Free Questions for SY0-601 by certsdeals

Shared by Gregory on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which Of the following supplies non-repudiation during a forensics investiga-tion?

Options:

A) Dumping volatile memory contents first

B) Duplicating a drive With dd

C) a SHA 2 signature of a drive image

D) Logging everyone in contact with evidence

E) Encrypting sensitive data

Answer:

C

Explanation:

A SHA 2 signature is a cryptographic hash function that produces a unique and fixed-length output for any given input.It can provide non-repudiation during a forensics investigation by verifying the integrity and authenticity of a drive image and proving that it has not been

altered or tampered with since it was created

Question 2

Question Type: MultipleChoice

A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

Options:

A) laaS

B) PasS

C) MaaS

D) SaaS

Answer:

D

Question 3

Question Type: MultipleChoice

A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data toss?

Options:

A) Logic bomb

B) Ransomware

C) Fileless virus

D) Remote access Trojans

E) Rootkit

Answer:

A

Question 4

Question Type: MultipleChoice

The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schem

a. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?

Options:

A) Tokenization

B) Masking

C) Full disk encryption

D) Mirroring

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

Options:

A) Recovery

B) Deterrent

C) Corrective

D) Detective

Answer:

C

Explanation:

Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

Question 6

Question Type: MultipleChoice

A SOC operator is analyzing a log file that contains the following entries:

Options:

A) SQL injection and improper input-handling attempts

B) Cross-site scripting and resource exhaustion attempts

C) Command injection and directory traversal attempts

D) Error handling and privilege escalation attempts

Answer:

C

Question 7

Question Type: MultipleChoice

During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

Options:

A) The forensic investigator forgot to run a checksum on the disk image after creation

B) The chain of custody form did not note time zone offsets between transportation regions

C) The computer was turned off. and a RAM image could not be taken at the same time

D) The hard drive was not properly kept in an antistatic bag when rt was moved

Answer:

A

Question 8

Question Type: MultipleChoice

A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an Iv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

Options:

A) Context-aware authentication

B) Simultaneous authentication of equals

C) Extensive authentication protocol

D) Agentless network access control

Answer:

A

Explanation:

An access control scheme that verifies an object's identity based on various environmental factors, like time, location, and behavior.

Question 9

Question Type: MultipleChoice

Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

Options:

A) The business continuity plan

B) The retention policy

C) The disaster recovery plan

D) The incident response plan

Answer:

A

Explanation:

BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.