➢ TOTAL QUESTIONS: 100

Question: 1

A(n)_____is a one-way mathematical function that maps variable values into smaller values of a fixed length.

A. Symmetric key
B. Algorithm
C. Back door
D. Hash function
E. Integrity

Answer: D

Question: 2

INFOSEC professionals are concerned about providing due care and due diligence. With whom should they consult, when protecting information assets?

A. Law enforcement in their region
B. Senior management, particularly business-unit owners
C. IETF enforcement officials
D. Other INFOSEC professionals
E. Their organizations' legal experts

Answer: E

Question: 3

How do virtual corporations maintain confidentiality?

A. Encryption
B. Checksum
C. Data hashes
D. Redundant servers
E. Security by obscurity

Answer: A

Question: 4

All of the following are possible configurations for a corporate intranet, EXCEPT:

A. Value-added network

B. Wide-area network
C. Campus-area network
D. Metropolitan-area network
E. Local-area network
Answer: A

Question: 5

Which of the following is NOT an auditing function that should be performed regularly?

A. Reviewing IDS alerts
B. Reviewing performance logs
C. Reviewing IDS logs
D. Reviewing audit logs
E. Reviewing system logs
Answer: B

Question: 6

The items listed below are examples of_____controls.
*Procedures and policies
*Employee security-awareness training
*Employee background checks
*Increasing management security awareness

A. Technical
B. Administrative
C. Role-based
D. Mandatory
E. Physical
Answer: B

Question: 7

Digital signatures are typically provided by a_____, where a third party verifies a key's authenticity.

A. Network firewall
B. Security administrator
C. Domain controller
D. Certificate Authority
E. Hash function
Answer: D

Question: 8

Which of the following is MOST likely to cause management to view a security-needs proposal as

invalid?

A. Real-world examples
B. Exaggeration
C. Ranked threats
D. Quantified risks
E. Temperate manner
Answer: B

Question: 9

What is mandatory sign-on? An authentication method that:

A. uses smart cards, hardware tokens, and biometrics to authenticate users; also known as threefactor authentication
B. requires the use of one-time passwords, so users authenticate only once, with a given set of credentials
C. requires users to re-authenticate at each server and access control
D. stores user credentials locally, so that users need only authenticate the first time a local machine is used
E. allows users to authenticate once, and then uses tokens or other credentials to manage subsequent authentication attempts
Answer: C

Question: 10

One individual is selected from each department, to attend a security-awareness course. Each person returns to his department, delivering the course to the remainder of the department. After trainingis complete, each person acts as a peer coach. Which type of training is this?

A. On-line training
B. Formal classroom training
C. Train-the-mentor training
D. Alternating-facilitator training
E. Self-paced training
Answer: C

Question: 11

Which of the following is a cost-effective solution for securely transmitting data between remote offices?

A. Standard e-mail
B. Fax machine
C. Virtual private network
D. Bonded courier
E. Telephone
Answer: C

Question: 12

Which of the following statements about the maintenance and review of information security policies is NOT true?

A. The review and maintenance of security policies should be tied to the performance evaluationsof accountable individuals.
B. Review requirements should be included in the security policies themselves.
C. When business requirements change, security policies should be reviewed to confirm that policies reflect the new business requirements.
D. Functional users and information custodians are ultimately responsible for the accuracy and relevance of information security policies.
E. In the absence of changes to business requirements and processes, information-security policy reviews should be annual.

Answer: D

Question: 13

Which of the following tests provides testing teams some information about hosts or networks?

A. Partial-knowledge test
B. Full-knowledge test
C. Zero-knowledge test

Answer: A

Question: 14

_____can mimic the symptoms of a denial-of-service attack, and the resulting loss in productivity can be no less devastating to an organization.

A. ICMP traffic
B. Peak traffic
C. Fragmented packets
D. Insufficient bandwidth
E. Burst traffic

Answer: D

Question: 15

Which of the following is the MOST important consideration, when developing securityawareness training materials?

A. Training material should be accessible and attractive.
B. Delivery mechanisms should allow easy development of additional materials, to complement core material.
C. Security-awareness training materials should never contradict an organizational security policy.
D. Appropriate language should be used to facilitate localization, should training materials require

translation.
E. Written documentation should be archived, in case of disaster.
Answer: C

Question: 16

To comply with the secure design principle of fail-safe defaults, what must a system do if it receives an instruction it does not understand? The system should:

A. send the instruction to a peer server, to see if the peer can execute.
B. not attempt to execute the instruction.
C. close the connection, and refuse all further traffic from the originator.
D. not launch its debugging features, and attempt to resolve the instruction.
E. search for a close match in the instruction set it understands.
Answer: B

Question: 17

Which of these metrics measure how a biometric device performs, when attempting to authenticate subjects? (Choose THREE.)

A. False Rejection Rate
B. User Acceptance Rate
C. Crossover Error Rate
D. False Acceptance Rate
E. Enrollment Failure Rate
Answer: A, C, D

Question: 18

Why should the number of services on a server be limited to required services?

A. Every open service represents a potential vulnerability.
B. Closed systems require special connectivity services.
C. Running extra services makes machines more efficient.
D. All services are inherently stable and secure.
E. Additional services make machines more secure.
Answer: A

Question: 19

_____intrusion detection involves comparing traffic to known characteristics of malicious traffic, known as attack signatures.

A. Pattern matching
B. Statistical anomaly
C. Behavioral analysis

D. Host
E. Network
Answer: A

Question: 20

Which of the following calculations is used when selecting countermeasures?

A. Annualized Rate of Occurrence
B. Single Loss Expectancy
C. Annualized Loss Expectancy
D. Business Impact Analysis
E. Business Continuity Plan
Answer: C

Question: 21

Virtual corporations typically use a(n)_____for maintaining centralized information assets.

A. Off-line repository
B. Floppy disk
C. Data warehouse
D. CD-ROM burner
E. Colocation
Answer: E

Question: 22

Which of these choices correctly describe denial-of-service (DoS) attacks? (Choose THREE.)

A. DoS attacks do not require attackers to have any privileges on a target system.
B. DoS attacks are nearly impossible to stop, once they begin.
C. DoS attacks free the target system of excessive overhead.
D. DoS ties up a system with so many requests, system resources are consumed, and performance degrades.
E. DoS attacks cause the attacked system to accept legitimate access requests.
Answer: A, B, D

Question: 23

Which of the following is NOT a restriction, for partners accessing internal corporate resources through an extranet?

A. Preventing modification of restricted information
B. Using restricted programs, to access databases and other information resources
C. Allowing access from any location
D. Preventing access to any network resource, other than those explicitly permitted