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

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

QUESTION 1

An enterprise\\'s Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise\\'s growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise\\'s website.

Which of the following should the CISO be MOST concerned about?

A. Poor capacity planning could cause an oversubscribed host, leading to poor performance on the company\\'s website.

B. A security vulnerability that is exploited on the website could expose the accounting service.

C. Transferring as many services as possible to a CSP could free up resources.

D. The CTO does not have the budget available to purchase required resources and manage growth.

Correct Answer: A

QUESTION 2

After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees\\' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees\\' devices into the network securely?

A. Distribute a NAC client and use the client to push the company\\'s private key to all the new devices.

B. Distribute the device connection policy and a unique public/private key pair to each new employee\\'s device.

C. Install a self-signed SSL certificate on the company\\'s RADIUS server and distribute the certificate\\'s public key to all new client devices.

D. Install an 802.1X supplicant on all new devices and let each device generate a self-signed certificate to use for network access.

Correct Answer: D

QUESTION 3

An enterprise solution requires a central monitoring platform to address the growing networks of various departments and agencies that connect to the network. The current vendor products are not adequate due to the growing number of

heterogeneous devices.

Which of the following is the primary concern?

A. Scalability

B. Usability

C. Accountability

D. Performance

Correct Answer: A

QUESTION 4

An electric car company hires an IT consulting company to improve the cybersecurity of us vehicles. Which of the following should achieve the BEST long-term result for the company?

A. Designing Developing add-on security components for fielded vehicles

B. Reviewing proposed designs and prototypes for cybersecurity vulnerabilities

C. Performing a cyber-risk assessment on production vehicles

D. Reviewing and influencing requirements for an early development vehicle

Correct Answer: B

QUESTION 5

A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration

B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat

C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats

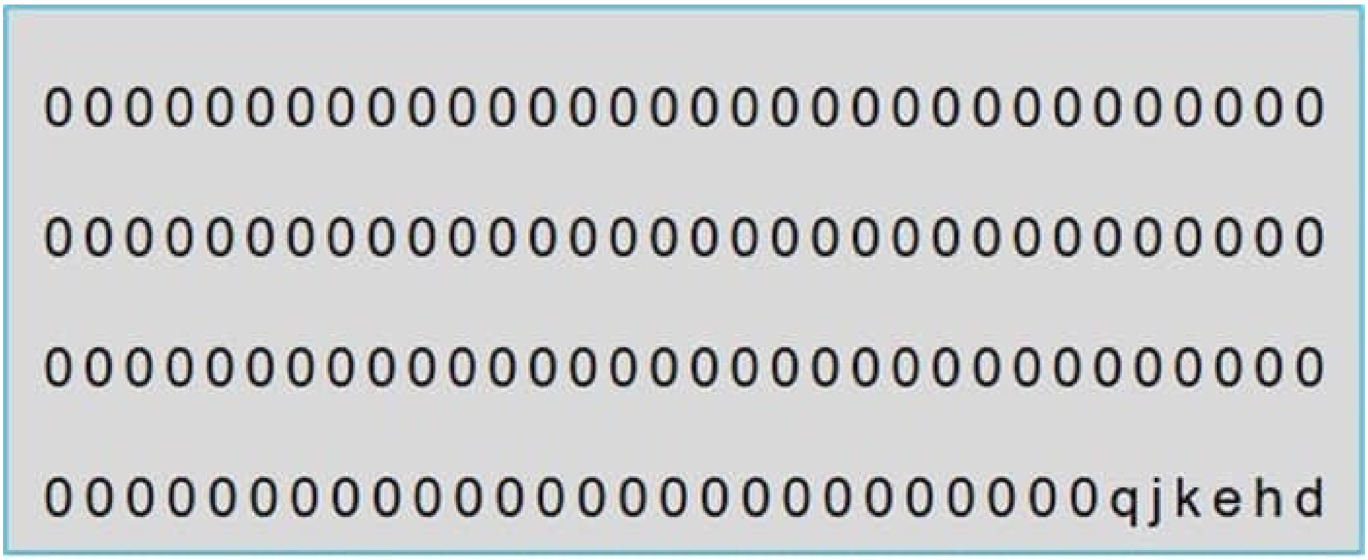
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A

QUESTION 6

A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:



```
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000qjkehd
```

Which of the following should be included in the auditor\\'s report based in the above findings?

A. The hard disk contains bad sectors

B. The disk has been degaussed.

C. The data represents part of the disk BIOS.

D. Sensitive data might still be present on the hard drives.

Correct Answer: A

QUESTION 7

The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working conditions, and all file integrity was verified

Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis

B. Continuity of operations plan

C. After-action report

D. Lessons learned

Correct Answer: A

QUESTION 8

A global company has decided to implement a cross-platform baseline of security settings for all company laptops. A security engineer is planning and executing the project. Which of the following should the security engineer recommend?

A. Replace each laptop in the company\\'s environment with a standardized laptop that is preconfigured to match the baseline settings

B. Create batch script files that will enable the baseline security settings and distribute them to global employees for execution

C. Send each laptop to a regional IT office to be reimaged with the new baseline security settings enabled and then redeployed

D. Establish GPO configurations for each baseline setting, test that each works as expected, and have each setting deployed to the laptops.

E. Leverage an MDM solution to apply the baseline settings and deploy continuous monitoring of security configurations.

Correct Answer: B

QUESTION 9

A large company with a very complex IT environment is considering a move from an on-premises, internally managed proxy to a cloud-based proxy solution managed by an external vendor. The current proxy provides caching, content filtering, malware analysis, and URL categorization for all staff connected behind the proxy. Staff members connect directly to the Internet outside of the corporate network. The cloud-based version of the solution would provide content filtering, TLS decryption, malware analysis, and URL categorization. After migrating to the cloud solution, all internal proxies would be decommissioned. Which of the following would MOST likely change the company\\'s risk profile?

A. 1. There would be a loss of internal intellectual knowledge regarding proxy configurations and application data flows.

2.

There would be a greater likelihood of Internet access outages due to lower resilience of cloud gateways.

3.

There would be data sovereignty concerns due to changes required in routing and proxy PAC files.

B. 1. The external vendor would have access to inbound and outbound gateway traffic.

2.

The service would provide some level of protection for staff working from home.

3.

Outages would be likely to occur for systems or applications with hard-coded proxy information.

C. 1. The loss of local caching would dramatically increase ISP charges and impact existing bandwidth.

2.

There would be a greater likelihood of Internet access outages due to lower resilience of cloud gateways.

3.

There would be a loss of internal intellectual knowledge regarding proxy configurations and application data flows.

D. 1. Outages would be likely to occur for systems or applications with hard-coded proxy information.

2.

The service would provide some level of protection for staff members working from home.

3.

Malware detection times would decrease due to third-party management of the service.

Correct Answer: D

QUESTION 10

A Chief Security Officer (CSO) is reviewing the organization\\'s incident response report from a recent incident. The details of the event indicate:

1.

A user received a phishing email that appeared to be a report from the organization\\'s CRM tool.

2.

The user attempted to access the CRM tool via a fraudulent web page but was unable to access the tool.

3.

The user, unaware of the compromised account, did not report the incident and continued to use the CRM tool with the original credentials.

4.

Several weeks later, the user reported anomalous activity within the CRM tool.

5.

Following an investigation, it was determined the account was compromised and an attacker in another country has gained access to the CRM tool.

6.

Following identification of corrupted data and successful recovery from the incident, a lessons learned activity was to be led by the CSO.

Which of the following would MOST likely have allowed the user to more quickly identify the unauthorized use of credentials by the attacker?

A. Security awareness training

B. Last login verification

C. Log correlation

D. Time-of-check controls

E. Time-of-use controls

F. WAYF-based authentication

Correct Answer: E

QUESTION 11

An administrator has enabled salting for users\\' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd

B. /etc/shadow

C. /etc/security

D. /etc/password

E. /sbin/logon

F. /bin/bash

Correct Answer: AB

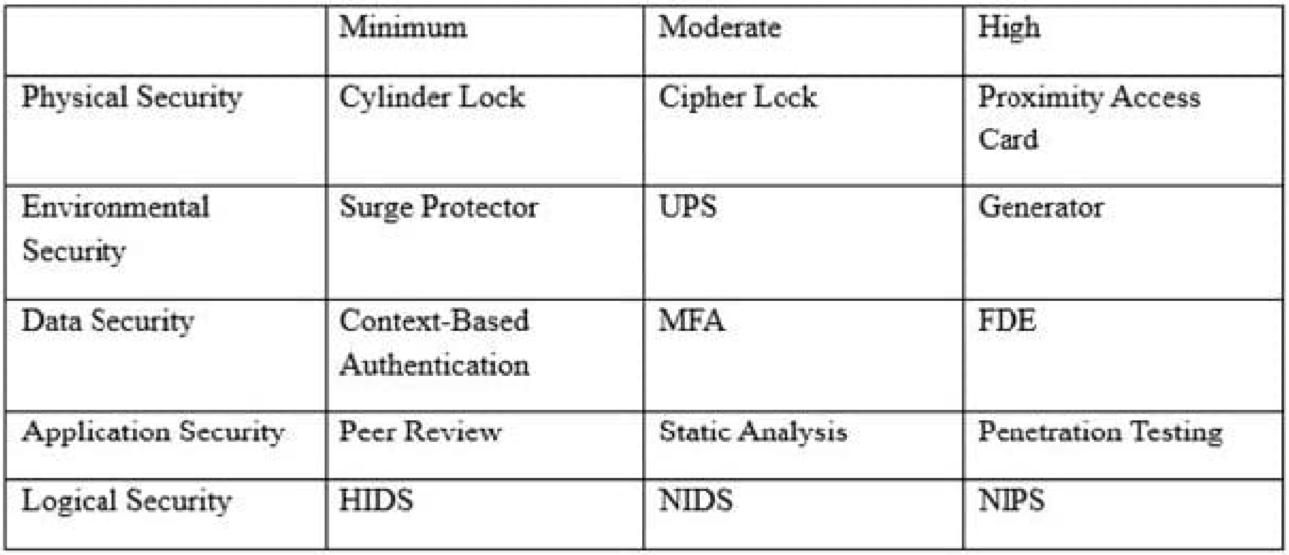
In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users\\' passwords means to store the passwords in an encrypted format.

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd\\'\\'. As this file is used by many tools (such as ``ls\\'\\') to display file ownerships, etc. by matching user id #\\'s with the user\\'s names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.

Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow\\'\\', contains encrypted password as well as other information such as account or password expiration values, etc.

QUESTION 12

An organization has established the following controls matrix:



	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:

Systems containing PII are protected with the minimum control set.

Systems containing medical data are protected at the moderate level.

Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentially of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these

requirements?

A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.

B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.

C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.

D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication.

Correct Answer: D

QUESTION 13

A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

A. Use an entropy-as-a-service vendor to leverage larger entropy pools.

B. Loop multiple pseudo-random number generators in a series to produce larger numbers.

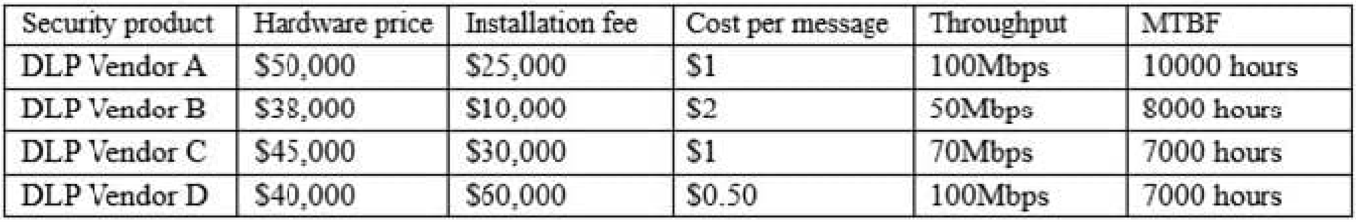
C. Increase key length by two orders of magnitude to detect brute forcing.

D. Shift key generation algorithms to ECC algorithms.

Correct Answer: A

QUESTION 14

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: A

QUESTION 15

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.

C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.

D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Correct Answer: D

VoIP is an integral part of network design and in particular remote access, that enables customers accessing and communicating with the company. If VoIP is unavailable then the company is in a situation that can be compared to downtime. And since the ISO is reviewing he summary of findings from the last COOP tabletop exercise, it can be said that the ISO is assessing the effect of a simulated downtime within the AAR.

CAS-003 Practice Test CAS-003 Study Guide CAS-003 Exam Questions