Vendor: CISCO

Exam Code: SY0-301

Exam Name: CompTIA Security+ Certification Exam
QUESTION 1
Which of the following combinations represents multifactor authentication?

A. Smart card and hard token  
B. Voice print analysis and facial recognition  
C. Username and PIN  
D. Cipher lock combination and proximity badge

Answer: D

QUESTION 2
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering  
B. Use WPA2-PSK  
C. Disable SSD broadcast  
D. Power down unused WAPs

Answer: C

QUESTION 3
Which of the following concepts defines the requirement for data availability?

A. Authentication to RADIUS  
B. Non-repudiation of email messages  
C. Disaster recovery planning  
D. Encryption of email messages

Answer: C

QUESTION 4
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to
prevent this in the future?

A. Business continuity planning
B. Quantitative assessment
C. Data classification
D. Qualitative assessment

Answer: C

QUESTION 5
Which of the following should Sara, a security administrator, perform periodically to reduce an organization's risk exposure by verifying employee access?

A. Account revalidation
B. Incident management
C. Qualitative analysis
D. Quantitative analysis

Answer: A

QUESTION 6
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Answer: A
QUESTION 7
Which of the following explains the difference between a public key and a private key?

A. The public key is only used by the client while the private key is available to all. Both keys are mathematically related.
B. The private key only decrypts the data while the public key only encrypts the data. Both keys are mathematically related.
C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
D. The private key is only used by the client and kept secret while the public key is available to all.

Answer: D

QUESTION 8
Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

A. RIPEMD
B. MD5
C. SHA
D. HMAC

Answer: D

QUESTION 9
A recent network attack caused several random computers to malfunction, even though those computers had the latest updates and patches applied. Which of the following describes this type of attack?

A. Targeted
B. DDoS
C. Zero day
D. Buffer overflow
QUESTION 10
Identifying a list of all approved software on a system is a step in which of the following practices?

A. Passively testing security controls
B. Application hardening
C. Host software baselining
D. Client-side targeting

Answer: C

QUESTION 11
Sara, an administrator, is hardening email application communication to improve security. Which of the following could be performed?

A. Remove gateway settings from the route table
B. Password protect the server BIOS
C. Disabling high I/O services
D. Require TLS when using SMTP

Answer: D

QUESTION 12
Sara, a security analyst, suspects that a rogue web server is running on the network. Which of the following would MOST likely be used to identify the server’s IP address?

A. Port scanner
B. Telnet
C. Traceroute
D. Honeypot

Answer: A
QUESTION 13
Pete, a security administrator, would like to implement laptop encryption to protect data. The Chief Executive Officer (CEO) believes this will be too costly to implement and decides the company will purchase an insurance policy instead. Which of the following is this an example of?

A. Risk avoidance
B. Risk deterrence
C. Risk acceptance
D. Risk transference

Answer: D

QUESTION 14
Which of the following network design elements will allow Jane, a security technician, to access internal company resources without the use of a DS3, Satellite, or T1 connection?

A. CSU/DSU
B. Firewall
C. Router
D. DSL

Answer: A

QUESTION 15
Jane, a security technician, has been called into a meeting with the management team who has a requirement for comprehensive vetting of specialized employees as part of the hiring process. Funding and resources are not an issue since staff members are in high risk positions and have access to sensitive data. Which of the following access control types BEST meets the requirement?

A. Rule based access control
B. Discretionary access control
C. Mandatory access control
D. Role based access control
QUESTION 16
Pete, an IT security technician, has been tasked with implementing physical security controls for his company's workstations. Which of the following BEST meets this need?

A. Host-based firewalls
B. Safe
C. Cable locks
D. Remote wipe

Answer: C

QUESTION 17
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

A. Business continuity planning
B. Continuity of operations
C. Business impact analysis
D. Succession planning

Answer: D

QUESTION 18
Which of the following technologies would allow the removal of a single point of failure?

A. Dual-homing a server
B. Clustering a SQL server
C. Adding a second VLAN to a switch
D. Assigning a second IP address to a NIC

Answer: B
QUESTION 19
A team is developing a new application with many different screens that users can access. The team decides to simplify access by creating just two internal application roles. One role is granted read-only access to the summary screen. The other role is granted update access to all screens. This simplified access model may have a negative security impact on which of the following?

A. Remote access
B. Identity management
C. Least privilege
D. Authentication

Answer: C

QUESTION 20
Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection
B. Theft of the physical database server
C. Cookies
D. Cross-site scripting

Answer: A