CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing

B. Rainbow tables attack

C. Dictionary attack

D. Brute force attack

Correct Answer: B

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

QUESTION 2

Which of the following is the GREATEST security concern with respect to BYOD?

A. The filtering of sensitive data out of data flows at geographic boundaries.

B. Removing potential bottlenecks in data transmission paths.

C. The transfer of corporate data onto mobile corporate devices.

D. The migration of data into and out of the network in an uncontrolled manner.

Correct Answer: D

QUESTION 3

During an audit, it was determined from a sample that four out of 20 former employees were still accessing their email accounts An information security analyst is reviewing the access to determine if the audit was valid Which of the following would assist with the validation and provide the necessary documentation to audit?

A. Examining the termination notification process from human resources and employee account access logs

B. Checking social media platforms for disclosure of company sensitive and proprietary information

C. Sending a test email to the former employees to document an undeliverable email and review the ERP access

D. Reviewing the email global account list and the collaboration platform for recent activity

Correct Answer: A

QUESTION 4

A company is in the process of re-architecting its sensitive system infrastructure to take advantage of on-demand computing through a public cloud provider The system to be migrated is sensitive with respect to latency availability, and integrity The infrastructure team agreed to the following

1.

Application and middleware servers will migrate to the cloud"; Database servers will remain on-site

2.

Data backup wilt be stored in the cloud

Which of the following solutions would ensure system and security requirements are met?

A. Implement a direct connection from the company to the cloud provider

B. Use a cloud orchestration tool and implement appropriate change control processes

C. Implement a standby database on the cloud using a CASB for data-at-rest security

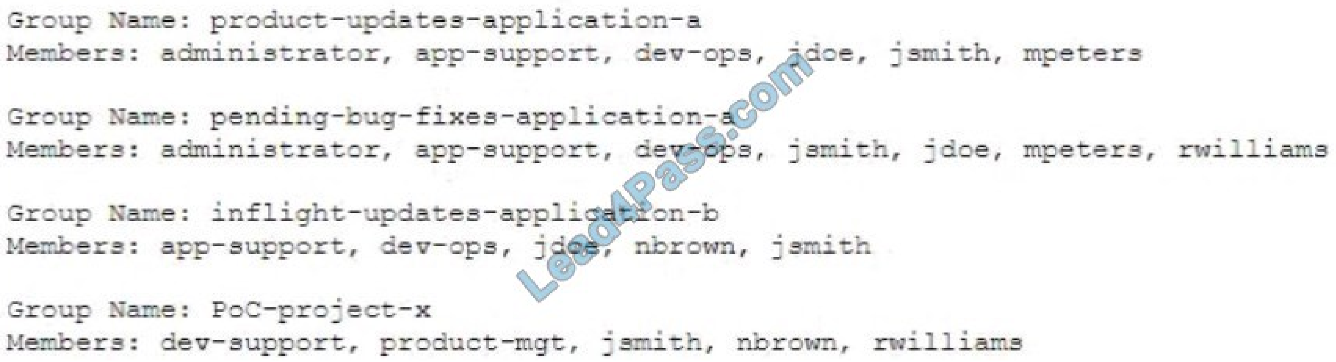
D. Use multizone geographic distribution with satellite relays

Correct Answer: A

QUESTION 5

Confidential information related to Application A. Application B and Project X appears to have been leaked to a competitor. After consulting with the legal team, the IR team is advised to take immediate action to preserve evidence for possible litigation and criminal charges.

While reviewing the rights and group ownership of the data involved in the breach, the IR team inspects the following distribution group access lists:



```
Group Name: product-updates-application-a
Members: administrator, app-support, dev-ops, jdoe, jsmith, mpeters

Group Name: pending-bug-fixes-application-a
Members: administrator, app-support, dev-ops, jsmith, jdoe, mpeters, rwilliams

Group Name: inflight-updates-application-b
Members: app-support, dev-ops, jdoe, nbrown, jsmith

Group Name: PoC-project-x
Members: dev-support, product-mgt, jsmith, nbrown, rwilliams
```

Which of the following actions should the IR team take FIRST?

A. Remove all members from the distribution groups immediately

B. Place the mailbox for jsmith on legal hold

C. Implement a proxy server on the network to inspect all outbound SMTP traffic for the DevOps group

D. Install DLP software on all developer laptops to prevent data from leaving the network.

Correct Answer: A

QUESTION 6

An organization is deploying IoT locks, sensors, and cameras, which operate over 802.11, to replace legacy building access control systems. These devices are capable of triggering physical access changes, including locking and unlocking doors and gates. Unfortunately, the devices have known vulnerabilities for which the vendor has yet to provide firmware updates.

Which of the following would BEST mitigate this risk?

A. Direct wire the IoT devices into physical switches and place them on an exclusive VLAN.

B. Require sensors to sign all transmitted unlock control messages digitally.

C. Associate the devices with an isolated wireless network configured for WPA2 and EAP-TLS.

D. Implement an out-of-band monitoring solution to detect message injections and attempts.

Correct Answer: C

QUESTION 7

Ann, a corporate executive, has been the recent target of increasing attempts to obtain corporate secrets by competitors through advanced, well-funded means. Ann frequently leaves her laptop unattended and physically unsecure in hotel rooms during travel. A security engineer must find a practical solution for Ann that minimizes the need for user training. Which of the following is the BEST solution in this scenario?

A. Full disk encryption

B. Biometric authentication

C. An eFuse-based solution

D. Two-factor authentication

Correct Answer: A

Exam B

QUESTION 8

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data

B. RAID configuration

C. Data de-duplication

D. Storage pool space allocation

E. Port scanning

F. LUN masking/mapping

G. Port mapping

Correct Answer: FG

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server\\'s access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in `Zoning\\'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

QUESTION 9

The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.

B. Social media is an ineffective solution because the policy may not align with the business.

C. Social media is an effective solution because it implements SSL encryption.

D. Social media is an ineffective solution because it is not primarily intended for business applications.

Correct Answer: B

Social media networks are designed to draw people\\'s attention quickly and to connect people is thus the main focus; security is not the main concern. Thus the CEO should decide that it would be ineffective to use social media in the company as it does not align with the company business.

QUESTION 10

A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

A. Inform the customer that the service provider does not have any control over third-party blacklist entries. The customer should reach out to the blacklist operator directly

B. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior

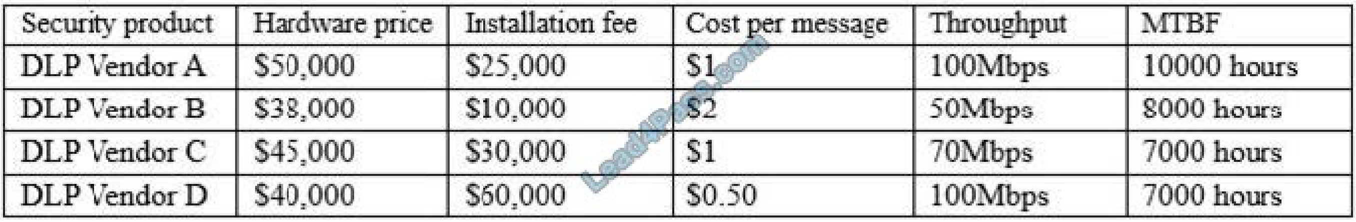
C. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic

D. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Correct Answer: D

QUESTION 11

A newly hired Chief Information Security Officer (CISO) is reviewing the organization\\'s security budget from the previous year. The CISO notices $100,000 worth of fines were paid for not properly encrypting outbound email messages. The CISO expects next year\\'s costs associated with fines to double and the volume of messages to increase by 100%. The organization sent out approximately 25,000 messages per year over the last three years. Given the table below:



Security product	Hardware price	Installation fee	Cost per message	Throughput	MTBF
DLP Vendor A	$50,000	$25,000	$1	100Mbps	10000 hours
DLP Vendor B	$38,000	$10,000	$2	50Mbps	8000 hours
DLP Vendor C	$45,000	$30,000	$1	70Mbps	7000 hours
DLP Vendor D	$40,000	$60,000	$0.50	100Mbps	7000 hours

Which of the following would be BEST for the CISO to include in this year\\'s budget?

A. A budget line for DLP Vendor A

B. A budget line for DLP Vendor B

C. A budget line for DLP Vendor C

D. A budget line for DLP Vendor D

E. A budget line for paying future fines

Correct Answer: E

QUESTION 12

An investigation showed a worm was introduced from an engineer\\'s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.

B. Implement role-based group policies on the management network for client access.

C. Utilize a jump box that is only allowed to connect to client from the management network.

D. Deploy a company-wide approved engineering workstation for management access.

Correct Answer: A

QUESTION 13

A company that has been breached multiple times is looking to protect cardholder data. The previous undetected attacks all mimicked normal administrative-type behavior. The company must deploy a host solution to meet the following requirements:

Detect administrative actions Block unwanted MD5 hashes Provide alerts Stop exfiltration of cardholder data

Which of the following solutions would BEST meet these requirements? (Choose two.)

A. AV

B. EDR

C. HIDS

D. DLP

E. HIPS

F. EFS

Correct Answer: BE

QUESTION 14

A security administrator is advocating for enforcement of a new policy that would require employers with privileged access accounts to undergo periodic inspections and review of certain job performance data. To which of the following policies is the security administrator MOST likely referring?

A. Background investigation

B. Mandatory vacation

C. Least privilege

D. Separation of duties

Correct Answer: C

QUESTION 15

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

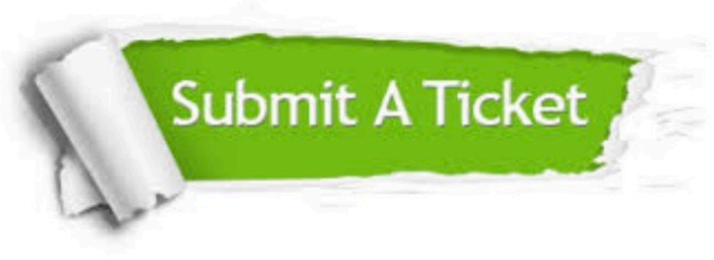
B. Job rotation

C. Least privilege

D. Employee termination procedures

Correct Answer: B

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.


Submit A Ticket

100%