Chapter 1: Introduction to Information Security

TRUE/FALSE

1. An indirect attack involves a hacker using a personal computer to break into a system.

   ANS: F PTS: 1 REF: 3

2. The value of information comes from the characteristics it possesses.

   ANS: T PTS: 1 REF: 6

3. By balancing information security and access, a completely secure information system can be created.

   ANS: F PTS: 1 REF: 8

4. The security blueprint is a detailed version of the security framework.

   ANS: T PTS: 1 REF: 25

5. One of the basic tenets of security architectures is the spheres of security.

   ANS: F PTS: 1 REF: 30

MULTIPLE CHOICE

1. Which term describes a subject or object's ability to use, manipulate, modify, or affect another subject or object?
   a. Attack
   b. Possession
   c. Exploit
   d. Access

   ANS: D PTS: 1 REF: 3

2. Which resource is a physical asset?
   a. Web site
   b. Computer system
   c. Data
   d. Information

   ANS: B PTS: 1 REF: 3

3. In information security, ____ exists when a vulnerability known to an attacker is present.
   a. threat
   b. loss
   c. risk
   d. exposure

   ANS: D PTS: 1 REF: 4

4. Which term identifies a single instance of an information asset suffering damage, unintended or unauthorized modification, or disclosure?
   a. Exploit
   b. Exposure
   c. Vulnerability
   d. Loss

   ANS: D PTS: 1 REF: 5

5. Organizations must minimize ____ to match their risk appetite.

a. threats
b. access
c. risk
d. loss

ANS: C PTS: 1 REF: 5

6. An unlocked door is an example of a(n) ____.
a. vulnerability
b. threat
c. risk
d. exploit

ANS: A PTS: 1 REF: 5-6

7. The CIA triad is based on three characteristics of information that form the foundation for many security programs: ____.
a. confidentiality, integrity, and asset
b. confidentiality, integrity, and availability
c. confidentiality, information, and availability
d. communication, information, and asset

ANS: B PTS: 1 REF: 7

8. The McCumber Cube provides a ____ description of the architectural approach widely used in computer and information security.
a. linear
b. triangular
c. graphical
d. semantic

ANS: C PTS: 1 REF: 8

9. Which individual interferes with or disrupts systems to protest the operations, policies, or actions of an organization or government agency?
a. Cyberterrorist
b. Packet monkey
c. Phreaker
d. Hacktivist

ANS: D PTS: 1 REF: 11

10. Which individual is considered to be a script kiddie who uses automated tools to inundate a Web site with a barrage of network traffic, usually resulting in a denial of service?
a. Cyberterrorist
b. Packet monkey
c. Phreaker
d. Hacktivist

ANS: B PTS: 1 REF: 12

11. Which threat is the most common intellectual property (IP) breach?
a. Software piracy
b. Spoofing
c. Shoulder surfing
d. Password cracking

ANS: A PTS: 1 REF: 12

12. Which attack is used when a copy of the hash of the user's password has been obtained?
a. Rainbow attack
b. Brute force attack
c. Dictionary attack
d. Spoofing

ANS: A PTS: 1 REF: 13

13. Which e-mail attack occurs when an attacker routes large quantities of e-mail to the target system?
a. Buffer overflow
b. Mail bomb
c. Spam
d. Timing attack

ANS: B PTS: 1 REF: 16

14. A(n) ____ is an application error that occurs when more data is sent to a buffer than it can handle.
    a. timing attack
    b. application control list
    c. dictionary attack
    d. buffer overflow

    ANS: D PTS: 1 REF: 17

15. Which security project team role is filled by a senior executive who promotes the project and ensures that it is supported, both financially and administratively, at the highest levels of the organization?
    a. Team leader
    b. Champion
    c. Chief information officer
    d. Chief information security officer

    ANS: B PTS: 1 REF: 19

16. Which security project team role is filled by individuals who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies?
    a. Security policy developers
    b. Risk assessment specialists
    c. Security professionals
    d. Team leader

    ANS: A PTS: 1 REF: 19

17. When organizations record versions of their policy in English and alternate languages, they are attempting to meet the ____ criteria to make the policy effective and legally enforceable.
    a. Comprehension (understanding)
    b. Compliance (agreement)
    c. Review (reading)
    d. Dissemination (distribution)

    ANS: C PTS: 1 REF: 20

18. A(n) ____ is a written statement of the organization's purpose.
    a. vision
    b. strategic plan
    c. framework
    d. mission

    ANS: D PTS: 1 REF: 21

19. An enterprise information security policy (EISP) is also known as a(n) ____.
    a. issue-specific security policy
    b. general security policy
    c. systems-specific security policy
    d. strategic planning policy

    ANS: B PTS: 1 REF: 21

20. There are two general methods for implementing technical controls within a specific application to enforce policy: ____ and configuration rules.
    a. assessment control lists
    b. authenticity control lists
    c. application control lists
    d. access control lists

    ANS: D PTS: 1 REF: 24

21. The ____ are the foundation of a security framework.
    a. spheres of security
    b. NIST documents
    c. layered implementations of security
    d. CIA triads

    ANS: A PTS: 1 REF: 28

COMPLETION

1. _____ is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

   ANS:
   Information security (InfoSec)
   Information security
   InfoSec

   PTS: 1 REF: 3

2. _____ is a technique used to gain unauthorized access to computers, wherein the intruder sends messages whose IP addresses indicate to the recipient that the messages are coming from a trusted host.

   ANS: Spoofing

   PTS: 1 REF: 15

3. A(n) _____ is a program or device that monitors data traveling over a network.

   ANS: sniffer

   PTS: 1 REF: 17

4. Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of information is referred to as _____.

   ANS: redundancy

   PTS: 1 REF: 30

5. A(n) _____ defines the boundary between the outer limit of an organization's security and the beginning of the outside world.

   ANS: security perimeter

   PTS: 1 REF: 30

MATCHING

Match each item with a statement below.

a. Accuracy
b. Authenticity
c. Availability
d. Confidentiality
e. Data owners
f. Data users
g. Integrity
h. Utility
i. Data custodians

1. People who work directly with data owners and are responsible for the storage, maintenance, and protection of the information.
2. The quality or state of having value for some purpose or end.
3. Enables authorized users to access information without interference or obstruction, and to receive it in the required format.

4. A term meaning information is free from mistakes or errors and has the value that the end user expects it to have.
5. People responsible for the security and use of a particular set of information.
6. A term meaning information remains whole, complete, and uncorrupted.
7. The protection of information from disclosure or exposure to unauthorized individuals or systems.
8. End users who work with the information to perform their daily jobs supporting the mission of the organization, and who therefore share the responsibility for data security.
9. A term referring to the quality or state of being genuine or original rather than a reproduction or fabrication.

1. ANS: I PTS: 1 REF: 6
2. ANS: H PTS: 1 REF: 7
3. ANS: C PTS: 1 REF: 6
4. ANS: A PTS: 1 REF: 6
5. ANS: E PTS: 1 REF: 6
6. ANS: G PTS: 1 REF: 7
7. ANS: D PTS: 1 REF: 6
8. ANS: F PTS: 1 REF: 7
9. ANS: B PTS: 1 REF: 6

SHORT ANSWER

1. List the four important organizational functions an information security program performs.

   ANS:
   An information security program performs four important organizational functions:
   - Protects the organization's ability to function
   - Enables the safe operation of applications implemented on the organization's IT systems
   - Protects the data the organization collects and uses
   - Safeguards the technology assets in use at the organization

   PTS: 1 REF: 9

2. How does a distributed denial-of-service (DDoS) attack work and why are they so dangerous?

   ANS:
   A distributed denial-of-service (DDoS) launches a coordinated stream of requests against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into zombies(or bots), machines that are directed remotely (usually via transmitted command) by the attacker to participate in the attack. DDoS attacks are the most difficult to defend against.

   PTS: 1 REF: 14

3. How does a man-in-the-middle attack work?

   ANS:

In the well-known man-in-the-middle attack, an attacker monitors (or sniffs) packets from the network, modifies them using IP spoofing techniques, and inserts them back into the network, allowing the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data. In a variant attack, the spoofing involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man-in-the-middle - that is, eavesdropper - in encrypted exchanges.

PTS: 1 REF: 15

4. Define social engineering and briefly describe how it is accomplished.

ANS:
Within the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. This can be done in several ways, and usually involves the perpetrator posing as a person higher in the organizational hierarchy than the victim. To prepare for this false representation, the perpetrator may have used social engineering against others in the organization to collect seemingly unrelated information that, when used together, makes the false representation more credible.

PTS: 1 REF: 17

5. Describe the chief information security officer (CISO) position.

ANS:
The chief information security officer (CISO) is the individual primarily responsible for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or a similar title. The CISO usually reports directly to the CIO, although in larger organizations it is common for one or more layers of management to exist between the two.

PTS: 1 REF: 18

6. Describe the issue-specific security policy (ISSP) and list three issues it may cover.

ANS:
The issue-specific security policy (ISSP), which requires frequent updates, addresses specific areas of technology, stating the organization’s position on each issue. Here are some of the issues it may cover:

- Use of company-owned networks and the Internet
- Use of telecommunications technologies (fax and phone)
- Use of e-mail
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of photocopy equipment

PTS: 1 REF: 22-23

7. Define configuration rule policies and compare them to access control lists(ACLs).

ANS:

Configuration rule policies are the specific instructions entered into a security system to regulate how it reacts to the data it receives. Rule-based policies are more specific to the operation of a system than access control lists(ACLs) are, and they may or may not deal with users directly. Many security systems - for example, firewalls, intrusion detection systems (IDSs), and proxy servers - use specific configuration rules to determine how the system handles each data element they process.

PTS: 1 REF: 24

8. Describe the purpose of the Security Area Working Group and RFC 2196.

ANS:
The Security Area Working Group acts as an advisory board for the protocols and areas developed and promoted by the Internet Society and the Internet Engineering Task Force (IETF), and although the group endorses no specific information security architecture, one of its requests for comment, RFC 2196: Site Security Handbook, offers a good discussion of important security issues. The handbook covers five basic areas of security, with detailed discussions on development and implementation. There are also chapters on such important topics as security policies, security technical architecture, security services, and security incident handling.

PTS: 1 REF: 28

9. Describe how benchmarking and best practices are used and where more information on best practices may be found.

ANS:
Benchmarking and best practices are methods used by some organizations to assess security practices. They don't provide a complete methodology for the design and implementation of all the practices needed by an organization; however, it is possible to formulate the desired outcome of the security process and work backwards toward an effective design. The Federal Agency Security Practices (FASP) Web site (fasp.nist.gov) is a popular place to look up best practices. FASP provides best practices for public agencies, but these practices can be adapted easily to private institutions. The documents found at this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.

PTS: 1 REF: 28

10. Discuss the layered implementation of security.

ANS:
One of the basic tenets of security architectures is the layered implementation of security. This layered approach is called defense in depth. To achieve defense in depth, an organization must establish multiple layers of security controls and safeguards, which can be organized into policy, training and education, and technology per the NSTISSC model. Although policy itself may not prevent attacks, it certainly prepares the organization to handle them, and coupled with other layers, it can deter attacks. This is true of training and education, which can also provide some defense against attacks stemming from employee ignorance and social engineering. Technology is also implemented in layers, with detection equipment working in tandem with reaction technology, all operating behind access control mechanisms.

PTS: 1 REF: 30