[2017 New Free Lead2pass CS0-001 PDF Guarantee 100% Get CS0-001 Certification

2017 May CompTIA Official New Released CS0-001 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Although the CompTIA CS0-001 dumps are very popular, Lead2pass offers a wide range of CompTIA CS0-001 exam dumps and will continue to release new study guide to meet the rapidly increasing demand of the IT industry. Following questions and answers are all new published by CompTIA Official Exam Center: http://www.lead2pass.com/cs0-001.html QUESTION 1 Which of the following BEST describes the offensive participants in a tabletop exercise? A. Red team B. Blue team C. System administrators D. Security analysts E. Operations team Answer: A 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 escalation. B. advanced persistent threat. C. malicious insider threat. D. spear phishing. Answer: B 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 planning B. Separation of duties C. Mandatory vacation D. Personnel training E. Job rotation Answer: BD 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 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 /usr Which 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 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 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 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 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. 3DES B. AES C. IDEA D. PKCS E. PGP F. SSL/TLS G. TEMPEST Answer: BDF QUESTION 10 After completing a vulnerability scan, the following output was noted: 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 Lead2pass offers the latest CompTIA CS0-001 dumps and a good range of CompTIA Certification CS0-001 answers. Most of our CompTIA CS0-001 exam dumps are exclusively prepared by the best brains and highly skilled professionals from the IT domain to ensure 100% pass in your CompTIA CS0-001 Exam. CS0-001 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDcHZDRDBubEExZjg 2017 CompTIA CS0-001 exam dumps (All 85 Q&As) from Lead2pass: http://www.lead2pass.com/cs0-001.html [100% Exam Pass Guaranteed]