[2018-June-NewValid Braindump2go CAS-002 VCE Dumps and CAS-002 PDF Dumps 900Q Offer[45-55

2018 June New CompTIA CAS-002 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-002 Real Exam Questions: 1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNQjRNekVOcFlaVm8?usp=sharingQUESTION 45Which of the following implementations of a continuous monitoring risk mitigation strategy is correct?A. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, and email alerts to NOC staff hourly.B. Audit successful and critical failed events, transfer logs to a centralized server once a month, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached.C. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are exceeded.D. Audit failed events only, transfer logs to a centralized server, implement manual audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached and exceeded.**Answer: C**QUESTION 46A company recently experienced a malware outbreak. It was caused by a vendor using an approved non-company device on the company's corporate network that impacted manufacturing lines, causing a week of downtime to recover from the attack.Which of the following reduces this threat and minimizes potential impact on the manufacturing lines?A. Disable remote access capabilities on manufacturing SCADA systems.B. Require a NIPS for all communications to and from manufacturing SCADA systems.C. Add anti-virus and client firewall capabilities to the manufacturing SCADA systems.D. Deploy an ACL that restricts access from the corporate network to the manufacturing SCADA systems.**Answer: D**QUESTION 47A company has a legacy virtual cluster which was added to the datacenter after a small company was acquired. All VMs on the cluster use the same virtual network interface to connect to the corporate data center LAN. Some of the virtual machines on the cluster process customer data, some process company financial data, and others act as externally facing web servers. Which of the following security risks can result from the configuration in this scenario?A. Visibility on the traffic between the virtual machines can impact confidentialityB. NIC utilization can exceed 50 percent and impact availabilityC. Shared virtual switches can negatively impact the integrity of network packetsD. Additional overhead from network bridging can affect availability**Answer: A**QUESTION 48Capital Reconnaissance, LLC is building a brand new research and testing location, and the physical security manager wants to deploy IP-based access control and video surveillance. These two systems are essential for keeping the building open for operations. Which of the following controls should the security administrator recommend to determine new threats against the new IP-based access control and video surveillance systems?A. Develop a network traffic baseline for each of the physical security systems.B. Air gap the physical security networks from the administrative and operational networks.C. Require separate non-VLANed networks and NIPS for each physical security system network.D. Have the Network Operations Center (NOC) review logs and create a CERT to respond to breaches.**Answer: A**QUESTION 49The Chief Information Security Officer (CISO) is researching ways to reduce the risk associated with administrative access of six IT staff members while enforcing separation of duties. In the case where an IT staff member is absent, each staff member should be able to perform all the necessary duties of their IT co-workers. Which of the following policies should the CISO implement to reduce the risk?A. Require the use of an unprivileged account, and a second shared account only for administrative purposes.B. Require role-based security on primary role, and only provide access to secondary roles on a case-by-case basis.C. Require separation of duties ensuring no single administrator has access to all systems.D. Require on-going auditing of administrative activities, and evaluate against risk-based metrics.**Answer: B**QUESTION 50As part of a new wireless implementation, the Chief Information Officer's (CIO's) main objective is to immediately deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard was not ratified by the IETF. The wireless vendor's products do support the pre-ratification version of 802.11r. The security and network administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. Which of the following is the BEST way to proceed?A. Purchase the equipment now, but do not use 802.11r until the standard is ratified.B. Do not purchase the equipment now as the client devices do not yet support 802.11r.C. Purchase the equipment now, as long as it will be firmware upgradeable to the final 802.11r standard.D. Do not purchase the equipment now; delay the implementation until the IETF has ratified the final 802.11r standard.**Answer: C** QUESTION 51A Chief Information Security Officer (CISO) has been trying to eliminate some IT security risks for several months. These risks are not high profile but still exist. Furthermore, many of these risks have been mitigated with innovative solutions. However, at this point in time, the budget is insufficient to deal with the risks. Which of the following risk strategies should be used?A. Transfer the risksB. Avoid the risksC. Accept the risksD. Mitigate the risks**Answer: C**QUESTION 52A company is planning to deploy an in-house Security Operations Center (SOC).One of the new requirements is to deploy a NIPS solution into the Internet facing environment.The SOC highlighted the following requirements:Perform fingerprinting on unfiltered inbound traffic to the company Monitor all inbound and outbound traffic to the DMZ'sIn which of the following places should the NIPS be placed in the network?A. In front of the Internet firewall and in front of the DMZsB. In front of the Internet firewall and in front of the internal firewallC. In front of the Internet firewall and behind the internal firewallD. Behind the Internet firewall and in front of the DMZs**Answer: A**QUESTION 53A security administrator wants to perform an audit of the company password file to ensure users are not using personal information such as addresses and birthdays as part of their password. The company employs 200,000 users, has virtualized environments with cluster and cloud-based computing resources, and enforces a minimum password length of 14 characters. Which of the following options is BEST suited to run the password auditing software and produce a report in the SHORTEST amount of time?A. The system administrator should take advantage of the company's cluster based computing resources, upload the password file to the cluster, and run the password cracker on that platform.B. The system administrator should upload the password file to a virtualized de-duplicated storage system to reduce the password entries and run a password cracker on that file.C. The system administrator should build a virtual machine on the administrator's desktop, transfer the password file to it, and run the a password cracker on the virtual machine.D. The system administrator should upload the password file to cloud storage and use on-demand provisioning to build a purpose based virtual machine to run a password cracker on all the users.**Answer: A**QUESTION 54An ecommerce application on a Linux server does not properly track the number of incoming connections to the server and may leave the server vulnerable to which of following?A. Buffer Overflow AttackB. Storage Consumption AttackC. Denial of Service AttackD. Race Condition**Answer: C**QUESTION 55The network administrator has been tracking the cause of network performance problems and decides to take a look at the internal and external router stats.Which of the following should the network administrator do to resolve the performance issue after analyzing the above information? A. The IP TOS field of business related network traffic should be modified accordingly.B. The TCP flags of business related traffic should be modified accordingly.C. An ACL should be placed on the external router to drop incoming ICMP packets.D. An ACL should be placed on the internal router to drop layer 4 packets to and from port 0.**Answer: A**!!!RECOMMEND!!! 1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Study Guide Video: YouTube Video: YouTube.com/watch?v=k4FW5mVem0w