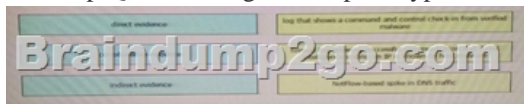
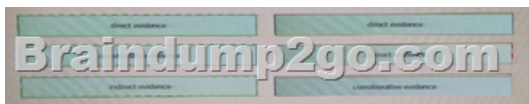


[2017-New-Exams100% Real Exam Questions-210-255 Exam VCE and PDF 70Q Download(51-60)

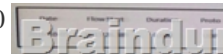
2017 March Cisco New 210-255: Implementing Cisco Cybersecurity Operations Exam Dumps (Full Version) Released Today! Free INSTANT Download [210-255 Exam Dumps \(PDF & VCE\) 70Q&As](#) Download from [www.Braindump2go.com](#) **Today!** 100% REAL Exam Questions! 100% Exam Pass Guaranteed! 1. |NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download <http://www.braindump2go.com/210-255.html> 2. |NEW 210-255 Exam Questions & Answers: <https://1drv.ms/f/s!AvI7wzKf6QBjgn5gut7hxGLZ6xws> QUESTION 51 Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space? A. confidentiality B. integrity C. availability D. complexity Answer: D QUESTION 52 Which Security Operations Center's goal is to provide incident handling to a country? A. Coordination Center B. Internal CSIRT C. National CSIRT D. Analysis Center Answer: C QUESTION 53 A CMS plugin creates two files that are accessible from the Internet: myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity? A. weaponization B. exploitation C. installation D. reconnaissance Answer: B QUESTION 54 Which two HTTP header fields relate to intrusion analysis? (Choose two). A. user-agent B. host C. connection D. language E. handshake type Answer: BC QUESTION 55 Drag and Drop Question Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.



Answer:



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 > TCPD. View > Extract Answer: C 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

!!!RECOMMEND!!! 1. |NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download

<http://www.braindump2go.com/210-255.html> 2. |NEW 210-255 Study Guide Video: YouTube Video:

[YouTube.com/watch?v=3fI6ShLIZQo](https://www.youtube.com/watch?v=3fI6ShLIZQo)