[CySA+ CS0-001 DumpsCS0-001 PDF Dumps(Full Version)321Q Download in Braindump2go(Q253-Q263)

2019/Feb Braindump2go CS0-001 Exam Dumps with PDF and VCE New Updated Today! Following are some new CS0-001 Real Exam Questions:1.|2019 Latest CS0-001 Exam Dumps (PDF & VCE) 321Q&As Instant Download:https://www.braindump2go.com/cs0-001.html2.|2019 Latest CS0-001 ExamQuestions & Answers Instant Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharingQUESTION 253A security analyst is reviewing packet captures to determine the extent of success during an attacker's reconnaissance phase following a recent incident.The following is a hex and ASCII dump of one such packet: Which of the following BEST describes this packet?A. DNS BIND version requestB. DNS over UDP standard queryC. DNS over TCP server status queryD. DNS zone transfer request **Answer: A**QUESTION 254A security operations team was alerted to abnormal DNS activity coming from a user's machine. The team performed a forensic investigation and discovered a host had been compromised. Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?A. PhishingB. PharmingC. Cache poisoningD. Data exfiltration**Answer: D**QUESTION 255Which of the following is the MOST secure method to perform dynamic analysis of malware that can sense when it is in a virtual environment?A. Place the malware on an isolated virtual server disconnected from the network.B. Place the malware in a virtual server that is running Windows and is connected to the network.C. Place the malware on a virtual server connected to a VLAN.D. Place the malware on a virtual server running SIFT and begin analysis.**Answer: A**QUESTION 256A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?A. Increase scan frequency.B. Perform credentialed scans.C. Update the security incident response plan.D. Reconfigure scanner to brute force mechanisms.**Answer: B**QUESTION 257Given a packet capture of the following scan: Which of the following should MOST likely be inferred on the scan's output?A. 192.168.1.115 is hosting a web server.B. 192.168.1.55 is hosting a web server. C. 192.168.1.55 is a Linux server.D. 192.168.1.55 is a file server.**Answer: D**QUESTION 258A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim's browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company's website?A. Logic bombB. RootkitC. Privilege escalationD. Cross-site scripting**Answer: D** QUESTION 259After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?A. To create a chain of evidence to demonstrate when the servers were patched.B. To harden the servers against new attacks.C. To provide validation that the remediation was active.D. To generate log data for unreleased patches.**Answer: B**QUESTION 260While reviewing web server logs, a security analyst notices the following code: Which of the following would prevent this code from performing malicious actions?A. Performing web application penetration testingB. Requiring the application to use input validationC. Disabling the use of HTTP and requiring the use of HTTPSD. Installing a network firewall in front of the application**Answer: C** QUESTION 261The board of directors made the decision to adopt a cloud-first strategy. The current security infrastructure was designed for on-premise implementation. A critical application that is subject to the Federal Information Security Management Act (FISMA) of 2002 compliance has been identified as a candidate for a hybrid cloud deployment model. Which of the following should be conducted FIRST?A. Develop a request for proposal.B. Perform a risk assessment.C. Review current security controls.D. Review the SLA for FISMA compliance.**Answer: C**QUESTION 262Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection. Which of the following should Joe use to BEST accommodate the vendor?A. Allow incoming IPSec traffic into the vendor's IP address.B. Set up a VPN account for the vendor, allowing access to the remote site.C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.D. Write a firewall rule to allow the vendor to have access to the remote site.**Answer: B**QUESTION 263A company's computer was recently infected with ransomware. After encrypting all documents, the malware logs a random AES-128 encryption key and associated unique identifier onto a compromised remote website. A ransomware code snippet is shown below: Based on the information from the code snippet, which of the following is the BEST way for a cybersecurity professional to monitor for the same malware in the future?A. Configure the company proxy server to deny connections to www.malwaresite.com.B. Reconfigure the enterprise antivirus to push more frequent to the clients.C. Write an ACL to block the IP address of www.malwaresite.com at the gateway firewall.D. Use an IDS custom

signature to create an alert for connections to www.malwaresite.com.**Answer: A**!!!RECOMMEND!!!1.|2019 Latest CS0-001 Exam Dumps (PDF & VCE) 321Q&As Instant Download:https://www.braindump2go.com/cs0-001.html2.|2019 Latest CS0-001 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=ZV4LytVliIk