ValidExamTopics
Your Trusted IT Exam Hub

Get Free Cisco 100-150 Dumps PDF Questions

Why risk failure? Download updated Cisco Certified Support Technician (CCST) Networking exam PDF questions today. Practice with real 100-150 dumps and verified answers designed to help you ace your certification quickly using 100-150 exam pdf questions and answers.

Thank You for Downloading 100-150 Exam PDF Demo

Sample Questions

QUESTION 1

An attacker sends an email impersonating the IT department asking a user to reset their password via a fake
link. Which type of attack is this?

A. Spear phishing [Correct]

B. SQL injection

C. DNS amplification

D. Man-in-the-middle

Correct Answer: A

Explanation

Spear phishing is a targeted email-based social-engineering attack where the attacker impersonates a trusted source to trick the victim into revealing credentials or installing malware. SQL injection targets databases, DNS amplification is a reflection DDoS, and MITM intercepts traffic between two parties.

QUESTION 2

Which symmetric encryption algorithm is currently recommended by NIST for protecting sensitive government data?

A. AES-256 [Correct]

B. DES

C. RC4

D. MD5

Correct Answer: A

Explanation

AES-256 is the recommended symmetric encryption algorithm for protecting sensitive data.
DES is deprecated (56-bit key), RC4 is broken, and MD5 is a hashing algorithm, not encryption.

Sample Questions

QUESTION 3

What is the primary purpose of a network firewall's default-deny rule at the end of an access control list?

A. To log all traffic

B. To explicitly drop any traffic not matched by previous allow rules [Correct]

C. To speed up packet processing

D. To balance load across multiple links

Correct Answer: B

Explanation

A default-deny (implicit deny) rule at the end of an ACL ensures that any traffic not explicitly allowed by prior rules is dropped. This is a foundational principle of least-privilege network security.

QUESTION 4

Which authentication factor is represented by a hardware token that generates a one-time password every 30 seconds?

A. Something you know

B. Something you have [Correct]

C. Something you are

D. Somewhere you are

Correct Answer: B

Explanation

A hardware token is 'something you have' - a possession factor. 'Something you know' is a password/PIN, 'something you are' is a biometric, and 'somewhere you are' is a location factor.

Sample Questions

QUESTION 5

During incident response, which phase follows 'Containment' in the standard SANS/NIST lifecycle?

A. Identification

B. Eradication [Correct]

C. Lessons learned

D. Preparation

Correct Answer: B

Explanation

The SANS/NIST incident response lifecycle is: Preparation ? Identification ? Containment ? Eradication ? Recovery ? Lessons Learned. Eradication removes the threat (e.g., malware, backdoors) after the incident has been contained.