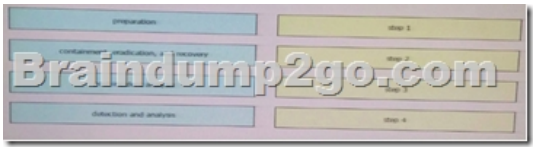
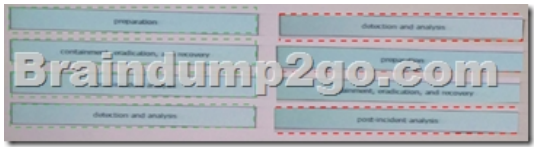
[2017-New-ExamsBraindump2go 210-255 VCE and PDF Dumps 70Q Free Offer(41-50)

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 41Which two options can be used by a threat actor to determine the role of a server? (Choose two.) A. PCAPB. tracertC. running processesD. hard drive configurationE. applications Answer: CD QUESTION 42Which option creates a display filter on Wireshark on a host IP address or name? A. ip.address == <address> or ip.network == <network>B. [tcp|udp] ip.[src|dst] port <port>C. ip.addr == <addr> or ip.name == <name>D. ip.addr == <addr> or ip.host == <host> Answer: A QUESTION 43Drag and Drop QuestionDrag and drop the elements of incident handling from the left into the correct order on the right.

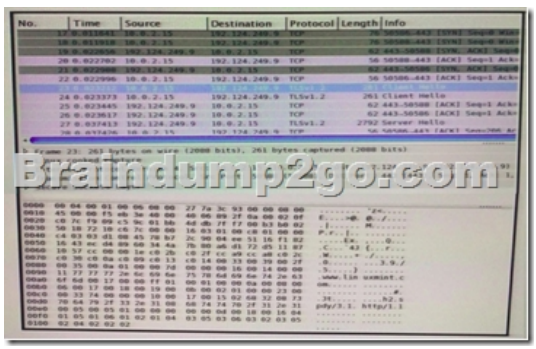


Answer:



QUESTION 44You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation? A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4O0) Gecko/20100101D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16 Answer: A QUESTION 45A 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. installation Answer: A QUESTION 46

Refer to the Exhibit. A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website? A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.B. The server at 10.67.10.5 has a virus.C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors. Answer: C QUESTION 47Which identifies both the source and destination location? A. IP addressB. URLC. portsD. MAC address Answer: C QUESTION 48Drag and Drop Question



Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

Answer:

QUESTION 49Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario? A. deterministicB. exploratoryC. probabilisticD. descriptive Answer: D QUESTION 50Which feature is used to find possible vulnerable services running on a server? A. CPU utilizationB. security policyC. temporary internet filesD. listening ports Answer: D !!!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=3fI6ShLlZQo