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.passapply.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the relationship between a vulnerability and a threat?

A. A threat exploits a vulnerability

B. A vulnerability is a calculation of the potential loss caused by a threat

C. A vulnerability exploits a threat

D. A threat is a calculation of the potential loss caused by a vulnerability

Correct Answer: A

QUESTION 2

What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic

B. Tapping interrogations detect and block malicious traffic

C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies

D. Inline interrogation detects malicious traffic but does not block the traffic

Correct Answer: A

A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management

QUESTION 3

In a SOC environment, what is a vulnerability management metric?

A. code signing enforcement

B. full assets scan

C. internet exposed devices

D. single factor authentication

Correct Answer: C

QUESTION 4

During a quarterly vulnerability scan, a security analyst discovered unused uncommon ports open and in a listening

state. Further investigation showed that the unknown application was communicating with an external IP address on an encrypted channel. A deeper analysis revealed a command and control communication on an infected server. At which step of the Cyber Kill Chain was the attack detected?

A. Exploitation

B. Actions on Objectives

C. Weaponization

D. Delivery

Correct Answer: B

QUESTION 5

Which type of evasion technique is accomplished by separating the traffic into smaller segments before transmitting across the network?

A. encryption

B. tunneling

C. proxies

D. fragmentation

Correct Answer: D