[Dec-2017-New90Q 210-250 PDF Dumps Free Downloading - Braindump2go[Q39-Q49

2017 Dec New Cisco 210-250 Exam Dumps with PPDF and VCE Free Updated Today! Following are some new added 210-250 Exam Questios:1.|2017 New 210-250 Exam Dumps (PDF & VCE) 90Q&As Download: https://www.braindump2go.com/210-250.html2.|2017 New 210-250 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNekdxX05OVnFXRXc?usp=sharingQUESTION 39A user reports difficulties accessing certain external web pages, When examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?A. insufficient network resourcesB. failure of full packet capture solutionC. misconfiguration of web filterD. TCP injectionAnswer: DQUESTION 40Which tool is commonly used by threat actors on a webpage to take advantage of the softwarevulnerabilitiesof a system to spread malware?A. exploit kitB. root kitC. vulnerability kitD. script kiddie kitAnswer: AQUESTION 41Refer to the exhibit. During an analysis this list of email attachments is found. Which files contain the same content? A. 1 and 4B. 3 and 4C. 1 and 3D. 1 and 2Answer: CQUESTION 42Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?A. integrity validationB. due diligenceC. need to knowD. least privilegeAnswer: DQUESTION 43Which term represents the chronological record of how evidence was collected- analyzed, preserved, and transferred?A. chain of evidenceB. evidence chronologyC. chain of custodyD. record of safekeepingAnswer: CQUESTION 44Which two tasks can be performed by analyzing the logs of a traditional stateful firewall? (Choose two.)A. Confirm the timing of network connections differentiated by the TCP 5-tupleB. Audit the applications used within a social networking web site.C. Determine the user IDs involved in an instant messaging exchange.D. Map internal private IP addresses to dynamically translated external public IP addressesE. Identify the malware variant carried by n SMTP connectionAnswer: ADQUESTION 45Which security monitoring data type is associated with application server logs?A. alert dataB. statistical dataC. session dataD. transaction dataAnswer: DQUESTION 46Where is a host-based intrusion detection system located?A. on a particular end-point as an agent or a desktop applicationB. on a dedicated proxy server monitoring egress trafficC. on a span switch portD. on a tap switch portAnswer: AQUESTION 47One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?A. Confidentiality, Integrity, and AvailabilityB. Confidentiality, Identity, and AvailabilityC. Confidentiality, Integrity, and AuthorizationD. Confidentiality, Identity, and AuthorizationAnswer: AQUESTION 48According to RFC 1035 which transport protocol is recommended for use with DNS queries?A. Transmission Control ProtocolB. Reliable Data ProtocolC. Hypertext Transfer ProtocolD. User Datagram ProtocolAnswer: DQUESTION 49Which definition describes the main purpose of a Security Information and Event Management solution ?A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threatsB. a monitoring interface that manages firewall access control lists for duplicate firewall filteringC. a relay server or device that collects then forwards event logs to another log collection deviceD. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security postureAnswer: D !!!RECOMMEND!!!1.|2017 New 210-250 Exam Dumps (PDF & VCE) 90Q&As Download: **https://www.braindump2go.com/210-250.html**2.|2017 New 210-250 Study guide Video: YouTube Video: YouTube.com/watch?v=Jdl4H6tmoAY