[2017-New-ExamsBraindump2go CS0-001 PDF and VCE Free Download[31-40

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 31A system administrator has reviewed the following output: Which of the following can a system administrator infer from the above output? A. The company email server is running a non-standard port.B. The company email server has been compromised.C. The company is running a vulnerable SSH server.D. The company web server has been compromised. Answer: A QUESTION 32An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement? A. HoneypotB. Jump boxC. SandboxingD. Virtualization Answer: A QUESTION 33An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure? A. Configure a script to automatically update the scanning tool.B. Manually validate that the existing update is being performed.C. Test vulnerability remediation in a sandbox before deploying.D. Configure vulnerability scans to run in credentialed mode. Answer: A QUESTION 34A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause? A. Attackers are running reconnaissance on company resources.B. Commands are attempting to reach a system infected with a botnet trojan.C. An insider is trying to exfiltrate information to a remote network. D. Malware is running on a company system. Answer: B QUESTION 35Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement? A. Forensic analysis reportB. Chain of custody reportC. Trends analysis reportD. Lessons learned report Answer: A QUESTION 36After scanning the main company's website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning: The analyst reviews a snippet of the offending code: Which of the following is the BEST course of action based on the above warning and code snippet? A. The analyst should implement a scanner exception for the false positive.B. The system administrator should disable SSL and implement TLS.C. The developer should review the code and implement a code fix.D. The organization should update the browser GPO to resolve the issue. Answer: D QUESTION 37An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability? A. Perform an unauthenticated vulnerability scan on all servers in the environment.B. Perform a scan for the specific vulnerability on all web servers.C. Perform a web vulnerability scan on all servers in the environment.D. Perform an authenticated scan on all web servers in the environment. Answer: B QUESTION 38Which of the following commands would a security analyst use to make a copy of an image for forensics use? A. ddB. wgetC. touchD. rm Answer: A QUESTION 39As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.) A. Timing of the scanB. Contents of the executive summary reportC. Excluded hostsD. Maintenance windowsE. IPS configurationF. Incident response policies Answer: AC QUESTION 40An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software.Which of the following BEST describes the type of threat in this situation? A. Packet of deathB. Zero-day malwareC. PII exfiltrationD. Known virus Answer: B !!!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