CAS-005 Valid Test Dumps | CAS-005 Latest Examprep

DOWNLOAD the newest ITExamDownload CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1DzT4TY-PShIZ6rR0RcYdtP8PnAJfGLwW

If you are the first time to buy the CAS-005 learning material online, or you have bought them for many times, there may be some problem that puzzle you, if you have any questions about the CAS-005 exam dumps, you can ask our service stuff for help. They have the professional knowledge of CAS-005 Training Materials, and they will be very helpful for solving your problem. In addition, we have free demo for you to try before buying the product, and you can have a try before purchasing.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.
Topic 2	• Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.
Topic 3	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

Topic 4	• Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.

>> CAS-005 Valid Test Dumps <<

CompTIA CAS-005 Latest Examprep | CAS-005 Latest Practice Questions

The clients at home and abroad can both purchase our CAS-005 study tool online. Our brand enjoys world-wide fame and influences so many clients at home and abroad choose to buy our CAS-005 test guide. Our company provides convenient service to the clients all around the world so that the clients all around the world can use our CAS-005 Study Materials efficiently. Our company boosts an entire sale system which provides the links to the clients all around the world so that the clients can receive our CAS-005 exam questions timely.

CompTIA SecurityX Certification Exam Sample Questions (Q170-Q175):

NEW QUESTION # 170
A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?

- A. The /etc/etc/sshd, configure file updating the ciphers
- B. The /etc/openssl.conf file, updating the virtual site parameter
- C. The /etc/nsswith.conf file, updating the name server
- D. The /etc/hosts file, updating the IP parameter

Answer: A

Explanation:
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed. By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.

NEW QUESTION # 171
Source code snippets for two separate malware samples are shown below:
Sample 1:
knockEmDown(String e) {
if(target.isAccessed()) {
target.toShell(e);
System.out.printIn(e.toString());
c2.sendTelemetry(target.hostname.toString + " is " + e.toString());
} else {
target.close();
}
}
Sample 2:
targetSys(address a) {
if(address.islpv4()) {
address.connect(1337);
address.keepAlive("paranoid");
String status = knockEmDown(address.current);
remote.sendC2(address.current + " is " + status);
} else {

throw Exception e;
}
}
Which of the following describes the most important observation about the two samples?

- A. The samples were probably written by the same developer.
- B. Both samples use IP connectivity for command and control.
- C. Sample 1 is the target agent while Sample 2 is the C2 server.
- D. Telemetry is first buffered and then transmitted in paranoid mode.

Answer: A

Explanation:
Step-by-Step Explanation:
Both samples share similar function names, variable naming styles, and logic flow, indicating that they were likely written by the same developer. This is a keyobservation in malware attribution, as cyber threat analysts often look for unique coding styles to link malware to specific threat actors.
The presence of C2 (Command and Control) communication in both samples supports this theory, as attackers often reuse parts of their own malware code across different attacks.

NEW QUESTION # 172
A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:
- Be efficient at protecting the production environment
- Not require any change to the application
- Act at the presentation layer
Which of the following techniques should be used?

- A. Random substitution
- B. Algorithmic
- C. Steganography
- D. Masking

Answer: D

Explanation:
Dynamic data masking works at the presentation layer, sitting between your database and application-and transforms sensitive fields (for example, showing "J*** S****" instead of "John Smith") without altering the underlying data or touching the application code. This approach efficiently protects production systems, requires no changes to the application, and enforces masking policies in real time.

NEW QUESTION # 173
After a penetration test on the internal network, the following report was generated:
Which of the following should be recommended to remediate the attack?

- A. Reimaging ADMIN01$
- B. Deleting SQLSV
- C. Resetting the local domain
- D. Rotating KRBTGT password

Answer: D

NEW QUESTION # 174
A security administrator has been provided with three separate certificates and is trying to organize them into a single chain of trust to deploy on a website. Given the following certificate properties:
Which of the following are true about the PKI hierarchy? (Choose two.)

- A. SuperTrust RSA 2018 is an intermediate CA.

- B. BudgetCert is an intermediate CA.
- C. BudgetCert is the top-level CA
- D. SuperTrust RSA 2018 is the top-level CA.
- E. www.budgetcert.com.is the top-level CA.
- F. www.budgetcert.com. is an intermediate CA.

Answer: C,D

Explanation:
Based on the given certificate properties:
SuperTrust RSA 2018 is an intermediate certificate authority (CA) because it is issued by BudgetCert Global Root CA, which is the top-level certificate authority. BudgetCert is the top-level CA (root CA) in this public key infrastructure (PKI) hierarchy, as it issues certificates to SuperTrust RSA 2018 and has no issuer of its own. Therefore, SuperTrust RSA 2018 is the intermediate CA, and BudgetCert is the top-level (root) CA in this PKI chain of trust. The www.budgetcert.com certificate is the leaf or end-entity certificate, which is used for the website itself.

NEW QUESTION # 175
.....

Today, in an era of fierce competition, how can we occupy a place in a market where talent is saturated? The answer is a certificate. What the certificate main? All kinds of the test CAS-005 certification, prove you through all kinds of qualification certificate, it is not hard to find, more and more people are willing to invest time and effort on the CAS-005 Exam Guide, because get the test CAS-005 certification is not an easy thing, so, a lot of people are looking for an efficient learning method. And here, fortunately, you have found the CAS-005 exam braindumps, a learning platform that can bring you unexpected experiences.

https://drive.google.com/open?id=1DzT4TY-PShlZ6rR0RcYdtP8PnAJfGLwW