# [November/2018100% Success-Braindump2go CS0-001 VCE and CS0-001 PDF 191Q Instant Download[Q98-Q108

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 98Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated "Critical". The administrator observed the following about the three servers:The servers are not accessible by the InternetAV programs indicate the servers have had malware as recently as two weeks ago The SIEM shows unusual traffic in the last 20 days Integrity validation of system files indicates unauthorized modifications Which of the following assessments is valid and what is the most appropriate NEXT step? (Select TWO).A. Servers may have been built inconsistentlyB. Servers may be generating false positives via the SIEMC. Servers may have been tampered withD. Activate the incident response planE. Immediately rebuild servers from known good configurationsF. Schedule recurring vulnerability scans on the servers**Answer: DE**QUESTION 99When reviewing network traffic, a security analyst detects suspicious activity: Based on the log above, which of the following vulnerability attacks is occurring?A. ShellShockB. DROWNC. ZeusD. HeartbleedE. POODLE**Answer: E**QUESTION 100An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?A. ImpersonationB. Privilege escalationC. Directory traversalD. Input injection**Answer: C**QUESTION 101Following a data compromise, a cybersecurity analyst noticed the following executed query:SELECT * from Users WHERE name = rick OR 1=1 Which of the following attacks occurred, and which of the following technical security controls would BEST reduce the risk of future impact from this attack? (Select TWO).A. Cookie encryptionB. XSS attackC. Parameter validationD. Character blacklistE. Malicious code executionF. SQL injectionAnswer: CFExplanation:**https://lwn.net/Articles/177037/**QUESTION 102 A security analyst is conducting traffic analysis and observes an HTTP POST to a web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?A. ExfiltrationB. DoSC. Buffer overflowD. SQL injection**Answer: A**QUESTION 103While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.B. Perform a network scan and identify rogue devices that may be generating the observed traffic.Remove those devices from the network.C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.**Answer: A**QUESTION 104Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?A. Threat intelligenceB. Threat informationC. Threat dataD. Advanced persistent threats**Answer: A** QUESTION 105During a web application vulnerability scan, it was discovered that the application would display inappropriate data after certain key phrases were entered into a webform connected to a SQL database server. Which of the following should be used to reduce the likelihood of this type of attack returning sensitive data?A. Static code analysisB. Peer review codeC. Input validationD. Application fuzzing**Answer: C**QUESTION 106A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.B. The file server is attempting to transfer malware to the workstation via SMB.C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.D. An attacker has gained control of the workstation and is port scanning the network.**Answer: C**QUESTION 107A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago.

However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?A. Invest in and implement a solution to ensure non-repudiationB. Force a daily password changeC. Send an email asking users not to share their credentialsD. Run a report on all users sharing their credentials and alert their managers of further actions**Answer: C**QUESTION 108A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions should the analyst do FIRST?A. Contact the Office of Civil Rights (OCR) to report the breachB. Notify the Chief Privacy Officer (CPO)C. Activate the incident response planD. Put an ACL on the gateway router**Answer: D**
!!!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