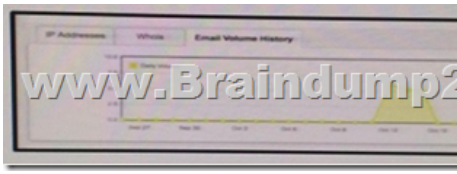
[Dec-2017-NewBraindump2go 85Q 210-255 PDF Dumps Share[Q56-Q66

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 56Refer to the exhibit. You notice that the email volume history has been abnormally high.Which potential result is true?



A. Email sent from your domain might be filtered by the recipient.B. Messages sent to your domain may be queued up until traffic dies down.C. Several hosts in your network may be compromised.D. Packets may be dropped due to network congestion.Answer: CQUESTION 57A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?A. reconnaissanceB. weaponizationC. deliveryD. installationAnswer: CQUESTION 58Which option is a misuse variety per VERIS enumerations?A. snoopingB. hackingC. theftD. assaultAnswer: BQUESTION 59Which CVSSv3 metric captures the level of access that is required for a successful attack?A. attack vectorB. attack complexityC. privileges requiredD. user interactionAnswer: CQUESTION 60From a security perspective, why is it important to employ a clock synchronization protocol on a network?A. so that everyone knows the local timeB. to ensure employees adhere to work schedule C. to construct an accurate timeline of events when responding to an incidentD. to guarantee that updates are pushed out according to scheduleAnswer: CQUESTION 61You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?A. deliveryB. reconnaissanceC. action on objectivesD. installationE. exploitationAnswer: AQUESTION 62Which two HTTP header fields relate to intrusion analysis? (Choose two).A. user-agentB. hostC. connectionD. languageE. handshake typeAnswer: ABQUESTION 63Which component of the NIST SP800-61 r2 incident handling strategy reviews data?A. preparationB. detection and analysisC. containment, eradication, and recoveryD. post-incident analysisAnswer: DQUESTION 64Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?A. URLB. hashC. IP addressD. destination portAnswer: BQUESTION 65Which data type is protected under the PCI compliance framework?A. credit card typeB. primary account numberC. health conditionsD. provision of individual careAnswer: BQUESTION 66What is accomplished in the identification phase of incident handling?A. determining the responsible userB. identifying source and destination IP addressesC. defining the limits of your authority related to a security eventD. determining that a security event has occurredAnswer: D!!! 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