

CAS-004 Reliable Dumps Sheet - First-grade Quiz 2026

CompTIA Latest CAS-004 Exam Discount



BONUS!!! Download part of DumpsTests CAS-004 dumps for free: <https://drive.google.com/open?id=1MQHR0Sgm5EM4t-OdD5at2gquZnDNZ9y>

Therefore, make the most of this opportunity of getting these superb exam questions for the CompTIA Advanced Security Practitioner (CASP+) Exam certification exam. We guarantee you that our top-rated CompTIA CAS-004 Practice Exam (PDF, desktop practice test software, and web-based practice exam) will enable you to pass the CAS-004 certification exam on the very first go.

CompTIA CAS-004 (CompTIA Advanced Security Practitioner (CASP+)) Certification Exam is designed to test the advanced security knowledge and skills of IT professionals. CAS-004 exam is intended for individuals with a minimum of 10 years of IT experience, including at least 5 years of hands-on technical security experience. The CASP+ certification is a globally recognized credential that validates the skills and knowledge required for advanced security roles.

The CASP+ certification is aimed at professionals who have a minimum of ten years of experience in IT administration, including at least five years of hands-on experience in technical security. CompTIA Advanced Security Practitioner (CASP+) Exam certification covers a broad range of topics, including risk management, enterprise security architecture, research and collaboration, and integration of computing, communications, and business disciplines.

>> CAS-004 Reliable Dumps Sheet <<

Latest CAS-004 Exam Discount, CAS-004 Valid Test Blueprint

In this high-speed world, a waste of time is equal to a waste of money. As an electronic product, our CAS-004 real study dumps have the distinct advantage of fast delivery. Once our customers pay successfully, we will check about your email address and other information to avoid any error, and send you the CAS-004 Prep Guide in 5-10 minutes, so you can get our CAS-004 exam questions at first time. And then you can start your study after downloading the CAS-004 exam questions in the email attachments.

CompTIA Advanced Security Practitioner (CASP+) is a certification exam that is designed to validate the advanced-level security skills and knowledge of IT professionals. CompTIA Advanced Security Practitioner (CASP+) Exam certification is intended for those who have a minimum of ten years of experience in IT administration, including at least five years of hands-on technical security

experience. CAS-004 Exam is ideal for those who want to enhance their expertise in enterprise security, risk management, research and analysis, and integration of computing, communications, and business disciplines.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q43-Q48):

NEW QUESTION # 43

A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.

Based on this agreement, this finding is BEST categorized as a:

- A. true negative.
- B. **false positive.**
- C. true positive.
- D. false negative.

Answer: B

NEW QUESTION # 44

A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:

- * Capable of early detection of advanced persistent threats.
- * Must be transparent to users and cause no performance degradation.
- + Allow integration with production and development networks seamlessly.
- + Enable the security team to hunt and investigate live exploitation techniques.

Which of the following technologies BEST meets the customer's requirements for security capabilities?

- A. Threat Intelligence
- B. **Deception software**
- C. Sandbox detonation
- D. Centralized logging

Answer: B

Explanation:

Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them. By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools¹². Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys¹³.

Deception software can meet the customer's requirements for security capabilities because:

It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged¹². It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources¹³. It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration¹³.

It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys¹³.

NEW QUESTION # 45

A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

- * A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.
- * A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.
- * The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

- A. Secure web gateway
- B. User behavior analysis
- C. **Software composition analysis**

- D. Dynamic analysis
- E. Stateful firewall

Answer: C

Explanation:

Explanation

Software composition analysis (SCA) is the best solution to help prevent this type of attack from being successful in the future. SCA is a process of identifying the third-party and open source components in the applications of an organization. This analysis leads to the discovery of security risks, quality of code, and license compliance of the components. SCA can help the security engineer to detect and remediate any vulnerabilities in a third-party library that was exploited by the hacker, such as updating to a newer and more secure version of the library. SCA can also help to enforce secure coding practices and standards, such as following the principle of least privilege and avoiding excessive privileges for local accounts. By using SCA, the security engineer can improve the security posture and resilience of the web application assets against future attacks. Verified References:

<https://www.synopsys.com/glossary/what-is-software-composition-analysis.html>

<https://www.geeksforgeeks.org/overview-of-software-composition-analysis/>

NEW QUESTION # 46

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

- A. 0
- B. 36,500
- **C. 0.5**
- D. 1

Answer: C

Explanation:

Reference: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/> The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is $2 / 4 = 0.5$. The other options are incorrect calculations. Verified References:

<https://www.comptia.org/blog/what-is-risk-management> <https://partners.comptia.org/docs/default-source/resources/casp- content-guide>

NEW QUESTION # 47

Which of the following should be established when configuring a mobile device to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden? (Select TWO).

- **A. proxy**
- B. Tunneling
- **C. MAC address randomization**
- D. VDI
- E. RDP
- F. MDM

Answer: A,C

Explanation:

The methods that can be used to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden are proxy and MAC address randomization. A proxy is a server that acts as an intermediary between a user and the internet, hiding the user's IP address and location from websites and other online services. A proxy can also encrypt the connection between the user and the proxy server, preventing anyone from snooping on the user's traffic. MAC address randomization is a feature that changes the MAC address of a mobile device periodically or when connecting to different networks. A MAC address is a unique identifier of a network interface that can be used to track the device's location and activity. MAC address randomization can help protect the user's privacy by making it harder for third parties to link the device to a specific user or network. Verified References:

<https://www.techtarget.com/searchsecurity/definition/proxy-server>

<https://www.techtarget.com/searchnetworking/definition/MAC-address-randomization>

<https://www.techtarget.com/searchsecurity/definition/MAC-address-Media-Access-Control-address>

NEW QUESTION # 48

• • • • •

Latest CAS-004 Exam Discount: <https://www.dumpstests.com/CAS-004-latest-test-dumps.html>

What's more, part of that DumpsTests CAS-004 dumps now are free: <https://drive.google.com/open?id=1MQHR0Sgm5EM4t-OdD5at2gquZnDNZ9y>