CompTIA SY0-201

CompTIA Security+ (2008 Edition) Exam

Version: 7.20

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

Answer: C

Explanation:

QUESTION NO: 10

Adding a second firewall to the perimeter of a network would provide:

A. user VLANs.
B. failover capability.
C. additional bandwidth.
D. management of VLANs.

Answer: B

Explanation:

QUESTION NO: 11

The security administrator is tasked with authenticating users to access an encrypted database. Authentication takes place using PKI and the encryption of the database uses a separate cryptographic process to decrease latency. Which of the following would describe the use of encryption in this situation?

A. Private Key encryption to authenticate users and private keys to encrypt the database
B. Private Key encryption to authenticate users and public keys to encrypt the database
C. Public key encryption to authenticate users and public keys to encrypt the database
D. Public key encryption to authenticate users and private keys to encrypt the database

Answer: D

Explanation:

QUESTION NO: 12

A security device prevents certain users from accessing the network remotely with specific applications, but allows VPN connections without any issues. Which of the following access control models is being used?

A. Mandatory
B. Rule-based

C. Discretionary
D. Role-based

Answer: B

Explanation:

QUESTION NO: 13

Which of the following would provide the MOST reliable proof that a datacenter was accessed at a certain time of day?

A. Video surveillance
B. Security log
C. Entry log
D. Proximity readers

Answer: A

Explanation:

QUESTION NO: 14

Which of the following application attacks typically involves entering a string of characters and bypassing input validation to display additional information?

A. Session hijacking
B. Zero day attack
C. SQL injection
D. Cross-site scripting

Answer: C

Explanation:

QUESTION NO: 15

Which of the following IDS/IPS systems is used to protect individual servers?

A. NIPS
B. NAC

C. GRE
D. HIPS

Answer: D

Explanation:

QUESTION NO: 16

Which of the following technologies directly addresses the need to restrict employees from browsing inappropriate websites?

A. Bastion host
B. Firewall
C. Proxy server
D. Content filter

Answer: D

Explanation:

QUESTION NO: 17

A security administrator working for a health insurance company needs to protect customer data by installing an HVAC system and a mantrap in the datacenter. Which of the following are being addressed? (Select TWO).

A. Integrity
B. Recovery
C. Clustering
D. Confidentiality
E. Availability

Answer: A,E

Explanation:

QUESTION NO: 18

Which of the following camera types would allow a security guard to track movement from one spot throughout a data center?

A. CCTV system
B. PTZ camera
C. Analog camera
D. Digital camera

Answer: B
Explanation:

QUESTION NO: 19

A user reports they are receiving odd emails. Upon investigation, the administrator finds that most of the users email boxes appear to be full and bouncing inbound emails at an alarming rate. Which of the following is MOST likely causing the problem?

A. There is a worm attacking the network.
B. the SMTP relay is not secured.
C. There is a virus attacking the email server.
D. The network is infected by adware.

Answer: D
Explanation:

QUESTION NO: 20

Which of the following describes when forensic hashing should occur on a drive?

A. After the imaging process and before the forensic image is captured
B. Before the imaging process and then after the forensic image is created
C. After the imaging process and after the forensic image is captured
D. Before and after the imaging process and then hash the forensic image

Answer: D
Explanation:

QUESTION NO: 21

A new file share has been created to store confidential exit interviews. Which of the following employees should have access to the file share?

A. Human Resources Manager
B. Chief Financial Officer
C. Human Resources Recruiter
D. System Administrator

Answer: A
Explanation:

QUESTION NO: 22

Which of the following is a valid three factor authentication combination?

A. PIN, thumb print, proximity card
B. PIN, proximity card, key
C. Retina scan, thumb print, proximity card
D. PIN, thumb print, retina scan

Answer: A
Explanation:

QUESTION NO: 23

A security administrator reviews the NIDS logs and notices fourteen unsuccessful logins with a subsequent successful login to a DMZ switch from a foreign IP address. Which of the following could have led to this network device being accessed?

A. Default account
B. Privilege escalation
C. Denial of service
D. Strong password

Answer: B
Explanation:

QUESTION NO: 24

Which of the following has an embedded cryptographic token?

A. PKI certificate
B. TACACS
C. ID badge
D. Smartcard

Answer: D
Explanation:

QUESTION NO: 25

A company runs a site, which has a search option available to the general public. The administrator is reviewing the site logs and notices an external IP address searching on the site at a rate of two hits per second. This is an indication of which of the following?

A. Man-in-the-middle attack
B. Data mining
C. Cross-site scripting attack
D. Denial of Service (DoS)

Answer: B
Explanation:

QUESTION NO: 26

Which of the following allows an attacker to identify vulnerabilities within a closed source software application?

A. Fuzzing
B. Compiling
C. Code reviews
D. Vulnerability scanning

Answer: A
Explanation:

QUESTION NO: 27

Using a combination of a fingerprint reader and retina scanner is considered how many factors of authentication?