[2017-New-DumpsCisco 600-199 Exam Dumps VCE(Full Version)60q Download in Braindump2go[Q1-Q10

2017 Feb. New Cisco 600-199 Exam Questions and Answers Updated Today!Free Download 600-199 Dumps and 600-199 VCE 60Q&As from www.braindump2go.com Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|NEW 600-199 Dumps and 600-199 PDF 60Q&As Download:http://www.braindump2go.com/600-199.html 2.|NEW 600-199 Exam Questions and 600-199 VCE Download:https://1drv.ms/f/s!AvI7wzKf6QBjgkm_DtWXO9h1Xwmc QUESTION 1Which describes the best method for preserving the chain of evidence? A. Shut down the machine that is infected, remove the hard drive, and contact the local authorities.B. Back up the hard drive, use antivirus software to clean the infected machine, and contact the local authorities. C. Identify the infected machine, disconnect from the network, and contact the local authorities.D. Allow user(s) to perform any business-critical tasks while waiting for local authorities. Answer: C QUESTION 2Which will be provided as output when issuing the show processes cpu command on a Cisco IOS router? A. router configurationB. CPU utilization of deviceC. memory used by device processesD. interface processing statistics Answer: B QUESTION 3Refer to the exhibit. Which protocol is used in this network traffic flow?

A. SNMPB. SSHC. DNSD. Telnet Answer: B QUESTION 4Which two types of data are relevant to investigating network security issues? (Choose two.) A. NetFlowB. device model numbersC. syslogD. routing tablesE. private IP addresses Answer: AC QUESTION 5In the context of a network security device like an IPS, which event would qualify as having the highest severity? A. remote code execution attemptB. brute force login attemptC. denial of service attackD. instant messenger activity Answer: A QUESTION 6Which event is likely to be a false positive? A. Internet Relay Chat signature with an alert context buffer containing #IPS_ROCS YayB. a signature addressing an ActiveX vulnerability alert on a Microsoft developer network documentation pageC. an alert for a long HTTP request with an alert context buffer containing a large HTTP GET request D. BitTorrent activity detected on ephemeral ports Answer: B QUESTION 7Given a Linux machine running only an SSH server, which chain of alarms would be most concerning? A. brute force login attempt from outside of the network, followed by an internal network scanB. root login attempt followed by brute force login attemptC. Microsoft RPC attack against the serverD. multiple rapid login attempts Answer: A QUESTION 8If a company has a strict policy to limit potential confidential information leakage, which three alerts would be of concern? (Choose three.) A. P2P activity detectedB. Skype activity detectedC. YouTube viewing activity detectedD. Pastebin activity detectedE. Hulu activity detected Answer: ABD QUESTION 9Which event is actionable? A. SSH login failedB. Telnet login failedC. traffic flow startedD. reverse shell detected Answer: D QUESTION 10Which would be classified as a remote code execution attempt? A. OLE stack overflow detectedB. null login attemptC. BitTorrent activity detectedD. IE ActiveX DoS Answer: A !!!RECOMMEND!!! 1.|NEW 600-199 Dumps and 600-199 PDF 60Q&As Download:http://www.braindump2go.com/600-199.html 2.|NEW 600-199 Study Guide: YouTube Video: YouTube.com/watch?v=AgHGXrA9L1M