CompTIA® Security+ (SY0-701) - Quiz Questions with Answers

1.0 General Security Concepts

1.

Which aspect of zero trust cybersecurity architecture refers to minimizing the impact in case there is a security breach?

- **Threat scope reduction**
- Adaptive identity
- Policy enforcement point
- Policy-driven access control

Correct answer: Threat scope reduction

Threat scope reduction refers to limiting the attack surface that can be exploited in a breach. Principles such as least privilege and identity-based network segmentation can aid in threat scope reduction.

Adaptive identity takes context into account when granting access rights. A policy enforcement point acts as a gatekeeper that ensures only authorized actions are permitted. Policy-driven access control refers to the automation of enforcing security policies.

2.

Which physical security control is often the first line of defense and can be augmented with barbed wire or razor wire at the top?

- **Fencing**
- Bollards
- Access control vestibules
- Honeynet

Correct answer: Fencing

Fencing is often the first line of defense for protecting a building. An 8-foot fence with barbed wire installed at a 45-degree angle is recommended to deter determined intruders.

Bollards are used to prevent vehicles from entering an area. An access control vestibule is used to allow only one authorized user at a time to enter an area. A honeynet is a fake network designed to entice attackers so they can be monitored.

3.

A zero trust security model divides logical components into what two types of planes?

- **Data and control**
- In-band and out-of-band
- Block and stream
- Symmetric and asymmetric

Correct answer: Data and control

A zero trust security model uses a data plane and a control plane. The data plane moves information, while the control plane manages intelligence around routing.

In-band and out-of-band refer to methods of network management. Block and stream are different ways to encrypt data. Symmetric and asymmetric are methods of key generation and sharing.

4.

Two users are communicating with each other through email. User 1 encrypts the message with a key made available by the recipient, user 2. The recipient is then able to read the message with their secret key so that only they can see the information. In response, user 2 sends a message back encrypted with the public key of user 1.

What type of key algorithm are they using?

- **Asymmetric**
- Symmetric
- Private
- Public

Correct answer: Asymmetric

Asymmetric key algorithms use a set of two different keys to encrypt and decrypt messages. The keys can be related, like symmetric keys, but it's not necessary. Two asymmetric keys are only related mathematically.

Symmetric algorithms do not use a public key. Private and public are two key types in asymmetric cryptography.

5.

After issues with the domain controllers, an administrator is ensuring that all of the servers synchronize their time with one another. This is being done with all systems, using the network time protocol (NTP).

Which of the following is sensitive to time differences and is likely the cause of the administrator's recent steps to synchronize them all?

- **Kerberos**
- DNS
- IPv4
- RDP

Correct answer: Kerberos

By design, Kerberos uses time in its tokens and therefore requires clients to be time-synchronized within five minutes of each other. Microsoft's Active Directory uses Kerberos for authentication and will have the individual domain controls periodically sync their time with a reliable internet server running the network time protocol (NTP).

DNS, IPv4, and RDP are not sensitive to minor time differences.

6.

What is the role of a policy enforcement point in a zero trust cybersecurity model?

To mediate requests by consulting with the policy administrator

To execute decisions made by the policy engine

To determine if subjects can access a resource based on policies

To limit the attack surface in case there is a security breach

---

Correct answer: To mediate requests by consulting with the policy administrator

The policy enforcement point acts as a gatekeeper that ensures only authorized actions are permitted. It forwards requests from clients and receives instructions from the policy administrator.

The policy administrator executes decisions made by the policy engine. The policy engine determines if subjects can access a resource based on policies. Threat scope reduction limits the attack surface in case there is a security breach.

7.

An administrator is analyzing an X.509 certificate. They want to know the authority that assigned the certificate. Which attribute will give them this information?

Issuer

Subject alternative names

Serial number

Common name

Correct answer: Issuer

The issuer attribute shows the certificate authority that created the certificate.

Subject alternative names show additional items protected by the certificate. The serial number differentiates certificates from others. The common name is the name associated with the public key.

8.

HR employees need to send personal and sensitive information to an employee for review. The information is regulated for privacy, and the HR resources need to ensure that only the recipient is able to open and view the information after authentication.

What can they use to encrypt the message into an unreadable form?

A cipher

A token

An index

A counter

Correct answer: A cipher

In cryptography, a cipher is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. It is also sometimes used to refer to the encrypted text message itself, although, in that case, the term "ciphertext" is preferred.

A token is used to replace sensitive data with a value that can later be replaced. An index is a data structure that increases data retrieval operations. A counter is a value that increments after each iteration.

9.

Which attribute of a digital certificate allows for specifying additional domains that are protected by the certificate?

- **SAN**
- CN
- Public key
- Validity period

Correct answer: SAN

A digital certificate has many attributes defined by the X.509 standard. The subject alternative name (SAN) allows for multiple DNS names supported by a single certificate.

The common name (CN) attribute contains the certificate owner. The public key attribute contains the actual public key used for secure communications. The validity period shows the dates that the certificate is valid.

10.

After an incident, an investigator generates a hash from the contents of a hard drive. What purpose does this hash value serve in an investigation?

Nonrepudiation

E-discovery

Data recovery

Secure wipe

Correct answer: Nonrepudiation

Nonrepudiation means that there is proof that someone cannot deny something, which can be accomplished by taking a hash value. Taking a hash value shows if the data has changed since it was first discovered.

11.

An administrator is planning the certificate requirements for a few new websites that will be made available to the public. They want to have the same root domain for several subdomains that divide up the applications.

Which of the following would work BEST for their situation?

Wildcard

Multiple certificates

Self-signed certificate

Root CA certificate

Correct answer: Wildcard

*A wildcard certificate begins with an asterisk (*) and can be bound to many websites that have different URLs, or names but bind back to the same root certificate. For example, if Acme Inc. used a wildcard certificate for *.acmeinc.com, they could have many subdomains, such as clients.acmeinc.com, blog.acmeinc.com, or mail.acmeinc.com and have the certificate work for each.*

Multiple certificates are not as efficient as wildcard certificates for subdomains. Self-signed certificates are used for domains that do not need to be trusted outside of an organization. Root CA certificates are self-signed.

12.

MD5 is a common hashing algorithm that was determined to be vulnerable with the advent of increased computing power but is still used to verify the integrity of files, emails, etc. Of the following vulnerabilities, which is MD5 MOST susceptible to?

Collision

Man-in-the-middle

Brute force

Decryption

Correct answer: Collision

A collision happens when two files receive the same MD5 hash, reducing their integrity. MD5 is also vulnerable to rainbow table attacks and pre-image attacks. Despite these vulnerabilities, MD5 is still used to verify files that have been downloaded from the internet, executable files, sensitive information, and more.

Man-in-the-middle attacks are likely in unencrypted networking protocols such as HTTP. Brute force attacks are likely with weak passwords. Decryption is likely with weak encryption protocols.

13.

Which of the following situations can be addressed by using honeyfiles?

A company wants to know when a system is breached

A company wants to have their administrative interface to a system located on a separate network

A company wants to block malicious sites based on their domain names

A company wants to monitor if any system files have changed

Correct answer: A company wants to know when a system is breached

Honeyfiles are files that are intended to be attractive to attackers. If a honeyfile is discovered to have been exfiltrated, it shows that the system has been breached.

Out-of-band management is used when a company wants to have their administrative interface to a system located on a separate network. DNS filtering is used when a company wants to block malicious sites based on domain names. File integrity monitors are used when a company wants to monitor if any system files have changed.

14.

A company wants to give their users the freedom to install any extra applications they feel that they need to be more productive. However, there are a few applications they do not want users to install because they may impact productivity.

What type of solution should they implement for this?

Block list

Allow list

Quarantine

Isolation

Correct answer: Block list

An application block list/deny list specifies the applications that are not permitted to run on an endpoint. These lists can be difficult to keep up to date as cybercriminals evolve their malware. For example, blocklists are less effective against zero-day threats and polymorphic malware.

An application allow list/approved list specifies the applications that are permitted to run on an endpoint. These lists must be kept up to date as the organization uses new applications and can cause issues if a legitimate application is excluded from the list. Endpoint security solutions commonly have quarantine functionality to prevent suspicious, malicious, or infected files from causing damage to an endpoint. Quarantining refers to disconnecting a system from the network rather than managing the risk posed by a particular application.

15.

Which of the following types of certificates is used as proof that a certificate owner is a legitimate business?

- **EV**
- DV
- Wildcard
- SAN

Correct answer: EV

Extended Validation (EV) certificates perform additional validation of a certificate owner, such as checking that it is a legitimate business.

Wildcard certificates validate an entire domain rather than a specific URL. This runs the risk that a rogue URL could be created and validated using the wildcard certificate. Subject alternative name (SAN) certificates can support multiple different common names, enabling the same server to support multiple URLs. A domain validation (DV) certificate is used to prove the identity of a website using SSL/TLS.

16.

The process of embedding secret messages has a rather long history. One method is to provide a seemingly normal communication that actually has secret information hidden within.

What is the term given to the science of writing hidden messages?

Steganography

Salting

Encryption

Key stretching

Correct answer: Steganography

Steganography is the science of hiding a secret message within an ordinary message, and the extraction of it at its destination. Steganography goes a step further than cryptography by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning the data will fail to know it contains encrypted data.

Salting involves adding data to a password to make it stronger. Cryptography uses ciphertext, which does not look like normal communication. Key stretching is a technique to make keys harder to attack with brute force.

17.

A trainer is explaining the various cryptographic topics that might be covered in the CompTIA exam. They're talking about a cipher that always uses a key of 13. For example, to encrypt a message, you count 13 characters past each plaintext letter. To decrypt the message, you trace back 13 characters in the alphabet from the ciphertext.

This is an example of which of the following?

- **Substitution cipher**
- Polyalphabetic substitution
- Transposition cipher
- Enigma machine

Correct answer: Substitution cipher

A substitution cipher works on a fixed system to swap plaintext with ciphertext. Because these systems use the same key and algorithm, they are not true forms of encryption. They are more a form of obfuscation, making the plaintext unclear or difficult to understand.

Polyalphabetic substitution uses multiple substitution alphabets for the same message. A transposition cipher scrambles letters in a certain manner. An enigma machine was a tool created during World War II to encrypt messages.

18.

An auditor is comparing a financial company's security processes to established industry standards. What activity are they involved in?

- **Gap analysis**
- Risk analysis
- Impact analysis
- Dynamic analysis

Correct answer: Gap analysis

A gap analysis looks at an organization's security controls and compares them to industry standards. Areas where the organization does not implement any controls are called gaps.

A risk analysis identifies any threats to an organization's systems or business processes. An impact analysis examines the effect of a system being taken offline. A dynamic analysis examines code while it is running.

19.

Which technique offers the BEST protection against polymorphic malware?

- **Allow list**
- Block list
- Deny list
- Revocation list

Correct answer: Allow list

Polymorphic malware changes its signature to avoid detection. An approved list will only allow specified applications to run, so it is the most restrictive.

An application blocklist/deny list specifies the applications that are not permitted to run on an endpoint. These lists can be difficult to keep up to date as cybercriminals evolve their malware. Revocation lists are used with digital certificates.

20.

A user is visiting a website using the HTTPS protocol. Which type of certificate are they MOST likely using to verify the authenticity of the website?

- **DV**
- EV
- SAN
- Wildcard

Correct answer: DV

Domain Validation (DV) certificates are used to prove the identity of a website using SSL/TLS in an HTTPS session. They are the simplest and most common types of certificates.

Wildcard certificates validate an entire domain rather than a specific URL. Subject Alternative Name (SAN) certificates can support multiple different common names, enabling the same server to support multiple URLs. Extended Validation (EV) certificates perform additional validation of a certificate owner, such as checking that it is a legitimate business.

21.

Which component of a zero trust cybersecurity architecture is responsible for making decisions in the control plane?

Policy-driven access control

Policy administrator

Policy enforcement point

Adaptive identity

Correct answer: Policy-driven access control

Policy-driven access control is performed by the policy engine in the control plane of a zero trust cybersecurity model. These policies define such things as access rights, permissions, and responses to various scenarios. The policy administrator consults the policy engine for decisions on access requests before relaying the result to the data plane.

The policy administrator consults the policy engine for decisions on access requests. The policy enforcement point accepts access requests from subjects in the data plane. Adaptive identity takes context into account when granting access rights.

22.

A security analyst is performing an audit on the security posture of the organization. They are evaluating various elements such as security awareness training, contingency planning, disaster recovery plans, and risk assessments.

Which control type are they auditing?

Managerial

Technical

Physical

Operational

Correct answer: Managerial

Managerial controls incorporate methods mandated by organizational policies or other guidelines. The primary stakeholders are executives and management, as they are those most likely to seek out risk determinations and reduce them with process changes. This can include items such as requirements to complete certain assessments, job rotation, segregation of duties, mandatory vacations, and more.

Technical security controls include firewalls and access control lists. Physical security controls include fences and door locks. Operational security controls include log monitoring and vulnerability assessments.

23.

Which of the following categories of controls is exemplified by using firewalls and encryption?

Technical

Operational

Physical

Managerial

Correct answer: Technical

Security controls can be classified into three categories, including:

- ***Managerial**: Managerial/administrative controls are policies, procedures, or guidelines. An organization's managerial controls are developed first and used as the basis for designing and implementing other security controls.*
- ***Operational**: Operational controls help an organization maintain normal operations. Backups or a policy stating that a system should be regularly reset are examples of operational controls.*
- ***Technical**: Technical/logical controls implement access management for a particular resource. Firewalls, passwords, encryption, and group policies are all examples of technical controls.*
- ***Physical**: Physical controls help to manage or prevent physical access to an organization's building, systems, etc. Fences, locked doors, etc. are examples of physical controls.*

24.

Some control goals deal with an event after it occurs, but there are a few that work before the event has happened. Controls such as cable locks, hardware locks, and warning signs act to discourage the threat.

Which of the following control types would these be examples of?

- **Deterrent**
- Corrective
- Detective
- Compensating

Correct answer: Deterrent

Deterrent controls act to discourage a threat before it has an opportunity to create a security incident. For example, cable locks and hardware locks discourage opportunistic thieves from taking advantage of unsecured hardware and locations. Security guards are also an excellent example because simply having one posted in a location is a significant deterrent to potential threats.

Corrective controls fix issues that have already occurred. Detective controls identify events that have occurred. Compensating controls mitigate risks that were made as exceptions to security policies.

25.

The owner of Smith Roofing has voiced concern that their workstation users might be able to install any application and potentially introduce malware. There are only a few applications that each user needs in order to fulfill their job duties.

What type of solution would meet their requirements and be the easiest to implement?

Allow list

Block list

Host-based firewall

Content filters

Correct answer: Allow list

An application allow list gives administrators the ability to specify a list of applications that can be used on a system. This prevents users from installing applications that could be malicious. It also limits some malware's ability to silently install malicious software on the system.

A block list requires more work because it must be updated regularly. A host-based firewall filters packets. A content filter blocks users from visiting certain sites.

26.

The chief executive officer at Smith Bank, a new financial startup, has hired you as a security consultant. Looking through surveillance video, you notice that sometimes, people pass through security points by closely following the person in front of them.

What type of security control should be put in place to address this?

Access control vestibule

Bollards

Sensors: infrared

Sensors: pressure

Correct answer: Access control vestibule

Access control vestibules are used to ensure that only one person at a time can pass through a control point. They are typically a small room with two doors.

Bollards are pillars or obstacles used to prevent vehicular access. Infrared sensors are used to detect heat radiation. Pressure sensors are used to detect movement by changes in pressure.

27.

An e-commerce site wants to allow users to store their credit card numbers without keeping the actual account numbers in their database. What security solution can they use that allows them to substitute the numbers for the real ones when needed?

Tokenization

Salting

Hashing

Attestation

Correct answer: Tokenization

Tokenization allows for sensitive data to be stored at a token service provider instead of being stored locally. The locally stored token can be replaced with the real value when needed.

Salting is used to add randomized data to values before hashing. Hashing is the one-way algorithm to turn a variable-length input into a fixed-length output. Attestation is the process of verifying that something is true by a third party.

28.

Which factor in modern cryptographic systems is critical for ensuring that encryption will not be compromised through cryptographic attacks?

Key length

Nonrepudiation

Integrity

Obfuscation

Correct answer: Key length

Modern cryptosystems use open algorithms, so the responsibility is placed on creating keys that are long and complex. The longer the key is, the more difficult it will be for an attacker to use cryptographic attacks against it.

Nonrepudiation refers to the inability for someone to deny that they sent a message. Integrity refers to ensuring that data is not altered. Obfuscation refers to methods to hide sensitive data.

29.

Smith Industries has several sister companies under its umbrella and wants to get a domain name that reflects that. They are reviewing several different forms. They require one that has different URLs for each company but shows that they are owned by Smith Industries.

Which of the following would they use?

Subject alternative name

Wildcard certificate

Self-signed certificate

Common name

Correct answer: Subject alternative name

*A subject alternative name (SAN) is used when an organization has several websites/URLs that need to be identified as being owned by the same organization. This is used in cases like Google, where they have domains such as *google.com, *.android.com, *.cloud.google.com, etc.*

A wildcard domain is good for subdomains of a domain. A self-signed certificate is used internally or for testing. A common name describes the certificate owner.

30.

Which type of physical control can offer both detection and response capabilities?

Security guards

Lighting

Fencing

Bollards

Correct answer: Security guards

Security guards are able to both identify security issues and respond to them, as well. They can be stationed in one area, kept in a central monitoring station, or roam the building.

Lighting is used to make an area more visible and feel safer. Fencing is used at a perimeter to deter attacks. Bollards are used to prevent vehicles from entering an area.

31.

Part of a public key infrastructure (PKI) is the relative authorities governing the certificates and providing an authoritative answer to whether a certificate is still valid or not.

Within a PKI system, what is used to list certificates that are no longer valid?

Certificate revocation list

Certificate list

Revocation firewall

Trust authority

Correct answer: Certificate revocation list

The certificate revocation list (CRL) is a list of certificates that are no longer valid or that have been revoked by the issuer. There are two states of revocation: revoked and on hold. Revoking a certificate is crucial when the private key of the public/private key pair becomes compromised. This leads to the encryption being vulnerable to all those who have the private key, and it will need to be replaced and all elements currently using it will need to be invalidated. Certificate revocation would also be invoked in instances of CA compromise, change of affiliation, etc.

The other answer choices are not accepted terminologies.

32.

A financial firm has a policy of using only the most current version of operating systems on their servers. However, they have an application that can only be run on a previous version. To address this, they place that system in its own isolated network.

What type of security control are they implementing?

Compensating

Preventative

Detective

Corrective

Correct answer: Compensating

Security controls can be classified into one of six different types, including:

- ***Preventative**: Preventative controls stop a security incident from occurring. A locked door to a secure area is an example of preventative control.*
- ***Detective**: Detective controls identify if a security incident has occurred. An intrusion detection system (IDS) and a security guard watching CCTV are examples of detective control.*
- ***Corrective**: Corrective controls mitigate a security incident after it has occurred. Backups are an example of corrective control because they can restore a system to its original state.*
- ***Deterrent**: Deterrent controls disincentivize an attacker from performing a malicious action. A barbed wire fence or a visible CCTV camera is an example of a physical deterrent control.*
- ***Compensating**: Compensating controls are used when the desired control can't be used and often relate to compliance requirements. For example, an organization might hire a security guard if it cannot build a fence around a rented building or if the fence is damaged.*
- ***Directive**: Directive controls include policies and procedures that tell users what they should do to keep systems secure.*

33.

Smith Industries is using multiple VPN servers and wants to centralize the authentication by switching over to a new Cisco VPN that is TCP-based and interfaces with their Active Directory servers.

Which of the following protocols should they use?

TACACS+

RADIUS

OAuth

Kerberos

Correct answer: TACACS+

The Terminal Access Controller Access-Control System Plus (TACACS+) is produced by Cisco as an alternative to RADIUS. Through encryption of the entire authentication process, and multiple challenges and responses between the server and client, TACACS+ provides enhanced security over RADIUS. Furthermore, TACACS+ can interface with a Microsoft Active Directory environment for authentication purposes.

RADIUS would not be used over TACACS+ in a Cisco environment. OAuth is used for authorization in single sign-on solutions. Kerberos is used in a context where clients need to access specific services and need to use an authentication server.

34.

A group of salespeople within an organization routinely travel, and there have been times when laptops were lost during these trips. Management is concerned that data could be stolen from these devices despite being password-protected. They are Windows-based laptops and are ultraportable.

What Windows application lets an administrator control whole disk encryption on a system?

BitLocker

Tripwire

Bitdefender

Splunk

Correct answer: BitLocker

BitLocker is an encryption application included with Windows. The administrator can control BitLocker settings through the group policy editor. BitLocker requires a USB to store the encrypted keys, and the hard drive must be configured with at least two partitions, one for the operating system and one for the encrypted data.

Tripwire is a file integrity monitoring solution. Bitdefender is antivirus software. Splunk is a security orchestration, automation, and response system.

35.

Which of the following categories of security controls includes log monitoring and reviewing user access?

Operational

Managerial

Technical

Physical

Correct answer: Operational

Security controls can be classified into three categories, including:

- ***Managerial**: Managerial/administrative controls are policies, procedures, or guidelines. An organization's managerial controls are developed first and used as the basis for designing and implementing other security controls.*
- ***Operational**: Operational controls help an organization maintain normal operations. Backups or a policy stating that a system should be regularly reset are examples of operational controls.*
- ***Technical**: Technical/logical controls implement access management for a particular resource. Firewalls, passwords, encryption, and group policies are all examples of technical controls.*
- ***Physical**: Physical controls help to manage or prevent physical access to an organization's building, systems, etc. Fences, locked doors, etc. are examples of physical controls.*

36.

What type of key is known to any party that wants to send a recipient an encrypted message?

- **Public**
- Private
- Symmetric
- Derivation

Correct answer: Public

The public key is used by any third party to encrypt a message and send it to a recipient. The recipient uses their private key to decrypt the message. This structure is exceedingly useful in private communications, as the public key is used to encrypt information so that only the user with the private key has the ability to decrypt it.

A private key is known only to the owner of that key. Symmetric keys are only shared between trusted parties. Derivation keys are derived from other keys.

37.

An attacker has infiltrated a government agency and intends to exfiltrate information to sell at a profit. In order to hide their tracks, they embed the sensitive information within the bits of normal documents that would be sent to their personal email address. Upon receipt at home, the attacker decrypts the information and provides it to the recipient.

Which of the following techniques did they likely use in this scenario?

Steganography

IV attack

Collision

Replay

Correct answer: Steganography

Steganography is the process of altering the underlying data, or white space, in order to obfuscate the hidden data within. It is possible to either manipulate the bits of data, such as the least significant, and embed the data among the file, or the data can be hidden in the white space of the file, the areas of unused data at the end of file clusters.

An initialization vector (IV) attack targets the random or nonce value used in a session. A collision attack targets algorithms that produce the same output with two different inputs. A replay attack replays intercepted data to gain unauthorized access to a system.

38.

Verifying that a sender or object is what they claim to be is the point of authentication. There have been methods specifically designed to verify, or authenticate, individuals in a communication stream so that they can generally trust who they are communicating with or trust that the document is real and not tampered with.

What is used to authenticate a document through mathematical computations?

Digital signature

Symmetric cryptography

Data masking

Private keys

Correct answer: Digital signature

A digital signature authenticates a document using math. It verifies that the sender is who they say they are. It tells the recipient that the name on the document is that of the actual user and not someone else. Similar to handwritten signatures on printed documents, this technique serves to provide a unique element to the form or document so that it can be tied to a single individual.

Symmetric cryptography requires sharing private keys and focuses on confidentiality rather than authenticity. Data masking involves hiding sensitive data with fake data. Private keys are needed along with public keys to show authenticity.

39.

Which of the following steps can an organization take to protect management consoles for switches?

Placing management ports on an isolated VLAN

Disabling logging and real-time monitoring

Turning off TOTP for authentication

Implementing FDE

Correct answer: Placing management ports on an isolated VLAN

Segmenting management traffic by using an isolated VLAN can enhance security. Other ways to harden network devices include keeping firmware updated, enabling logging, applying ACLs, changing default settings, and using secure protocols.

Logging and real-time monitoring are useful for managing security on a network device. Time-based one-time passwords (TOTP) can improve authentication. Full-drive encryption (FDE) is used with storage devices.

40.

For enhanced security, the standard profile for a firewall is to allow only connections that have specifically been described in the filters and to restrict all other access. What type of access control is this?

- **Implicit deny**
- Least privilege
- Separation of duties
- Job rotation

Correct answer: Implicit deny

This access control practice automatically denies all users except those explicitly given access to the object. This method is good for highly sensitive, confidential data.

Least privilege refers to only giving users the minimal amount of privileges they need to complete their job. Separation of duties refers to ensuring that a critical job function requires more than one person to complete. Job rotation refers to ensuring that users are cross-trained in multiple roles.

41.

What is one advantage of asymmetric encryption over symmetric encryption?

Non-repudiation

Confidentiality

Bulk encryption

Speed

Correct answer: Non-repudiation

Asymmetric encryption allows for non-repudiation because a private key corresponds to a public key that authenticates digital signatures. Since the private key is only known to the owner, it assures authentication.

Both symmetric and asymmetric encryption offer confidentiality. Symmetric encryption can be used for bulk encryption and is faster.

42.

A company is performing a periodic risk assessment. Which of the following categories of security controls are they engaged in?

Managerial

Operational

Technical

Logical

Correct answer: Managerial

Security controls can be classified into three categories, including:

- ***Managerial**: Managerial/administrative controls are policies, procedures, or guidelines. An organization's managerial controls are developed first and used as the basis for designing and implementing other security controls.*
- ***Operational**: Operational controls help an organization maintain normal operations. Backups or a policy stating that a system should be regularly reset are examples of operational controls.*
- ***Technical**: Technical/logical controls implement access management for a particular resource. Firewalls, passwords, encryption, and group policies are all examples of technical controls.*
- ***Physical**: Physical controls help to manage or prevent physical access to an organization's building, systems, etc. Fences, locked doors, etc. are examples of physical controls.*

43.

An administrator is configuring an access control list and wants connections to be denied by default. In this type of ACL, what part contains the specific traffic that should be permitted?

Explicit allow

Implicit allow

Explicit deny

Implicit deny

Correct answer: Explicit allow

An access control list (ACL) contains lists of traffic that is allowed and disallowed. When traffic is allowed to pass, it should be in the "explicit allow" list. When you implicitly allow traffic, all traffic is allowed to access the network unless you specifically deny it. ACLs implicitly disallow traffic unless specific access is given through user permissions.

44.

What type of encryption uses a single key for both encryption and decryption?

- **Symmetric**
- Asymmetric
- Stream
- Block

Correct answer: Symmetric

Symmetric key algorithms use a single key, identical keys, or closely related keys for both encryption and decryption. It's also referred to as a secret key or private key. Examples are DES, 3DES, and AES.

Asymmetric cryptography uses a public and private key. Stream ciphers operate on bits of a message at a time. Block ciphers operate on blocks of a message.

45.

Which component of the control plane in a zero trust cybersecurity model provides context to user authentication?

- **Adaptive identity**
- Threat scope reduction
- Policy-driven access control
- Policy administrator

Correct answer: Adaptive identity

Adaptive identity takes context into account when granting access rights. It considers factors such as where the user is logging in from, what device they are using, and whether their device meets security standards.

Threat scope reduction refers to limiting the attack surface that can be exploited in a breach. Policy-driven access control refers to the automation of enforcing security policies. A policy administrator communicates with the data plane using decisions based on the policy engine.

46.

Security is never guaranteed within an environment, especially against advanced persistent threats. Considering that a device or network will inevitably be penetrated, it is best to preemptively secure the sensitive information through encryption. This ensures that even if the passwords are stolen, they are not easily readable. Taken a step further, it is possible to make password hashes resistant to cracking.

What is the term given to adding randomization to the hashing process in encrypted passwords?

- **Salting**
- Hashing
- Steganography
- Data masking

Correct answer: Salting

Salting randomizes the hashing done in password encryption. This makes it more difficult for the attacker to crack a password using cryptanalysis attacks. By throwing in the additional random elements, previously computed values become less valuable. Common words and numbers are no longer what the password hash represents, as it now has random characters or values added to the hash that the password cracking program is not aware of.

Hashing is the process of using an algorithm to turn a variable-length input into a fixed-length value. Steganography is the process of hiding a message in a different medium. Data masking involves replacing sensitive information in a dataset with fake data.

47.

Which of the following deceptive technologies would a passwords.txt file be an example of?

Honeyfiles

Honeypot

Honeynet

Honeytoken

Correct answer: Honeyfiles

Honeyfiles are fake files on a real system filled with data designed to entice an attacker. For example, a file named passwords.txt can detect an intrusion if the attacker opens it.

A honeypot is a computer that pretends to be real and is intentionally vulnerable. A honeynet is an entire fake network made up of honeypots. A honeytoken is data that is attractive to an attacker that can be tracked.

48.

A company suspects that sensitive information has been exfiltrated by an insider. To detect suspicious behavior, they set up a database entry disguised as sensitive information, then configure their DLP to alert when that data has been infiltrated.

What type of deception technology is the company using?

- **Honeytoken**
- Honeypot
- ACL
- TTP

Correct answer: Honeytoken

A honeytoken is data that has been created to attract an attacker. It can then be tracked by an IDS/IPS/DLP solution.

A honeypot is an entire system that is designed to be broken into by an attacker. An access control list (ACL) is a tool for deciding whether to permit or deny an action. Tactics, techniques, and procedures (TTP) are identifiable methods and strategies that attackers use.

49.

Executives are working on new methods to maintain growth in the organization and handle operations in the event of any disasters or disruptions. They want to ensure that vulnerable business processes are identified and mission-essential functions are prioritized.

Which of the following would help them accomplish this?

BIA

RPO

Vulnerability assessment

Penetration test

Correct answer: BIA

A business impact analysis (BIA) is an important component of a business continuity plan (BCP). It enables an organization to pinpoint critical elements and processes necessary for business operations. Identifying the mission-essential functions allows for prioritization in the event of restoration efforts and identification of vulnerable business processes that support these mission-critical functions.

A recovery point objective (RPO) is the maximum acceptable amount of data loss in the event of an incident. A vulnerability assessment is a scan of a network or system to identify weaknesses. A penetration test seeks to actively exploit vulnerabilities in a network or system.

50.

An administrator is working on resolving a recent case of DNS poisoning that an attacker carried out within the local network. They want to ensure that future DNS updates are coupled with a digital signature in order to provide data integrity and validity.

Which of the following could they implement to achieve this?

DNSSEC

DNS filtering

Reverse lookups

DHCP

Correct answer: DNSSEC

The primary risk with DNS is DNS poisoning, which can be achieved through sending spoofed DNS records to a DNS server in the hope that it will accept them as valid and present them to clients that request DNS information. Domain name system security extensions (DNSSEC) provide a suite of tools to ensure that the DNS structure is backed by valid digital signatures and trusted authorities.

DNS filtering is used to block malicious domains. Reverse lookups are used to retrieve an IP address from a domain name. DHCP is used to dynamically allocate IP addresses.

51.

The CompTIA Security+ exam covers areas such as implementing the appropriate security controls, which can have a positive impact on an organization's overall security posture. Controls such as log monitoring, trend analysis, security audits, video surveillance, and motion detection all fall under which of the following control categories?

Detective

Preventive

Corrective

Compensating

Correct answer: Detective

Detective controls are used to detect when vulnerabilities and weaknesses have been exploited; they notify the individuals who can stop the security incident. Detective controls discover the event after it has occurred and provide the ability for a reactive response.

Preventive controls include encryption and firewalls to stop incidents before they occur. Corrective controls address issues after they have occurred. Compensating controls mitigate risks that appear due to exceptions from a security policy.

52.

Acme Manufacturing is starting a web store to provide direct customer sales of their products. They want to create a secure front-end for the payment processing and use a secure encryption algorithm.

What is a common asymmetric key algorithm that Acme could use for credit card security?

RSA

AES

DES

Triple DES

Correct answer: RSA

Rivest-Shamir-Adleman (RSA) is a common public key cryptography algorithm used in credit card security and TLS/SSL. Key lengths for RSA are much longer than those in symmetric cryptosystems.

AES, DES, and Triple DES are symmetric cryptosystems.

53.

Smith Consulting is moving to a new headquarters and is concerned about physical security. They want to ensure that guards can have real-time visual access to all entry points into the building, and that this information can be accessed later.

What type of security control should they implement for this?

Video surveillance

Sensors: infrared

Lighting

Honeynet

Correct answer: Video surveillance

Video surveillance lets areas of a building be monitored centrally. It also keeps a record that can be referred to later.

Infrared sensors detect heat radiation. Lighting can be used to make an area feel safer. A honeynet is a fake network designed to attract attackers so they can be studied.

54.

Before authenticating a user, an organization checks the user's location and device to understand the context of the authentication request. What aspect of a zero trust cybersecurity approach is the organization following?

Adaptive identity

Threat scope reduction

Policy-driven access control

Implicit trust zones

Correct answer: Adaptive identity

Adaptive identity takes context into account when granting access rights. It considers factors such as where the user is logging in from, what device they are using, and whether their device meets security standards.

Threat scope reduction refers to limiting the attack surface that can be exploited in a breach. Policy-driven access control refers to the automation of enforcing security policies. Implicit trust zones are areas where explicit verification is not required.

55.

An administrator wants to be certain that if a company's laptop is lost or stolen, the contents of the hard drive will be encrypted. Which feature can make sure that the entire drive is encrypted?

FDE

UEFI

RAID

DLP

Correct answer: FDE

Full disk encryption (FDE) is a security feature that allows an entire disk to be encrypted. This is accomplished on Windows through their BitLocker implementation. In order to boot the system, a user must be in possession of the keys to decrypt the drive.

UEFI is a type of firmware. RAID is used for redundancy and to increase performance of disks. DLP is used to prevent data exfiltration.

56.

Which of the following domains will be covered under the certificate for *.example.com?

- **test1.example.com**
- www.test1.example.com
- test1.example.org
- test1.www.example.com

Correct answer: test1.example.com

A certificate with a wildcard in the name is valid for subdomains. It only covers one level of subdomains, so sub-subdomains are not covered.

57.

A security firm wants to ensure that their messages are secure and authentic. They want to provide encryption to these messages through various digital signatures and certificates.

Which of the following is a large system of software, policies, and procedures used for digital signatures and certificates?

- **PKI**
- HSM
- TPM
- FDE

Correct answer: PKI

A public key infrastructure (PKI) is an entire system of hardware and software, policies and procedures, and people. It's used to distribute, manage, store, and revoke digital certificates. The public key is only able to encrypt information and the private key is only able to decrypt information. The public and private keys are matched, so that information encrypted with the public key can only be decrypted by the associated private key.

A hardware security module (HSM) is a hardware device that handles key management and cryptographic operations. The Trusted Platform Management (TPM) is a component that ensures systems are secure. Full-device encryption (FDE) is used to automatically encrypt hard drives.

58.

A new junior security resource has been hired at Acme Inc. and is asking questions about various security elements. One of his questions was about what the three items in the CIA triad are.

What would you tell the junior tech?

Confidentiality, Integrity, Availability

Confidentiality, Interoperability, Availability

Centralization, Integrity, Availability

Confidentiality, Integrity, Access levels

Correct answer: Confidentiality, Integrity, Availability

The CIA triad includes confidentiality, integrity, and availability. Confidentiality prevents disclosure of information to unauthorized people. Integrity ensures that data has not been tampered with. Availability ensures that data is available to those who need it, regardless of the security used on it.

59.

An older business is deploying credit card processing and a new web store front end. They are investigating the security requirements for the potential web application development.

Which of the following algorithms is asymmetrical and often used in e-commerce because it works well with credit card security and TLS/SSL?

RSA

AES

DES

3DES

Correct answer: RSA

RSA is widely used to protect data such as email and other data transmitted over the internet. It is an asymmetric encryption method that uses both a public key and a private key matched pair and is widely used in protocols such as SSL, WEP, and RDP. It's known for its simplicity. The RSA algorithm and its developers, Ron Rivest, Adi Shamir, and Leonard Adleman, laid the groundwork for modern asymmetrical encryption methods.

AES, DES, and 3DES are symmetric cryptography standards.

60.

What is the role of stakeholders in the change management process?

Holding a vested interest in the outcome of the organization's processes

Analyzing the impact of a change to other systems in the organization

Testing a potential change before it is implemented in production systems

Taking ownership of a change to ensure its successful completion

---

Correct answer: Holding a vested interest in the outcome of the organization's processes

A stakeholder includes anyone with a vested interest in the positive outcome of an organization. Stakeholders are not only investors, but also employees, suppliers, creditors, and regulatory bodies.

Analyzing the impact of a change to other systems in the organization, testing a potential change before it is implemented in production systems, and taking ownership of a change to ensure its successful completion are roles completed by individual employees rather than the responsibility of all stakeholders.

61.

Symmetrical keys rely on the key remaining unknown, which presents difficulty when attempting to communicate securely with another party. If an attacker obtains the key, they can compromise all messages sent with that key.

What term is used for the situation in which security ensures that the compromising of one message will not lead to the compromising of another?

PFS

PGP

PKCS

NTP

Correct answer: PFS

TLS used with Diffie-Hellman works in ephemeral mode, meaning that keys are generated during each portion of the key establishment process. This ephemeral process achieves perfect forward secrecy (PFS).

Pretty good privacy (PGP) is an encryption program that provides confidentiality and authentication. Public key cryptography standards (PKCS) is a set of formats for cryptographic operations using public key cryptography. The Network Time Protocol (NTP) is used to synchronize clocks.

62.

An executive comes up with a business idea while on their personal, unprotected computer. They type their plan into a document and want to ensure that the document is secure. Which type of encryption will be MOST convenient to use in this situation?

File-level encryption

Volume encryption

FDE

TDE

Correct answer: File-level encryption

File-level encryption lets a user encrypt individual files rather than entire drives or partitions. It is useful for targeting an important file.

Volume encryption is used on an entire volume of a disk. Full-disk encryption (FDE) encrypts an entire drive. Transparent data encryption (TDE) is used to encrypt entire databases.

63.

Where does a blockchain store a history of its transactions?

Open public ledger

Relational database

Digital certificate

Hardware security module

Correct answer: Open public ledger

A blockchain uses an open public ledger for storing transactions. This allows for transparency even as the ledger is cryptographically secured.

A relational database is centralized and stores data in rows and columns. A digital certificate is a public key for encrypting data and verifying authenticity. A hardware security module is a device to generate, store, and manage cryptographic keys.

64.

A junior administrator is being briefed on the various components of security within the organization. The technical lead mentions the "three As" of security. What comprises the AAA of computer security?

Authentication, Authorization, Accounting

Authentication, Access, Accounting

Authentication, Access, Availability

Availability, Authorization, Accounting

Correct answer: Authentication, Authorization, Accounting

The "three As" in computer security include authentication, authorization, and accounting.

- ***Authentication**: confirms a user's identity using some kind of authentication scheme*
- ***Authorization**: controls the authenticated user's access rights and permissions to certain objects*
- ***Accounting**: tracks data usage and network resources for auditing purposes*

65.

There are instances in which satisfying security requirements is impractical or too difficult to implement. These instances require special mechanisms that provide some level of security, but they do not give the same level of security as a full-control solution.

Which of the following BEST fits this description?

Compensating controls

Preventive controls

Detective controls

Directive controls

Correct answer: Compensating controls

Compensating controls are alternatives to primary controls for certain instances in which the primary control is impractical or too difficult to implement. For example, an organization may use smart cards to allow employees network access, but newly hired employees don't receive their badges immediately. In these cases, a time-based one-time password (TOTP) might be implemented as a compensating control.

Preventive controls are used to stop an incident before it occurs. Detective controls identify events that have already occurred. Directive controls inform users of what they should do to meet security objectives.

66.

Which protocol can be used to determine if a certificate has been revoked?

OCSP

LDAP

SCAP

SNMP

Correct answer: OCSP

The Online Certificate Status Protocol (OCSP) is used to automatically check if a certificate has been revoked or is in good standing with the certificate's CA. This request can be sent by a browser.

LDAP is used for directory information. SCAP is used to automate security issues. SNMP is used for managing network devices.

67.

An administrator wants to encrypt all communications from systems on one network with systems on another network. Which mode of IPSec should be used in this situation?

Tunnel

Transport

Counter

Incognito

Correct answer: Tunnel

Tunnel mode is used when IP traffic is encapsulated and sent outside of a LAN across a WAN to another network. This occurs in VPNs that use IPSec.

Transport mode is used for communication between two devices. Counter mode is used with block ciphers. Incognito mode is a web browser option.

68.

Backups are an example of which of the following types of security controls?

Corrective

Preventive

Compensating

Detective

Correct answer: Corrective

Security controls can be classified into one of six different types, including:

- ***Preventive**: Preventative controls stop a security incident from occurring. A locked door to a secure area is an example of preventative control.*
- ***Detective**: Detective controls identify if a security incident has occurred. An intrusion detection system (IDS) and a security guard watching CCTV are examples of detective control.*
- ***Corrective**: Corrective controls mitigate a security incident after it has occurred. Backups are an example of corrective control because they can restore a system to its original state.*
- ***Deterrent**: Deterrent controls disincentivize an attacker from performing a malicious action. A barbed wire fence or a visible CCTV camera is an example of a physical deterrent control.*
- ***Compensating**: Compensating controls are used when the desired control can't be used and often relate to compliance requirements. For example, an organization might hire a security guard if it cannot build a fence around a rented building or if the fence is damaged.*
- ***Directive**: Directive controls include policies and procedures that tell users what they should do to keep systems secure.*

69.

A company has received a request from law enforcement to recover some encrypted data. What should IT staff refer to before retrieving a key from escrow and using it to decrypt a user's data without their knowledge?

Key recovery policy

Sender Policy Framework

Acceptable use policy

Policy Enforcement Point

Correct answer: Key recovery policy

A key recovery policy should be used by an organization so that employees can refer to it when keys are needed to be recovered. This can happen during situations such as system recovery situations, employee departures, or law enforcement requests.

The Sender Policy Framework is used to prevent email spoofing. An acceptable use policy is used to tell users how they can use company equipment. A Policy Enforcement Point is used for access control.

70.

Which of the following types of security controls is a security guard monitoring CCTV?

Detective

Corrective

Compensating

Deterrent

Correct answer: Detective

Security controls can be classified into one of six different types, including:

- ***Preventative**: Preventative controls stop a security incident from occurring. A locked door to a secure area is an example of preventative control.*
- ***Detective**: Detective controls identify if a security incident has occurred. An intrusion detection system (IDS) and a security guard watching CCTV are examples of detective control.*
- ***Corrective**: Corrective controls mitigate a security incident after it has occurred. Backups are an example of corrective control because they can restore a system to its original state.*
- ***Deterrent**: Deterrent controls disincentivize an attacker from performing a malicious action. A barbed wire fence or a visible CCTV camera is an example of a physical deterrent control.*
- ***Compensating**: Compensating controls are used when the desired control can't be used and often relate to compliance requirements. For example, an organization might hire a security guard if it cannot build a fence around a rented building or if the fence is damaged.*
- ***Physical**: Physical controls help to manage or prevent physical access to an organization's building, systems, etc. Fences, locked doors, etc. are examples of physical controls.*

71.

A company wants to implement a single security device that will handle deep packet inspection and intrusion prevention. What type of device should they use?

- **NGFW**
- Layer 4 firewall
- WAF
- Proxy server

Correct answer: NGFW

A next-generation firewall (NGFW) handles numerous security duties, including deep packet inspection, IDS/IPS, and anti-malware. This can reduce the number of devices needed to secure a network.

A Layer 4 firewall focuses on filtering by IP addresses, port numbers, and transport protocols. A web application firewall focuses on protecting a web application. A proxy server is used for purposes such as content filtering and caching.

72.

Which of the following use cases is ideal for using a honeytoken?

A company wants to be alerted if a malicious attacker is trying to exfiltrate data

A company wants to prevent unauthorized users from using their email servers

A company wants to add extra protection to their web application servers

A company wants to actively block attack attempts on their systems

---

Correct answer: A company wants to be alerted if a malicious attacker is trying to exfiltrate data

A honeytoken is fake data that is designed to be tracked in case it is exfiltrated. It can be detected by an IDS, IPS, or DLP solution when it is being exfiltrated.

SPF is used when a company wants to prevent unauthorized users from using their email servers. A web application firewall is used when a company wants to add extra protection to their web application servers. An IPS is used when a company wants to actively block attack attempts on their systems.

73.

A security research company wants to analyze what attackers do when they have compromised a system. To that end, they set up a DNS server with a known vulnerability that can be easily exploited.

What type of deception technology are they using?

Honeypot

Honeynet

Honeyfile

Fake telemetry

Correct answer: Honeypot

A honeypot is a computer that pretends to be real and is intentionally vulnerable. It is designed to attract an attacker's attention, waste their time, and provide useful data for security personnel. These are often virtual machines because virtualization makes it easier to reset them to a clean state after an attack.

A honeynet is an entire fake network made up of honeypots. It requires more work than a honeypot or honeyfiles. Honeyfiles are fake files on a real system filled with data designed to entice an attacker. For example, a file named passwords.txt can detect an intrusion if the attacker opens it. Fake telemetry is fake data designed to test solutions that analyze security solutions that monitor and use this telemetry data. It is not a deceptive technology.

74.

A systems administrator is generating a certificate for a developer in the organization. This certificate is not signed by a trusted CA, but it will not be used outside the organization, so that does not present a problem.

Which of the following is being used in this situation?

- **Self-signed certificate**
- Wildcard certificate
- EV certificate
- DV certificate

Correct answer: Self-signed certificate

A self-signed certificate is usually used within a private enterprise via a private CA in the organization. While not trusted by default, automated methods can be used to spread the appropriate certificates to workstations and servers to trust and then be used to eliminate the need to purchase certificates from public CAs.

Wildcard certificates are used for subdomains. An Extended Validation (EV) certificate performs extra verifications on the certificate holder. A Domain Validation (DV) certificate verifies that the certificate holder has control of the domain name.

75.

In a PKI system, what holds a copy of a user's private key in case it is lost or needs to be accessed by authorized third parties, such as with government court orders?

Key escrow

Password manager

Secure enclave

Honeytoken

Correct answer: Key escrow

Certificate keys can be held in escrow. Key escrow is when a secure copy of a user's private key is held as a backup in case the key is lost. It's also used so that third parties can gain access to data that's encrypted with a certain key.

A password manager is a tool for individuals to manage multiple passwords. A secure enclave is a high-security area where a system can make computations in isolation. A honeytoken is a file that can be tracked if exfiltrated by a threat actor.

76.

Which type of sensor detects movement by sensing touches or steps?

Pressure

Infrared

Microwave

Ultrasonic

Correct answer: Pressure

A pressure sensor can detect pressure from touches, steps, or even air pressure.

Infrared sensors detect heat signature changes. Microwave sensors detect frequency alterations made by moving objects. Ultrasonic sensors detect sound waves.

77.

Which of the following privacy-enhancing technologies involves a lookup table?

- **Tokenization**
- Masking
- Encryption
- Hashing

Correct answer: Tokenization

Tokenization replaces sensitive data with a non-sensitive token. A lookup table maps the token to the sensitive data for retrieval when needed.

Masking replaces sensitive data with an asterisk or similar character. For example, all but the last four digits of credit card numbers are often masked on receipts. Encryption scrambles data in a way that makes it unreadable and unusable without knowledge of the decryption key. Hashing creates a fixed-length value from an input of any length which can be used to verify the integrity of files.

78.

Which phrase accurately describes asymmetric cryptography?

A cryptographic system that uses public and private keys

A cryptographic system that uses the same key for encryption and decryption

A cryptographic system that only encrypts one way, such that the plaintext cannot be derived from the ciphertext

A cryptographic system that allows one party to prove they know a piece of information without revealing the information itself

---

Correct answer: A cryptographic system that uses public and private keys

Asymmetric cryptography uses a publicly known key that can be distributed to others and a private key that is only known to the owner. Asymmetric cryptography is used for public key infrastructure (PKI) which allows for digital certificates.

Symmetric cryptography is a cryptographic system that uses the same key for encryption and decryption. A hash function is cryptography that only encrypts one way, such that the plaintext cannot be derived from the ciphertext. Zero-knowledge proofs are cryptographic systems that allow one party to prove they know a piece of information without revealing the information itself.

79.

A user wants to install a new application on their system to increase their productivity. However, their workstation has a policy that blocks all programs except for a few that it permits.

What type of solution is the company using to protect their workstations?

Allow list

Block list

Quarantine

Isolation

Correct answer: Allow list

An application allow list/approved list specifies the applications that are permitted to run on an endpoint. These lists must be kept up to date as the organization uses new applications and can cause issues if a legitimate application is excluded from the list.

An application block list/deny list specifies the applications that are not permitted to run on an endpoint. These lists can be difficult to keep up to date as cybercriminals evolve their malware. For example, blocklists are less effective against zero-day threats and polymorphic malware. Endpoint security solutions commonly have quarantine functionality to prevent suspicious, malicious, or infected files from causing damage to an endpoint. Isolation refers to disconnecting a system from the network rather than managing the risk posed by a particular application.

80.

Which of the following security solutions is recommended for confirming that a file has not been modified by an attacker?

Hashing

Salting

Normalization

Tokenization

Correct answer: Hashing

Hashing uses an algorithm to perform an irreversible operation on data, replacing it with a fixed-size hash. The original data can't be retrieved from the hash, but it is possible to verify that another piece of data matches the original data by comparing their hashes.

Salting adds a random, unique value to data before it is hashed, ensuring that identical inputs produce different hashes. This is recommended for password storage and protects against rainbow tables. Normalization is when databases are broken up into multiple tables to reduce the level of redundancy. Tokenization replaces sensitive data in a database with a non-sensitive token. The mapping of tokens to data is stored securely elsewhere and can be used to look up the sensitive data if needed,

81.

A company wants to prevent employees from making changes to systems that can have unintended consequences. What is one example of an activity that should be restricted for desktop users?

Unauthorized software installations

Multi-factor authentication

System restarts

Application restarts

Correct answer: Unauthorized software installations

Unauthorized software installations can lead to unintended consequences to a system. A change management process can help ensure that any changes to a system are thoroughly tested before implementation.

Multi-factor authentication is a best practice for securing logins. Desktop users should be able to restart their own systems and applications without affecting the rest of the network.

82.

The algorithms PBKDF2 and Bcrypt are related to which of the following?

Key stretching

Ephemeral keys

Perfect forward secrecy

Salting

Correct answer: Key stretching

Key stretching, or key strengthening, uses PBKDF2, Bcrypt, or similar key derivation algorithms to turn a weak password into a stronger encryption key.

An ephemeral key is used to encrypt a single message, protecting against brute force key guessing attacks. Perfect forward secrecy is when an algorithm generates ephemeral keys for each communication session. Salting involves adding a random, unique, public value to a password before hashing it for storage. This protects against rainbow table attacks and makes it harder for an attacker to identify accounts with weak or reused passwords.

83.

The administrator of an employee database only wants to encrypt the information of senior-level employees. What type of encryption should they use to target this?

Record-level

Column-level

Database-level

Partition-level

Correct answer: Record-level

In an employee database, each employee is represented by a row. Record-level encryption will encrypt single rows of a database.

Column-level encryption will encrypt entire columns of data in a database, such as employee IDs of all employees. Database-level encryption targets an entire database. Partition-level encryption encrypts an entire partition of a drive.

84.

An IT consultant is reviewing a small business's infrastructure and environment. They discover that the organization is using a powerful workstation as a server and user device. The system runs Windows 10 for user interaction and has hypervisor software that is running several servers.

Which type of hypervisor is being used in this situation?

- **Hosted**
- Bare metal
- Physical
- Type I

Correct answer: Hosted

A hosted hypervisor runs "on top" of an operating system. This makes it dependent on the operating system, and the hypervisor cannot directly access the machine's hardware. Examples of hosted hypervisors include Microsoft Virtual PC, Windows Virtual PC (for Windows 7), Hyper-V (Windows 8 and 10), and VMware Workstation.

Bare metal, or type I, hypervisors run directly on the physical hardware without needing an operating system.

85.

Which category of security control is a firewall?

- **Technical**
- Managerial
- Administrative
- Operational

Correct answer: Technical

Security controls can be classified into four categories, including:

- ***Managerial**: Managerial/administrative controls are policies, procedures, or guidelines. An organization's managerial controls are developed first and used as the basis for designing and implementing other security controls.*
- ***Operational**: Operational controls help an organization maintain normal operations. Backups or a policy stating that a system should be regularly reset are examples of operational controls.*
- ***Technical**: Technical/logical controls implement access management for a particular resource. Firewalls, passwords, encryption, and group policies are all examples of technical controls.*
- ***Physical**: Physical controls help to manage or prevent physical access to an organization's building, systems, etc. Fences, locked doors, etc. are examples of physical controls.*

86.

When a company implements volume-level encryption, what type of data are they encrypting?

- **Data at rest**
- Data in transit
- Data in use
- Data in communication

Correct answer: Data at rest

Volume-level encryption refers to data that is encrypted on a volume of a hard drive. Data at rest is data that is being stored.

Data in transit, or communication, is data that is being sent across a network or between two systems. Data in use is data in active memory or on a computer screen.

87.

Which concept ensures that CAs can be the basis for authenticity and integrity?

Root of trust

Federation

Public ledger

Secure enclave

Correct answer: Root of trust

Certificate authorities (CAs) use a hierarchical structure, with the root CA taken offline unless needed. The top-most CA needs to be secured in order for all subordinate CAs to be trusted.

A federation allows users to access multiple systems with a single set of credentials. A public ledger is a distributed list secured by a blockchain consensus mechanism. A secure enclave is a secure execution environment on Apple devices.

88.

A company changes to a new software application for processing invoices. However, the company fails to install necessary libraries that the new application needs, which causes systems to crash.

Which technical implication of making changes did the company fail to account for?

Dependencies

Allow lists

Service restarts

Legacy applications

Correct answer: Dependencies

Some applications or services have other dependencies that they rely on. If those dependencies are not present, it can cause the system to fail.

Allow lists create an issue if a needed application is not included in it. Service restarts can be an issue if vulnerabilities appear while the system is being restarted. Legacy applications cause an issue if they are no longer supported.

89.

When a secure hashing algorithm is included with a system that offers non-repudiation, what can be implemented?

Digital signatures

Steganography

Tokenization

Open public ledgers

Correct answer: Digital signatures

On their own, hashing functions do not offer non-repudiation, so they cannot guarantee that a message originated from the claimed sender. When hashing is combined with public key cryptography, it can then offer non-repudiation and be used for digital signatures.

Steganography is used to hide messages in other media. Tokenization is used to replace sensitive data with tokens. An open public ledger is used to keep track of transactions.

90.

Which of the following is focused on database efficiency, not security?

- **Normalization**
- Tokenization
- Hashing
- Salting

Correct answer: Normalization

Normalization is when databases are broken up into multiple tables to reduce the level of redundancy.

Tokenization replaces sensitive data in a database with a non-sensitive token. The mapping of tokens to data is stored securely elsewhere and can be used to look up the sensitive data if needed. Hashing performs an irreversible operation on data, replacing it with a fixed-size hash. The original data can't be retrieved, but it is possible to verify that another piece of data matches the original data by comparing their hashes. Salting adds a random, unique value to data before it is hashed, ensuring that identical inputs produce different hashes. This is recommended for password storage and protects against rainbow tables.

91.

Why is ownership important in the change management process?

To ensure that someone is responsible for the project being carried out effectively

To verify that the planned project will meet the business goals of the organization

To analyze all the impacts that a change will have on other systems

To carry out operations to restore a system to its previous state in case there is an issue with the change

---

Correct answer: To ensure that someone is responsible for the project being carried out effectively

Giving ownership to an individual for a change ensures that someone will take responsibility for it. The individual in charge is typically a CISO.

Verifying that the planned project will meet the business goals of the organization is accomplished in the approval process. Analyzing all the impacts that a change will have on other systems is done during the impact analysis. Carrying out operations to restore a system to its previous state in case there is an issue with the change is the role of a backout plan.

92.

An application at Smith Industries is built on older encryption algorithms, and it is taking more time than expected to come up with a replacement. The security engineers want to enhance the security of the encryption without changing the programming much.

What technique can they use to turn their weak keys into enhanced, more powerful keys?

Key stretching

Data masking

Steganography

Tokenization

Correct answer: Key stretching

Key stretching is a technique that processes a weak key and outputs an enhanced and more powerful key. It increases the key size to 128 bits, which makes it much stronger against brute force attacks. Increasing the key length can help ward off brute force and rainbow table attacks. Essentially, the key stretching techniques salt the passwords with additional random bits to make them even more complex.

Data masking is the process of protecting sensitive information by replacing the data with fake values. Steganography is concealing information in an alternate medium, such as image files. Tokenization involves substituting sensitive data with tokens.

93.

An administrator wants to create a fake network designed to lure in potential hackers. This will allow them to get alerted to an intruder and study the behavior of how they move between systems.

What term describes what the administrator is creating?

- **Honeynet**
- Honeypot
- Honeyfile
- Honeytoken

Correct answer: Honeynet

A honeynet is an entire network designed to catch potential threat actors. They allow a researcher to study how an attacker moves around a network.

A honeypot is a single system. A honeyfile is just a file designed to alert an administrator when it is accessed. A honeytoken is data that is attractive to attackers and can be tracked by researchers.

94.

An organization has decided to install a fence to help prevent unauthorized individuals from entering the organization's premises. What category of control is this an example of?

Physical

Operational

Technical

Managerial

Correct answer: Physical

A fence is an example of a physical security control. Other examples of physical controls include locks and security guards.

Operational controls include log monitoring and vulnerability management. Technical controls include firewalls and access control lists. Managerial controls include risk assessments and change management procedures.

95.

Which of the following is recommended for password storage to protect against rainbow table attacks?

Salting

Hashing

Tokenization

Normalization

Correct answer: Salting

Salting adds a random, unique value to data before it is hashed, ensuring that identical inputs produce different hashes. This is recommended for password storage and protects against rainbow tables.

Hashing performs an irreversible operation on data, replacing it with a fixed-size hash. The original data can't be retrieved, but it is possible to verify that another piece of data matches the original data by comparing their hashes. Tokenization replaces sensitive data in a database with a non-sensitive token. The mapping of tokens to data is stored securely elsewhere and can be used to look up the sensitive data if needed. Normalization is when databases are broken up into multiple tables to reduce the level of redundancy.

96.

Which of the following forms of data protection is MOST commonly used to protect credit card data on receipts, websites, etc.?

Masking

Encryption

Tokenization

Rights management

Correct answer: Masking

Some commonly-used data protection solutions include:

- *Masking, which replaces sensitive data with an asterisk or similar character. For example, all but the last four digits of credit card numbers are often masked on receipts, websites, etc.*
- *Encryption, which scrambles data in a way that makes it unreadable and unusable without knowledge of the decryption key.*
- *Tokenization, which replaces sensitive data with a non-sensitive token. A lookup table maps the token to the sensitive data for retrieval when needed.*
- *Rights management, which places security controls in place to prevent data loss. For example, an email may disallow forwarding or screenshots, and copy-paste may be disabled when a device is showing sensitive information.*

97.

A security testing group is interested in analyzing current threats and trends in the digital landscape. They want to attract and trap potential attackers in order to learn about and counteract hacking attempts.

What type of technology should they use for this?

Honeypot

Firewall

Proxy

Rootkit

Correct answer: Honeypot

A honeypot attracts the hacker away from the real network to isolate them in a monitored area. It contains dummy resources and data to look like it's of value to the attacker. The attacker's methods are then analyzed and studied to improve security overall. Honeypots are capable of catching threats because they present an attractive target for attackers; they entice hackers to try any methods they have to gain access to the target.

A firewall allows or denies traffic based on a ruleset. A proxy handles requests between a client and server. A rootkit is a tool that an attacker uses to get administrative access to a system.

98.

Which encryption algorithm was proposed by the U.S. government in 1977 but is no longer considered secure?

DES

AES

MD5

SHA

Correct answer: DES

The Data Encryption Standard (DES) is an outdated cryptosystem that was once used for secure government communications. 3DES, one if its common variants, is also now considered insecure.

Advanced Encryption Standard (AES) was developed to replace DES. MD5 was released in 1991 and is not recommended due to vulnerabilities. SHA is a suite of hashing functions that is still used today.

99.

What physical control can be added to a building's parking lot and other dark areas to make them feel more secure?

Lighting

Bollards

Sensors: ultrasonic

Access badges

Correct answer: Lighting

Good lighting can deter intruders into an area, which will increase feelings of safety.

Bollards are used to prevent vehicles from entering an area. Ultrasonic sensors are primarily used for proximity detection. Access badges are used to authenticate users for entering a building.

100.

You are working with the security team to implement proper security controls. One of the systems has an operating system that is no longer supported. However, it can't be upgraded to a new operating system due to the antiquated software in use. In order to address this issue, the security team has chosen to simply isolate the system by removing it from the network.

Which type of security control is being implemented?

- **Compensating**
- Corrective
- Detective
- Deterrent

Correct answer: Compensating

A compensating control does not apply directly to the vulnerable system, but can help offset (or compensate for) the lack of a direct control. In this scenario, a direct control would be to update the operating system to a supported version. Since this is not possible, the security team has simply isolated the system from the rest of the network to compensate for the direct fix.

Corrective controls fix issues that have already occurred. Detective controls identify issues that have occurred. Deterrent controls try to prevent a threat actor from even attempting to make a security issue.