This page was exported from - Braindump2go Exam Dumps Free Download
Export date: Thu Mar 28 15:04:25 2024 / +0000 GMT

[May-2018-NewValid Braindump2go CAS-003 Brain Dumps PDF 270Q Offer[78-88

2018 May New CompTIA CAS-003 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-003 Real Exam Questions:1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharing QUESTION 78An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?A. Implement data analytics to try and correlate the occurrence times.B. Implement a honey pot to capture traffic during the next attack.C. Configure the servers for high availability to handle the additional bandwidth. D. Log all traffic coming from the competitor's public IP addresses.Answer: AExplanation:There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.QUESTION 79Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.The information security team has been a part of the department meetings and come away with the following notes:Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.Sales is asking for easy order tracking to facilitate feedback to customers. Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy. Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.Which of the following departments' request is in contrast to the favored solution?A. ManufacturingB. LegalC. SalesD. Quality assuranceE. Human resourcesAnswer: EExplanation:The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite.QUESTION 80An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?A. Deploy custom HIPS signatures to detect and block the attacks. B. Validate and deploy the appropriate patch.C. Run the application in terminal services to reduce the threat landscape.D. Deploy custom NIPS signatures to detect and block the attacks.Answer: BExplanation:If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.QUESTION 81A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?A. Implement an Acceptable Use Policy which addresses malware downloads.B. Deploy a network access control system with a persistent agent.C. Enforce mandatory security awareness training for all employees and contractors.D. Block cloud-based storage software on the company network.Answer: DExplanation:The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network. We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage

services such as Dropbox or OneDrive.QUESTION 82Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:POST /login.aspx HTTP/1.1Host: comptia.orgContent-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=trueWhich of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?A. Remove all of the post data and change the request to /login.aspx from POST to GETB. Attempt to brute force all usernames and passwords using a password crackerC. Remove the txtPassword post data and change alreadyLoggedIn from false to trueD. Remove the txtUsername and txtPassword post data and toggle submit from true to falseAnswer: CExplanation:The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of `ann' and also a password of `ann'.The text "alreadyLoggedIn=false" is saying that Ann is not already logged in. To test whether we can bypass the authentication, we can attempt the login without the password and we can see if we can bypass the `alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.QUESTION 83A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?A. -45 percentB. 5.5 percentC. 45 percentD. 82 percentAnswer: DExplanation: Return on investment = Net profit / Investmentwhere:Net profit = gross profit ?expensesinvestment = stock + market outstanding[when defined as?] + claimsQUESTION 84The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0 Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1aA packet capture shows the following:09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 6553409:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534 09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534Which of the following is occurring on the network?A. A man-in-the-middle attack is underway on the network.B. An ARP flood attack is targeting at the router.C. The default gateway is being spoofed on the network.D. A denial of service attack is targeting at the router.Answer: D Explanation:The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.QUESTION 85Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500ether f8:1e:af:ab:10:a3inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5inet 192.168.1.14 netmask 0xffffff00 broadcast 192.168.1.255inet6 2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconfinet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary nd6 options=1<PERFORMNUD>media: autoselectstatus: activeGiven this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).A. The devices use EUI-64 formatB. The routers implement NDPC. The network implements 6to4 tunnelingD. The router IPv6 advertisement has been disabledE. The administrator must disable IPv6 tunnelingF. The administrator must disable the mobile IPv6 router flagG. The administrator must disable the IPv6 privacy extensionsH. The administrator must disable DHCPv6 option code 1Answer: BGExplanation:IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.QUESTION 86Drag and Drop QuestionIT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.Answer: Explanation:Vendor may accidentally or maliciously make changes to the IT system ?Allow view-only access.With view-only access, the third party can view the desktop but cannot interact with it. In other words, they cannot control the keyboard or mouse to make any changes.Desktop sharing traffic may be intercepted by network attackers ?Use SSL for remote sessions.SSL (Secure Sockets Layer) encrypts data in transit between computers. If an attacker intercepted the traffic, the data would be encrypted and therefore unreadable to the attacker. No guarantees that shoulder surfing attacks are not occurring at the vendor ?Identified control gap.Shoulder surfing is where someone else gains information by looking at your computer screen. This should be identified as a risk. A control gap occurs when

there are either insufficient or no actions taken to avoid or mitigate a significant risk.Vendor may inadvertently see confidential material from the company such as email and IMs - Limit desktop session to certain windows.The easiest way to prevent a third party from viewing your emails and IMs is to close the email and IM application windows for the duration of the desktop sharing session.QUESTION 87After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?A. The binary files used by the application have been modified by malware.B. The application is unable to perform remote attestation due to blocked ports.C. The restored image backup was encrypted with the wrong key.D. The hash key summary of hardware and installed software no longer match.Answer: DExplanation:Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system. For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation. Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.QUESTION 88Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).A. Code reviewB. SandboxC. Local proxyD. FuzzerE. Port scannerAnswer: CDExplanation:C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it.
!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download: YouTube Video: YouTube.com/watch?v=wiypGN6OqiA