#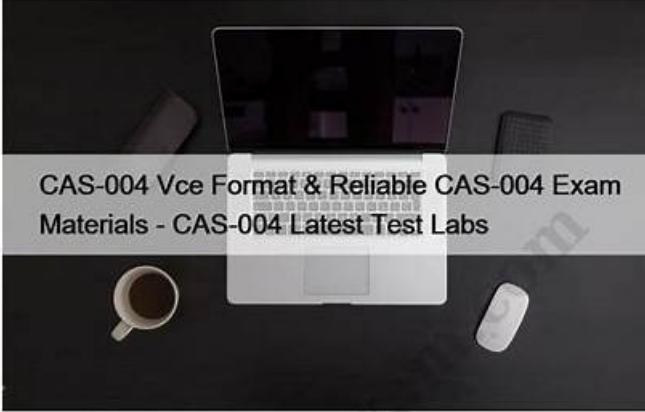 Reliable CAS-004 Latest Braindumps Ebook & Leading Provider in Qualification Exams & Verified Complete CAS-004 Exam Dumps

Our CAS-004 test guide keep pace with contemporary talent development and makes every learner fit in the needs of the society. There is no doubt that our CAS-004 latest question can be your first choice for your relevant knowledge accumulation and ability enhancement. Moreover, CAS-004 exam questions have been expanded capabilities through partnership with a network of reliable local companies in distribution, software and product referencing for a better development. That helping you pass the CAS-004 Exam with our CAS-004 latest question successfully has been given priority to our agenda.

The CASP+ exam covers a wide range of security topics, including risk management, enterprise security architecture, research and collaboration, integration of computing, communications, and business disciplines, and technical integration of enterprise components. CAS-004 Exam is designed to assess the candidate's ability to implement and manage security solutions that are effective against advanced threats, as well as their ability to analyze and interpret security data to make informed decisions.

>> CAS-004 Latest Braindumps Ebook <<

Complete CAS-004 Exam Dumps, Valid CAS-004 Exam Experience

CompTIA Advanced Security Practitioner (CASP+) certification is designed for experienced IT professionals who want to demonstrate their advanced cybersecurity skills and knowledge. CompTIA Advanced Security Practitioner (CASP+) Exam certification validates the skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. The CompTIA CASP+ certification is recognized globally and is highly regarded in the cybersecurity industry as it focuses on practical, hands-on skills that can be applied in real-world scenarios.

To pass the CASP+ certification exam, candidates must have a deep understanding of security concepts and be able to solve complex security problems. CAS-004 Exam consists of 90 multiple-choice and performance-based questions that test the candidate's knowledge and skills in various security domains. CAS-004 exam also includes real-world scenarios that require the candidate to apply their knowledge of security concepts to solve problems. CompTIA Advanced Security Practitioner (CASP+) Exam certification exam is intended for professionals who are responsible for securing complex enterprise environments and who have experience with enterprise security architecture, incident response, and risk management. Overall, the CASP+ certification provides a valuable credential for IT professionals who want to advance their careers in the field of cybersecurity.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q83-Q88):

NEW QUESTION # 83

A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

- A. Deploying a honeypot
- B. Installing a network firewall
- C. Implementing an IDS
- D. Placing a WAF inline

Answer: D

NEW QUESTION # 84

A security analyst is reviewing the following vulnerability assessment report:

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

- A. Server 4
- B. Server 3
- C. Server 1
- D. Server 2

Answer: D

Explanation:
In a vulnerability assessment report, the "exploit" field is used to indicate whether or not a particular vulnerability can be exploited, or used to attack the system. The "Yes" value in this field indicates that the vulnerability can be exploited, while the "POC" (Proof of Concept) value indicates that a proof of concept for exploiting the vulnerability has been developed, but it is not known if the vulnerability can actually be exploited in a real-world attack.
So the correct remediation priorities should be:
1) Server2
2) Server3
3) Server1
4) Server4

NEW QUESTION # 85
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

- A. Local caching
- B. SD-WAN vertical heterogeneity
- C. Content delivery network
- D. Distributed connection allocation

Answer: B

Explanation:
Explanation
SD-WAN (software-defined wide area network) vertical heterogeneity is a technique that can help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. SD-WAN vertical heterogeneity involves using different types of network links (such as broadband, cellular, or satellite) for different types of traffic (such as voice, video, or data) based on their performance and security requirements. This can optimize the network efficiency and reliability, as well as provide granular visibility and control over traffic flows. Distributed connection allocation is not a technique for preserving network bandwidth and increasing speed, but a method for distributing network connections among multiple servers or devices. Local caching is not a technique for preserving network bandwidth and increasing speed, but a method for storing frequently accessed data locally to reduce latency or load times. Content delivery network is not a technique for preserving network bandwidth and increasing speed, but a system of distributed servers that deliver web content to users based on their geographic location.
Verified References:
https://www.comptia.org/blog/what-is-sd-wan
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION # 86
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

- A. Account enumerator
- B. Password cracker
- C. Port scanner
- D. Exploitation framework

Answer: B

NEW QUESTION # 87
A security analyst observes the following while looking through network traffic in a company's cloud log:

Which of the following steps should the security analyst take FIRST?

- A. Quarantine 10.0.5.52 and run a malware scan against the host.
- B. Isolate 10.0.50.6 via security groups.
- C. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.
- D. Access 10.0.5.52 via EDR and identify processes that have network connections.

Answer: A

NEW QUESTION # 88

......