

210-255^{Q&As}

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/210-255.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

- A. so that everyone knows the local time
- B. to ensure employees adhere to work schedule
- C. to construct an accurate timeline of events when responding to an incident
- D. to guarantee that updates are pushed out according to schedule

Correct Answer: C

QUESTION 2

A 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. reconnaissance
- B. weaponization
- C. delivery
- D. installation

Correct Answer: C

QUESTION 3

Which machine risk to be infected or something like that?

DOMAINS

-100 TO 100

THE HIGHER NUMBER IS SAFER

ABC.COM	100
DEF.COM	-75
123.COM	0

DOMAIN NAME

IP ADDRESSE

ABC.COM	10.0.0.1
DEF.COM	209.165.201.130
123.COM	209.165.200.120

MACHINE	LINK
10.1.0.1	209.165.201.130/443
172.11.5.5	10.0.0.1/80
XXXXX	209.165.200.130/80

- A. 10.1.0.1
- B. 172.11.5.5
- C. Other option

Correct Answer: A

QUESTION 4

DRAG DROP

```
%ASA-6-302015: Built inbound TCP connection 12879515 for  
outside:192.168.1.1/2196 to inside:192.168.2.2/22
```

Refer to the exhibit. Drag and drop the items from the left onto the correct 5-tuple on the right.

Select and Place:

192.168.1.1	Source Port
192.168.2.2	Protocol
2196	Source IP
22	Destination IP
TCP	Destination Port

Correct Answer:

	TCP
	2196
	192.168.1.1
	192.168.2.2
	22

QUESTION 5

What does the CSIRT incident response provider usually do?

- A. provide incident handling services to their parent organization.
- B. provide incident handling services to a country
- C. coordinate and facilitate the handling of incidents across various CSIRTs
- D. focus on synthesizing data from various sources to determine trends and patterns in incident activity
- E. handle reports of vulnerabilities in their software or hardware products
- F. offer incident handling services as a for-fee service to other organizations

Correct Answer: D

[Latest 210-255 Dumps](#)

[210-255 PDF Dumps](#)

[210-255 Practice Test](#)