This page was exported from - Actual Test Dumps With VCE and PDF Download
Export date: Thu Mar 28 23:54:10 2024 / +0000 GMT

[May-2017 Dumps Premium 85q CS0-001 Exam Questions Download From PassLeader

New Updated CS0-001 Exam Questions from PassLeader CS0-001 PDF dumps! Welcome to download the newest PassLeader CS0-001 VCE dumps: http://www.passleader.com/cs0-001.html (85 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 1**Which of the following BEST describes the offensive participants in a tabletop exercise? A. Red teamB. Blue teamC. System administratorsD. Security analystsE. Operations team **Answer: A NEW QUESTION 2**After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of ____. A. privilege escalationB. advanced persistent threatC. malicious insider threatD. spear phishing **Answer: B NEW QUESTION 3**A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.) A. Succession planningB. Separation of dutiesC. Mandatory vacationD. Personnel trainingE. Job rotation **Answer: BD NEW QUESTION 4**A security analyst received a compromised workstation. The workstation's hard drive may contain evidence of criminal activities. Which of the following is the FIRST thing the analyst must do to ensure the integrity of the hard drive while performing the analysis? A. Make a copy of the hard drive.B. Use write blockers.C. Runrm -Rcommand to create a hash.D. Install it on a different machine and explore the content. **Answer: B NEW QUESTION 5**File integrity monitoring states the following files have been changed without a written request or approved change. The following change has been made:chmod 777 -Rv /usrWhich of the following may be occurring? A. The ownership pf /usr has been changed to the current user.B. Administrative functions have been locked from users.C. Administrative commands have been made world readable/writable.D. The ownership of/usr has been changed to the root user. **Answer: C NEW QUESTION 6**A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT? A. The analyst should create a backup of the drive and then hash the drive.B. The analyst should begin analyzing the image and begin to report findings.C. The analyst should create a hash of the image and compare it to the original drive's hash.D. The analyst should create a chain of custody document and notify stakeholders. **Answer: C NEW QUESTION 7**An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan? A. Conduct a risk assessment.B. Develop a data retention policy.C. Execute vulnerability scanning.D. Identify assets. **Answer: D NEW QUESTION 8**A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP? A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.B. The corporate network should have a wireless infrastructure that uses open authentication standards.C. Guests using the wireless network should provide valid identification when registering their wireless devices.D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server. **Answer: C NEW QUESTION 9**An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select three.) A. 3DESB. AESC. IDEAD. PKCSE. PGPF. SSL/TLSG. TEMPEST **Answer: BDF NEW QUESTION 10**After completing a vulnerability scan, the following output was noted: CVE-2011-3389QID 42366 ? SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerabilityCheck with:openssl s_client -connect qualys.jive.mobile.com:443 ? tlsl -cipher ?AES:CAMELLIA:SEED:3DES:DES?Which of the following vulnerabilities has been identified? A. PKI transfer vulnerability.B. Active Directory encryption vulnerability.C. Web application cryptography vulnerability.D. VPN tunnel vulnerability. **Answer: A NEW QUESTION 11**?? Download the newest PassLeader CS0-001 dumps from passleader.com now! 100% Pass Guarantee! CS0-001 PDF dumps & CS0-001 VCE dumps: http://www.passleader.com/cs0-001.html (85 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