[Dec-2017-NewFree Download Braindump2go 210-255 PDF and VCE Dumps for Pass 210-255 Cisco Exam[Q41-Q51

 2017 New Cisco 210-255 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 210-255 Exam Questions: 1.|2017 New 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: https://www.braindump2go.com/210-255.html2.|2017 New 210-255 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharingQUESTION 41Which Security Operations Center's goal is to provide incident handling to a country?A.   Coordination CenterB.   Internal CSIRTC.   National CSIRTD.   Analysis CenterAnswer: CQUESTION 42A 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.   weaponizationB.   exploitationC.   installationD.   reconnaissanceAnswer: BQUESTION 43Which goal of data normalization is true?A.   Reduce data redundancy.B.   Increase data redundancy.C.   Reduce data availability.D.   Increase data availabilityAnswer: AQUESTION 44 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: BQUESTION 45Which process is being utilized when IPS events are removed to improve data integrity?A.   data normalizationB.   data availabilityC.   data protectionD.   data signatureAnswer: AQUESTION 46Which element is included in an incident response plan?A.   organization missionB.   junior analyst approvalC.   day-to-day firefightingD.   siloed approach to communicationsAnswer: AQUESTION 47In 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 storingB.   free space fragmentationC.   alternate data streamingD.   defragmentationAnswer: BQUESTION 48In the context of incident handling phases, which two activities fall under scoping? (Choose two.)A.   determining the number of attackers that are associated with a security incidentB.   ascertaining the number and types of vulnerabilities on your networkC.   identifying the extent that a security incident is impacting protected resources on the networkD.   determining what and how much data may have been affectedE.   identifying the attackers that are associated with a security incidentAnswer: DEQUESTION 49Which regular expression matches "color" and "colour"?A.   col[0-9]+ourB.   colo?urC.   colou?rD.   ]a-z]{7}Answer: CQUESTION 50During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?A.   examinationB.   reportingC.   collectionD.   investigationAnswer: AExplanation:Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data. Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.QUESTION 51Which option allows a file to be extracted from a TCP stream within Wireshark?A.   File > Export ObjectsB.   Analyze > ExtractC.   Tools > Export > TCPD.   View > ExtractAnswer: A!!! RECOMMEND!!!1.|2017 New 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: https://www.braindump2go.com/210-255.html2.|2017 New 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=zDNlMgoc1zI