[2017-New-ExamsBraindump2go 210-255 Questions and Answers Instant Download(11-20)

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 11You 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.   exploitation Answer: D QUESTION 12Which string matches the regular expression r(ege)+x? A.   rxB.   regeegexC.   r(ege)xD.   rege+x Answer: A QUESTION 13

Refer to the exhibit. Which type of log is this an example of? A.   syslogB.   NetFlow logC.   proxy logD.   IDS log Answer: A QUESTION 14Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic? A.   TTLsB.   portsC.   SMTP repliesD.   IP addresses Answer: A QUESTION 15Which stakeholder group is responsible for containment, eradication, and recovery in incident handling? A.   facilitatorsB.   practitionersC.   leaders and managersD.   decision makers Answer: A QUESTION 16

Refer 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: C QUESTION 17Drag and Drop Question Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5 record from a security event on the right.

Answer:

QUESTION 18Which statement about threat actors is true? A.   They are any company assets that are threatened.B.   They are any assets that are threatened.C.   They are perpetrators of attacks.D.   They are victims of attacks. Answer: B QUESTION 19Which data element must be protected with regards to PCI? A.   past health conditionB.   geographic locationC.   full nameD.   recent payment amount Answer: D QUESTION 20What mechanism does the Linux operating system provide to control access to files? A.   privileges requiredB.   user interactionC.   file permissionsD.   access complexity Answer: C   !!!RECOMMEND!!! 1.|NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Downloadhttp://www.braindump2go.com/210-255.html 2.|NEW 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=3fI6ShLlZQo