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.leads4pass.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 netstat command show ports? (Choose two)

A. netstat a

B. netstat -l

C. netstat -v

D. netstat -g

Correct Answer: AB

QUESTION 2

Which description of probabilistic analysis is true?

A. probable proof of a user\\'s identity

B. lack of proof of a user\\'s identity

C. definitive proof of a user\\'s identity

D. false proof of a user\\'s identity

Correct Answer: A

QUESTION 3

Which purpose of data mapping is true?

A. Visualize data.

B. Find extra vulnerabilities.

C. Discover the identities of attackers

D. Check that data is correct.

Correct Answer: D

QUESTION 4

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 5

You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. reconnaissance

B. weaponization

C. delivery

D. action on objectives

Correct Answer: D

[210-255 PDF Dumps](#)   [210-255 Study Guide](#)   [210-255 Braindumps](#)