GOMYCODE Security+ MCQ - Ch01

anisnasri322@gmail.com Changer de compte

Non partagé

Brouillon enregistré

* Indique une question obligatoire

Name: *

Nasri Anis

Which component of the Zero Trust architecture evaluates access requests against predefined policies to decide whether to grant access? *

- ⦿ Adaptive Identity
- ◯ Policy Enforcement Point (PEP)
- ◯ Policy Administrator
- ◯ Policy Engine

When a system checks a user's permissions to determine which files they are allowed to access, which part of the AAA framework is being exercised? *

- ◯ Authentication
- ◯ Accounting
- ⦿ Authorisation
- ◯ Identification

Which type of encryption is generally faster but faces challenges with safely sharing keys? *

○ Steganography

○ Asymmetric Encryption

◉ Symmetric Encryption

○ Hashing

Why is it important to have a backout procedure during a system change? *

○ To automate the installation process

○ To inform stakeholders of the success

◉ To revert changes if issues occur

○ To define the scope of the change

What is the ultimate outcome of a gap analysis beyond just a report? *

○ A list of terminated employees

○ A signed non-disclosure agreement

◉ A roadmap for security improvement

○ An automated firewall policy

An organisation wants to identify the difference between its current security posture and its desired state. What process should they initiate? *

○ Risk Assessment

◉ Gap Analysis

○ Business Impact Analysis

○ Vulnerability Scan

Which system is used to centralise the management of various keys and automate key rotation? *

○ Online Certificate Status Protocol (OCSP)

◉ Key Management System (KMS)

○ Policy Enforcement Point (PEP)

○ Certificate Authority (CA)

To protect sensitive data and cryptographic operations even if the main CPU is compromised, what dedicated security processor is used? *

○ Secure Enclave

○ Trusted Platform Module

○ Policy Engine

◉ Hardware Security Module

If a web server is decommissioned, what should happen to its digital certificate? *

○ It should be revoked

○ It should be masked

○ It should be escrowed

○ It should be renewed

Which certificate field allows a single certificate to support multiple domains such as a wildcard? *

○ Issuer

○ Signature Algorithm

○ Serial Number

○ Subject Alternative Name (SAN)

Which entity is responsible for assessing the risk, impact, and timing of a proposed change in a formal change management process? *

○ The End-user

○ The Change Control Board (CCB)

○ The Application Owner

○ The Security Guard

?

In the AAA framework, which process is responsible for tracking resource usage, such as login times and data sent? *

○ Authentication

○ Authorisation

◉ Auditing

○ Accounting

What is added to a password before hashing to ensure rainbow table attacks are ineffective? *

○ Digital Signature

◉ Salt

○ Certificate

○ Token

Which of the following is an example of a Managerial Preventive control? *

○ On-boarding policy

○ Security policy training

○ Reviewing login reports

◉ Separation of duties

A security administrator is implementing firewalls and anti-virus software across the organisation's network. Which control category do these implementations fall under? *

- ⦿ Technical Controls
- ○ Physical Controls
- ○ Operational Controls
- ○ Managerial Controls

Which technology provides a hardware-based root of trust for a single device and can store keys for full-disk encryption like BitLocker? *

- ○ HSM
- ○ KMS
- ○ Secure Enclave
- ⦿ TPM

An organisation hires security guards and implements a mandatory security awareness training programme for all employees. What category of security control is being utilised? *

- ○ Technical Controls
- ⦿ Operational Controls
- ○ Physical Controls
- ○ Managerial Controls

In a Zero Trust environment, which plane is responsible for the actual processing * of frames, packets, and network data?

○ Policy Plane

○ Management Plane

○ Control Plane

◉ Data Plane

An organisation is required by management to have a third party hold copies of * their private keys. What is this practice called?

○ Key Revocation

○ Key Stretching

◉ Key Escrow

○ Key Exchange

A network administrator is configuring security zones. Which zone would typically * encompass the public internet?

○ Internal trusted zone

◉ Untrusted zone

○ External zone

○ DMZ zone

An administrator embeds fictitious API credentials in a public cloud share to detect unauthorised access. What is this specific piece of data called? *

○ Honeytoken ●

○ Honeyfile

○ Steganography

○ Honeynet

What is the main disadvantage of using a Certificate Revocation List? *

○ It only works with symmetric keys

● It may not be as real time as OCSP

○ It requires a hardware enclave

○ It is not managed by a CA

During a gap analysis, a security team establishes a reference point using NIST SP 800-171. What is this reference point called? *

○ Roadmap

● Baseline

○ Security Zone

○ Benchmark

An attacker hides a secret message within the pixels of a digital image. This is an *
example of what?

○ Steganography

○ Hashing

○ Tokenization

○ Data Masking

Which control type is designed to discourage an intrusion attempt without *
necessarily providing a physical or technical barrier to entry?

○ Preventive

○ Corrective

○ Deterrent

○ Detective

A security administrator needs to check the status of a certificate in real time *
during an SSL handshake. Which protocol should they use?

○ CRL

○ CSR

○ KMS

○ OCSP

Which encryption method uses two distinct but mathematically related keys, where only the private key can decrypt data encrypted by the public key? *

○ Symmetric Encryption

○ Hashing

● Asymmetric Encryption

○ Obfuscation

When using asymmetric encryption to communicate securely, which key is used to encrypt the data sent to a destination? *

○ The sender's private key

○ The destination's private key

○ The sender's public key

● The destination's public key

What must a user submit to a Certificate Authority to request a digital certificate? *

○ A symmetric key

● A Certificate Signing Request (CSR)

○ A Certificate Revocation List (CRL)

○ A private key and identity info

A company wants to issue certificates for its internal servers without paying an external vendor. What should they implement? *

○ Key Escrow

○ Data Masking

● PKI with an Internal CA

○ A Web of Trust

A security professional is tasked with ensuring that messages cannot be modified during transit without detection. Which tenet of the CIA triad does this address? *

○ Non-repudiation

● Integrity

○ Confidentiality

○ Availability

A company replaces sensitive credit card numbers with temporary, non-sensitive placeholders not mathematically related to the original data. What is this called? *

○ Data Masking

● Tokenization

○ Encryption

○ Obfuscation

After a digital transaction, a user claims they never sent the request. However, the *
system uses digital signatures to prove the user's involvement. What concept is
being applied here?

○ Accounting

○ Authorisation

◉ Non-repudiation

○ Integrity

Which security architecture assumes that no device, process, or person is *
inherently trusted, regardless of their location on the network?

○ Honeynet

○ Air-gapping

○ Defence in Depth

◉ Zero Trust

Which of the following does a digital signature provide? *

○ Privacy Integrity Redundancy

◉ Integrity Authentication Non-Repudiation

○ Confidentiality Availability Authentication

○ Authorisation Accounting Availability

Which component of the CIA triad focuses on ensuring that systems and networks are up and running for authorised users? *

○ Confidentiality

○ Authentication

◉ Availability

○ Integrity

To attract and trap malicious actors, a security team sets up a fake server with enticing but false data. What is this called? *

◉ Honeypot

○ Gap Analysis

○ Honeytoken

○ Secure Enclave

In a large data centre, what device would be used to provide cryptographic functions and secure key storage for thousands of devices simultaneously? *

○ SSD

◉ HSM

○ TPM

○ CCB

Which process involves making a key more secure by hashing it multiple times? *

○ Tokenization

○ Key Exchange

○ Data Masking

◉ Key Stretching

A technician is configuring a power generator to ensure the server room remains functional during a blackout. According to the sources, what category and type of control is a power generator? *

○ Physical Compensating

○ Operational Deterrent

◉ Technical Compensating

○ Physical Corrective

Envoyer   Effacer le formulaire

Google Forms