



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.geekcert.com/cas-003.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A manufacturing company's security engineer is concerned a remote actor may be able to access the ICS that is used to monitor the factory lines. The security engineer recently proposed some techniques to reduce the attack surface of the ICS to the Chief Information Security Officer (CISO). Which of the following would BEST track the reductions to show the CISO the engineer's plan is successful during each phase?

- A. Conducting tabletop exercises to evaluate system risk
- B. Contracting a third-party auditor after the project is finished
- C. Performing pre- and post-implementation penetration tests
- D. Running frequent vulnerability scans during the project

Correct Answer: A

QUESTION 2

Following a recent outage, a systems administrator is conducting a study to determine a suitable bench stock on server hard drives.

Which of the following metrics is MOST valuable to the administrator in determining how many hard drives to keep-on hand?

- A. TTR
- B. ALE
- C. MTBF
- D. SLE
- E. RPO

Correct Answer: C

QUESTION 3

An online bank has contracted with a consultant to perform a security assessment of the bank's web portal. The consultant notices the login page is linked from the main page with HTTPS, but when the URL is changed to HTTP, the browser is automatically redirected back to the HTTPS site. Which of the following is a concern for the consultant, and how can it be mitigated?

- A. XSS could be used to inject code into the login page during the redirect to the HTTPS site. The consultant should implement a WAF to prevent this.
- B. The consultant is concerned the site is using an older version of the SSL 3.0 protocol that is vulnerable to a variety of attacks. Upgrading the site to TLS 1.0 would mitigate this issue.



C. The HTTP traffic is vulnerable to network sniffing, which could disclose usernames and passwords to an attacker. The consultant should recommend disabling HTTP on the web server.

D. A successful MITM attack Could intercept the redirect and use sslstrip to decrypt further HTTPS traffic. Implementing HSTS on the web server would prevent this.

Correct Answer: D

QUESTION 4

A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day exploit and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server.

Which of the following should the analyst use to confirm this suspicion?

- A. File size
- B. Digital signature
- C. Checksums
- D. Anti-malware software
- E. Sandboxing

Correct Answer: B

QUESTION 5

A networking administrator was recently promoted to security administrator in an organization that handles highly sensitive data. The Chief Information Security Officer (CISO) has just asked for all IT security personnel to review a zero-day vulnerability and exploit for specific application servers to help mitigate the organization's exposure to that risk. Which of the following should the new security administrator review to gain more information? (Choose three.)

- A. CVE database
- B. Recent security industry conferences
- C. Security vendor pages
- D. Known vendor threat models
- E. Secure routing metrics
- F. Server's vendor documentation
- G. Verified security forums
- H. NetFlow analytics

Correct Answer: BDG



VCE & PDF

GeekCert.com

<https://www.geekcert.com/cas-003.html>

2024 Latest geekcert CAS-003 PDF and VCE dumps Download

[CAS-003 VCE Dumps](#)

[CAS-003 Exam Questions](#)

[CAS-003 Braindumps](#)