This page was exported from - Braindump2go Free Exam Dumps with PDF and VCE Collection
Export date: Thu Nov 21 22:44:02 2024 / +0000 GMT

[2017-New-ExamsBraindump2go CS0-001 Exam Questions Instant Download[1-10

2017 May New CompTIA CS0-001 Exam Dumps with VCE and PDF Updated in www.Braindump2go.com Today!100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|2017 Version New CS0-001 Exam Dumps (VCE & PDF) 85Q&As Download: http://www.braindump2go.com/cs0-001.html 2.|2017 Version New CS0-001 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharing QUESTION 11A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer? A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation. Answer: A QUESTION 12A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website? A. VPNB. HoneypotC. WhitelistingD. DMZE. MAC filtering Answer: C QUESTION 13A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types `history' into the prompt, and sees this line of code in the latest bash history: This concerns the analyst because this subnet should not be known to users within the company. Which of the following describes what this code has done on the network? A. Performed a ping sweep of the Class C network.B. Performed a half open SYB scan on the network.C. Sent 255 ping packets to each host on the network.D. Sequentially sent an ICMP echo reply to the Class C network. Answer: A QUESTION 14A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response? A. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.B. Change all devices and servers that support it to 636, as encrypted services run by default on 636.C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636. Answer: B QUESTION 15A security analyst is reviewing IDS logs and notices the following entry: Which of the following attacks is occurring? A. Cross-site scriptingB. Header manipulationC. SQL injectionD. XML injection Answer: C QUESTION 16A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details? A. Acceptable use policyB. Service level agreementC. Rules of engagementD. Memorandum of understandingE. Master service agreement Answer: B QUESTION 17A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover? A. POS malwareB. RootkitC. Key loggerD. Ransomware Answer: A QUESTION 18Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.) A. COBITB. NISTC. ISO 27000 seriesD. ITILE. OWASP Answer: DE QUESTION 19A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following if the MOST likely explanation for this? A. The administrator entered the wrong IP range for the assessment.B. The administrator did not wait long enough after applying the patch to run the assessment.C. The patch did not remediate the vulnerability.D. The vulnerability assessment returned false positives. Answer: C QUESTION 20An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue.Which of the following should be applied? A. MACB. TAPC. NACD. ACL Answer: C !!!RECOMMEND!!! 1.|2017 Version New CS0-001 Exam Dumps (VCE & PDF) 85Q&As Download: http://www.braindump2go.com/cs0-001.html 2.|2017 Version New CS0-001 Study Guide Video: YouTube Video:

YouTube.com/watch?v=ZR1G8DM-DRA