ISLEVER

SY0-301

CompTIA Security+ 2011

DEMO

https://www.islever.com/sy0-301.html

https://www.islever.com/comptia.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

Topic 1, Volume A

QUESTION NO: 1

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: 2

Which of the following devices is BEST suited for servers that need to store private keys?

A. Hardware security module
B. Hardened network firewall
C. Solid state disk drive
D. Hardened host firewall

Answer: A
Explanation:

QUESTION NO: 3

All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.
B. RC4.
C. SHA-512.
D. MD4.

Answer: B
Explanation:

QUESTION NO: 4

In regards to secure coding practices, why is input validation important?

A. It mitigates buffer overflow attacks.
B. It makes the code more readable.
C. It provides an application configuration baseline.
D. It meets gray box testing standards.

Answer: A
Explanation:

QUESTION NO: 5

Which of the following would be used when a higher level of security is desired for encryption key storage?

A. TACACS+
B. L2TP
C. LDAP
D. TPM

Answer: D
Explanation:

QUESTION NO: 6

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

A. Firewall
B. Application
C. IDS
D. Security

Answer: D
Explanation:

QUESTION NO: 7

Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

A. Registration
B. CA
C. CRL
D. Recovery agent

Answer: C
Explanation:

QUESTION NO: 8

Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

A. Smartcard
B. Token
C. Discretionary access control
D. Mandatory access control

Answer: A
Explanation:

QUESTION NO: 9

Which of the following devices would MOST likely have a DMZ interface?

A. Firewall
B. Switch
C. Load balancer
D. Proxy

Answer: A
Explanation: