

[March-2019-New100% Real Exam Questions-Braindump2go CAS-003 Exam Dumps PDF 401Q Download

2019/March Braindump2go CAS-003 Exam Dumps with PDF and VCE New Updated Today! Following are some new CAS-003 Exam Questions:

1. |2019 Latest Braindump2go CAS-003 Exam Dumps (PDF & VCE) Instant Download: <https://www.braindump2go.com/cas-003.html> 2. |2019 Latest Braindump2go CAS-003 Exam Questions & Answers Instant Download: <https://drive.google.com/drive/folders/11eVcvdRTGUBIESzBX9a6YIPUYiZ4xoHE?usp=sharing>

New Question A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).
A. Physical penetration test of the datacenter to ensure there are appropriate controls.
B. Penetration testing of the solution to ensure that the customer data is well protected.
C. Security clauses are implemented into the contract such as the right to audit.
D. Review of the organizations security policies, procedures and relevant hosting certifications.
E. Code review of the solution to ensure that there are no back doors located in the software.
Answer: CD
Explanation: Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following: Company profile, strategy, mission, and reputation Financial status, including reviews of audited financial statements Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks Process expertise, methodology, and effectiveness Quality initiatives and certifications Technology, infrastructure stability, and applications Security and audit controls Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors Insurance Disaster recovery and business continuity policies C and D form part of Security and audit controls.

New Question An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC. Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).
A. Static and dynamic analysis is run as part of integration
B. Security standards and training is performed as part of the project
C. Daily stand-up meetings are held to ensure security requirements are understood
D. For each major iteration penetration testing is performed
E. Security requirements are story boarded and make it into the build
F. A security design is performed at the end of the requirements phase
Answer: AD
Explanation: SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks. Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code. For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

New Question An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).
A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash
Answer: AB
Explanation: In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format. Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk. Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc.

New Question Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?
A. Research new technology vendors to look for potential products.

secure lab.C. Construct a series of VMs to host the malware environment.D. Create a proposal and present it to management for approval.
Answer: D
Explanation: Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation within the company's business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it.

New Question
A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?
A. Agile
B. SDLC
C. Waterfall
D. Joint application development
Answer: A
Explanation: In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

New Question
A security administrator is shown the following log excerpt from a Unix system:
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh
2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh
2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh
2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh
2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh
2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh
Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).
A. An authorized administrator has logged into the root account remotely.
B. The administrator should disable remote root logins.
C. Isolate the system immediately and begin forensic analysis on the host.
D. A remote attacker has compromised the root account using a buffer overflow in sshd.
E. A remote attacker has guessed the root password using a dictionary attack.
F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
G. A remote attacker has compromised the private key of the root account.
H. Change the root password immediately to a password not found in a dictionary.
Answer: CE
Explanation: The log shows six attempts to log in to a system. The first five attempts failed due to 'failed password'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has guessed the root password using a dictionary attack. The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access.

New Question
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?
A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust
Answer: C
Explanation: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM. IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform. The TPM is the hardware root of trust. Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust. Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust).
!!!RECOMMEND!!!
1. |2019 Latest Braindump2go CAS-003 Exam Dumps (PDF & VCE) Instant Download: <https://www.braindump2go.com/cas-003.html>
2. |2019 Latest Braindump2go CAS-003 Study Guide Video Instant Download: YouTube Video: [YouTube.com/watch?v=WCO0vTnXfrk](https://www.youtube.com/watch?v=WCO0vTnXfrk)