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.geekcert.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 two useful pieces of information can be collected from the IPv4 protocol header? (Choose two.)

A. UDP port which the traffic is destined

B. source IP address of the packet

C. UDP port from which the traffic is sourced

D. TCP port from which the traffic was source

E. destination IP address of the packet

Correct Answer: BE

QUESTION 2

What information is unnecessary for determining the appropriate containment strategy according to NIST SP800-61 r2?

A. attack vector used to compromise the system

B. effectiveness of the strategy

C. time and resources needed to implement the strategy

D. need for evidence preservation

Correct Answer: A

Reference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf page 35

QUESTION 3

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

QUESTION 4

Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

A. Analysis Center

B. National CSIRT

C. Internal CSIRT

D. Physical Security

Correct Answer: C

QUESTION 5

Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space?

A. confidentiality

B. integrity

C. availability

D. complexity

Correct Answer: C