**Chapter 1 Review Questions**

1. Each of the following is a reason it is difficult to defend against today’s attackers except \_\_\_\_\_\_\_\_\_\_\_.

a. complexity of attack tools – PG9

b. weak patch distribution

c. greater sophistication of attacks

d. delays in patching software products

2. In a general sense, “security” is

a. protection from only direct actions

b. using reverse attack vectors (RAV) for protection

c. only available on hardened computers and systems

d. the necessary steps to protect a person or property from harm – PG11

3. \_\_\_\_\_\_\_\_\_\_\_\_\_ensures that only authorized parties can view the information.

a. Confidentiality – PG12

b. Availability

c. Integrity

d. Authorization

4. Each of the following is a successive layer in which information security is achieved except \_\_\_\_\_\_\_\_\_\_\_.

a. products

b. purposes – PG14

c. procedures

d. people

5. By definition, a(n) \_\_\_\_\_\_\_\_\_ is a person or thing that has the power to carry out a threat.

a. vulnerability

b. exploit

c. threat agent – PG16

d. risk

6. \_\_\_\_\_\_\_\_\_\_ ensures that the individual is who they claim to be.

a. Authentication – PG13

b. Accounting

c. Access control

d. Certification

7. Each of the following is a goal of information security except \_\_\_\_\_\_\_\_\_\_\_\_.

a. foil cyberterrorism

b. avoid legal consequences

c. decrease user productivity – PG16

d. prevent data theft

8. The \_\_\_\_\_\_\_\_\_ requires that enterprises must guard protected health information and implement policies and procedures to safeguard it.

a. Hospital Protection and Insurance Association Agreement (HPIAA)

b. Sarbanes-Oxley Act (Sarbox)

c. Gramm-Leach-Bliley Act (GLBA)

d. Health Insurance Portability and Accountability Act (HIPAA) – PG18

9. Utility companies, telecommunications, and financial services are considered prime targets of\_\_\_\_\_\_\_\_\_\_\_\_\_ because attackers can significantly disrupt business and personal activities by destroying a few targets.

a. white hat hackers

b. script kiddies

c. computer spies

d. cyberterrorists – PG23

10. After an attacker has probed a network for information, the next step is to \_\_\_\_\_\_\_\_\_\_\_.

a. penetrate any defenses – PG24

b. paralyze networks and devices

c. circulate to other systems

d. modify security settings

11. An organization that purchased security products from different vendors is demonstrating which security principle?

a. obscurity

b. diversity – PG26

c. limiting

d. layering

12. Each of the following can be classified as an “insider” except \_\_\_\_\_\_\_\_\_\_\_.

a. business partners

b. contractors

c. cybercriminals – PG20

d. employees

13. \_\_\_\_\_\_\_\_\_\_ are a network of attackers, identity thieves, and financial fraudsters.

a. Script kiddies

b. Hackers

c. Cybercriminals – PG22

d. Spies

14. Each of the following is a characteristic of cybercriminals except \_\_\_\_\_\_\_\_\_\_\_.

a. better funded

b. less risk-averse

c. low motivation – PG22

d. more tenacious

15. Each of the following is a characteristic of cybercrime except \_\_\_\_\_\_\_\_\_.

a. targeted attacks against financial networks

b. exclusive use of worms and viruses – PG22

c. unauthorized access to information

d. theft of personal information

16. An example of a(n) \_\_\_\_\_\_\_\_ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password.

a. threat agent

b. threat

c. vulnerability – PG16

d. asset exploit (AE)

17. \_\_\_\_\_\_\_\_\_ requires banks and financial institutions to alert customers of their poli- cies and practices in disclosing customer information and to protect all electronic and paper documents containing personally identifiable financial information.

a. California Savings and Loan Security Act (CS&LSA)

b. Gramm-Leach-Bliley Act (GLBA) – PG18

c. USA Patriot Act

d. Sarbanes-Oxley Act (Sarbox)

18. The term \_\_\_\_\_\_\_\_\_\_\_ is sometimes used to identify anyone who illegally breaks into a computer system.

a. hacker – PG20

b. cyberterrorist

c. Internet Exploiter

d. cyberrogue

19. An example of \_\_\_\_\_\_\_\_\_\_ is not revealing the type of computer, operating system, software, and network connection a computer uses.

a. obscurity – PG27

b. limiting

c. diversity

d. layering

20. The \_\_\_\_\_\_\_\_\_ is primarily responsible for assessment, management, and implementation of security

a. security manager

b. security administrator

c. Chief Information Security Officer (CISO) – PG4

d. security technician

**Chapter 2 Review Questions**

1. A \_\_\_\_\_\_\_\_\_\_ requires a user to transport it from one computer to another.

a. worm

b. rootkit

c. virus – PG46

d. Trojan

2. Each of the following is an action that a virus can take except \_\_\_\_\_\_\_\_\_\_.

a. transport itself through the network to another device – PG46

b. cause a computer to crash

c. erase files from a hard drive

d. make multiple copies of itself and consume all of the free space in a hard drive

3. Each of the following is a different type of computer virus except \_\_\_\_\_\_\_\_\_\_\_\_\_.

a. program virus

b. macro virus

c. remote virus – PG47

d. boot virus

4. Li downloads a program that prints coupons, but in the background it silently collects her passwords. Li has actually downloaded a \_\_\_\_\_\_\_\_.

a. virus

b. worm

c. Trojan – PG49

d. logic bomb

5. To completely remove a rootkit from a computer, you should \_\_\_\_\_\_\_\_\_\_.

a. flash the ROM BIOS

b. erase and reinstall all files in the WINDOWS folder

c. expand the Master Boot Record

d. reformat the hard drive and reinstall the operating system – PG51

6. Each of the following could be a logic bomb except \_\_\_\_\_\_\_\_\_\_.

a. erase all data if John Smith’s name is removed from the list of employees

b. reformat the hard drive three months after Susan Jones left the company

c. send spam e-mail to all users – PG51

d. if the company’s stock price drops below $10, then credit Jeff Brown with 10 additional years of retirement credit.

7. \_\_\_\_\_\_\_ is an image spam that is divided into multiple images, and each piece of the message is divided and then layered to create a complete and legible message.

a. Word splitting

b. Geometric variance

c. GIF layering – PG63

d. Split painting

8. \_\_\_\_\_\_ is a general term used for describing software that gathers information without the user’s consent.

a. Adware

b. Scrapeware

c. Pullware

d. Spyware – PG54

9. Each of the following is true regarding a keylogger except \_\_\_\_\_\_\_\_.

a. hardware keyloggers are installed between the keyboard connector and computer keyboard or USB port

b. software keyloggers are easy to detect – PG56

c. keyloggers can be used to capture passwords, credit card numbers, or personal information

d. software keyloggers can be designed to send captured information automatically back to the attacker through the Internet

10. The preferred method today of bot herders for command and control of zombies is to use \_\_\_\_\_\_\_\_.

a. Internet Relay Chat (IRC) – PG52

b. e-mail

c. Hypertext Transport Protocol (HTTP)

d. spam

11. Which of the following is a social engineering technique that uses flattery on a victim?

a. Conformity

b. Friendliness

c. Fear

d. Ingratiation – PG58

12. \_\_\_\_\_\_\_ sends phishing messages only to wealthy individuals.

a. Spear phishing

b. Target phishing

c. Microing

d. Whaling – PG59

13. \_\_\_\_\_\_\_\_\_\_\_ is unsolicited instant messaging.

a. Spam

b. Vishing

c. SMS Phishing (SMS-P)

d. Spim – PG62

14. Erin pretends to be a manager from another city and calls Nick to trick him into giving her his password. What social engineering attack has Erin performed?

a. Aliasing

b. Luring

c. Impersonation – PG58

d. Duplicity

15. How can an attacker use a hoax?

a. A hoax could convince a user that a bad Trojan is circulating and that he should change his security settings. – PG63

b. By sending out a hoax, an attacker can convince a user to read his e-mail more often.

c. A user who receives multiple hoaxes could contact his supervisor for help.

d. Hoaxes are not used by attackers today.

16. Which of the following is not an item that could be retrieved through dumpster diving that would provide useful information?

a. Calendars

b. Memos

c. Organizational charts

d. Books – PG65

17. \_\_\_\_\_\_\_\_\_\_ is following an authorized person through a secure door.

a. Tagging

b. Tailgating – PG66

c. Social Engineering Following (SEF)

d. Backpacking

18. Each of the following is the reason adware is scorned except \_\_\_\_\_\_\_.

a. it displays the attackers programming skills – PG55

b. it displays objectionable content

c. it can cause a computer to crash or slow down

d. it can interfere with a user’s productivity

19. An attacker who controls multiple zombies in a botnet is known as a \_\_\_\_\_\_\_\_\_.

a. zombie shepherd

b. rogue IRC

c. bot herder – PG52

d. cyberrobot

20. Observing someone entering a keypad code from a distance is known as \_\_\_\_\_\_\_\_\_.

a. shoulder surfing – PG66

b. piggybacking

c. spoofing

d. watching