Exam CS0-003 Forum, CS0-003 Latest Dumps

BONUS!!! Download part of SurePassExams CS0-003 dumps for free: https://drive.google.com/open?id=1ePHL-N-fdbH8aO_b7xd3bCKCp6Jodj5y

Although the passing rate of our CS0-003 simulating exam is nearly 100%, we can refund money in full if you are still worried that you may not pass. You don't need to worry about the complexity of the refund process at all, we've made it quite simple. As long as you provide us with proof that you failed the exam after using our CS0-003, we can refund immediately. If you encounter any problems during the refund process, you can also contact our customer service staff at any time. They will help you solve the problem as quickly as possible. That is to say, our CS0-003 Exam Questions almost guarantee that you pass the exam. Even if you don't pass, you don't have to pay any price for our CS0-003 simulating exam. I hope we have enough sincerity to impress you.

The CS0-003 exam is designed to test candidates on a range of topics related to cybersecurity, including threat and vulnerability management, incident response, compliance and regulations, security operations and monitoring, and more. CS0-003 Exam consists of multiple-choice questions and performance-based simulations, and candidates are required to demonstrate their ability to apply their knowledge in real-world scenarios.

>> Exam CS0-003 Forum <<

CS0-003 Latest Dumps, New CS0-003 Test Discount

We provide three versions to let the clients choose the most suitable equipment on their hands to learn the CS0-003 study materials such as the smart phones, the laptops and the tablet computers. We provide the professional staff to reply your problems about our study materials online in the whole day and the timely and periodical update to the clients. So you will definitely feel it is your fortune to buy our CS0-003 Study Materials.

CompTIA CS0-003 (CompTIA Cybersecurity Analyst (CySA+) Certification) is a certification exam that is aimed at validating the technical skills and knowledge required to secure and protect computer systems and networks. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification exam is designed for IT professionals who want to specialize in cybersecurity and is recognized globally as a leading certification for cybersecurity analysts.

CompTIA Cybersecurity Analyst (CySA+) certification exam, also known as CS0-003, is a highly respected and in-demand certification in the field of cybersecurity. CS0-003 Exam is designed to validate the skills of professionals who are responsible for detecting, preventing, and responding to cybersecurity threats. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is designed to equip candidates with the knowledge and skills necessary to analyze data and identify potential cyber threats, as well as develop and implement effective cybersecurity strategies.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q366-Q371):

NEW QUESTION # 366
A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the

attack?

- A. Scan the employee's computer with virus and malware tools.
- B. Contact human resources and recommend the termination of the employee.
- C. Assign security awareness training to the employee involved in the incident.
- D. Review the actions taken by the employee and the email related to the event

Answer: D

Explanation:
In case of a phishing attack, it's crucial to review what actions were taken by the employee and analyze the phishing email to understand its nature and impact.References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 246; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 255.

NEW QUESTION # 367
A technician is analyzing output from a popular network mapping tool for a PCI audit:
Which of the following best describes the output?

- A. The host is allowing insecure cipher suites.
- B. The host is not up or responding.
- C. The host is running excessive cipher suites.
- D. The Secure Shell port on this host is closed

Answer: A

Explanation:
The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used.
Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

NEW QUESTION # 368
Which of the following is the best authentication method to secure access to sensitive data?

- A. Alphanumeric/special character username and passphrase for login
- B. An assigned device that generates a randomized code for login
- C. Biometrics and a device with a personalized code for login
- D. A one-time code received by email and push authorization for login

Answer: C

Explanation:
The best practice for securing access to sensitive data is to implement multifactor authentication (MFA), which combines multiple factors of authentication to enhance security.
* Option B (Biometrics + Device with a Personalized Code) uses two strong factors:
* Biometrics (something you are)
* A device with a personalized code (something you have)This combination significantly reduces the risk of unauthorized access.
* Option A (Randomized Code) is good but weaker than biometrics because it relies only on something you have.
* Option C (Passphrase) is single-factor authentication, which is susceptible to brute-force attacks.

* Option D (One-time Code + Push Notification) is useful, but email-based authentication can be vulnerable to phishing and MITM attacks.

NEW QUESTION # 369
An IDS is triggered during after-hours operations. The indicator records an abnormal amount of SYN requests being sent to port 21 from numerous external systems. A security analyst reports this information to the IR team for further investigation. Which of the following best describes this incident?

- A. A DDoS attack through the FTP port
- B. A reconnaissance attack through the SSH port
- C. A sniff attack through the DNS port
- D. A buffer overflow attack through the Telnet port

Answer: A

Explanation:
Port 21 is used for FTP. An abnormal number of SYN requests from many external systems indicates a SYN flood, a type of Distributed Denial of Service (DDoS) attack targeting the FTP service to overwhelm the server and disrupt availability.

NEW QUESTION # 370
Which of the following characteristics ensures the security of an automated information system is the most effective and economical?

- A. Optimized prior to the addition of security
- B. Customized to meet specific security threats
- C. Originally designed to provide necessary security
- D. Subjected to intense security testing

Answer: C

Explanation:
Comprehensive Detailed Explanation:The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as
"security by design." Here's a breakdown of each option and why option A is correct:
* A. Originally designed to provide necessary security
* Explanation: Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.
* Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing the costs associated with later modifications.
* Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.
* B. Subjected to intense security testing
* While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.
* C. Customized to meet specific security threats
* Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.
* D. Optimized prior to the addition of security
* Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.
References:
NIST SP 800-160: Systems Security Engineering, which emphasizes designing systems with security integrated from the beginning.
OWASP Security by Design Principles: Explores how security considerations are most effective when included early in development.

NEW QUESTION # 371

......

CS0-003 Latest Dumps: https://www.surepassexams.com/CS0-003-exam-bootcamp.html

P.S. Free & New CS0-003 dumps are available on Google Drive shared by SurePassExams: https://drive.google.com/open?id=1ePHL-N-fdbH8aO_b7xd3bCKCp6Jodj5y