SY0-401.exam.1068q

Number: SY0-401
Passing Score: 800
Time Limit: 120 min
File Version: 1

Comptia SY0-401

CompTIA Security+ Certification

Sections

1. Network Security
2. Compliance and Operational Security
3. Threats and Vulnerabilities
4. Application, Data and Host Security
5. Access Control and Identity Management
6. Cryptography
7. Mixed Questions

Exam A

QUESTION 1
Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

A. Hashing
B. Stream ciphers
C. Steganography
D. Block ciphers

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way – it is not reversible.

QUESTION 2
A software developer wants to prevent stored passwords from being easily decrypted. When the password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as:

A. Symmetric cryptography.
B. Private key cryptography.
C. Salting.
D. Rainbow tables.

Correct Answer: C
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Salting can be used to strengthen the hashing when the passwords were encrypted. Though hashing is a one-way algorithm, it does not mean that it cannot be hacked. One method to hack a hash is though rainbow tables and salt is the counter measure to rainbow tables. With salt a password that you typed in and that has been encrypted with a hash will yield a letter combination other than what you actually type in when it is rainbow table attacked.

QUESTION 3
Which of the following concepts describes the use of a one-way transformation in order to validate the integrity of a program?

A. Hashing
B. Key escrow
C. Non-repudiation
D. Steganography

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:
It must be one-way – it is not reversible.
Variable-length input produces fixed-length output – whether you have two characters or 2 million, the hash size is the same.
The algorithm must have few or no collisions – in hashing two different inputs does not give the same output.

QUESTION 4
The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

A. TwoFish
B. SHA-512
C. Fuzzy hashes
D. HMAC

Correct Answer: C
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Hashing is used to ensure that a message has not been altered. It can be useful for positively identifying malware when a suspected file has the same hash value as a known piece of malware. However, modifying a single bit of a malicious file will alter its hash value. To counter this, a continuous stream of hash values is generated for rolling block of code. This can be used to determine the similarity between a suspected file and known pieces of malware.

QUESTION 5
An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-to-peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

A. A full scan must be run on the network after the DAT file is installed.
B. The signatures must have a hash value equal to what is displayed on the vendor site.
C. The definition file must be updated within seven days.
D. All users must be logged off of the network prior to the installation of the definition file.

Correct Answer: B
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

A hash value can be used to uniquely identify secret information. This requires that the hash function is collision resistant, which means that it is very hard to find data that generate the same hash value and thus it means that in hashing two different inputs will not yield the same output. Thus, the hash value must be equal to that displayed on the vendor site.

QUESTION 6
Which of the following would a security administrator use to verify the integrity of a file?

A. Time stamp
B. MAC times
C. File descriptor
D. Hash

Correct Answer: D
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and it is a one-way transformation in order to validate the integrity of data.

QUESTION 7
Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

A. Confidentiality
B. Compliance
C. Integrity
D. Availability

Correct Answer: C
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Integrity means the message can't be altered without detection.

QUESTION 8
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

A. SHA1
B. MD2
C. MD4
D. MD5

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA (1 or 2) is preferred over Message Digest Algorithm.

QUESTION 9
Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

A. Steganography
B. Hashing
C. Encryption
D. Digital Signatures

Correct Answer: D
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

QUESTION 10
An email client says a digital signature is invalid and the sender cannot be verified.

Which of the following concepts is the recipient concerned with?

A. Integrity
B. Availability
C. Confidentiality
D. Remediation

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Digital Signatures is used to validate the integrity of the message and the sender. Integrity means the message can't be altered without detection.

QUESTION 11
A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

A. Integrity of downloaded software.
B. Availability of the FTP site.
C. Confidentiality of downloaded software.
D. Integrity of the server logs.

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

QUESTION 12
It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission.

Which of the following types of security control are they concerned about?

A. Integrity
B. Safety
C. Availability
D. Confidentiality

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Integrity means that the messages/ data is not altered. PII is personally identifiable information that can be used to uniquely identify an individual. PII can be used to ensure the integrity of data/messages.

QUESTION 13
Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit.

Which of the following concepts relates this concern to?

A. Availability
B. Integrity
C. Accounting
D. Confidentiality

Correct Answer: B
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring nonrepudiation via digital signatures supports integrity.

QUESTION 14
Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

A. Recipient's private key
B. Sender's public key
C. Recipient's public key
D. Sender's private key

Correct Answer: B
Section: Compliance and Operational Security
Explanation

Explanation/Reference:

Explanation:

When the sender wants to send a message to the receiver, it's important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus, the recipient uses the sender's public key to verify the sender's identity.

QUESTION 15
Digital signatures are used for ensuring which of the following items? (Choose two.)

A. Confidentiality
B. Integrity
C. Non-Repudiation
D. Availability
E. Algorithm strength

Correct Answer: BC
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system. Thus non-repudiation also impacts on integrity.

QUESTION 16
Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Choose two.)

A. The CA's public key
B. Ann's public key
C. Joe's private key
D. Ann's private key
E. The CA's private key
F. Joe's public key

Correct Answer: DF
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If

the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be.

QUESTION 17
Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Choose two.)

A. The CA's public key
B. Joe's private key
C. Ann's public key
D. The CA's private key
E. Joe's public key
F. Ann's private key

Correct Answer: AE
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus, Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. This process provides message integrity, nonrepudiation, and authentication.
A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual. If Joe wants to send Ann an encrypted e-mail, there should be a mechanism to verify to Ann that the message received from Mike is really from Joe. If a third party (the CA) vouches for Joe and Ann trusts that third party, Ann can assume that the message is authentic because the third party says so.

QUESTION 18
A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform?

A. Remove all previous smart card certificates from the local certificate store.
B. Publish the new certificates to the global address list.
C. Make the certificates available to the operating system.
D. Recover the previous smart card certificates.

Correct Answer: B
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

CAs can be either private or public, with VeriSign being one of the best known of the public variety. Many operating system providers allow their systems to be configured as CA systems. These CA systems can be used to generate internal certificates that are used within a business or in large external settings. The process provides certificates to the users. Since the user in question has been re-issued a smart card, the user must receive a new certificate by the CA to allow the user to send digitally signed email. This is achieved by

publishing the new certificates to the global address list.

QUESTION 19
Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
B. The website is using a wildcard certificate issued for the company's domain.
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self-signed certificate.

Correct Answer: C
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. In typical public key infrastructure (PKI) arrangements, a digital signature from a certificate authority (CA) attests that a particular public key certificate is valid (i.e., contains correct information). Users, or their software on their behalf, check that the private key used to sign some certificate matches the public key in the CA's certificate. Since CA certificates are often signed by other, "higher-ranking," CAs, there must necessarily be a highest CA, which provides the ultimate in attestation authority in that particular PKI scheme.
Localhost is a hostname that means this computer and may be used to access the computer's own network services via its loopback network interface. Using the loopback interface bypasses local network interface hardware. In this case the HTTPS://127.0.01 was used and not HTTPS//localhost

QUESTION 20
Certificates are used for: (Choose two.)

A. Client authentication.
B. WEP encryption.
C. Access control lists.
D. Code signing.
E. Password hashing.

Correct Answer: AD
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication.

QUESTION 21
Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

A. The intermediate CA certificates were not installed on the server.
B. The certificate is not the correct type for a virtual server.
C. The encryption key used in the certificate is too short.

D. The client's browser is trying to negotiate SSL instead of TLS.

Correct Answer: A
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't.

QUESTION 22
Which of the following can be used to ensure digital certificates? (Choose two.)

A. Availability
B. Confidentiality
C. Verification
D. Authorization
E. Non-repudiation

Correct Answer: BE
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. Digital certificates refer to cryptography which is mainly concerned with Confidentiality, Integrity, Authentication, Nonrepudiation and Access Control. Nonrepudiation prevents one party from denying actions they carried out.

QUESTION 23
A certificate used on an e-commerce web server is about to expire.

Which of the following will occur if the certificate is allowed to expire?

A. The certificate will be added to the Certificate Revocation List (CRL).
B. Clients will be notified that the certificate is invalid.
C. The e-commerce site will not function until the certificate is renewed.
D. The e-commerce site will no longer use encryption.

Correct Answer: B
Section: Compliance and Operational Security
Explanation

Explanation/Reference:
Explanation:

A similar process to certificate revocation will occur when a certificate is allowed to expire. Notification will be sent out to clients of the invalid certificate. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known. The owner of a certificate can request that it be revoked at any time, or the administrator can make the request.

QUESTION 24
An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate