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.geekcert.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 step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis

B. preparation

C. eradication

D. containment

Correct Answer: A

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity

Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).

Ref: 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

How does an attacker observe network traffic exchanged between two users?

A. port scanning

B. man-in-the-middle

C. command injection

D. denial of service

Correct Answer: B

QUESTION 4

Why is encryption challenging to security monitoring?

A. Encryption analysis is used by attackers to monitor VPN tunnels.

B. Encryption is used by threat actors as a method of evasion and obfuscation.

C. Encryption introduces additional processing requirements by the CPU.

D. Encryption introduces larger packet sizes to analyze and store.

Correct Answer: B

QUESTION 5

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

A. central key management server

B. web of trust

C. trusted certificate authorities

D. registration authority data

Correct Answer: C