Name: _____ Class: _____ Date: _____

chapter 1

Indicate whether the statement is true or false.

1. Today, many attack tools are freely available and do not require any technical knowledge to use.
   a. True
   b. False

2. In a well-run information security program, attacks will never get through security perimeters and local defenses.
   a. True
   b. False

3. Attack tools can initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.
   a. True
   b. False

4. Script kiddies typically have advanced knowledge of computers and networks.
   a. True
   b. False

5. There is a straightforward and easy solution to securing computers.
   a. True
   b. False

Indicate the answer choice that best completes the statement or answers the question.

6. Which of the following is NOT a factor that contributes to difficulties faced in defending against attacks?
   a. Universally connected devices
   b. Greater sophistication of attacks
   c. Enhanced encryption algorithms
   d. Faster detection of vulnerabilities

7. Which of the following is a type of action that has the potential to cause harm?
   a. asset
   b. vulnerability
   c. threat
   d. threat agent

8. What does the FBI define as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents?"
   a. information warfare
   b. cyberware

chapter 1

c. cyberterrorism
d. eTerrorism

9. Which term is best described as a person or element that has the power to carry out a threat?
a. threat agent
b. vulnerability
c. risk
d. attack agent

10. Security is ____ convenience.
a. more important than
b. inversely proportional to
c. proportional to
d. less important than

11. Which of the following involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain?
a. White hat hacking
b. Identity theft
c. Cyberterrorism
d. Digital fraud

12. Which phrase best describes security?
a. the procedures used to protect data
b. the goal to be free from danger as well as the process that achieves that freedom
c. the protection of data from harm
d. the process of hiding sensitive data with the goal of maintaining privacy

13. Where are you most likely to find a PKES system?
a. An automobile
b. An airplane
c. A railroad car
d. A government building

14. Terrorists who turn their attacks to the network and computer infrastructure to cause panic among citizens are known as which of the following?
a. cyberterrorists
b. spies
c. hackers
d. hacktivists

Name: _____ Class: _____ Date: _____

chapter 1

15. What is a flaw or weakness that allows a threat agent to bypass security?

a. risk
b. vulnerability
c. asset
d. threat

16. Information contained on devices is protected by three layers: Two of the layers are products and policies and procedures. What is the third layer?

a. people
b. systems
c. applications
d. tools

17. Which law requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information?

a. Sarbox
b. COPPA
c. GLBA
d. HIPAA

18. From January 2005 through July 2015, approximately how many electronic data records in the United States were breached, exposing to attackers a range of personal electronic data, such as address, Social Security numbers, health records, and credit card numbers?

a. 456,000
b. 22 million
c. 853 million
d. 660 billion

19. Which of the following ensures that data is accessible when needed to authorized users?

a. Confidentiality
b. Non-repudiation
c. Integrity
d. Availability

20. Which attacker category might have the objective of retaliation against an employer?

a. cybercriminal
b. insider
c. hactivist
d. state-sponsored attacker

21. How do attackers today make it difficult to distinguish an attack from legitimate traffic?

chapter 1

a. by using a common language
b. by using diverse interfaces
c. by using common Internet protocols
d. by using simple scripting

22. Under which law must healthcare enterprises guard protected health information and implement policies and procedures to safeguard it, whether it be in paper or electronic format?

a. Sarbox
b. COPPA
c. GLBA
d. HIPAA

23. Which term is best described as individuals who want to attack computers yet who lack the knowledge of computers and networks needed to do so?

a. Hackers
b. Elites
c. Crackers
d. Script kiddies

24. In the past, which term was commonly used to refer to a person who uses advanced computer skills to attack computers?

a. slacker
b. hacker
c. white-hat
d. black-hat

25. What term is frequently used to describe the tasks of securing information that is in a digital format?

a. network security
b. information assurance
c. information security
d. information warfare

26. Which of the following ensures that information is correct and no unauthorized person or malicious software has altered it?

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

Enter the appropriate word(s) to complete the statement.

27. A(n) _____ is defined as something that has a value.

Name: _____ Class: _____ Date: _____

chapter 1

28. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information are sometimes known as _____.

29. In a general sense, _____ can be defined as the necessary steps to protect a person or property from harm.

30. It is vital to have _____ security on all of the personal computers to defend against any attack that breaches the perimeter.

31. It is important that action be taken in advance in order to _____. This may involve keeping backup copies of important data stored in a safe place.

Match each item with a statement below.

a. authentication
b. authorization
c. confidentiality
d. cybercrime
e. exploit kit
f. identity theft
g. insiders
h. integrity
i. threat vector

32. steps that ensure that the individual is who he or she claims to be

33. the process of providing proof of genuineness

34. the act of providing permission or approval to technology resources

35. targeted attacks against financial networks, unauthorized access to information, and the theft of personal information

36. automated attack package that can be used without an advanced knowledge of computers

37. stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain

38. employees, contractors, and business partners who can be responsible for an attack

39. security actions that ensure that the information is correct and no unauthorized person or malicious software has altered the data

40. the means by which an attack could occur

Name: _____ Class: _____ Date: _____

chapter 1

41. Discuss the difficulties in defending systems when dealing with user confusion.

42. Briefly describe hactivists from an information security point of view.

43. Discuss the difficulties in defending against distributed attacks.

44. Discuss the difficulties in defending against the speed of attacks.

45. Discuss the difficulties in defending against the availability and simplicity of attack tools.

46. What is PKES and what are its risks?

47. Discuss the difficulties in defending systems when there are delays in security updating products.

48. Discuss the difficulties in defending against the greater sophistication of attacks.

49. Briefly describe state notification and security laws.

50. What are cybercriminals?

Name: _____ Class: _____ Date: _____

chapter 1

Answer Key

1. True

2. False

3. True

4. False

5. False

6. c

7. c

8. c

9. a

10. b

11. b

12. b

13. a

14. a

15. b

16. a

17. c

18. c

19. d

20. b

21. c

22. d

23. d

24. b

chapter 1

25. c

26. d

27. asset

28. cybercrime

29. security

30. local

31. minimize losses

32. a

33. b

34. c

35. d

36. e

37. f

38. g

39. h

40. i

41. Increasingly, users are called upon to make difficult security decisions regarding their computer systems, sometimes with little or no information to direct them. It is not uncommon for a user to be asked security questions such as Do you want to view only the content that was delivered securely? or Is it safe to quarantine this attachment? or Do you want to install this extension? With little or no direction, users are inclined to provide answers to questions without understanding the security risks. In addition, popular information that is circulated about security through consumer news outlets or websites is often inaccurate or misleading, resulting in even more user confusion.

42. Hactivists are motivated by ideology. Unlike cyberterrorists, who launch attacks against nations, hactivists (a combination of the words hack and activism) direct their attacks at specific Web sites. Generally these attacks are intended to promote a political agenda and are in retaliation for a prior event. For example, hactivists might attempt to disable a bank's Web site because that bank stopped accepting online payments that were deposited into accounts belonging to the hactivists.

43. Attackers can use hundreds of thousands of computers under their control in an attack against a single server or network. This "many against one" approach makes it virtually impossible to stop an attack by identifying and blocking a single source.

44. With modern technology attackers can quickly scan millions of devices to find weaknesses and launch attacks with unprecedented speed. Today's attack tools initiate new attacks without any human participation, thus increasing the

speed at which systems are attacked.

45. Whereas in the past an attacker needed to have an extensive technical knowledge of networks and computers, as well as the ability to write a program to generate the attack, that is no longer the case. Today's attack tools do not require any sophisticated knowledge. In fact, many of the tools have a graphical user interface (GUI) that allows the user to easily select options from a menu. These tools are freely available or can be purchased from other attackers at a low cost.

46. Many cars today offer a Passive Keyless Entry and Start (PKES) system, which allows the driver to unlock the doors and start the car without having to take the key out of her pocket or purse. All a driver has to do is get close enough to the car for the wireless signal from their key fob to be detected by the car, and once detected the doors automatically unlock and the engine can be started by pushing a button on the dashboard. One risk of a PKES is that an attacker can use an amplifier to strengthen the signal from the key fob to the car, thereby giving the attacker access to the car even though the key fob may be up to 50 feet away.

47. Hardware and software vendors are overwhelmed trying to keep pace with updating their products against attacks. One antivirus software security institute receives more than 390,000 submissions of potential malware each day.15 At this rate the antivirus vendors would have to create and distribute updates every few seconds to keep users fully protected. This delay in distributing security updates adds to the difficulties in defending against attacks.

48. Attacks are becoming more complex, making it more difficult to detect and defend against them. Attackers today use common Internet tools and protocols to send malicious data or commands to attack computers, making it difficult to distinguish an attack from legitimate traffic. Other attack tools vary their behavior so the same attack appears differently each time, further complicating detection.

49. These laws typically require businesses to inform residents within a specific period of time (typically 48 hours) if a breach of personal information has or is believed to have occurred. The penalties for violating these laws can be sizeable. Businesses must make every effort to keep electronic data secure from hostile outside forces to ensure compliance with these laws and avoid serious legal consequences.

50. The generic term cybercriminals is often used to describe individuals who launch attacks against other users and their computers (another generic word is simply attackers). However, strictly speaking cybercriminals are a loose network of attackers, identity thieves, and financial fraudsters who are highly motivated, less risk averse, well funded, and tenacious. Some security experts believe that many cybercriminals belong to organized gangs of young attackers, often clustered in Eastern European, Asian, and Third World regions.