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.pass4itsure.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

During a security event investigation, a junior analyst fails to create an image of a server\\'s hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

A. Continuity of operations

B. Chain of custody

C. Order of volatility

D. Data recovery

Correct Answer: C

QUESTION 2

A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company\\'s RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:

1.

An HOTP service is installed on the RADIUS server.

2.

The RADIUS server is configured to require the HOTP service for authentication.

The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.

Which of the following should be implemented to BEST resolve the issue?

A. Replace the password requirement with the second factor. Network administrators will enter their username and then enter the token in place of their password in the password field.

B. Configure the RADIUS server to accept the second factor appended to the password. Network administrators will enter a password followed by their token in the password field.

C. Reconfigure network devices to prompt for username, password, and a token. Network administrators will enter their username and password, and then they will enter the token.

D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices.

Correct Answer: B

QUESTION 3

The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used?

A. Avoid

B. Mitigate

C. Transfer

D. Accept

Correct Answer: D

QUESTION 4

A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1.

Information should be sourced from the trusted master data source.

2.

There must be future requirements for identity proofing of devices and users.

3.

A generic identity connector that can be reused must be developed.

4.

The current project scope is for internally hosted applications only.

Which of the following solution building blocks should the security architect use to BEST meet the requirements?

A. LDAP, multifactor authentication, oAuth, XACML

B. AD, certificate-based authentication, Kerberos, SPML

C. SAML, context-aware authentication, oAuth, WAYF

D. NAC, radius, 802.1x, centralized active directory

Correct Answer: A

QUESTION 5

A development team releases updates to an application regularly. The application is compiled with several standard open-source security products that require a minimum version for compatibility. During the security review portion of the development cycle, which of the following should be done to minimize possible application vulnerabilities?

A. The developers should require an exact version of the open-source security products, preventing the introduction of new vulnerabilities.

B. The application development team should move to an Agile development approach to identify security concerns faster

C. The change logs for the third-party libraries should be reviewed for security patches, which may need to be included in the release.

D. The application should eliminate the use of open-source libraries and products to prevent known vulnerabilities from being included.

Correct Answer: C