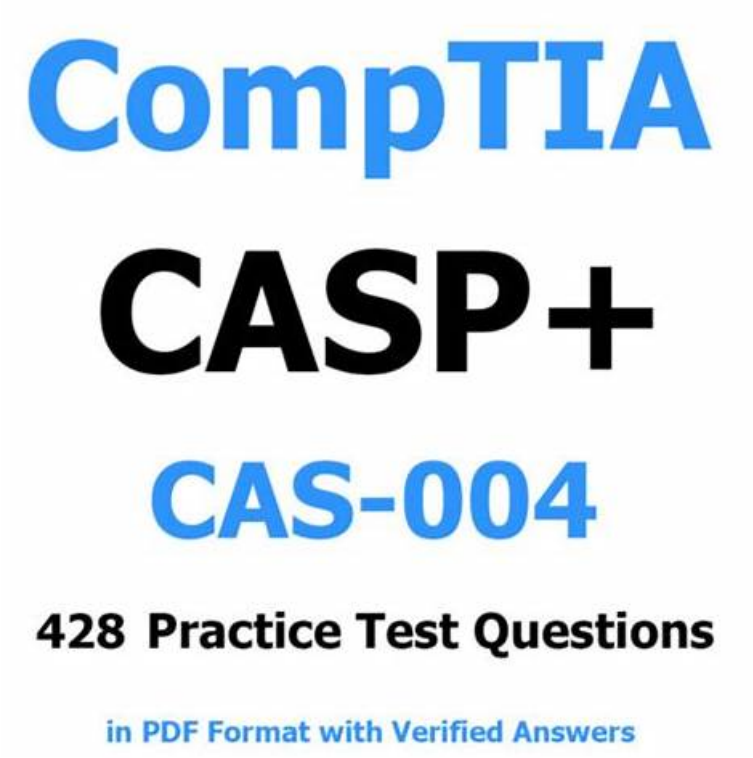
100% Pass Quiz 2025 CompTIA CAS-004: Professional CompTIA Advanced Security Practitioner (CASP+) Exam Reliable Test Book



P.S. Free & New CAS-004 dumps are available on Google Drive shared by Braindumpsqa: https://drive.google.com/open?id=1xiiJpe51zibdnAOKVoQv_AqG0EjopMFx

The best way for candidates to know our CompTIA CAS-004 training dumps is downloading our free demo. We provide free PDF demo for each exam. This free demo is a small part of the official complete CompTIA Advanced Security Practitioner (CASP+) Exam CAS-004 training dumps. The free demo can show you the quality of our exam materials. You can download any time before purchasing.

CompTIA CASP+ certification is an advanced-level certification program that validates the skills and knowledge of cybersecurity professionals. The program is vendor-neutral, covers a wide range of security topics, and is recognized globally by employers and government agencies. IT professionals who hold the CASP+ certification are in high demand and can command higher salaries and better job opportunities.

The CASP+ certification is aimed at professionals who are responsible for the security of their organization's IT environment. CAS-004 Exam covers a wide range of topics, including risk management, enterprise security architecture, research and collaboration, and integration of computing, communications, and business disciplines. CompTIA Advanced Security Practitioner (CASP+) Exam certification validates the skills and knowledge required to design and implement secure solutions in complex enterprise environments.

>> CAS-004 Reliable Test Book <<

2025 CAS-004 Reliable Test Book - CompTIA CompTIA Advanced Security Practitioner (CASP+) Exam - Trustable Exam CAS-004 Forum

Without bothering to stick to any formality, our CAS-004 learning quiz can be obtained within five minutes. No need to line up or queue up to get our CAS-004 practice materials. They are not only efficient on downloading aspect, but can expedite your process of review. No harangue is included within CAS-004 Training Materials and every page is written by our proficient experts with

dedication. Our website experts simplify complex concepts and add examples, simulations, and diagrams to explain anything that might be difficult to understand.

CompTIA CAS-004 Exam is an excellent way for IT security professionals to demonstrate their advanced knowledge and skills in the field of information security. CompTIA Advanced Security Practitioner (CASP+) Exam certification is widely recognized throughout the industry and can open up new career opportunities for individuals looking to advance their careers in IT security. The CASP certification is a valuable asset for those looking to demonstrate their expertise in securing their organization's critical information and assets.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q314-Q319):

NEW QUESTION # 314
After investigating a recent security incident, a SOC analyst is charged with creating a reference guide for the entire team to use. Which of the following should the analyst create to address future incidents?

- A. Root cause analysis
- B. Communication plan
- C. Runbook
- D. Lessons learned

Answer: C

Explanation:
A runbook is a detailed guide that provides step-by-step instructions on how to respond to specific types of incidents. It is used by the SOC team to ensure a consistent, organized, and efficient response to incidents. In this case, after the incident investigation, creating a runbook would help standardize the response process for future security incidents, enabling the team to act quickly and effectively. CASP+ emphasizes the importance of having detailed runbooks for incident response as part of an organization's overall incident response strategy.
References:
* CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Incident Response and Runbooks)
* CompTIA CASP+ Study Guide: Incident Response Procedures and Runbooks

NEW QUESTION # 315
A security consultant has been asked to recommend a secure network design that would:
* Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
* Limit operational disruptions.
Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

- A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
- B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
- C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
- D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

Answer: D

Explanation:
OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.
To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:
Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.
Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.

NEW QUESTION # 316
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

- A. Utilize the SAN certificate to enable a single certificate for all regions.
- B. Configure certificate pinning inside the application.
- C. Enable HSTS on the application's server side for all communication.
- D. Deploy client certificates to all devices in the network.

Answer: B

Explanation:
Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:
Ensure that only trusted servers can communicate with the application, by rejecting any server certificate that does not match one of the pinned certificates or public keys.
Protect the confidentiality, integrity, and authenticity of the chat messages, by preventing any attacker from intercepting, modifying, or impersonating them.
Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION # 317
A security researcher identified the following messages while testing a web application:

```
/file/admin/myprofile.php ERROR file does not exist.
/file/admin/userinfo.php ERROR file does not exist.
/file/admin/adminprofile.php ERROR file does not exist.
/file/admin/admininfo.php ERROR file does not exist.
/file/admin/universalprofile.php ERROR file does not exist.
/file/admin/universalinfo.php ERROR file does not exist.
/file/admin/restrictedprofile.php ACCESS is denied.
/file/admin/restrictedinfo.php ERROR file does not exist.
```


Which of the following should the researcher recommend to remediate the issue?

- A. Elimination of the use of unsafe functions
- B. Proper error handling
- C. Packet inspection
- D. Software composition analysis

Answer: B

Explanation:
The log messages in the image display detailed error messages, indicating improper error handling, which can expose sensitive information to potential attackers. Proper error handling ensures that error messages do not reveal underlying application details (such as file paths or configuration information) that could be exploited. This aligns with the best practices in secure coding and is a core concept in CASP+. Rather than exposing the inner workings of the application, the system should return generic error messages to users while logging detailed information securely for internal troubleshooting.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Secure Coding, Error Handling) CompTIA CASP+ Study Guide: Web Application Security and Proper Error Handling Techniques

NEW QUESTION # 318
A security engineer is assessing a legacy server and needs to determine if FTP is running and on which port. The service cannot be turned off, as it would impact a critical application's ability to function. Which of the following commands would provide the

information necessary to create a firewall rule to prevent that service from being exploited?

- A. netstat -tulpn
- B. systemctl list-unit-file --type service ftpd
- C. service ftpd status
- D. chkconfig --list
- E. service --status-all | grep ftpd

Answer: A

Explanation:
The netstat -tulpn command is used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The -tulpn options specifically show TCP and UDP connections with the process ID and the name that is listening on each port, which would provide the necessary information to identify if FTP is running and on which port without turning the service off. This information can then be used to create a precise firewall rule to prevent the FTP service from being exploited.

NEW QUESTION # 319
.....