[March-2018Download Braindump2go 210-255 Exam Questions PDF 85Q Free[34-44

2018 March New Cisco 210-255 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 210-255 Real Exam Questions:1.|2018 Latest 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: https://www.braindump2go.com/210-255.html2.|2018 Latest 210-255 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharing QUESTION 34Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?A. true positiveB. true negativeC. false positiveD. false negativeAnswer: AQUESTION 35Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?A. confidentialityB. integrityC. availabilityD. complexityAnswer: AQUESTION 36During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?A. collectionB. examinationC. reportingD. investigationAnswer: AQUESTION 37Which information must be left out of a final incident report? A. server hardware configurationsB. exploit or vulnerability usedC. impact and/or the financial lossD. how the incident was detectedAnswer: BQUESTION 38Which two components are included in a 5-tuple? (Choose two.)A. port numberB. destination IP addressC. data packetD. user nameE. host logsAnswer: BCQUESTION 39In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model'?A. victim demographics, incident description, incident details, discovery & responseB. victim demographics, incident details, indicators of compromise, impact assessmentC. actors, attributes, impact, remediationD. actors, actions, assets, attributesAnswer: DQUESTION 40 Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?A. 1986B. 2318C. 2542D. 2317Answer: DQUESTION 41Which two options can be used by a threat actor to determine the role of a server? (Choose two.)A. PCAPB. tracertC. running processesD. hard drive configurationE. applicationsAnswer: CDQUESTION 42Which option creates a display filter on Wireshark on a host IP address or name?A. ip.address == <address> or ip.network == <network>B. [tcp|udp] ip.[src|dst] port <port>C. ip.addr == <addr> or ip.name == <name>D. ip.addr == <addr> or ip.host == <host>Answer: AQUESTION 43Drag and Drop QuestionDrag and drop the elements of incident handling from the left into the correct order on the right. Answer: QUESTION 44You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4O0) Gecko/20100101D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16Answer: A!!!RECOMMEND!!!1.|2018 Latest 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: https://www.braindump2go.com/210-255.html2.|2018 Latest 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=di0FBePt_-w