[2017-New-ExamsInstant CS0-001 Exam Dumps VCE Free Download in Braindump2go[21-30

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 21Review the following results: Which of the following has occurred? A. This is normal network traffic.B. 123.120.110.212 is infected with a Trojan.C. 172.29.0.109 is infected with a worm.D. 172.29.0.109 is infected with a Trojan. Answer: A QUESTION 22A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements? A. Utilizing an operating system SCAP pluginB. Utilizing an authorized credential scanC. Utilizing a non-credential scanD. Utilizing a known malware plugin Answer: A QUESTION 23A network technician is concerned that an attacker is attempting to penetrate the network, and wants to set a rule on the firewall to prevent the attacker from learning which IP addresses are valid on the network. Which of the following protocols needs to be denied? A. TCPB. SMTPC. ICMPD. ARP Answer: C QUESTION 24An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use? A. WiresharkB. QualysC. netstatD. nmapE. ping Answer: C QUESTION 25In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed? A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first. Answer: D QUESTION 26An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed? A. Anti-malware application B. Host-based IDSC. TPM data sealingD. File integrity monitoring Answer: C QUESTION 27A security analyst is reviewing the following log after enabling key-based authentication. Given the above information, which of the following steps should be performed NEXT to secure the system? A. Disable anonymous SSH logins.B. Disable password authentication for SSH.C. Disable SSHv1.D. Disable remote root SSH logins. Answer: B QUESTION 28A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform? A. Continue monitoring critical systems.B. Shut down all server interfaces.C. Inform management of the incident.D. Inform users regarding the affected systems. Answer: C QUESTION 29A security professional is analyzing the results of a network utilization report. The report includes the following information: Which of the following servers needs further investigation? A. hr.dbprod.01B. R&D.file.srvr.01C. mrktg.file.srvr.02D. web.srvr.03 Answer: BSection: (none)Explanation/Reference: QUESTION 30A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform? A. Use the IP addresses to search through the event logs.B. Analyze the trends of the events while manually reviewing to see if any of the indicators match.C. Create an advanced query that includes all of the indicators, and review any of the matches.D. Scan for vulnerabilities with exploits known to have been used by an APT. 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