Chapter 1: Introduction to Information Security

TRUE/FALSE

1. To achieve the maximum confidentiality and integrity found in a completely secure information system would require that the system not allow access (or availability) to anyone.

   ANS: T PTS: 1 REF: 5

2. A majority of organizations use information systems primarily to support their strategic planning.

   ANS: F PTS: 1 REF: 6

3. Acceptance is a viable solution only if the organization has evaluated the risk and determined that the implementation of additional controls or strategies is not justified, due to cost or other organizational issues.

   ANS: T PTS: 1 REF: 10

4. To make sound decisions about information security, management must be informed about the various threats facing the organization, its people, applications, data, and information systems.

   ANS: T PTS: 1 REF: 12

5. Brute force attacks are often successful against systems that have adopted the usual security practices recommended by manufacturers.

   ANS: F PTS: 1 REF: 19

MULTIPLE CHOICE

1. _____ means that information is free from mistakes or errors.

   a. Accuracy
   b. Availability
   c. Confidentiality
   d. Integrity

   ANS: A PTS: 1 REF: 4

2. The _____ is based on a model developed by the U.S. Committee on National Systems Security (CNSS).

   a. TVA worksheet
   b. C.I.A. triangle
   c. McCumber Cube
   d. man-in-the-middle attack

   ANS: C PTS: 1 REF: 4

3. The _____ would typically NOT be a member of the security project team.

   a. CIO
   b. systems adminstrator
   c. CISO
   d. All of these could be a member of the security project team

   ANS: D PTS: 1 REF: 7

4. End users are _____.

   a. not important to the security of an organization

b. a part of the security project team
c. all risk assessment specialists
d. often considered data custodians

ANS: B PTS: 1 REF: 7

5. A data ____ might be a specifically identified role or part of the duties of a systems administrator.
a. owner
b. custodian
c. manager
d. user

ANS: B PTS: 1 REF: 8

6. A(n) ____ is a category of object, person, or other entity that poses a potential risk of loss to an asset.
a. risk
b. exploit
c. threat
d. attack

ANS: C PTS: 1 REF: 8

7. When a computer is the ____ of an attack, it is used as an active tool to conduct the attack.
a. subject
b. victim
c. object
d. direction

ANS: A PTS: 1 REF: 8

8. A(n) ____ attack is when a system is compromised and used to attack other systems.
a. direct
b. indirect
c. object
d. subject

ANS: B PTS: 1 REF: 8

9. A(n) ____ is a weakness or fault in the mechanisms that are intended to protect information and information assets from attack or damage.
a. threat
b. exploit
c. vulnerability
d. risk

ANS: C PTS: 1 REF: 9

10. A ____ attempts to protect internal systems from outside threats.
a. security perimeter
b. botnet
c. risk management strategy
d. buffer overflow

ANS: A PTS: 1 REF: 10

11. ____ refers to multiple layers of security controls and safeguards is called.
a. A DMZ
b. A security perimeter
c. Defense in depth
d. Layered redundancy

ANS: C PTS: 1 REF: 11

12. According the to CSI/FBI Computer Crime and Security Survey, the most dominant type of attack for the last decade was ____.
a. insider abuse
b. denial of service
c. physical loss (theft)
d. malware infection

ANS: D PTS: 1 REF: 12

13. The threat of ____ involves a malicious individual observing another’s password by watching the victim while they are performing system login activities.

a. packet monkeys

b. intellectual property

c. shoulder surfing

d. script kiddies

ANS: C PTS: 1 REF: 16

14. An individual who hacks the public telephone network to make free calls or disrupt services is called a ____.

a. phreaker

b. hactivist

c. packet monkey

d. cyberterrorist

ANS: A PTS: 1 REF: 17

15. A virus that is embedded in the automatically executing scipts commonly found in word processors, spreadsheets, and database applications is called a ____.

a. worm

b. boot virus

c. Trojan horse

d. macro virus

ANS: D PTS: 1 REF: 17

16. A prolonged increase in power is called a ____.

a. spike

b. surge

c. sag

d. fault

ANS: B PTS: 1 REF: 17

17. Attempting to determine a password that is not known to the attacker is often called ____.

a. brute force

b. hacking

c. cracking

d. spamming

ANS: C

Brute force would imply blind guessing. Cracking may involve guiession but can also involve dictionary attacks or other means.

PTS: 1 REF: 18

18. In a ____ attack, the attacker sends a large number of connection or information requests to a target in an attempt to overwhelm its capacity and make it unavailable for legitimate users.

a. man-in-the-middle

b. sniffer

c. dictionary

d. denial-of-service (DoS)

ANS: D PTS: 1 REF: 19

19. ____ is a technique used to gain unauthorized access to computers, wherein the attacker assumes or simulates an address that indicate to the victim that the messages are coming from the address of a trusted host.

a. Sniffing

b. Spoofing

c. Spamming

d. DDoS

ANS: B PTS: 1 REF: 20

20. A ____ is an e-mail attack in which the attacker routes large quantities of e-mail to the target system hoping to overwhelm the target with so much irrelevant email that legitimate email cannot be used.

a. spam attack

b. mail bomb

c. sniffer

d. cracker

ANS: B PTS: 1 REF: 21

21. ____ attacks may involve individuals posing as new employees or as current employees desperately requesting assistance to avoid getting fired.

a. Buffer overflow	c. Social engineering
b. Cracking	d. Spoofing

ANS: C PTS: 1 REF: 22

COMPLETION

1. The ____________________ is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization.

   ANS:
   CIO
   chief information officer
   chief information officer (CIO)

   PTS: 1 REF: 7

2. An organization will often create a network security ____________________, which defines the boundary between the outer limit of an organization's security and the beginning of the outside network.

   ANS: perimeter

   PTS: 1 REF: 10

3. The most common Intellectual Property breach is ____________________.

   ANS: software piracy

   PTS: 1 REF: 16

4. In a(n) ____________________ attack, the attacker monitors (or sniffs) packets from the network, modifies them using Internet Protocol spoofing techniques, and then inserts them back into the network.

   ANS: man-in-the-middle

   PTS: 1 REF: 20

5. A(n) ____________________ is an application error that occurs when more data is sent to a buffer than it can handle.

   ANS: buffer overflow

   PTS: 1 REF: 22

MATCHING

Match each item with a statement below.

a. data custodian
b. Trojan horse
c. integrity
d. back door
e. balance
f. worm
g. accuracy
h. data owner
i. confidentiality

1. Responsible for the security and use of a particular set of information.
2. Information is protected from disclosure or exposure to unauthorized individuals or systems.
3. Involves operating an information system that meets the high level of availability sought by system users as well as the confidentiality and integrity needs of system owners and security professionals
4. Responsible for the storage, maintenance, and protection of the information.
5. Software programs that reveals its designed behavior only when activated.
6. Information remains whole, complete, and uncorrupted.
7. Malicious program that replicates itself constantly.
8. Component in a system that allows the attacker to access the system at will, bypassing standard login controls.
9. Information is free from mistakes or errors.

1.	ANS: H	PTS: 1	REF: 8
2.	ANS: I	PTS: 1	REF: 4
3.	ANS: E	PTS: 1	REF: 5
4.	ANS: A	PTS: 1	REF: 8
5.	ANS: B	PTS: 1	REF: 17
6.	ANS: C	PTS: 1	REF: 4
7.	ANS: F	PTS: 1	REF: 17
8.	ANS: D	PTS: 1	REF: 17
9.	ANS: G	PTS: 1	REF: 4

SHORT ANSWER

1. Describe characteristic of utility as it relates to information.

ANS:
The information has value for some purpose or end. To have utility, information must be in a format meaningful to the end user. For example, U.S. Census data can be overwhelming and difficult to understand; however, when properly interpreted, it reveals valuable information about the voters in a district, what political parties they belong to, their race, gender, age, and so on.

PTS: 1 REF: 4

2. What important organizational functions are performed by Information Security?

ANS:
Information security performs these four important organizational functions:
1. Protects the organization’s ability to function.
2. Enables the safe operation of applications implemented on the organization’s IT systems.
3. Protects the data the organization collects and uses.
4. Safeguards the technology assetsin use at the organization.

PTS: 1 REF: 5

3. Describe the balance between information security and access.

ANS:
Information security must balance protection of information and information assets with the availability of that information to its authorized users. It is possible to permit access to a system so that it is available to anyone, anywhere, anytime, through any means—that is, maximum availability. However, this poses a danger to both the confidentiality and the integrity of the information. On the other hand, to achieve the maximum confidentiality and integrity found in a completely secure information system would require that the system not allow access to anyone.

PTS: 1 REF: 5

4. Describe the importance of enabling the safe operation of applications.

ANS:
Organizations are under immense pressure to acquire and operate integrated, efficient, and capable information systems. They need to safeguard applications, particularly those that serve as important elements of the infrastructure of the organization, such as operating system platforms, electronic mail (e-mail), instant messaging (IM), and all the other applications that make up the current IT environment.

PTS: 1 REF: 6

5. What is the role of the chief information security officer (CISO)?

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, information security officer (ISO), chief security officer (CSO), or by a similar title. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two.

PTS: 1 REF: 7

6. What are the responsibilities of a data custodian?

ANS:
Data custodians work directly with data owners and are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, the custodian may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific practices and procedures specified in the security policies and plans, and reporting to the data owner.

PTS: 1 REF: 8

7. Describe the difference between direct and indirect attacks.

ANS:

A direct attack is when a hacker uses a personal computer to break into a system. An indirect attack is when a system is compromised and used to attack other systems, such as in a botnet (a collection of software programs that operate autonomously to attack systems and steal user information) or other distributed denial-of-service attack. Direct attacks originate from the threat itself. Indirect attacks originate from a system or resource that itself has been attacked and is malfunctioning or working under the control of a threat.

PTS: 1 REF: 8

8. What is defense in depth?

ANS:
One of the basic tenets of security architecture 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, as per the CNSS model discussed earlier. While 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 non-technical attacks such as employee ignorance and social engineering. Social engineering occurs when attackers try to use social interaction with members of the organization to acquire information that can be used to make further exploits against information assets possible.

PTS: 1 REF: 11

9. Describe a dictionary attack.

ANS:
The dictionary attack, which is a variation on the brute force attack, narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations. Organizations can use such dictionaries themselves to disallow passwords during the reset process and thus guard against easy to-guess passwords. In addition, rules requiring additional numbers and/or special characters make the dictionary attack less effective. Another variant, called a rainbow attack, makes use of a pre-computed hash using a time-memory tradeoff technique that uses a database of pre-computed hashes from sequentially calculated passwords to look up the hashed password and read out the text version, with no brute force required.

PTS: 1 REF: 19

10. Provide an example of a social engineering attack.

ANS:
An example of a social engineering attack is the so-called Advance Fee Fraud (AFF), which is known internationally as the “4-1-9” fraud (named after a section of the Nigerian penal code). The perpetrators of 4-1-9 schemes often use fictitious companies, such as the Nigerian National Petroleum Company. Alternatively, they may invent other entities, such as a bank, a government agency, or a nongovernmental organization such as a lottery corporation. This scam is notorious for stealing funds from gullible individuals, first by requiring them to send money up-front in order to participate in a proposed money-making venture, and then by charging an endless series of fees. These 4-1-9 schemes have even been linked to kidnapping, extortion, and murder; and they have, according to the United States Secret Service, bilked over $100 million from unsuspecting Americans lured into disclosing personal banking information.

PTS: 1 REF: 22