

[March-2018] 100% Real 210-255 VCE 85Q Free Download in Braindump2go [56-65]

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.html> 2. | 2018 Latest 210-255 Exam Questions & Answers Download:

<https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharing> QUESTION 56 During which phase of

the forensic process are tools and techniques used to extract the relevant information from the collective data? A. examination B.

reporting C. collection D. investigation Answer: B QUESTION 57 Which option allows a file to be extracted from a TCP stream

within Wireshark? A. File > Export Objects B. Analyze > Extract C. Tools > Export > TCP D. View > Extract Answer:

QUESTION 58 Which CVSSv3 metric captures the level of access that is required for a successful attack? A. attack vector B.

attack complexity C. privileges required D. user interaction Answer: C QUESTION 59 From a security perspective, why is it

important to employ a clock synchronization protocol on a network? A. so that everyone knows the local time B. to ensure

employees adhere to work schedule C. to construct an accurate timeline of events when responding to an incident D. to guarantee

that updates are pushed out according to schedule Answer: D QUESTION 60 Refer to the exhibit. Which type of log is this an

example of? A. IDS log B. proxy log C. NetFlow log D. syslog Answer: A QUESTION 61 Which goal of data normalization is

true? A. Reduce data redundancy B. Increase data redundancy C. Reduce data availability D. Increase data

availability Answer: C QUESTION 62 Which description of a retrospective malware detection is true? A. You use Wireshark to

identify the malware source B. You use historical information from one or more sources to identify the affected host or file C.

You use information from a network analyzer to identify the malware source D. You use Wireshark to identify the affected host or

file Answer: B QUESTION 63 Which process is being utilized when IPS events are removed to improve data integrity? A. data

normalization B. data availability C. data protection D. data signature Answer: B QUESTION 64 Which element is included in an

incident response plan? A. organization mission B. junior analyst approval C. day-to-day firefighting D. siloed approach to

communications Answer: A QUESTION 65 In Microsoft Windows, as files are deleted the space they were allocated eventually is

considered available for use by other files. This creates alternating used and unused areas of various sizes. What is this called? A.

network file storing B. free space fragmentation C. alternate data streaming D. defragmentation Answer: A !!!RECOMMEND!!!

1. | 2018 Latest 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: <https://www.braindump2go.com/210-255.html> 2. | 2018

Latest 210-255 Study Guide Video: YouTube Video: [YouTube.com/watch?v=di0FBePt_-w](https://www.youtube.com/watch?v=di0FBePt_-w)