[May-2018-NewBraindump2go CAS-003 Dumps VCE and PDF 270Q Free Offer[45-55

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 45A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following: Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)A. Install HIPSB. Enable DLPC. Install EDRD. Install HIDSE. Enable application blacklistingF. Improve patch management processesAnswer: BEQUESTION 46A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client- facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?A. Install a HIPS on the web serversB. Disable inbound traffic from offending sourcesC. Disable SNMP on the web serversD. Install anti-DDoS protection in the DMZAnswer: AQUESTION 47An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website. Which of the following types of attack vector did the penetration tester use?A. SQLiB. CSRFC. Brute forceD. XSSE. TOC/TOUAnswer: BQUESTION 48A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltrationB. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threatC. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threatsD. The company should install a temporary CCTV system to detect unauthorized access to physical officesAnswer: AQUESTION 49An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?A. The employee manually changed the email client retention settings to prevent deletion of emailsB. The file that contained the damaging information was mistagged and retained on the server for longer than it should have beenC. The email was encrypted and an exception was put in place via the data classification applicationD. The employee saved a file on the computer's hard drive that contained archives of emails, which were more than two years oldAnswer: DQUESTION 50An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)A. Black box testingB. Gray box testingC. Code reviewD. Social engineeringE. Vulnerability assessmentF. PivotingG. Self-assessmentH. White teamingI. External auditingAnswer: AEFQUESTION 51An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)A. Magic link sent to an email addressB. Customer ID sent via push notificationC. SMS with OTP sent to a mobile numberD. Third-party social loginE. Certificate sent to be installed on a device F. Hardware tokens sent to customersAnswer: CEQUESTION 52A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?A. Issue digital certificates to all users, including

owners of group mailboxes, and enable S/MIMEB. Federate with an existing PKI provider, and reject all non-signed emailsC. Implement two-factor email authentication, and require users to hash all email messages upon receiptD. Provide digital certificates to all systems, and eliminate the user group or shared mailboxesAnswer: AQUESTION 53The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).A. Block traffic from the ISP's networks destined for blacklisted IPs.B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.D. Notify customers when services they run are involved in an attack. E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.Answer: DEExplanation:Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.QUESTION 54The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.Answer: BExplanation:Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field.QUESTION 55A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated. Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.Which of the following meets these requirements?A. Use OpenID and allow a third party to authenticate users.B. Use TLS with a shared client certificate for all users.C. Use SAML with federated directory services.D. Use Kerberos and browsers that support SAML.Answer: AExplanation:Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again. Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam.!!!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