

[Dec-2018] Download Free Braindump2go 210-255 VCE Dumps for 210-255 Exam Preparation [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.html> | 2018 Latest 210-255 Exam Questions & Answers

Download: <https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharing>

QUESTION 109 Which option is the common artifact used to uniquely identify a detected file?
A. file size
B. file extension
C. file timestamp
D. file hash
Answer: D

QUESTION 110 Which two useful pieces of information can be collected from the IPv4 protocol header? (Choose two.)
A. UDP port which the traffic is destined
B. source IP address of the packet
C. UDP port from which the traffic is sourced
D. TCP port from which the traffic was source
E. destination IP address of the packet
Answer: B

QUESTION 111 Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?
A. effectiveness of the strategy
B. time and resource needed to implement the strategy
C. need for evidence preservation
D. attack vector used to compromise the system
Answer: D

QUESTION 112 Which 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 integrity
C. data preservation
D. volatile data collection
Answer: B

QUESTION 113 Which function does an internal CSIRT provide?
A. incident handling services across various CSIRTs
B. incident handling services for a country's government
C. incident handling services for a parent organization
D. incident handling services as a service for other organization
Answer: C

QUESTION 114 Which 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 115 The 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 PSIRT
B. National PSIRT
C. National CSIRT
D. Federal CSIRT
Answer: C

QUESTION 116 Which two options are the primary 5-tuple components? (Choose two.)
A. destination IP address
B. header length
C. sequence number
D. checksum
E. source IP address
Answer: A

QUESTION 117 According to NIST-SP800-61R2, which option should be contained in the issue tracking system?
A. incidents related to the current incident
B. incident unrelated to the current incident
C. actions taken by nonincident handlers
D. latest public virus signatures
Answer: A

QUESTION 118 Employees 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 positive
B. false negative
C. false positive
D. true negative
Answer: C

QUESTION 119 Which purpose of data mapping is true?
A. Visualize data.
B. Find extra vulnerabilities.
C. Discover the identities of attackers.
D. 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.html> | 2018 Latest 210-255 Study Guide Video: YouTube Video: [YouTube.com/watch?v=G_SGMZcy-bE](https://www.youtube.com/watch?v=G_SGMZcy-bE)