ISLEVER

SY0-401

CompTIA Security+ Certification Exam

DEMO

https://www.islever.com/sy0-401.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

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

A. TCP/IP
B. SSL
C. SCP
D. SSH

Answer: B
Explanation:

QUESTION NO: 2

A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO’s requirements?

A. Username and password
B. Retina scan and fingerprint scan
C. USB token and PIN
D. Proximity badge and token

Answer: C
Explanation:

QUESTION NO: 3

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

A. Screen lock
B. Voice encryption
C. GPS tracking
D. Device encryption

Answer: A
Explanation:

QUESTION NO: 4

Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly?

A. Protocol analyzer
B. Baseline report
C. Risk assessment
D. Vulnerability scan

Answer: A
Explanation:

QUESTION NO: 5

Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations

Answer: C
Explanation:

QUESTION NO: 6

A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people. Which of the following would allow the security administrator to test the lack of security controls for those applications with the least impact to the system?

A. Penetration test
B. Vulnerability scan
C. Load testing
D. Port scanner

Answer: B
Explanation:

QUESTION NO: 7

Which of the following risk concepts requires an organization to determine the number of failures per year?

A. SLE
B. ALE
C. MTBF
D. Quantitative analysis

Answer: B
Explanation:

QUESTION NO: 8

A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

A. Disabling unnecessary accounts
B. Rogue machine detection
C. Encrypting sensitive files
D. Implementing antivirus

Answer: B
Explanation:

QUESTION NO: 9

Three of the primary security control types that can be implemented are.

A. Supervisory, subordinate, and peer.
B. Personal, procedural, and legal.
C. Operational, technical, and management.
D. Mandatory, discretionary, and permanent.