[November/2018Valid Braindump2go CS0-001 PDF Dumps 191Q Offer[Q109-Q119

2018/November Braindump2go CS0-001 Exam Dumps with PDF and VCE New Updated Today! Following are some new CS0-001 Real Exam Questions:1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 191Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Exam Questions & Answers Download: **https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharing**QUESTION 109Given the following access log: Which of the following accurately describes what this log displays?A. A vulnerability in jQueryB. Application integration with an externally hosted databaseC. A vulnerability scan performed from the InternetD. A vulnerability in Javascript **Answer: C**QUESTION 110A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following: Which of the following mitigation techniques is MOST effective against the above attack?A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.C. The company should implement the following ACL at their gateway firewall:DENY IP HOST 192.168.1.1 170.43.30.0/24.D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.**Answer: A**QUESTION 111An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).A. Drive adaptersB. Chain of custody form C. Write blockersD. Crime tapeE. Hashing utilitiesF. Drive imager**Answer: BC**QUESTION 112A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?A. A compensating controlB. Altering the password policyC. Creating new account management proceduresD. Encrypting authentication traffic**Answer: D**QUESTION 113A threat intelligence analyst who works for a financial services firm received this report:"There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called "LockMaster" by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector." The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions should the analyst do NEXT? (Select TWO).A. Advise the firewall engineer to implement a block on the domainB. Visit the domain and begin a threat assessmentC. Produce a threat intelligence message to be disseminated to the companyD. Advise the security architects to enable full-disk encryption to protect the MBRE. Advise the security analysts to add an alert in the SIEM on the string "LockMaster"F. Format the MBR as a precaution**Answer: BD** QUESTION 114The Chief Information Security Officer (CISO) has asked the security staff to identify a framework on which to base the security program. The CISO would like to achieve a certification showing the security program meets all required best practices. Which of the following would be the BEST choice?A. OSSIMB. SDLCC. SANSD. ISO**Answer: D**QUESTION 115A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).A. Prevent users from accessing personal email and file-sharing sites via web proxyB. Prevent flash drives from connecting to USB ports using Group PolicyC. Prevent users from copying data from workstation to workstationD. Prevent users from using roaming profiles when changing workstationsE. Prevent Internet access on laptops unless connected to the network in the office or via VPNF. Prevent users from being able to use the copy and paste functions**Answer: ABE**QUESTION 116The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?A. Activate the escalation checklistB. Implement the incident response planC. Analyze the forensic imageD. Perform evidence acquisitionAnswer: DExplanation:**https://staff.washington.edu/dittrich/misc/forensics/**QUESTION 117A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud- based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?B. The cloud providerC. The data ownerD. The cybersecurity analystE. The system administrator**Answer: B** QUESTION 118A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?A. Reserved MACsB. Host IPsC. DNS routing tablesD. Gateway settings **Answer: A**QUESTION 119An executive tasked a security analyst to aggregate past logs, traffic, and alerts on a particular attack vector. The analyst was then tasked with analyzing the data and making predictions on future complications regarding this attack

vector. Which of the following types of analysis is the security analyst MOST likely conducting?A. Trend analysisB. Behavior analysisC. Availability analysisD. Business analysis**Answer: A**!!!RECOMMEND!!!1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 191Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Study Guide Video: YouTube Video: YouTube.com/watch?v=Glotb7fHvk4