CAS-004 Reliable Exam Pdf - Real CAS-004 Torrent

2026 Latest CertkingdomPDF CAS-004 PDF Dumps and CAS-004 Exam Engine Free Share: https://drive.google.com/open?id=1kK6hEwIh_0MN9p2GlU6xFhGLA1U4FIvI

We should formulate a set of high efficient study plan to make the CAS-004 exam dumps easier to operate. Here our products strive for providing you a comfortable study platform and continuously upgrade CAS-004 test prep to meet every customer's requirements. Under the guidance of our CAS-004 Test Braindumps, 20-30 hours' preparation is enough to help you obtain the CompTIA certification, which means you can have more time to do your own business as well as keep a balance between a rest and taking exams.

What is the importance of CompTIA CAS-004 Certification

The CompTIA Advanced Security Practitioner certification (CASP) is the highest available certification in the market today. The CASP exam is an intense, eight-hour test designed to test your knowledge of advanced security concepts such as security architecture and design, penetration testing, risk management, forensics, ethical hacking and legal implications of IT security issues. CompTIA has announced the addition of a new certification exam which is also covered in **CompTIA CAS-004 Exam Dumps**, for their portfolio of certifications they offer to go along with the existing CompTIA A+ and Network+ certifications. The new exam is called "CompTIA Advanced Security Practitioner" or CAS-004. This new certification will be given as part of a continuous assessment program. This means that after you've earned the CAS-001 (CompTIA's entry level security certification) and the CAS-003 (their intermediate level security certification), you can then continue your education by taking the CAS-004 exam.

>> CAS-004 Reliable Exam Pdf <<

Real CAS-004 Torrent & CAS-004 Exam Vce Free

We always learned then forget, how to solve this problem, the answer is to have a good memory method, our CAS-004 exam question will do well on this point. Our CAS-004 real exam materials have their own unique learning method, abandon the traditional rote learning, adopt diversified memory patterns, such as the combination of text and graphics memory method, to distinguish between the memory of knowledge. Our CAS-004 learning reference files are so scientific and reasonable that you can buy them safely.

What are the steps to follow for the registration of CompTIA CAS-004 Exam Certification?

- Then, click on "CERTIFICATION EXAMINER"

- Go to the official website of CompTIA

- Print out those instructions and follow them carefully

- You must pay for your exam at the time it is administered. There is no other way to take the test. All payments must be made by credit card. We do not accept checks or money orders.

- Finally, fill out all the required information and submit payment

- Within 1-3 days, you will receive a letter from a local exam center with more detailed instructions

- Bring the required documents and a pen or pencil

- You will receive an e-mail from us immediately with the details of your purchase

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q46-Q51):

NEW QUESTION # 46
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

- A. Alerting the misconfigured service account password
- B. Restricting external port 22 access
- C. Modifying the AllowUsers configuration directive
- D. Implementing host-key preferences

Answer: C

NEW QUESTION # 47
The results of an internal audit indicate several employees reused passwords that were previously included in a published list of compromised passwords.
The company has the following employee password policy:

Attribute	Requirement
Complexity	Enabled
Character class	Special character, number
Length	10 characters
History	8
Maximum age	60 days
Minimum age	0

Which of the following should be implemented to best address the password reuse issue?
(Choose two.)

- A. Increase the history to 20.
- B. Increase the maximum age to 120 days.
- C. Add case-sensitive requirements to character class.
- D. Increase the character length to 12.
- E. Decrease the maximum age to 30 days.

- F. Remove the complexity requirements.
- G. Increase the minimum age to two days.

Answer: A,D

NEW QUESTION # 48
A company security engineer arrives at work to face the following scenario:
1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data Which of the following threat actors Is MOST likely involved?

- A. APT/nation-state
- B. Competitor
- C. Script kiddie
- D. Organized crime

Answer: A

Explanation:
An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: "Advanced Persistent Threats," Wiley, 2018.
https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition-p-9781119396582

NEW QUESTION # 49
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk In adopting this solution?

- A. The inability to obtain company data when migrating to another service
- B. The inability to require the service provider process data in a specific country
- C. The inability to assign access controls to comply with company policy
- D. The inability to conduct security assessments against a service provider

Answer: A

NEW QUESTION # 50
A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role-based access, and one-time authentication. Which of the following will need to be implemented to achieve this objective? (Select THREE).

- A. Continuous integration
- B. Firewall
- C. Least privilege
- D. Continuous validation
- E. VPN
- F. Iaas
- G. PKI
- H. Policy automation

Answer: C,D,H

Explanation:

A) Least privilege is a principle that states that every entity or resource should only have the minimum level of access or permissions necessary to perform its function. Least privilege can help enforce granular and dynamic policies that limit the exposure and impact of potential breaches. Least privilege can also help prevent privilege escalation and abuse by malicious insiders or compromised accounts.

C) Policy automation is a process that enables the creation, enforcement, and management of security policies using automated tools and workflows. Policy automation can help simplify and streamline the implementation of zero trust architecture by reducing human errors, inconsistencies, and delays. Policy automation can also help adapt to changing conditions and requirements by updating and applying policies in real time.

F) Continuous validation is a process that involves verifying the identity, context, and risk level of every request and transaction throughout its lifecycle. Continuous validation can help ensure that only authorized and legitimate requests and transactions are allowed to access or transfer data. Continuous validation can also help detect and respond to anomalies or threats by revoking access or terminating sessions if the risk level changes.

B) VPN is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. VPN stands for Virtual Private Network, which is a technology that creates a secure tunnel between a device and a network over the internet. VPN can provide confidentiality, integrity, and authentication for network communications, but it does not provide zero trust security by itself. VPN still relies on network-based perimeters and does not verify every request or transaction at a granular level.

D) PKI is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates can be used to prove the identity and authenticity of the certificate holders, as well as to encrypt and sign data. PKI can provide encryption and authentication for data communications, but it does not provide zero trust security by itself. PKI still relies on trusted authorities and does not verify every request or transaction at a granular level.

E) Firewall is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. Firewall can provide protection against unauthorized or malicious network access, but it does not provide zero trust security by itself. Firewall still relies on network-based perimeters and does not verify every request or transaction at a granular level.

G) Continuous integration is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Continuous integration is a software development practice that involves merging code changes from multiple developers into a shared repository frequently and automatically. Continuous integration can help improve the quality, reliability, and performance of software products, but it does not provide zero trust security by itself. Continuous integration still relies on code-based quality assurance and does not verify every request or transaction at a granular level.

H) IaaS is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS can provide scalability, flexibility, and cost-efficiency for IT infrastructure, but it does not provide zero trust security by itself. IaaS still relies on cloud-based security controls and does not verify every request or transaction at a granular level.

(Need Quick help to double verify the Answers that based on CompTIA CASP+ documents and resources) Give me following format:

Question no: (Number only)

Correct answer: (Answer option in bold)

Explanation:

Least privilege, policy automation, and continuous validation are some of the key elements that need to be implemented to achieve the objective of transitioning to a zero trust architecture. Zero trust architecture is a security model that assumes no implicit trust for any entity or resource, regardless of their location or ownership. Zero trust architecture requires verifying every request and transaction before granting access or allowing data transfer. Zero trust architecture also requires minimizing the attack surface and reducing the risk of lateral movement by attackers.

Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources) Verified Reference: (Related URLs AND Make sure Links are working and verified references)

NEW QUESTION # 51

......