[Nov-2018Braindump2go 252Q CS0-001 PDF and CS0-001 VCE Free Download[Q192-202

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 192A security analyst is reviewing a report from the networking department that describes an increase in network utilization, which is causing network performance issues on some systems.A top talkers report over a five-minute sample is included. Given the above output of the sample, which of the following should the security analyst accomplish FIRST to help track down the performance issues?A. Perform reverse lookups on each of the IP addresses listed to help determine if the traffic is necessary.B. Recommend that networking block the unneeded protocols such as Quicktime to clear up some of the congestion.C. Put ACLs in place to restrict traffic destined for random or non-default application ports.D. Quarantine the top talker on the network and begin to investigate any potential threats caused by the excessive traffic.**Answer: A**QUESTION 193During the forensic a phase of security investigation, it was discovered that an attacker was able to find private keys on a poorly secured team shared drive. The attacker used those keys to intercept and decrypt sensitive traffic on a web server. Which of the following describes this type of exploit and the potential remediation?A. Session hijacking; network intrusion detection sensorsB. Cross-site scripting; increased encryption key sizesC. Man-in-the-middle; well-controlled storage of private keysD. Rootkit; controlled storage of public keys**Answer: C** QUESTION 194Which of the following is a vulnerability when using Windows as a host OS for virtual machines?A. Windows requires frequent patching.B. Windows virtualized environments are typically unstable.C. Windows requires hundreds of open firewall ports to operate.D. Windows is vulnerable to the "ping of death".**Answer: D**QUESTION 195A penetration tester is preparing for an audit of critical systems that may impact the security of the environment. This includes the external perimeter and the internal perimeter of the environment. During which of the following processes is this type of information normally gathered?A. TimingB. ScopingC. AuthorizationD. Enumeration**Answer: B**QUESTION 196A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDsC. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attackD. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB portE. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking**Answer: CD**QUESTION 197Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following: Which of the following would BEST accomplish the task assigned to the analyst?A. 3 [0-9]d-2[0-9]d-4[0-9]dB. d(3)-d(2)-d(4)C. ?[3]-?[2]-?[3]D. d[9] `XXX-XX-XX'**Answer: B**QUESTION 198A recently issued audit report highlighted exceptions related to end-user handling of sensitive data and access credentials. A security manager is addressing the findings. Which of the following activities should be implemented?A. Update the password policyB. Increase training requirementsC. Deploy a single sign-on platformD. Deploy Group Policy Objects**Answer: B**QUESTION 199 During which of the following NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?A. CategorizeB. SelectC. ImplementD. Access**Answer: B** QUESTION 200A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike. Which of the following describes what may be occurring?A. Someone has logged on to the sinkhole and is using the device.B. The sinkhole has begun blocking suspect or malicious traffic.C. The sinkhole has begun rerouting unauthorized traffic.D. Something is controlling the sinkhole and causing CPU spikes due to malicious utilization.**Answer: C**QUESTION 201Alerts have been received from the SIEM, indicating infections on multiple computers. Base on threat characteristics, these files were quarantined by the host-based antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT?A. Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation.B. Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM.C.

Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers.D. Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot.Permit the URLs classified as uncategorized to and from that host.**Answer: B**QUESTION 202Which of the following has the GREATEST impact to the data retention policies of an organization?A. The CIA classification matrix assigned to each piece of dataB. The level of sensitivity of the data established by the data ownerC. The regulatory requirements concerning the data setD. The technical constraints of the technology used to store the data**Answer: D**
!!!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