CERTSHOP

CompTIA® Security+ (SY0-601) - Quiz Questions with Answers

1.0 General Security Concepts

1.

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.

2.

A new web application is being developed for Acme Inc.'s customers. The executives are concerned that there might be vulnerabilities in the entry fields and other areas, so they want to perform testing.

Which type of testing sends random data to an application to test for vulnerabilities?

- **Fuzz testing**
- Stress testing
- Static analysis
- Load testing

Correct answer: Fuzz testing

Fuzz testing (also referred to as fuzzing) sends random data to a website to test for vulnerabilities. This type of testing is done without knowing the source code of the application.

Stress testing involves sending large amounts of traffic to a service until it fails. Static analysis involves examining source code. Load testing involves seeing how an application behaves at different load levels.

3.

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.

4.

A security administrator at Acme Inc. is auditing and, if necessary, implementing various controls around the organization. They have reviewed the encryption, antivirus software, intrusion detection and prevention systems and firewalls, and have audited user permissions.

Which of the following control categories is this administrator auditing?

- **Technical**
- Operational
- Managerial
- Physical

Correct answer: Technical

Technical controls use technology to close gaps and reduce vulnerabilities in an organization. An administrator installs and configures the technical controls, after which the technical controls operate autonomously to protect and secure the systems.

Operational controls include log monitoring and vulnerability management. Managerial controls include risk assessments and change management procedures. Physical controls help to manage or prevent physical access to an organization's building, systems, etc.

5.

Which type of certificate is created and used by a root CA?

- **Self-signed**
- Third-party
- EV
- Wildcard

Correct answer: Self-signed

A root certificate authority (CA) needs to create its own certificate and sign it itself. All other systems will get their certificate from the root CA.

Third-parties do not sign a root CA. An Extended Validation (EV) certificate is signed by a CA to verify the identity of owners of issued certificates. A wildcard certificate is a certificate valid for any subdomains.

6.

An administrator is working at a growing organization. The owner approaches the administrator with the concern that new employees may not want to follow the rules and could potentially install prohibited applications such as music streaming or file-sharing software.

What can the administrator use to specify specific programs that should NOT be installed on workstations?

Block list

Allow list

Quarantines

URL filtering

Correct answer: Block list

Application block listing specifically blocks certain applications from being installed. For instance, if an administrator found that Skype was causing a problem with data leakage, they could specifically block it from being installed on any machine.

An allow list specifically allows certain programs to be installed, which can be easier to maintain than a block list. A quarantine is an area where programs can be isolated from a system or network. URL filtering is used to prevent access to certain websites.

7.

Which of the following is a widely accepted international public key infrastructure (PKI) standard to verify that a public key is matched to the user, host, or application that is contained within the certificate?

X.509

X.500

X.25

X.700

Correct answer: X.509

Most certificates are based on the X.509 standard, which is the common PKI standard developed by the ITU-T that often incorporates the single sign-on authentication method. An X.509 certificate contains information regarding the identity of the recipient. Standard information in an X.509 certificate would be as follows:

- *Version*
- *Serial number*
- *Algorithm information*
- *Issuer name*
- *Length of certificate validity*
- *Name of the identity the certificate is issued to*
- *Public key*
- *Extensions (optional)*

X.500 standards relate to directory services. The X.25 standard relates to packet switching. X.700 protocols relate to OSI for communications.

8.

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.*

9.

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.*

10.

Which type of encryption targets an entire database?

- **TDE**
- CLE
- Volume encryption
- Partition-level encryption

Correct answer: TDE

Database encryption typically encrypts either the entire database or individual columns. Transport data encryption (TDE) is used to encrypt the entire database at the file level.

Column-level encryption (CLE) encrypts specific columns of a database. Volume encryption encrypts an entire logical volume of a drive. Partition-level encryption encrypts an entire partition of a drive.

11.

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.

12.

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.

13.

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.

14.

Which of the following categories of controls is made up of policies, guidelines, and procedures?

Managerial

Operational

Technical

Physical

Correct answer: Managerial

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.*

15.

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.

16.

Which type of security control includes policies and procedures that employees should follow?

- **Directive**
- Deterrent
- Corrective
- Compensating

Correct answer: Directive

Directive controls are used to inform employees about how they can achieve security objectives. Some examples include policies and standard operating procedures.

Deterrent controls try to dissuade an attacker from starting an attack. Corrective controls fix issues that have already occurred. Compensating controls mitigate risks that were introduced due to exceptions that were made.

17.

Which type of sensor detects movement by sensing frequency alterations?

- **Microwave**
- Ultrasonic
- Infrared
- Pressure

Correct answer: Microwave

Microwave sensors emit microwaves and then detect the reflected waves. If the reflected waves have a change in frequency, it indicates that there is movement.

Ultrasonic sensors use sound waves and rely on echoes. Infrared sensors use heat signatures. Pressure sensors detect touches or changes in air pressure.

18.

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.

19.

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.

20.

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.

21.

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.

22.

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.

23.

Which of the following techniques helps to protect against rainbow table attacks?

Salting

Steganography

Tokenization

Hashing

Correct answer: Salting

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.

Steganography involves hiding messages in other media, such as images. Tokenization involves protecting sensitive data by replacing it with placeholder data. Hashing involves a one-way function of turning a message of any length into a fixed-length value.

24.

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.

25.

An administrator wants to ensure that a file is not tampered with. To do so, they use a function that takes the file as input and creates a unique, repeatable output from it. If the file is subsequently changed, then the function's output would also change from the original.

What is this an example of?

- **Hashing**
- Salting
- Tokenization
- Data masking

Correct answer: Hashing

A hash function is a mathematical procedure that converts a variable-sized amount of data into a smaller block of data. It's designed to take an arbitrary data block from a file or message, use it as input, and, from that block, produce a fixed hash value that can be verified by the recipient.

Salting is the process of making a password more secure by adding random characters. Tokenization involves replacing real data with placeholder data that can be retrieved later. Data masking involves hiding sensitive data with fake data.

26.

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.

27.

Which technical implication of a failed change management process can result in a large revenue loss due to a system remaining offline?

Downtime

Service restart

Application restart

Dependencies

Correct answer: Downtime

Downtime refers to the time when a system is offline due to technical difficulties. This has the greatest effect on revenue loss if an organization does not have a business continuity plan in place.

Service and application restarts represent a potential vulnerability as security controls may not all be brought online at the same time. Dependencies occur when one system requires another system in order to operate.

28.

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.

29.

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.

30.

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.

31.

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.

32.

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.

33.

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.

34.

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.

35.

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.

36.

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.

37.

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.

38.

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.

39.

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.

40.

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.

41.

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.

42.

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.

43.

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.

44.

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.

45.

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*

46.

An online retailer wants their customers to be assured that they are securely communicating with the company's trusted web servers. What type of organization can they contact to help them with this?

Certificate authority

ISO

IANA

Directory service

Correct answer: Certificate authority

A certificate authority proves the identity of an organization so they can be issued a digital certificate used for securing communications. Users can verify the certificate from the CA by using the CA's public key.

The International Organization for Standardization (ISO) sets standards in various industries. The Internet Assigned Numbers Authority (IANA) allocates IP addresses to organizations. A directory service is used to organize such things as users, network resources, and data on a network.

47.

What technical implication can occur when system changes involve service restarts?

Lapses in security during the restart process

Lack of backup data if the system does not restart correctly

Additional software automatically added to deny lists after restart

End of support for outdated applications after restart

Correct answer: Lapses in security during the restart process

When a system is restarted, not all security processes may come online at the same time. This can allow an attacker to take advantage of temporary holes in security during the restart.

Lack of backup data if the system does not come back online is an issue regarding having backup files. Additional software automatically added to deny lists is not a result of system restarts. End of support for outdated applications is an issue with legacy applications.

48.

Which of the following is a chip built into a computer that provides secure storage for cryptographic keys?

TPM

Password key

Password vault

HSM

Correct answer: TPM

A Trusted Platform Module (TPM) is an embedded chip on a computer that can securely store encryption keys, credentials, and other sensitive cryptographic data.

A password key is a password, i.e., a secret that is used to access an app, website, or computer. A password vault, or password manager, such as LastPass or 1Password, is an encrypted vault of a user's passwords that is unlocked with a master password. A hardware security module (HSM) performs the same function as a TPM but typically isn't built into the system. It might be a card, an external device, or a cloud-based service.

49.

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.

50.

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.

51.

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.*

52.

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.*

53.

Which statement accurately describes a requirement for cryptographic hash functions?

A hash function should be free of collisions to be considered secure

A hash function is two-way, so the input can be inferred from the output

A hash function takes a fixed-length input and creates a variable-length output

A hash value should be resource-intensive to compute

Correct answer: A hash function should be free of collisions to be considered secure

Hash functions need to avoid collisions to be considered secure. A collision occurs when two different inputs create the same hash.

A hash function should be a one-way operation. A hash function takes a variable-length input and creates a fixed-length output. A hash value should be relatively easy to compute.

54.

Security guards and fences are an example of which of the following categories of security controls?

Physical

Operational

Technical

Managerial

Correct answer: 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.

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

55.

Certificates require a neutral third party to act as a trusted entity to establish trust and issue certificates. This element is critical to public key infrastructure (PKI) because they issue the SSL certificates that web browsers use to authenticate content sent from web servers.

What is the entity that issues these certificates to users?

CA

RA

KDC

SOC

Correct answer: CA

A certificate authority (CA) is the entity (usually a server) that issues certificates to users. In a PKI system, the CA is known as a trusted third party. The internet's PKI systems use a CA as a trusted entity for the certificates to authenticate individuals and servers. These certificates will hold data about the entity that issued the certificate along with cryptographic data necessary to verify the identity of the entity linked to the digital certificate.

A registration authority (RA) assists by verifying applicants' identity. A key distribution center (KDC) is used with Kerberos for authentication between clients and services. A security operations center (SOC) is a centralized unit in an organization responsible for security.

56.

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.

57.

Which of the following is a key stretching algorithm?

- **PBKDF2**
- AES
- Blowfish
- DES

Correct answer: PBKDF2

Password-Based Key Derivation Function 2 (PBKDF2) is a salting technique that incorporates a pseudo-random function to protect passwords. PBKDF2 is in use in many applications, such as Wi-Fi Protected Access II (WPA2), Apple's iOS mobile operating system, and Cisco operating systems.

AES and DES are used for symmetric key encryption. Blowfish is used for symmetric key block ciphers.

58.

While performing an audit, a security analyst reviews the control types incorporated at Acme Inc. They look at security elements that include fences, warning signs, security guards, mantraps, CCTV, and lighting.

These are all examples of which of the following control types?

Physical

Technical

Operational

Managerial

Correct answer: Physical

Physical controls are those that can be physically touched. Items such as fences, guard posts, mantraps, lighting, and signs are all included in the physical control category. Some physical controls are also technical controls, such as CCTV and fire extinguishers, because you can touch them, but you use technology to facilitate their function.

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

59.

A company's web server is being slowed down by having to perform cryptographic processes. An administrator would like to offload the cryptographic processing to a dedicated system to improve performance.

What type of solution should they implement for this?

HSM

TPM

Password vault

Password key

Correct answer: HSM

A hardware security module (HSM) performs the same function as a TPM but typically isn't built into the system. It might be a card, an external device, or a cloud-based service.

A password key is a password, i.e., a secret that is used to access an app, website, or computer. A password vault or password manager such as LastPass or 1Password is an encrypted vault of a user's passwords that is unlocked with a master password. A Trusted Platform Module (TPM) is an embedded chip on a computer that can securely store encryption keys, credentials, and other sensitive cryptographic data.

60.

Data backups are an example of which of the following types of security controls?

Operational

Managerial

Technical

Physical

Correct answer: Operational

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 impact the physical world. Locks, fences, security cameras, and perimeter lighting are examples of physical controls.*

61.

A security administrator is evaluating the configuration of controls in the organization. They are currently looking at controls that run on the server hardware to ensure encryption is present, controls that periodically scan for viruses, and controls that prevent intrusions.

These are all examples of which of the following categories of controls?

Technical controls

Administrative controls

Physical controls

Deterministic goals

Correct answer: Technical controls

Technical controls use technology to reduce the chance of vulnerabilities in a given system. The administrator installs the control on the system and configures it to provide protection automatically. Items such as encryption, antivirus software, and intrusion detection systems would all be classified as technical controls.

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. Physical controls help to manage or prevent physical access to an organization's building or systems. Fences, locked doors, etc. are examples of physical controls.

62.

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.

63.

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.

64.

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.

65.

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.*

66.

An administrator has a dual-boot system with Windows and Linux installed on a single disk. They want to encrypt the entire Linux portion of the disk but do not need Windows to be encrypted.

Which encryption level for data at rest should they use in this situation?

Partition

Full-disk

File

Volume

Correct answer: Partition

The disk partition with Linux can be encrypted while leaving the partition with Windows unencrypted. This can encrypt everything in Linux without needing to worry about volume or file-level encryption.

Full-disk encryption will encrypt all data on a hard drive. File-level encryption is used to encrypt single files. Volume-level encryption lies between file- and partition-level encryption.

67.

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.

68.

A security administrator is reviewing various controls at Smith Industries to ensure that the organization is adequately protected. They have finished reviewing the hardening of the business systems, the usage of security training and awareness, and the presence of security guards in the appropriate locations.

Which of the following control types is being reviewed?

Preventive

Detective

Corrective

Compensating

Correct answer: Preventive

Security controls that prevent incidents and security events are called preventive controls. The hardening of a business system prevents exploitation of the system through known methods and makes it more difficult for an attacker. Security training prevents social engineering attacks, such as phishing, by increasing employee awareness and knowledge.

Detective controls identify events before they occur. Corrective controls remediate events after they have occurred. Compensating controls mitigate risks that cannot be controlled through primary measures.

69.

After installing a new security update, a system continually shuts down. When following a change management procedure, what should be implemented to restore the system to its previous state?

Backout plan

Test results

Standard operating procedures

Impact analysis

Correct answer: Backout plan

A backout plan is an important part of the change management process because there is always the possibility that things do not go according to plan. This will restore the system to its previous state before it was changed.

Test results are used to check changes before they are implemented. Standard operating procedures are used to inform users on how to operate systems on a day-to-day basis. An impact analysis is used to study how a change will affect other systems.

70.

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.

71.

What type of control is a locked door to a server room?

Preventive

Directive

Corrective

Compensating

Correct answer: Preventive

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

- ***Preventive**: Preventive 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 inform users how they can be more secure. This can include policies and procedures.*

72.

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.

73.

Which of the following is a symmetric encryption standard that is commonly used with TLS?

- **AES**
- RSA
- Elliptic curve
- SHA

Correct answer: AES

The Advanced Encryption Standard (AES) is a symmetric cipher with key strengths of 128, 192, and 256 bits. It is commonly used in wireless security, TLS, and file/disk encryption.

RSA and elliptic curve are asymmetric cryptosystems. SHA is a hashing function.

74.

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.

75.

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.

76.

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.

77.

An administrator has discovered that a critical business function is using FTP, which is presenting a security risk due to the plaintext credentials being sent over the network. They want to implement a secure protocol that uses TLS to transmit the data to take advantage of the preexisting security infrastructure.

Which of the following protocols should the administrator use?

- **FTPS**
- HTTP
- SMTP
- SNMP

Correct answer: FTPS

FTP Secure (FTPS) is an extension of FTP and uses TLS to encrypt FTP traffic.

HTTP is used to send unencrypted web traffic. SMTP is used to send email traffic. SNMP is for sending network management messages.

78.

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.

79.

Which phrase BEST describes a zero trust cybersecurity model?

Never trust, always verify

Moat and castle

Defense-in-depth

Good fences make good neighbors

Correct answer: Never trust, always verify

In a zero trust cybersecurity model, there is no inherent trust for local devices. All devices need to be continually validated.

The other answer choices are principles of cybersecurity models that focus on strong perimeters.

80.

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.

81.

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.

82.

Which technology uses an open public ledger that uses a consensus mechanism to ensure integrity?

Blockchain

Key stretching

Digital certificates

Steganography

Correct answer: Blockchain

A blockchain is a decentralized and distributed ledger technology that keeps track of all transactions in blocks. Each block is secured cryptographically to prevent tampering, and various blockchains use different consensus mechanisms to agree on how transactions should be validated and secured.

Key stretching is used to make short passwords into longer ones. Digital certificates are public keys used to encrypt communications and for proving authenticity. Steganography involves hiding information in another type of media, such as images.

83.

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.

84.

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.

85.

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.

86.

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.

87.

A website developer is creating a new site for the Acme organization so that they can process customer invoices with greater ease. The system will have usernames and passwords for the employees. The developer wants to ensure that the passwords would not be vulnerable to cracking if they were stolen from the server by an attacker.

Which of the following should they use to increase the difficulty of cracking a password hash?

- **Salt**
- Rainbow table
- Token
- Rootkit

Correct answer: Salt

A password salt is a random set of data that is added to a password hash to make an attacker's attempt to decrypt the data much more difficult. It can add additional characters to the password to make it longer, and the system keeps track of which characters were added and removes them before decrypting the hash.

A rainbow table is a table of pre-computed hashes for passwords. A token is used to obfuscate data. A rootkit is malicious software that gives administrative access to a system.

88.

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.*

89.

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.

90.

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.

91.

Which type of security control is used to prevent vehicles from entering a certain area?

- **Bollards**
- Access control vestibules
- Access badges
- Video surveillance

Correct answer: Bollards

Bollards can be posts, pillars, or planters that are placed around an area to keep vehicles from entering. They are sometimes designed to be movable or raised/lowered when needed.

An access control vestibule is used to allow only one person at a time to pass through a control point. Access badges are used to authenticate users for entrance to an area. Video surveillance is used to monitor an area in real time and keep a record of events.

92.

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.

93.

What is a digitally signed electronic document that binds a public key with a user identity?

- **Certificate**
- Blockchain
- Zero-day
- Keylogger

Correct answer: Certificate

Certificates are digitally signed electronic documents that bind a public key with a user identity. The identity information might include a person's name and organization or other relevant details. Certificates have several common elements, such as serial number, issuer, validity date, subject, public key, and appropriate usage for the certificate.

A blockchain is used to record transactions. A zero-day is an exploit that has not been patched by a vendor. A keylogger is a device or software that records a user's keystrokes.

94.

Which part of change management involves ensuring that a project is aligned with an organization's goals?

Approval process

Backout plan

Impact analysis

Maintenance window

Correct answer: Approval process

The approval process for a change is the first part of change management. Before a change is made, it must be approved by stakeholders who agree that it aligns with the core business.

A backout plan is used to revert a system to its previous state in case there is a problem with the change. An impact analysis involves examining how a change will impact other systems. A maintenance window is a scheduled downtime for fixing things.

95.

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.

96.

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.

97.

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.

98.

Key stretching is a technique used to enhance the security of stored passwords. There are various common key stretching techniques that incorporate different methods to make a password more secure.

Which of the following is based on the Blowfish block cipher and salts the password before doing multiple rounds of hashing?

- **Bcrypt**
- PBKDF2
- Argon2
- HKDF

Correct answer: Bcrypt

Based on the Blowfish block cipher, Bcrypt salts the password by adding additional random bits throughout the hash before it is hashed with the Blowfish algorithm. It can even perform this process multiple times to further protect the system. It is used in many Unix and Linux distributions to protect the passwords in the shadow password file.

PBKDF2 applies a pseudorandom function multiple times to the input password. Argon2 uses memory costs to tune key stretching to make passwords harder to crack. HKDF repeats the extraction and expansion steps multiple times.

99.

Which component in a zero trust cybersecurity model notifies policy enforcement points about decisions regarding access to network resources?

Policy administrator

Subject

Data plane

Policy engine

Correct answer: Policy administrator

The policy administrator communicates with policy enforcement points after consulting the policy engine to determine if access to resources should be granted or not. Policy administrators and policy engines are in the control plane, while policy enforcement points are in the data plane.

A subject is the entity that makes the access request. The data plane is the area where data is passed through. The policy engine is the component that makes the decisions.