[March-2019-NewBraindump2go CAS-003 PDF Dumps 401Q Free Offer

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 risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?A. Subjective and based on an individual's experience.B. Requires a high degree of upfront work to gather environment details.C. Difficult to differentiate between high, medium, and low risks.D. Allows for cost and benefit analysis.E. Calculations can be extremely complex to manage.Answer: AExplanation:Using likelihood and consequence to determine risk is known as qualitative risk analysis. With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system.After qualitative analysis has been performed, you can then perform quantitative risk analysis. A Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk. Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.New QuestionJoe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).A. Jailbroken mobile deviceB. Reconnaissance toolsC. Network enumeratorD. HTTP interceptorE. Vulnerability scannerF. Password crackerAnswer: DEExplanation:Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.To assess the security of the application server itself, you should use a vulnerability scanner.A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.New QuestionA security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?A. Memorandum of AgreementB. Interconnection Security AgreementC. Non-Disclosure AgreementD. Operating Level AgreementAnswer: BExplanation:The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.New QuestionA well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?A. Residual Risk calculationB. A cost/benefit analysisC. Quantitative Risk AnalysisD. Qualitative Risk AnalysisAnswer: CExplanation:Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.New QuestionA 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.New QuestionAn 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: BExplanation: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.New QuestionNews 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.New QuestionCompany 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.New QuestionWireless 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.New QuestionA 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.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.!!!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