This page was exported from - Braindump2go Exam Dumps Free Download
Export date: Thu Mar 28 15:50:38 2024 / +0000 GMT

[May-2018-NewExam Pass 100%!Braindump2go CAS-003 VCE and CAS-003 PDF 270Q Instant Download[56-66

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 56A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).A. Use AES in Electronic Codebook modeB. Use RC4 in Cipher Block Chaining modeC. Use RC4 with Fixed IV generationD. Use AES with cipher text paddingE. Use RC4 with a nonce generated IVF. Use AES in Counter modeAnswer: EFExplanation:In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.QUESTION 57A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?A. Use fuzzing techniques to examine application inputsB. Run nmap to attach to application memoryC. Use a packet analyzer to inspect the stringsD. Initiate a core dump of the applicationE. Use an HTTP interceptor to capture the text stringsAnswer: DExplanation:Applications store information in memory and this information include sensitive data, passwords, and usernames and encryption keys. Conducting memory/core dumping will allow you to analyze the memory content and then you can test that the strings are indeed encrypted.QUESTION 58The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?A. Revise the corporate policy to include possible termination as a result of violationsB. Increase the frequency and distribution of the USB violations reportC. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offenseD. Implement group policy objectsAnswer: DExplanation:A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.QUESTION 59An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?A. Replicate NAS changes to the tape backups at the other datacenter.B. Ensure each server has two HBAs connected through two routes to the NAS.C. Establish deduplication across diverse storage paths.D. Establish a SAN that replicates between datacenters.Answer: DExplanation:A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN. Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array- based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN)

or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site.QUESTION 60An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).A. Implement hashing of data in transitB. Session recording and captureC. Disable cross session cut and pasteD. Monitor approved credit accountsE. User access audit reviewsF. Source IP whitelistingAnswer: CEFExplanation:Data sovereignty is a legal concern where the data is governed by the laws of the country in which the data resides. In this scenario the company does not want the data to fall under the law of the country of the organization to whom back office process has be outsourced to. Therefore we must ensure that data can only be accessed on local servers and no copies are held on computers of the outsource partner. It is important therefore to prevent cut and paste operations.Privacy concerns can be addressed by ensuring the unauthorized users do not have access to the data. This can be accomplished though user access auditing, which needs to be reviewed on an ongoing basis; and source IP whitelisting, which is a list of IP addresses that are explicitly allowed access to the system.QUESTION 61The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?A. HIPSB. UTMC. AntivirusD. NIPSE. DLPAnswer: AExplanation:In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.QUESTION 62An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?A. Use the pass the hash techniqueB. Use rainbow tables to crack the passwordsC. Use the existing access to change the passwordD. Use social engineering to obtain the actual passwordAnswer: AExplanation:With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.QUESTION 63 Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).A. Check log files for logins from unauthorized IPs.B. Check /proc/kmem for fragmented memory segments.C. Check for unencrypted passwords in /etc/shadow.D. Check timestamps for files modified around time of compromise.E. Use lsof to determine files with future timestamps.F. Use gpg to encrypt compromised data files.G. Verify the MD5 checksum of system binaries.H. Use vmstat to look for excessive disk I/O.Answer: ADGExplanation:The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.QUESTION 64The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?A. Develop an information classification scheme that will properly secure data on corporate systems.B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.C. Publish a policy that addresses the security requirements for working remotely with company equipment.D. Work with mid-level managers to identify and document the proper procedures for telecommuting.Answer: CExplanation:The question states that "the organization has not addressed telecommuting in the past". It is

therefore unlikely that a company policy exists for telecommuting workers. There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies. In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.QUESTION 65A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.Proposal:External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?A. -$30,000B. $120,000C. $150,000D. $180,000Answer: AExplanation:Return on investment = Net profit / Investmentwhere:Net profit = gross profit expenses.orReturn on investment = (gain from investment - cost of investment) / cost of investment Subscriptions = 5,000 x 12 = 60,000 per annum10 incidents @ 10,000 = 100.000 per annumreduce by 50% = 50,000 per annum Thus the rate of Return is -10,000 per annum and that makes for -$30,000 after three years.QUESTION 66A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?A. Remove contact details from the domain name registrar to prevent social engineering attacks.B. Test external interfaces to see how they function when they process fragmented IP packets.C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.Answer: BExplanation:Fragmented IP packets are often used to evade firewalls or intrusion detection systems.Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port).One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan.Fragmented packet Port ScanThe scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.!!!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