[January 2018 Free Lead2pass CompTIA CAS-002 Exam Questions Download 900q

Free Share CAS-002 PDF Dumps With Lead2pass Updated Exam Questions: https://www.lead2pass.com/cas-002.html QUESTION 1A telecommunication company has recently upgraded their teleconference systems to multicast. Additionally, the security team has instituted a new policy which requires VPN to access the company's video conference.All parties must be issued a VPN account and must connect to the company's VPN concentrator to participate in the remote meetings.Which of the following settings will increase bandwidth utilization on the VPN concentrator during the remote meetings? A. IPSec transport mode is enabledB. ICMP is disabledC. Split tunneling is disabledD. NAT-traversal is enabledAnswer: C QUESTION 2Which of the following can aid a buffer overflow attack to execute when used in the creation of applications? A. Secure cookie storageB. Standard librariesC. State managementD. Input validation Answer: B QUESTION 3Several critical servers are unresponsive after an update was installed. Other computers that have not yet received the same update are operational, but are vulnerable to certain buffer overflow attacks. The security administrator is required to ensure all systems have the latest updates while minimizing any downtime.Which of the following is the BEST risk mitigation strategy to use to ensure a system is properly updated and operational? A. Distributed patch management system where all systems in production are patched as updates are released.B. Central patch management system where all systems in production are patched by automatic updates as they are released.C. Central patch management system where all updates are tested in a lab environment after being installed on a live production system.D. Distributed patch management system where all updates are tested in a lab environment prior to being installed on a live production system. Answer: D QUESTION 4Which of the following is true about an unauthenticated SAMLv2 transaction? A. The browser asks the SP for a resource. The SP provides the browser with an XHTML format. The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.B. The browser asks the IdP for a resource. The IdP provides the browser with an XHTML format. The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.C. The browser asks the IdP to validate the user. The IdP sends an XHTML form to the SP and a cookie to the browser. The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.D. The browser asks the SP to validate the user. The SP sends an XHTML form to the IdP. The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource. Answer: A QUESTION 5The internal auditor at Company ABC has completed the annual audit of the company's financial system. The audit report indicates that the accounts receivable department has not followed proper record disposal procedures during a COOP/BCP tabletop exercise involving manual processing of financial transactions.Which of the following should be the Information Security Officer's (ISO's) recommendation? (Select TWO). A. Wait for the external audit resultsB. Perform another COOP exerciseC. Implement mandatory trainingD. Destroy the financial transactionsE. Review company procedures Answer: CE QUESTION 6A system designer needs to factor in CIA requirements for a new SAN. Which of the CIA requirements is BEST met by multipathing? A. ConfidentialityB. AuthenticationC. IntegrityD. Availability Answer: D QUESTION 7The Chief Information Officer (CIO) comes to the security manager and asks what can be done to reduce the potential of sensitive data being emailed out of the company. Which of the following is an active security measure to protect against this threat? A. Require a digital signature on all outgoing emails.B. Sanitize outgoing content.C. Implement a data classification policy.D. Implement a SPAM filter. Answer: B QUESTION 8Which of the following BEST defines the term e-discovery? A. A product that provides IT-specific governance, risk management, and compliance.B. A form of reconnaissance used by penetration testers to discover listening hosts.C. A synonymous term for computer emergency response and incident handling.D. A process of producing electronically stored information for use as evidence. Answer: D QUESTION 9A data breach occurred which impacted the HR and payroll system. It is believed that an attack from within the organization resulted in the data breach. Which of the following should be performed FIRST after the data breach occurred? A. Assess system statusB. Restore from backup tapesC. Conduct a business impact analysisD. Review NIDS logs Answer: A QUESTION 10Employees have recently requested remote access to corporate email and shared drives. Remote access has never been offered; however, the need to improve productivity and rapidly responding to customer demands means staff now requires remote access. Which of the following controls will BEST protect the corporate network? A. Develop a security policy that defines remote access requirements. Perform regular audits of user accounts and reviews of system logs.B. Secure remote access systems to ensure shared drives are read only and access is provided through a SSL portal. Perform regular audits of user accounts and reviews of system logs.C. Plan and develop security policies based on the assumption that external environments have active hostile threats.D. Implement a DLP program to log data accessed by users connecting via remote access.Regularly perform user revalidation. Answer: C **CAS-002 dumps full version (PDF&VCE):** https://www.lead2pass.com/cas-002.html Large amount of free **CAS-002** exam questions on

Google Drive: https://drive.google.com/open?id=13j5iOL_XYuK24xlefcIzTQtqmeQfLY7K