[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.html2.|2019 Latest Braindump2go CAS-003 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharingNew QuestionA 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: CDExplanation: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 effectivenessQuality initiatives and certificationsTechnology, infrastructure stability, and applications Security and audit controlsLegal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors InsuranceDisaster recovery and business continuity policiesC and D form part of Security and audit controls.New QuestionAn 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 integrationB. Security standards and training is performed as part of the projectC. Daily stand-up meetings are held to ensure security requirements are understoodD. For each major iteration penetration testing is performedE. Security requirements are story boarded and make it into the buildF. A security design is performed at the end of the requirements phaseAnswer: 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 QuestionAn 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/passwdB. /etc/shadowC. /etc/securityD. /etc/passwordE. /sbin/logonF. /bin/bashAnswer: ABExplanation: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 QuestionJoe 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.

Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirements. Test the product and make a product recommendation.B. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased. C. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.D. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provider. Give access to internal security employees so that they can inspect the application payload data.E. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.Answer: AExplanation:A request for a Proposal (RFP) is in essence an invitation that you present to vendors asking them to submit proposals on a specific commodity or service. This should be evaluated, then the product should be tested and then a product recommendation can be made to achieve the desired outcome.New QuestionA company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.Answer: BExplanation: Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc). Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.New QuestionThe IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?A. Contact the local authorities so an investigation can be started as quickly as possible.B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.D. Refer the issue to management for handling according to the incident response process.Answer: DExplanation:The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.New QuestionA security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.Logs:Log 1:Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packetsLog 2:
HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaLog 3:Security Error AlertEvent ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the clientLog 4:Encoder oe = new OracleEncoder ();String query = "Select user_id FROM user_data WHERE user_name = ` "+ oe.encode ( req.getParameter("userID") ) + " ` and user_password = ` "+ oe.encode ( req.getParameter("pwd") ) +" ` ";VulnerabilitiesBuffer overflowSQL injectionACLXSSWhich of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).A. Log 1B. Log 2C. Log 3D. Log 4E. Buffer overflowF. ACLG. XSSH. SQL injectionAnswer: BEExplanation:Log 2 indicates that the security breach originated from an external source. And the vulnerability that can be associated with this security breach is a buffer overflow that happened when the amount of data written into the buffer exceeded the limit of that particular buffer.New QuestionA member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?A. Purchase new hardware to keep the malware isolated.B. Develop a policy to outline what will be required in the

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: DExplanation:Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation with in 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 QuestionA 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. AgileB. SDLC. WaterfallD. Joint application developmentAnswer: AExplanation: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 ssh22013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh22013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh22013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh22013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh22013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2Which 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: CEExplanation: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 QuestionA 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 trustB. Continuous chain of trustC. Chain of trust with a hardware root of trustD. Software-based trust anchor with no root of trustAnswer: CExplanation: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.html2.|2019 Latest Braindump2go CAS-003 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=WCO0vTnXfrk