Types of CAS-004 Exam Practice Test Questions

P.S. Free & New CAS-004 dumps are available on Google Drive shared by PassLeader: https://drive.google.com/open?id=11xot0MUrZy3CV4Khtu0YKyRY3750W2FV

We are sure you can seep great deal of knowledge from our CAS-004 study prep in preference to other materials obviously. Our CAS-004 practice materials have variant kinds including PDF, app and software versions. As CAS-004 Exam Questions with high prestige and esteem in the market, we hold sturdy faith for you. And you will find that our CAS-004 learning quiz is quite popular among the candidates all over the world.

The CASP+ exam is a performance-based certification that tests the candidates on their ability to handle complex security scenarios in real-world situations. CAS-004 exam covers a wide range of topics, including enterprise security, risk management, research and analysis, integration of computing, communications and business disciplines, and technical integration of enterprise components. CAS-004 Exam is designed to assess the candidates' ability to apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers. The CASP+ certification is highly regarded in the industry and is recognized by government agencies and private corporations worldwide.

>> Exam CAS-004 Book <<

CAS-004 Valid Test Book & New CAS-004 Test Pattern

If you are a person who desire to move ahead in the career with informed choice, then the CAS-004 test material is quite beneficial for you. Our CAS-004 pdf is designed to boost your personal ability in your industry. To enhance your career path with your certification, you need to use the valid and Latest CAS-004 Exam Guide to assist you for success. Our CAS-004 practice torrent offers you the realistic and accurate simulations of the real test. The aim of our CAS-004 practice torrent is to help you successfully pass the CAS-004 exam.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q355-Q360):

NEW QUESTION # 355
A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

- A. SAN
- B. CA
- C. CRL
- D. ocsp

Answer: A

Explanation:
The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.
example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.
com, which can cover any subdomain under that domain. Verified References:
* https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name
* https://www.techtarget.com/searchsecurity/definition/wildcard-certificate
* https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/

NEW QUESTION # 356
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

- A. An active-active solution within the same tenant
- B. An on-premises solution as a backup
- C. A load balancer with a round-robin configuration
- D. A multicloud provider solution

Answer: D

Explanation:
A multicloud provider solution is the best option for proceeding with the digital transformation while ensuring SLA (service level agreement) requirements in the event of a CSP (cloud service provider) incident. A multicloud provider solution is a strategy that involves using multiple CSPs for different cloud services or applications, such as infrastructure, platform, or software as a service. A multicloud provider solution can provide resiliency, redundancy, and availability for cloud services or applications, as it can distribute the workload and risk across different CSPs and avoid single points of failure or vendor lock-in. An on-premises solution as a backup is not a good option for proceeding with the digital transformation, as it could involve high costs, complexity, or maintenance for maintaining both cloud and on-premises resources, as well as affect the scalability or flexibility of cloud services or applications. A load balancer with a round-robin configuration is not a good option for proceeding with the digital transformation, as it could introduce latency or performance issues for cloud services or applications, as well as not provide sufficient resiliency or redundancy in case of a CSP incident. An active-active solution within the same tenant is not a good option for proceeding with the digital transformation, as it could still be affected by a CSP incident that impacts the entire tenant or region, as well as increase the costs or complexity of managing multiple instances of cloud services or applications. Verified References:
https://www.comptia.org/blog/what-is-multicloudhttps://partners.comptia.org/docs/default-source/resources/casp

NEW QUESTION # 357
A security architect is reviewing the following proposed corporate firewall architecture and configuration:
Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443.
Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

- A. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

- B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
- C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
- D. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
- E. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
- F. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

Answer: A,C

Explanation:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should only connect to preapproved corporate database servers.
And the subnet 10.0.2.10/32 falls within the 10.0.0.0/16 corporate network leading us to conclude that F is the only answer that fulfills that requirement.
Answers B, C, D, and E are all wrong because they are permitting the firewall to access the Internet or be accessed by the internet. This is a big No when you configure firewall rules.
Firewall do not need to access or be accessed by anybody besides pre-defined internal systems that are in charge of configuring and updating them.
So Only A and F are permittable answers in this case regardless of what conditions are stated.

NEW QUESTION # 358
A security architect examines a section of code and discovers the following:
char username[20]
char password[20]
gets(username)
checkUserExists(username)
Which of the following changes should the security architect require before approving the code for release?

- A. Prevent more than 20 characters from being entered.
- B. Add a password parameter to the checkUserExists function.
- C. Allow only alphanumeric characters for the username.
- D. Make the password variable longer to support more secure passwords.

Answer: A

Explanation:
The code snippet presents a buffer size risk where the user input (username) is accepted without limiting the number of characters, potentially leading to buffer overflow vulnerabilities. The best solution is to implement input validation that limits the input to a maximum of 20 characters, matching the buffer size defined in the code. This prevents overflow attacks by ensuring that user input does not exceed the allocated memory space. Other options, like adding more parameters or allowing alphanumeric characters, do not directly address the root cause of buffer overflow vulnerabilities.

NEW QUESTION # 359
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.
Based on the output above, from which of the following process IDs can the analyst begin an investigation?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Explanation:

The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.
linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified References:
https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source
/resources/casp-content-guide

NEW QUESTION # 360
.....

Are you still hesitating about which kind of CAS-004 exam torrent should you choose to prepare for the exam in order to get the related certification at ease? Our CAS-004 Exam Torrent can help you get the related certification at ease and CAS-004 Practice Materials are compiled by our company for more than ten years. I am glad to introduce our study materials to you. Our company has already become a famous brand all over the world in this field since we have engaged in compiling the CAS-004 practice materials for more than ten years and have got a fruitful outcome. You are welcome to download it for free in this website before making your final decision.