[19/Feb/2019 Updated Professional 321q CS0-001 Braindump For Free Download Now

New Updated CS0-001 Exam Questions from PassLeader CS0-001 PDF dumps! Welcome to download the newest PassLeader CS0-001 VCE dumps:&#160;https://www.passleader.com/cs0-001.html (321 Q&As) Keywords: CS0-001 exam dumps, CS0-001 exam questions, CS0-001 VCE dumps, CS0-001 PDF dumps, CS0-001 practice tests, CS0-001 study guide, CS0-001 braindumps, CompTIA Cybersecurity Analyst (CSA+) Exam P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ NEW QUESTION 300 A 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.&#160;&#160;&#160; Phishing B.&#160;&#160;&#160; Pharming C.&#160;&#160;&#160; Cache poisoning D.&#160;&#160;&#160; Data exfiltration Answer: D NEW QUESTION 301 Which 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.&#160;&#160;&#160; Place the malware on an isolated virtual server disconnected from the network. B.&#160;&#160;&#160; Place the malware in a virtual server that is running Windows and is connected to the network. C.&#160;&#160;&#160; Place the malware on a virtual server connected to a VLAN. D.&#160;&#160;&#160; Place the malware on a virtual server running SIFT and begin analysis. Answer: A NEW QUESTION 302 A 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.&#160;&#160;&#160; Increase scan frequency. B.&#160;&#160;&#160; Perform credentialed scans. C.&#160;&#160;&#160; Update the security incident response plan. D.&#160;&#160;&#160; Reconfigure scanner to brute force mechanisms. Answer: B NEW QUESTION 303 A 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.&#160;&#160;&#160; Logic bomb B.&#160;&#160;&#160; Rootkit C.&#160;&#160;&#160; Privilege escalation D.&#160;&#160;&#160; Cross-site scripting Answer: D NEW QUESTION 304 After 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.&#160;&#160;&#160; To create a chain of evidence to demonstrate when the servers were patched. B.&#160;&#160;&#160; To harden the servers against new attacks. C.&#160;&#160;&#160; To provide validation that the remediation was active. D.&#160;&#160;&#160; To generate log data for unreleased patches. Answer: B NEW QUESTION 305 The 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.&#160;&#160;&#160; Develop a request for proposal. B.&#160;&#160;&#160; Perform a risk assessment. C.&#160;&#160;&#160; Review current security controls. D.&#160;&#160;&#160; Review the SLA for FISMA compliance. Answer: C NEW QUESTION 306 Joe, 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.&#160;&#160;&#160; Allow incoming IPSec traffic into the vendor's IP address. B.&#160;&#160;&#160; Set up a VPN account for the vendor, allowing access to the remote site. C.&#160;&#160;&#160; Turn off the firewall while the vendor is in the office, allowing access to the remote site. D.&#160;&#160;&#160; Write a firewall rule to allow the vendor to have access to the remote site. Answer: B NEW QUESTION 307 A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal? A.&#160;&#160;&#160; Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources. B.&#160;&#160;&#160; Open port 3389 on the firewall to the server to allow users to connect remotely. C.&#160;&#160;&#160; Set up a jump box for all help desk personnel to remotely access system resources. D.&#160;&#160;&#160; Use the company's existing web server for remote access and configure over port 8080. Answer: A NEW QUESTION 308 After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)

A.&#160;&#160;&#160; Data ownership policy B.&#160;&#160;&#160; Password policy C.&#160;&#160;&#160; Data classification policy D.&#160;&#160;&#160; Data retention policy E.&#160;&#160;&#160; Acceptable use policy F.&#160;&#160;&#160; Account management policy Answer: BF NEW QUESTION 309 Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of- cycle vulnerability scan? A.&#160;&#160;&#160; Newly discovered PII on a server. B.&#160;&#160;&#160; A vendor releases a critical patch update. C.&#160;&#160;&#160; A critical bug fix in the organization's application. D.&#160;&#160;&#160; False positives identified in production. Answer: B NEW QUESTION 310 A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company's firewall, while all production networks are protected by a stateful firewall. Which of the following would BEST allow an external penetration tester to determine which one is the honeynet's network? A.&#160;&#160;&#160; Banner grab B.&#160;&#160;&#160; Packet analyzer C.&#160;&#160;&#160; Fuzzer D.&#160;&#160;&#160; TCP ACK scan Answer: D NEW QUESTION 311 A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value? A.&#160;&#160;&#160; Access control list network segmentation that prevents access to the SCADA devices inside the network. B.&#160;&#160;&#160; Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices. C.&#160;&#160;&#160; Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network. D.&#160;&#160;&#160; SCADA systems configured with `SCADA SUPPORT'=ENABLE. Answer: B NEW QUESTION 312 A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ: - SQL injection on an infrequently used web server that provides files to vendors - SSL/TLS not used for a website that contains promotional information The scan also shows the following vulnerabilities on internal resources: - Microsoft Office Remote Code Execution on test server for a human resources system - TLS downgrade vulnerability on a server in a development network In order of risk, which of the following should be patched FIRST? A.&#160;&#160;&#160; Microsoft Office Remote Code Execution B.&#160;&#160;&#160; SQL injection C.&#160;&#160;&#160; SSL/TLS not used D.&#160;&#160;&#160; TLS downgrade Answer: A NEW QUESTION 313 A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring? A.&#160;&#160;&#160; Personnel training B.&#160;&#160;&#160; Separation of duties C.&#160;&#160;&#160; Mandatory vacation D.&#160;&#160;&#160; Backup server Answer: D NEW QUESTION 314 While reviewing three months of logs, a security analyst notices probes from random company laptops going to SCADA equipment at the company's manufacturing location. Some of the probes are getting responses from the equipment even though firewall rules are in place, which should block this type of unauthorized activity. Which of the following should the analyst recommend to keep this activity from originating from company laptops? A.&#160;&#160;&#160; Implement a group policy on company systems to block access to SCADA networks. B.&#160;&#160;&#160; Require connections to the SCADA network to go through a forwarding proxy. C.&#160;&#160;&#160; Update the firewall rules to block SCADA network access from those laptop IP addresses. D.&#160;&#160;&#160; Install security software and a host-based firewall on the SCADA equipment. Answer: A NEW QUESTION 315 An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use? A.&#160;&#160;&#160; CIS benchmark B.&#160;&#160;&#160; Nagios C.&#160;&#160;&#160; OWASP D.&#160;&#160;&#160; Untidy E.&#160;&#160;&#160; Cain & Abel Answer: A NEW QUESTION 316 A company provides wireless connectivity to the internal network from all physical locations for company-owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem? A.&#160;&#160;&#160; The access point is blocking access by MAC address. Disable MAC address filtering. B.&#160;&#160;&#160; The network is not available. Escalate the issue to network support. C.&#160;&#160;&#160; Expired DNS entries on users' devices. Request the affected users perform a DNS flush. D.&#160;&#160;&#160; The access point is a rogue device. Follow incident response procedures. Answer: D NEW QUESTION 317 ...... Download the newest PassLeader CS0-001 dumps from passleader.com now! 100% Pass Guarantee! CS0-001 PDF dumps & CS0-001 VCE dumps:&#160;https://www.passleader.com/cs0-001.html (321 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ