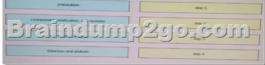
[2017-New-ExamsBraindump2go 210-255 Questions and Answers 70Q Free Offer(41-50)

2017 March Cisco New 210-255: Implementing Cisco Cybersecurity Operations Exam Dumps (Full Version) Released Today!Free INSTANT Download <u>210-255 Exam Dumps (PDF & VCE) 70Q&As</u> 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://ldrv.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.





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: 400) 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

No.	Time	Source	Destination	Protocol	Length	Info		
	17 0.011641	10.0.7.15	192.124.249.9	TOP	76	30305-443	ENVN3	Seque ML
	18 0.011918	10.0.2.15	192.124.249.9	TOP	76	50588.443	ESYN3	Seque MU
	19.0.022656	192.124.249.9	10.0.2.15	TOP	62	443-50588	ESYN,	ACK] See
	20 0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443	[ACK]	Seq=1 Act
	21 0.022908	192.124.249.9	10.0.2.15	TOP	62	443-50586	ESYN.	ACK] Seq
	22.0.022996	10.0.2.15	192.124.249.9	TCP	56	50506-443	[ACK]	Seq=1 Ack
	24 0.023373	10.0.2.15	192.124.249.9	TL5v1.2		Client He		
	25 0.023445	192,124,249.9	10.0.2.15	TCP		443-50588		
	26 0.023617	192.124.249.9	10.0.2.15	TCP		443-50506		Seq-1 Ack
	27 0.037413	192.124.249.9	10.0.2.15	TL5v1.2		Server Hel		
	78 6 637476	16.6.2.15	192 124 249 9	TOP	5.6	50505-441	TACKT	5,000,206-8
110	Feil	ale U	GLA	20		46	I)	"[A]
3	ifeid	Pelt	લામા	Sh-			9	"LA
L L 0000		Field	QUUI	29	joj	FØ.	Ø	Ĩ.f.]"
			والدا *****	29	<u>j</u> 0	EG.	9	"LA
	00 04 00 01 1 45 00 00 15 50 72 19		ولللا		j©.	5 <u>6</u>	9	"LA
	00 04 00 01 1 45 00 01 1 50 7/2 19 09 50 10 7/2 10		والدا *****	29	j	ic.	9	"[AA
0000 0010 0020 0030 0050 0050	00 04 00 01 1 45 00 00 15 50 72 19		وللل		jo.	je.	9	"(AA
0000 0010 0020 0030 0040 0040 0040 0040	00 04 00 01 0 45 00 00 15 60 70 19 00 50 18 72 10 61 43 03 d1 10 37 cc 00 61 90 60		وللل			ie.	<u>o</u>	"(AA
50000 0010 0020 0040 0050 0050 0050 0050	66 64 60 61 1 45 60 66 15 50 10 72 10 50 13 72 10 16 43 ec 44 10 57 c 00 c 0 35 c 0 6a		74 35 93 00 00 0 66 99 27 0a 00 0 87 77 77 00 53 b 53 01 00 0 0 11 6 7 10 44 01 72 05 10 04 00 11 16 7 10 44 01 72 05 14 00 13 00 20 10 10 14 00 13 00 10 10 10		<u>j</u> ej 1.	IG.	O.	AA)"
0000 0010 0020 0030 0040 0040 0040 0040	00 04 00 01 0 45 00 00 15 60 70 19 00 50 18 72 10 61 43 03 d1 10 37 cc 00 61 90 60	Angerer Ang	74 35 93 00 00 0 66 99 27 0a 00 0 87 77 77 00 53 b 53 01 00 0 0 11 6 7 10 44 01 72 05 10 04 00 11 16 7 10 44 01 72 05 14 00 13 00 20 10 10 14 00 13 00 10 10 10	()		5 G	9	"LAA
	66 64 60 61 1 45 60 60 61 1 45 60 60 61 1 45 80 60 7 1 10 12 7 10 1 14 35 60 60 13 16 43 ec 44 10 31 10 16 35 60 60 11 10 37 60 11 11 17 70 17 <		74 3c 93 00 00 0 66 99 27 0a 00 0 80 77 77 00 03 0 30 01 00 c8 01 0 0 04 ce 31 15 f 10 a6 d1 72 d3 1 16 00 04 ce 31 0 14 ce 31 00 14 0 14 00 14 0 10 15 1 14 00 13 00 39 00 14 0			59	9	"[1]
0000 0010 0020 0050 0050 0050 0050 0050	00 04 00 011 45 00 06 05 50 18 72 19 51 10 21 51 10	Arre	74 3c 93 00 00 0 66 99 27 0a 00 0 80 77 77 00 03 0 30 01 00 c8 01 0 0 04 ce 31 15 f 10 a6 d1 72 d3 1 16 00 04 ce 31 0 14 ce 31 00 14 0 14 00 14 0 10 15 1 14 00 13 00 39 00 14 0			5 G	0	"[1]
E 00000 0010 0020 0040 0050 0000 0000 0000 0000 000	00 04 00 011 45 00 06 05 50 18 72 19 51 10 21 51 10	Aure 0 05 08 08 27 0 05 08 08 27 0 05 08 08 08 0 05 08 08 0 0 08 0 0 08 08 0 0 08 0 08 08 0				5.5	I.	"LA
0000 0010 0020 0050 0050 0050 0050 0050	00 04 00 011 45 00 06 05 50 18 72 19 51 10 21 51 10	Arre C C C C C C C C C C C C C C C C C C				9 (5) 	J.	"[AA

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:	source address	destination address
	destination address	Sectoration post
	source port	source port
	muaninste	02010EGOIUD
	Eytes transmitted	number of packets transmitted
	producció	bytes transmitted
	Incq mutanities	produced

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=3fl6ShLlZQo