[May-2018-New100% Success-Braindump2go CAS-003 VCE and PDF Dumps 270Q Instant Download[67-77

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 67A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?A. Determining how to install HIPS across all server platforms to prevent future incidentsB. Preventing the ransomware from re-infecting the server upon restore C. Validating the integrity of the deduplicated dataD. Restoring the data will be difficult without the application configurationAnswer: DExplanation:Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.Since the backup application configuration is not accessible, it will require more effort to recover the data.Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.QUESTION 68An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?A. Implementing federated network access with the third party.B. Using a HSM at the network perimeter to handle network device access.C. Using a VPN concentrator which supports dual factor via hardware tokens.D. Implementing 802.1x with EAP-TTLS across the infrastructure.Answer: DExplanation:IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.QUESTION 69The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?A. The company should mitigate the risk.B. The company should transfer the risk.C. The company should avoid the risk.D. The company should accept the risk.Answer: BExplanation:To transfer the risk is to deflect it to a third party, by taking out insurance for example.QUESTION 70A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?A. A separate physical interface placed on a private VLAN should be configured for live host operations.B. Database record encryption should be used when storing sensitive information on virtual servers.C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of

sensitive data.D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.Answer: A Explanation:VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.QUESTION 71An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?A. Independent verification and validationB. Security test and evaluationC. Risk assessmentD. Ongoing authorizationAnswer: DExplanation:Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time. Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.QUESTION 72During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?A. Notify senior management, secure the scene, capture volatile storage, capture non- volatile storage, implement chain of custody, and analyze original media.B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.C. Implement chain of custody, take inventory, secure the scene, capture volatile and non- volatile storage, and document the findings.D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.Answer: DExplanation:The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.QUESTION 73A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?A. Spiral modelB. Incremental modelC. Waterfall modelD. Agile modelAnswer: C Explanation:The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through identified phases.QUESTION 74The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?A. Race conditionB. Click-jackingC. Integer overflowD. Use after freeE. SQL injectionAnswer: CExplanation:Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.QUESTION 75The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?A. $6,000B. $24,000C. $30,000D. $96,000Answer: AExplanation:Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)SLE = AV x EF = $120 000 x 20% = $ 24,000 (this is over 4 years) Thus ALE = $ 24,000 / 4 = $ 6,000QUESTION 76A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:10.235.62.11 - [02/Mar/2014:06:13:04] "GET/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.B. The security administrator is concerned with XSS, and the developer should normalize Unicode

characters on the browser side.C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.Answer: CExplanation:The code in the question is an example of a SQL Injection attack. The code `1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation. 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.QUESTION 77Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string:user@hostname:~$ sudo nmap -O 192.168.1.54Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:TCP/22TCP/111 TCP/512-514TCP/2049TCP/32778Based on this information, which of the following operating systems is MOST likely running on the unknown node?A. LinuxB. WindowsC. SolarisD. OSXAnswer: CExplanation:TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.!!!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