[Dec-2018170Q Exam 210-255 Dumps Free Download in Braindump2go[Q109-119

Dec/2018 Braindump2go 210-255 Exam Dumps with PDF and VCE New Updated Today! Following are some new 210-255 Real Exam Questions:1.|2018 Latest 210-255 Exam Dumps (PDF & VCE) 170Q Download:https://www.braindump2go.com/210-255.html2.|2018 Latest 210-255 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharingQUESTION 109Which option is the common artifact used to uniquely identify a detected file?A. file sizeB. file extensionC. file timestampD. file hash**Answer: D**QUESTION 110Which two useful pieces of information can be collected from the IPv4 protocol header? (Choose two.)A. UDP port which the traffic is destinedB. source IP address of the packetC. UDP port from which the traffic is sourced D. TCP port from which the traffic was sourceE. destination IP address of the packet**Answer: BE**QUESTION 111Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?A. effectiveness of the strategyB. time and resource needed to implement the strategyC. need for evidence preservationD. attack vector used to compromise the system**Answer: D**QUESTION 112Which type verification typically consists of using tools to compute the message digest of the original and copies data, then comparing the digests to make sure that they are the same?A. evidence collection order B. data integrityC. data preservationD. volatile data collection**Answer: B**QUESTION 113Which function does an internal CSIRT provide?A. incident handling services across various CSIRTsB. incident handling services for a country's governmentC. incident handling services for a parent organizationD. incident handling services as a service for other organization**Answer: C** QUESTION 114Which expression creates a filter on a host IP address or name?A. [src|dst] host <host host >B. [tcp|udp] [src|dst] port<port>C. ether [src|dst] host<ehost>D. gateway host <host>**Answer: A**QUESTION 115The united State CERT provides cybersecurity protection to Federal, civilian, and executive branch agencies through intrusion detection and prevention capabilities. Which type of incident response team is this an example of?A. Federal PSIRTB. National PSIRTC. National CSIRTD. Federal CSIRT**Answer: C**QUESTION 116Which two potions are the primary 5-tuple components? (Choose two)A. destination IP addressB. header lengthC. sequence numberD. checksumE. source IP address**Answer: AE**QUESTION 117 According to NIST-SP800-61R2, which option should be contained in the issue tracking system?A. incidents related to the current incidentB. incident unrelated to the current incidentC. actions taken by nonincident handlersD. latest public virus signatures **Answer: A**QUESTION 118Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?A. true positiveB. false negativeC. false positiveD. true negative**Answer: C**QUESTION 119Which purpose of data mapping is true?A. Visualize data.B. Find extra vulnerabilities.C. Discover the identities of attackersD. Check that data is correct.**Answer: A**!!!RECOMMEND!!!1.|2018 Latest 210-255 Exam Dumps (PDF & VCE) 170Q Download:https://www.braindump2go.com/210-255.html2.|2018 Latest 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=G_SGMZcy-bE