ISLEVER

SY0-201

CompTIA Security+(2008 Edition) Exam

DEMO

https://www.islever.com/sy0-201.html
https://www.islever.com/comptia.html

Topic 1, Volume A

QUESTION NO: 1

Which of the following cryptography types provides the same level of security but uses smaller key sizes and less computational resources than logarithms which are calculated against a finite field?

A. Elliptical curve
B. Diffie-Hellman
C. Quantum
D. El Gamal

Answer: A
Explanation:

QUESTION NO: 2

Which of the following BEST describes the purpose of fuzzing?

A. To decrypt network sessions
B. To gain unauthorized access to a facility
C. To hide system or session activity
D. To discover buffer overflow vulnerabilities

Answer: D
Explanation:

QUESTION NO: 3

A security administrator is reviewing remote access and website logs. The administrator notices that users have been logging in at odd hours from multiple continents on the same day. The security administrator suspects the company is the victim of which of the following types of attack?

A. TCP/IP hijacking
B. Spoofing
C. Replay
D. Domain name kiting

Answer: C
Explanation:

QUESTION NO: 4

Which of the following is the default rule found in a corporate firewalls access control list?

A. Anti-spoofing
B. Permit all
C. Multicast list
D. Deny all

Answer: D
Explanation:

QUESTION NO: 5

Which of the following is the BEST choice of cryptographic algorithms or systems for providing whole disk encryption?

A. One time pad
B. PGP
C. MD5
D. TKIP

Answer: C
Explanation:

QUESTION NO: 6

Which of the following allows a malicious insider to covertly remove information from an organization?

A. NAT traversal
B. Steganography
C. Non-repudiation
D. Protocol analyzer

Answer: B
Explanation:

QUESTION NO: 7

The server log shows 25 SSH login sessions per hour. However, it is a large company and the administrator does not know if this is normal behavior or if the network is under attack. Where should the administrator look to determine if this is normal behavior?

A. Change management
B. Code review
C. Baseline reporting
D. Security policy

Answer: C
Explanation:

QUESTION NO: 8

Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.

Answer: B
Explanation:

QUESTION NO: 9

Which of the following software should a security administrator implement if several users are stating that they are receiving unwanted email containing advertisements?

A. Host-based firewalls
B. Anti-spyware
C. Anti-spam
D. Anti-virus