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.pass2lead.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

Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local

B. physical

C. network

D. adjacent

Correct Answer: B

QUESTION 2

DRAG DROP

```
sIP | dIP| sPort | dPort | pro | packets | bytes | flags | sTime | duration| |eTime
10.232.38.20 | 208.100.26.233 | 80 | 39613 | 6 | 60 | 3120 | A | 2016/10/09T00:09:43.112 | 1774.708 | 2016/10/09T00:39:17.820 |
```

Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5r record from a security event on the right.

Select and Place:

source address	10.232.38.20
destination address	3120
source port	80
number of packets transmitted	208.100.26.233
bytes transmitted	60
protocol	39613
destination port	TCP

Correct Answer:

	source address
	bytes transmitted
	source port
	destination address
	number of packets transmitted
	destination port
	protocol

![Pass2Lead](https://Pass2Lead.com)
QUESTION 3

Which compliance framework applies to safeguarding a patient prescription list?

A. PCI

B. SOX

C. HIPAA

D. COBIT

Correct Answer: C

QUESTION 4

When evidence is collected, what does NIST SP800-86 specify as a guideline to follow for the order of collection?

A. order of volatility

B. order of importance

C. most difficult to access first

D. least difficult to access first

Correct Answer: B

QUESTION 5

Which incident handling phase is focused on minimizing the impact of the incident?

A. reporting

B. remediation

C. containment

D. scoping

Correct Answer: C

[210-255 PDF Dumps](#)　　　　[210-255 VCE Dumps](#)　　　　[210-255 Exam Questions](#)