200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.pass4itsure.com/200-201.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 evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

A. resource exhaustion

B. tunneling

C. traffic fragmentation

D. timing attack

Correct Answer: A

Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of resource exhaustion is "consuming the resources necessary to perform an action." Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

QUESTION 2

What is a difference between data obtained from Tap and SPAN ports?

A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.

B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.

C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.

D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

Correct Answer: D

Reference: https://www.gigamon.com/resources/resource-library/white-paper/to-tap-or-to-span.html

QUESTION 3

An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified\\'? (Choose two.)

A. SOX

B. PII

C. PHI

D. PCI

E. copyright

Correct Answer: BE

QUESTION 4

An organization\\'s security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?

A. by most active source IP

B. by most used ports

C. based on the protocols used

D. based on the most used applications

Correct Answer: A

QUESTION 5

Which type of attack involves executing arbitrary commands on the operating system to escalate privileges?

A. Apache log

B. cross-site scripting

C. command injection

D. SQL injection

Correct Answer: C