network. John has been assigned a project to build a network for the sales department of the company. It is important for the LAN to continue working even if there is a break in the cabling. Which of the following topologies should John use to accomplish the task?

A. Star

B. Mesh

C. Bus

D. Ring

ANSWER: B

Explanation:

Mesh is correct because it provides multiple physical paths between network devices. In a full mesh topology, every node has a direct connection to every other node; in a partial mesh, critical nodes have more than one connection. This path redundancy means that if one cable is cut or one link fails, traffic can be rerouted through another available connection, allowing communication to continue rather than creating a single point of failure. For a sales LAN where availability is a stated requirement, a mesh design directly addresses resilience against cabling failures. Modern switched networks commonly implement this principle through redundant links and resilient Layer 2 or Layer 3 designs. Redundant paths must be managed appropriately to prevent forwarding loops; for example, Ethernet networks may use Spanning Tree Protocol or routed designs to retain availability while maintaining a loop-free forwarding topology. Cisco describes redundant network design and the mechanisms used to sustain connectivity during failures in its Spanning Tree Protocol overview. The general networking concept of mesh topology and its multiple interconnections is also summarized by IBM Think: What is a mesh network?.

QUESTION NO: 13

Which of the following algorithms can be used to check the integrity of a file?

158

Each correct answer represents a complete solution. Choose two.

A. md5

B. rsa

C. blowfish

D. sha

ANSWER: A D

Explanation:

MD5 and SHA can be used to check file integrity because they are cryptographic hash algorithms. A hash function processes a file of arbitrary length and produces a fixed-length digest. A recipient or system can calculate the digest of the file when it is created, retain the expected digest securely, and later recalculate the digest from the received or stored file. Matching digests provide evidence that the file's contents have not changed since the reference hash was created. This is the common basis for publishing checksums alongside software downloads and for detecting accidental corruption or unauthorized modification.

For modern security architectures, SHA-256 or another SHA-2/SHA-3-family digest should be preferred for new integrity controls because MD5 has known collision weaknesses. Nevertheless, MD5 remains an algorithm capable of producing a file hash and can detect ordinary, non-adversarial corruption when its reference value is trusted; this is why it satisfies the question's basic integrity-checking criterion. NIST describes approved hash functions and their integrity role in FIPS 180-4, while the IETF's RFC 6151 documents MD5's security limitations and the need to avoid relying on it where collision resistance is required. See NIST FIPS 180-4 and RFC 6151.

QUESTION NO: 14

Fill in the blank with the appropriate security method. _____ is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer- based information system.

A. Access control

ANSWER: A

Explanation:

Access control is correct because it is the security discipline and set of mechanisms used to regulate who or what may enter physical locations or use information-system resources. An authorized authority defines access rules and enforces them so that subjects, such as people, processes, or devices, receive only the access appropriate to their identity, role, purpose, and

authorization. In a physical facility, access control can govern entry to buildings, rooms, or restricted zones through mechanisms such as badges, locks, guards, and biometric readers. In a computer-based information system, it governs the ability to view, create, modify, execute, or otherwise use data, applications, systems, and services. This definition spans both physical and logical environments, which is essential to security architecture: protections must be consistently applied to resources regardless of where they reside. NIST describes access control as the process of granting or denying specific requests to obtain and use information-processing services and related data. Its access-control guidance also addresses enforcement of authorized logical access to systems and physical access to facilities. See NIST CSRC: Access Control and NIST SP 800-53, Access Control family.

QUESTION NO: 15

Which of the following is the most secure method of authentication?

A. Smart card

B. Anonymous

C. Username and password

D. Biometrics

ANSWER: D

Explanation:

Biometrics is the best answer among the listed choices because it authenticates an individual based on an inherence characteristic, such as a fingerprint, facial characteristics, or iris pattern. Unlike a password, a biometric characteristic is not simply a secret that can be guessed, reused, or disclosed through ordinary credential-sharing. It also provides stronger assurance that the person presenting for authentication is the enrolled individual than anonymous access or an identifier-and-password combination. In the traditional authentication-factor model used in security architecture, biometrics represents “something you are,” and it is commonly treated as a strong factor when implemented with reliable sensors, protected biometric templates, presentation-attack detection, and suitable matching thresholds.

In an operational architecture, biometrics should generally be paired with another authenticator to form multifactor authentication, particularly for higher-risk access. NIST notes that biometric samples are used to activate or unlock an authenticator and that biometric authentication requires a physical authenticator in addition to the biometric characteristic. That implementation guidance does not change the intended comparison here: as a standalone category in this set of answers, biometrics is the strongest authentication method. See NIST SP 800-63B: Digital Identity Guidelines—Authentication and NIST Computer Security Resource Center: Biometric Authentication.

QUESTION NO: 16

Which of the following protocols provides the highest level of VPN security with a VPN connection that uses the L2TP protocol?

A. IPSec

B. PPPoE

C. PPP

D. TFTP

ANSWER: A

Explanation:

IPSec is correct because L2TP provides tunneling but does not itself provide confidentiality, integrity protection, or strong peer authentication for the traffic carried in the tunnel. In the standard L2TP/IPSec VPN design, IPSec supplies these security services while L2TP carries the PPP frames. IPSec Encapsulating Security Payload (ESP) protects the data in

transit through encryption and integrity mechanisms, and Internet Key Exchange (IKE) establishes security associations and authenticates the communicating VPN peers. This combined approach is commonly called L2TP/IPSec and is a widely supported remote-access VPN configuration.

RFC 3193 specifies the use of L2TP over IPSec and describes IPSec as the mechanism used to secure L2TP traffic, including protection against spoofing, replay, disclosure, and modification. In practical deployments, UDP port 500 and UDP port 4500 are commonly used for IKE and NAT traversal, while UDP port 1701 is used for L2TP after IPSec protection has been established. The key architectural point is that IPSec is the security layer that turns L2TP tunneling into a protected VPN connection. See RFC 3193: Securing L2TP using IPSec and RFC 4301: Security Architecture for IP.

QUESTION NO: 17

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

A. Man trap

B. Biometric device

C. Host Intrusion Detection System (HIDS)

D. Network Intrusion Detection System (NIDS)

ANSWER: A

Explanation:

A man trap is a physical access-control arrangement consisting of two interlocking doors enclosing a small, controlled space. It can be configured so that only one door may be opened at a time during normal entry and exit, preventing an individual from passing directly from an unsecured area into a protected area. When an alarm condition occurs, the access-control system can lock both doors, containing the person in the intervening space—often called the dead-space—until security personnel assess and resolve the event. This design supports anti-tailgating, anti-piggybacking, and controlled authentication procedures at high-security boundaries. Its effectiveness depends on integrating door locks, sensors, alarm monitoring, emergency egress requirements, and response procedures. NIST physical and environmental protection controls specifically identify mantraps as a mechanism for controlling physical access and preventing unauthorized entry. See NIST SP 800-53 Rev. 5, Physical and Environmental Protection controls and the related NIST definition of a mantrap.

QUESTION NO: 18 - (SIMULATION)

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility? A. Hot Site B. Mobile Site C. Warm Site D. Cold Site

ANSWER: See the explanation for the answer

Explanation:

Answer: A. Hot Site

A hot site is a fully operational alternate processing facility maintained in a constant state of readiness. It includes the required servers, workstations, communications links, and supporting infrastructure to take over primary operations with minimal delay.

Hot site: Fully equipped and operational; fastest recovery.
Warm site: Has some equipment/infrastructure but requires additional setup and restoration.
Cold site: Typically provides space and basic utilities only; systems must be installed.
Mobile site: A transportable facility, which may be configured at varying readiness levels.

QUESTION NO: 19

Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing Secure Sockets Layer (SSL). Which of the following types of encryption does SSL use? Each correct answer represents a complete solution. Choose two.

A. Synchronous

B. Secret

C. Asymmetric

D. Symmetric

ANSWER: C D

Explanation:

SSL, and its modern successor TLS, use both asymmetric and symmetric cryptography because they serve distinct roles in establishing and protecting a web session. Asymmetric cryptography is used during the handshake to authenticate the server through its certificate and to support secure key establishment. The certificate contains a public key and is validated by the client, providing the cryptographic basis for the client to confirm it is communicating with the intended server. Depending on the TLS cipher suite and protocol version, the asymmetric mechanism may be RSA key transport or an ephemeral Diffie-Hellman key exchange authenticated with a signature.

After the handshake establishes shared session keys, symmetric cryptography protects the application data exchanged between the browser and web server. Symmetric encryption is appropriate for this continuing data flow because it is substantially more efficient than public-key operations and can securely encrypt large volumes of traffic. TLS additionally applies integrity protection, either through a separate MAC in older suites or authenticated encryption modes such as AES-GCM or ChaCha20-Poly1305 in modern suites. NIST describes TLS as using public-key cryptography for authentication and key establishment, followed by symmetric cryptography for data protection. See NIST SP 800-52 Rev. 2 and RFC 8446: The Transport Layer Security Protocol Version 1.3.

QUESTION NO: 20

Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

A. Kerberos requires continuous availability of a central server.

B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.

C. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.

D. Kerberos requires the clocks of the involved hosts to be synchronized.

ANSWER: A D

Explanation:

Kerberos requires continuous availability of a central server. Kerberos depends on a Key Distribution Center (KDC), which provides the Authentication Service and Ticket-Granting Service functions used to issue ticket-granting tickets and service tickets. In practice, this central service must be highly available, commonly through redundant KDCs, because users cannot obtain new tickets when the KDC is unavailable. Existing unexpired tickets can permit some ongoing access, but KDC availability remains an essential architectural requirement for normal authentication operations and ticket renewal.

Kerberos requires the clocks of the involved hosts to be synchronized. Kerberos uses timestamps and bounded ticket lifetimes to limit replay attacks. A client, KDC, and application server must therefore maintain time within the permitted clock-skew window. RFC 4120 specifies that a server checks the timestamp in an authenticator and rejects it when it falls outside the allowed skew; the default maximum skew is commonly five minutes. Reliable time synchronization, typically using NTP with appropriately secured infrastructure, is consequently a core deployment requirement. See RFC 4120: The Kerberos Network Authentication Service and CISA guidance on Kerberos security.

QUESTION NO: 21

An organization is establishing security requirements for software obtained from third-party suppliers and open-source repositories. Which of the following practices should be included to improve software supply chain security? Each correct answer represents a complete solution. Choose three.

A. Maintain a software bill of materials

B. Require digitally signed software artifacts

C. Perform dependency vulnerability scanning

D. Disable verification of package signatures

ANSWER: A B C

Explanation:

A **software bill of materials (SBOM)** provides an inventory of software components and dependencies, helping the organization determine whether deployed products contain vulnerable or prohibited components. **Digitally signed software artifacts** support verification that code, packages, or updates originated from an approved source and were not altered after signing.

Dependency vulnerability scanning identifies known vulnerabilities in direct and transitive third-party components so that affected software can be prioritized for remediation, replacement, or compensating controls. These practices provide visibility, integrity assurance, and vulnerability-management support throughout the software supply chain. See NIST SP 800-218, Secure Software Development Framework and CISA Software Bill of Materials resources.

QUESTION NO: 22

Which of the following is responsible for maintaining certificates in a public key infrastructure (PKI)?

A. Domain Controller

B. Certificate User

C. Certification Authority

D. Internet Authentication Server

ANSWER: C

Explanation:

Certification Authority is correct because it is the trusted PKI entity that manages the certificate lifecycle. A CA validates certificate applicants according to its established policies, issues and digitally signs certificates that bind an identity to a public key, and maintains certificate-status information throughout each certificate's usable life. This maintenance includes actions such as renewing certificates, revoking certificates when their associated private keys are compromised or their identity information is no longer valid, and publishing revocation status through mechanisms such as certificate revocation lists or the Online Certificate Status Protocol.

The CA's signature allows relying parties to verify that a certificate was issued by a trusted authority and that the public-key binding can be trusted within the scope defined by the CA's certificate policies and certification practice statement. In a hierarchical PKI, subordinate CAs may perform these functions under a root CA's authority, but they are still Certification Authorities. NIST describes a CA as the entity that issues certificates and manages the certificate lifecycle, while RFC 5280 defines the certificate and revocation-profile framework used by CAs. See NIST's Certification Authority definition and RFC 5280.

QUESTION NO: 23

Which of the following refers to a location away from the computer center where document copies and backup media are kept?

A. Storage Area network

B. Off-site storage

C. On-site storage

D. Network attached storage

ANSWER: B

Explanation:

Off-site storage is the correct term for a secure location physically separated from the primary computer center where an organization keeps copies of important documents, backup media, system images, and other recovery materials. Physical separation is essential to business continuity and disaster recovery because an incident affecting the primary site—such as a fire, flood, extended power outage, theft, or other localized disaster—may also destroy resources stored at that same location. An off-site facility helps ensure that recoverable copies remain available when they are needed to restore systems, records, and business operations.

For the storage arrangement to provide meaningful resilience, the organization should establish documented handling procedures, maintain an inventory and retention schedule, protect media with appropriate environmental and physical safeguards, and regularly verify that backups can be restored. The off-site location should also be sufficiently distant from the primary facility that both locations are unlikely to be affected by the same event, while still supporting the organization's recovery-time and recovery-point requirements. NIST discusses maintaining backup copies separately from primary systems in its contingency-planning guidance: NIST SP 800-34 Rev. 1, Contingency Planning Guide. Additional guidance on protecting and testing backups is available from the Cybersecurity and Infrastructure Security Agency.

QUESTION NO: 24

Which of the following are the goals of a public key infrastructure (PKI)? Each correct answer represents a part of the solution. Choose all that apply.

A. Authenticity

B. Globalization

C. Mobility

D. Integrity

E. Confidentiality

F. Nonrepudiation

ANSWER: A D E F

Explanation:

PKI is the people, policies, processes, and technology used to create, distribute, validate, revoke, and manage public-key certificates and their associated keys. Its security goals include **Authenticity**, because certificates bind a verified identity to a public key and enable relying parties to validate that binding. PKI also supports **Integrity**: digital signatures detect whether signed data has been altered after the signer created the signature. **Confidentiality** is supported when a recipient's validated public key is used to encrypt data or to protect key-establishment material, ensuring that only the holder of the corresponding private key can recover the protected information. Finally, **Nonrepudiation** can be supported through digital signatures when the PKI provides reliable identity proofing, protects private signing keys, records appropriate evidence, and maintains certificate status information. These capabilities depend on trusted certificate issuance and validation, including checking certificate validity and revocation status. NIST describes public-key certificates as binding an identity to a public key and identifies digital signatures and encryption among public-key cryptography's core uses. See NIST SP 800-57 Part 1 Rev. 5 and NIST PKI Concepts and Models.

QUESTION NO: 25

In which of the following Person-to-Person social engineering attacks does an attacker pretend to be an outside contractor, delivery person, etc., in order to gain physical access to the organization?

A. In person attack

B. Third-party authorization attack

C. Impersonation attack

D. Important user posing attack

ANSWER: C

Explanation:

Impersonation attack is correct because the attacker adopts a believable identity or role—such as a contractor, courier, maintenance worker, vendor representative, or delivery person—to obtain trust and physical entry. The impersonated role supplies a plausible business reason to be near restricted areas and can encourage employees, reception staff, or security personnel to waive normal identity-verification and visitor-control procedures. This attack exploits the tendency to cooperate with individuals who appear legitimate, are dressed appropriately, carry convincing props or paperwork, and act as though they are expected on site.

In a physical-security architecture, impersonation is addressed through consistently enforced visitor-management controls: independently verifying the visitor's identity and appointment, confirming the sponsoring employee or department, issuing time-limited visitor credentials, requiring escorts where appropriate, and challenging access attempts that bypass reception or controlled entrances. Organizations should ensure these controls apply even when the claimed person appears urgent, familiar with workplace terminology, or presents a convincing occupational identity. NIST's physical and environmental protection guidance includes visitor-access control requirements, while CISA highlights the value of training personnel to recognize social-engineering attempts. See NIST SP 800-53, Physical and Environmental Protection controls and CISA social engineering guidance.

QUESTION NO: 26

Which of the following is a correct sequence of different layers of Open System

Interconnection (OSI) model?

A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer

B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer

C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer

D. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

ANSWER: D

Explanation:

The correct sequence is **Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer**. Ordered from the lowest layer to the highest, the OSI reference model describes how communications move from the physical transmission medium upward to services used by applications. The Physical layer carries raw bits through signaling and media. The Data Link layer organizes transmission across a local link, including framing and media access. The Network layer provides logical addressing and routing between networks. The Transport layer provides end-to-end transport services, such as segmentation, reliability, and flow control. Above this, the Session layer establishes, manages, and terminates communication dialogs; the Presentation layer handles data representation functions such as format translation, encryption, and compression; and the Application layer supplies network services directly to end-user applications. This ordering is the canonical seven-layer OSI architecture and is useful for consistently locating networking functions and troubleshooting responsibilities. Cisco's overview of the model lists these same layers in

order, and the ISO standard is the source of the OSI basic reference model. See Cisco: What Is the OSI Model? and ISO/IEC 7498-1: OSI Basic Reference Model.

QUESTION NO: 27

Which of the following encryption methods does the SSL protocol use in order to provide communication privacy, authentication, and message integrity? Each correct answer represents a part of the solution. Choose two.

A. Public key

B. IPsec

C. MS-CHAP

D. Symmetric

ANSWER: A D

Explanation:

SSL, and its successor TLS, use a hybrid cryptographic design that combines public-key cryptography with symmetric cryptography. Public key cryptography is used during the handshake to authenticate a communicating party through its certificate and to securely establish or protect shared key material. This lets a client validate the identity represented by the server certificate before sensitive application data is exchanged. After the handshake establishes session keys, symmetric cryptography protects the actual application traffic. Symmetric session encryption is suitable for bulk data because it is substantially more efficient than public-key operations and provides confidentiality for the ongoing communication. The protocol also applies integrity protection to records, historically through a keyed message authentication code and, in modern TLS cipher suites, commonly through authenticated encryption. Thus, public key cryptography supplies authentication and secure key establishment, while symmetric cryptography supplies efficient protection for the session's data. Although SSL is obsolete and should not be deployed, its architecture established this model, which remains fundamental to TLS. See the historical SSL specification in RFC 6101 and the current TLS specification in RFC 8446.