Exam Number/Code: SY0-401

Exam Name: CompTIA Security+ Certification

Version: Demo

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

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

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

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

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

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

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

QUESTION NO: 8
Please be aware that if you do not accept these terms you will not be allowed to take this

CompTIA exam and you will forfeit the fee paid.

A. RETURN TO EXAM
B. EXIT EXAM

Answer: A

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.

Answer: C

QUESTION NO: 10
The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

A. Recovery
B. Follow-up
C. Validation
D. Identification
E. Eradication
F. Containment

Answer: D