[2017-New-ExamsCS0-001 Dumps PDF 85q Instant Download in Braindump2go[41-50

2017 May New CompTIA CS0-001 Exam Dumps with VCE and PDF Updated in www.Braindump2go.com Today!100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|2017 Version New CS0-001 Exam Dumps (VCE & PDF) 85Q&As Download: http://www.braindump2go.com/cs0-001.html 2.|2017 Version New CS0-001 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharing QUESTION 41An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive? A. Reports show the scanner compliance plug-in is out-of-date.B. Any items labeled `low' are considered informational only.C. The scan result version is different from the automated asset inventory.D. `HTTPS' entries indicate the web page is encrypted securely. Answer: B QUESTION 42Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this? A. ACLB. SIEMC. MACD. NACE. SAML Answer: A QUESTION 43After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer. Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services? A. DENY TCP ANY HOST 10.38.219.20 EQ 3389B. DENY IP HOST 10.38.219.20 ANY EQ 25C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389D. DENY TCP ANY HOST 192.168.1.10 EQ 25 Answer: A QUESTION 44The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization? A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router. Answer: C QUESTION 45While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation? A. The analyst is not using the standard approved browser.B. The analyst accidently clicked a link related to the indicator.C. The analyst has prefetch enabled on the browser in use.D. The alert in unrelated to the analyst's search. Answer: C QUESTION 46An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation? A. Zero-day attackB. Known malware attackC. Session hijackD. Cookie stealing Answer: A QUESTION 47A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment? A. A passive scanning engine located at the core of the network infrastructureB. A combination of cloud-based and server-based scanning enginesC. A combination of server-based and agent-based scanning enginesD. An active scanning engine installed on the enterprise console Answer: D QUESTION 48A cybersecurity analyst is completing an organization's vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report? A. Processor utilizationB. Virtual hostsC. Organizational governanceD. Log dispositionE. Asset isolation Answer: B QUESTION 49A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization? A. A manual log review from data sent to syslogB. An OS fingerprinting scan across all hostsC. A packet capture of data traversing the server networkD. A service discovery scan on the network Answer: B QUESTION 50A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following

should the analyst implement? A. Self-service password resetB. Single sign-onC. Context-based authenticationD. Password complexity Answer: C !!!RECOMMEND!!! 1.|2017 Version New CS0-001 Exam Dumps (VCE & PDF) 85Q&As Download: http://www.braindump2go.com/cs0-001.html 2.|2017 Version New CS0-001 Study Guide Video: YouTube Video: YouTube.com/watch?v=ZR1G8DM-DRA