CAS-002 Q&As

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition

B. Encryption of the SSD at the file level

C. FDE of each logical volume on the SSD

D. FDE of the entire SSD as a single disk

Correct Answer: A

QUESTION 2

A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud

B. Aligning their client intake with the resources available

C. Using a community cloud with adequate controls

D. Outsourcing the service to a third party cloud provider

Correct Answer: C

QUESTION 3

Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

A. Check log files for logins from unauthorized IPs.

B. Check /proc/kmem for fragmented memory segments.

C. Check for unencrypted passwords in /etc/shadow.

D. Check timestamps for files modified around time of compromise.

E. Use lsof to determine files with future timestamps.

F. Use gpg to encrypt compromised data files.

G. Verify the MD5 checksum of system binaries.

H. Use vmstat to look for excessive disk I/O.

Correct Answer: ADG

QUESTION 4

A Chief Information Security Officer (CISO) has been trying to eliminate some IT security risks for several months. These risks are not high profile but still exist. Furthermore, many of these risks have been mitigated with innovative solutions.

However, at this point in time, the budget is insufficient to deal with the risks.

Which of the following risk strategies should be used?

A. Transfer the risks

B. Avoid the risks

C. Accept the risks

D. Mitigate the risks

Correct Answer: C

QUESTION 5

Unit testing for security functionality and resiliency to attack, as well as developing secure code and exploit mitigation, occur in which of the following phases of the Secure Software Development Lifecycle?

A. Secure Software Requirements

B. Secure Software Implementation

C. Secure Software Design

D. Software Acceptance

Correct Answer: B

QUESTION 6

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.

B. Require each user to log passwords used for file encryption to a decentralized repository.

C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.

D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

Correct Answer: D

QUESTION 7

Company GHI consolidated their network distribution so twelve network VLANs would be available over dual fiber links to a modular L2 switch in each of the company\\'s six IDFs. The IDF modular switches have redundant switch fabrics and power supplies. Which of the following threats will have the GREATEST impact on the network and what is the appropriate remediation step?

A. Threat: 802.1q trunking attack Remediation: Enable only necessary VLANs for each port

B. Threat: Bridge loop Remediation: Enable spanning tree

C. Threat: VLAN hopping Remediation: Enable only necessary VLANs for each port

D. Threat: VLAN hopping Remediation: Enable ACLs on the IDF switch

Correct Answer: B

QUESTION 8

A vulnerability research team has detected a new variant of a stealth Trojan that disables itself when it detects that it is running on a virtualized environment. The team decides to use dedicated hardware and local network to identify the Trojan\\'s behavior and the remote DNS and IP addresses it connects to. Which of the following tools is BEST suited to identify the DNS and IP addresses the stealth Trojan communicates with after its payload is decrypted?

A. HIDS

B. Vulnerability scanner

C. Packet analyzer

D. Firewall logs

E. Disassembler

Correct Answer: C

QUESTION 9

Two separate companies are in the process of integrating their authentication infrastructure into a unified single sign-on system. Currently, both companies use an AD backend and two factor authentication using TOTP. The system administrators have configured a trust relationship between the authentication backend to ensure proper process flow. How should the employees request access to shared resources before the authentication integration is complete?

A. They should logon to the system using the username concatenated with the 6-digit code and their original password.

B. They should logon to the system using the newly assigned global username: first.lastname#### where #### is the second factor code.

C. They should use the username format: LAN\first.lastname together with their original password and the next 6-digit code displayed when the token button is depressed.

D. They should use the username format: first.lastname@company.com, together with a password and their 6-digit code.

Correct Answer: D

QUESTION 10

A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent

B. 5.5 percent

C. 45 percent

D. 82 percent

Correct Answer: D

QUESTION 11

A security administrator wants to verify and improve the security of a business process which is tied to proven company workflow. The security administrator was able to improve security by applying controls that were defined by the newly released company security standard. Such controls included code improvement, transport encryption, and interface restrictions. Which of the following can the security administrator do to further increase security after having exhausted all the technical controls dictated by the company\\'s security standard?

A. Modify the company standard to account for higher security and meet with upper management for approval to implement the new standard.

B. Conduct a gap analysis and recommend appropriate non-technical mitigating controls, and incorporate the new controls into the standard.

C. Conduct a risk analysis on all current controls, and recommend appropriate mechanisms to increase overall security.

D. Modify the company policy to account for higher security, adapt the standard accordingly, and implement new technical controls.

Correct Answer: B

QUESTION 12

A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system

B. Review vendor selection process

C. Calculate the ALE for the event

D. Discussion of event timeline

E. Assigning of follow up items

Correct Answer: DE

QUESTION 13

A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.

Proposal:

External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.

The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000

B. $120,000

C. $150,000

D. $180,000

Correct Answer: A

QUESTION 14

The Chief Information Security Officer (CISO) of a small bank wants to embed a monthly testing regiment into the security management plan specifically for the development area. The CISO\\'s requirements are that testing must have a low risk of impacting system stability, can be scripted, and is very thorough. The development team claims that this will lead to a higher degree of test script maintenance and that it would be preferable if the testing was outsourced to a third party. The CISO still maintains that third-party testing would not be as thorough as the third party lacks the introspection of the development team. Which of the following will satisfy the CISO requirements?

A. Grey box testing performed by a major external consulting firm who have signed a NDA.

B. Black box testing performed by a major external consulting firm who have signed a NDA.

C. White box testing performed by the development and security assurance teams.

D. Grey box testing performed by the development and security assurance teams.

Correct Answer: C

QUESTION 15

Using SSL, an administrator wishes to secure public facing server farms in three subdomains:

dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 0

B. 1

C. 3

D. 6

Correct Answer: C