[Nov-2018Download CS0-001 PDF from Braindump2go[Q214-231

2018/November Braindump2go CS0-001 Exam Dumps with PDF and VCE New Updated Today! Following are some new CS0-001 Real Exam Questions:1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 252Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharingQUESTION 214During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?A. Power off the computer and remove it from the network.B. Unplug the network cable and take screenshots of the desktop.C. Perform a physical hard disk image.D. Initiate chain-of-custody documentation.**Answer: A**QUESTION 215A security analyst has determined the security team should take action based on the following log: Which of the following should be used to improve the security posture of the system?A. Enable login account auditing.B. Limit the number of unsuccessful login attempts.C. Upgrade the firewalls.D. Increase password complexity requirements.**Answer: B**QUESTION 216An organization has recently experienced a data breach. A forensic analysis confirmed the attacker found a legacy web server that had not been used in over a year and was not regularly patched. After a discussion with the security team, management decided to initiate a program of network reconnaissance and penetration testing. They want to start the process by scanning the network for active hosts and open ports. Which of the following tools is BEST suited for this job?A. PingB. NmapC. NetstatD. ifconfigE. WiresharkF. L0phtCrack**Answer: B**QUESTION 217A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?A. PHIB. PCIC. PIID. IP**Answer: B**QUESTION 218An 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 indicate that findings are informational.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 219A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purpose of exfiltrating data. The following are four snippets taken from running netstat ?an on separate Windows workstations: Based on the above information, which of the following is MOST likely to be exposed to this malware?A. Workstation AB. Workstation BC. Workstation CD. Workstation D**Answer: A**QUESTION 220An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the insurance company's app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause?A. The MDM server is misconfigured.B. The app does not employ TLS.C. USB tethering is enabled.D. 3G and less secure cellular technologies are not restricted.**Answer: B**QUESTION 221A cybersecurity consultant found common vulnerabilities across the following services used by multiple servers at an organization: VPN, SSH, and HTTPS. Which of the following is the MOST likely reason for the discovered vulnerabilities?A. Leaked PKI private keyB. Vulnerable version of OpenSSLC. Common initialization vectorD. Weak level of encryption entropyE. Vulnerable implementation of PEAP**Answer: D**QUESTION 222A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future?A. Implement a manual patch management application package to regain greater control over the process.B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.C. Implement service monitoring to validate that tools are functioning properly.D. Set services on the patch management server to automatically run on start-up.**Answer: D**QUESTION 223Which of the following could be directly impacted by an unpatched vulnerability in vSphere ESXi?A. The organization's physical routersB. The organization's mobile devicesC. The organization's virtual infrastructureD. The organization's VPN**Answer: C**QUESTION 224A security analyst performed a review of an organization's software development life cycle. The analyst reports that the life cycle does not contain in a phase in which team members evaluate and provide critical feedback on another developer's code. Which of the following assessment techniques is BEST for describing the analyst's report?A. Architectural evaluationB. WaterfallC. Whitebox testingD. Peer review**Answer: D**QUESTION 225The Chief Security Officer (CSO) has requested a vulnerability report of systems on the domain,

identifying those running outdated OSs. The automated scan reports are not displaying OS version details, so the CSO cannot determine risk exposure levels from vulnerable systems. Which of the following should the cybersecurity analyst do to enumerate OS information as part of the vulnerability scanning process in the MOST efficient manner?A. Execute the ver commandB. Execute the nmap ?p commandC. Use Wireshark to export a listD. Use credentialed configuration**Answer: A**QUESTION 226 Organizational policies require vulnerability remediation on severity 7 or greater within one week. Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:The organization has three Apache web servers: The results of a recent vulnerability scan are shown below: The team performs some investigation and finds a statement from Apache: Which of the following actions should the security team perform?A. Ignore the false positive on 192.168.1.22B. Remediate 192.168.1.20 within 30 daysC. Remediate 192.168.1.22 within 30 daysD. Investigate the false negative on 192.168.1.20**Answer: C**QUESTION 227A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reversed external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent?A. Broadcast stormsB. Spoofing attacksC. DDoS attacksD. Man-in-the-middle attacks**Answer: B** QUESTION 228A server contains baseline images that are deployed to sensitive workstations on a regular basis. The images are evaluated once per month for patching and other fixes, but do not change otherwise. Which of the following controls should be put in place to secure the file server and ensure the images are not changed?A. Install and configure a file integrity monitoring tool on the server and allow updates to the images each month.B. Schedule vulnerability scans of the server at least once per month before the images are updated.C. Require the use of two-factor authentication for any administrator or user who needs to connect to the server.D. Install a honeypot to identify any attacks before the baseline images can be compromised.**Answer: A**QUESTION 229A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)A. Human resourcesB. Public relationsC. LegalD. Executive managementE. IT management**Answer: D**QUESTION 230A security analyst received several service tickets reporting that a company storefront website is not accessible by internal domain users. However, external users are accessing the website without issue. Which of the following is the MOST likely reason for this behavior?A. The FQDN is incorrect.B. The DNS server is corrupted.C. The time synchronization server is corrupted.D. The certificate is expired.**Answer: B**QUESTION 231Which of the following utilities could be used to resolve an IP address to a domain name, assuming the address has a PTR record?A. ifconfig B. pingC. arpD. nbtstat**Answer: B**!!!RECOMMEND!!!1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 252Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Study Guide Video: YouTube Video: YouTube.com/watch?v=m9hajso3rNc