This page was exported from - Braindump2go Exam Dumps Free Download
Export date: Fri Mar 29 7:29:36 2024 / +0000 GMT

[May-2018-NewFree CAS-003 PDF and VCE Dumps Offered by Braindump2go[1-11

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=sharingQUESTION 1A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information: Which of the following commands would have provided this output?A. arp -sB. netstat -aC. ifconfig -arpD. sqlmap -w**Answer: B**QUESTION 2A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?A. SPFB. S/MIMEC. TLSD. DKIM**Answer: D**QUESTION 3A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacksB. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patchesC. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for useD. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functionsE. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authenticationF. Implement application blacklisting enforced by the operating systems of all machines in the enterprise**Answer: CD**QUESTION 4A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?A. Multi-tenancy SaaSB. Hybrid IaaSC. Single-tenancy PaaSD. Community IaaS**Answer: C**QUESTION 5Drag and Drop QuestionA security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once. Answer: QUESTION 6Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?A. Key risk indicatorsB. Lessons learnedC. Recovery point objectivesD. Tabletop exercise**Answer: A**QUESTION 7A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows: The tool needs to be responsive so service teams can query it, and then perform an automated response action. The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs. The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.Which of the following need specific attention to meet the requirements listed above? (Choose three.)A. ScalabilityB. LatencyC. AvailabilityD. UsabilityE. RecoverabilityF. Maintainability**Answer: BCE**QUESTION 8After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements: Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?A. Product AB. Product BC. Product CD. Product DE. Product E**Answer: E**QUESTION 9A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?A. The OS version is not compatibleB. The OEM is prohibitedC. The device does not support FDED. The device is rooted**Answer: D**QUESTION 10A security administrator was informed that a server unexpectedly

rebooted. The administrator received an export of syslog entries for analysis: Which of the following does the log sample indicate? (Choose two.)A. A root user performed an injection attack via kernel moduleB. Encrypted payroll data was successfully decrypted by the attackerC. Jsmith successfully used a privilege escalation attackD. Payroll data was exfiltrated to an attacker-controlled hostE. Buffer overflow in memory paging caused a kernel panicF. Syslog entries were lost due to the host being rebooted**Answer: CE**QUESTION 11The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controlsB. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awarenessC. corporate general counsel requires a single system boundary to determine overall corporate risk exposureD. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns**Answer: A**!!!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