Name:_____ Class:_____ Date:_____

Chapter 2

Indicate whether the statement is true or false.

1. Because of how a rootkit replaces operating system files, it can be difficult to remove a rootkit from a system.
   a. True
   b. False

2. Spreading similarly to a virus, a worm inserts malicious code into a program or data file.
   a. True
   b. False

3. Successful attacks on computers today consist of a single element, malicious software programs that are created to infiltrate computers with the intent to do harm.
   a. True
   b. False

4. A macro is a series of instructions that can be grouped together as a single command.
   a. True
   b. False

5. Software keyloggers are programs that silently capture all keystrokes, including passwords and sensitive information.
   a. True
   b. False

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

6. Which of the following is malicious computer code that reproduces itself on the same computer?
   a. virus b. worm
   c. adware d. spyware

7. Of the three types of mutating malware, what type changes its internal code to one of a set number of predefined mutations whenever it is executed?
   a. Oligomorphic malware
   b. Polymorphic malware
   c. Metamorphic malware
   d. Statimorphic malware

8. What term below is used to describe a means of gathering information for an attack by relying on the weaknesses of individuals?
   a. Phreaking b. Hacking
   c. Social engineering d. Reverse engineering

9. What type of malware consists of a set of software tools used by an attacker to hide the actions or presence of other types of malicious software, such as Trojans, viruses, or worms?
   a. rootkit b. backdoor
   c. wrapper d. shield

Name:_____ Class:_____ Date:_____

Chapter 2

10. How many different Microsoft Windows file types can be infected with a virus?
    a. 50 b. 60
    c. 70 d. 80

11. One of the armored virus infection techniques utilizes encryption to make virus code more difficult to detect, in addition to separating virus code into different pieces and inject these pieces throughout the infected program code. What is the name for this technique?
    a. stealth b. appender
    c. Swiss cheese d. split

12. Computer code that is typically added to a legitimate program but lies dormant until it is triggered by a specific logical event is known as a?
    a. Trojan b. logic bomb
    c. macro virus d. metamorphic virus

13. What is the term used to describe unsolicited messages received on instant messaging software?
    a. Spam
    b. Spim
    c. Splat
    d. Crust

14. The two types of malware that require user intervention to spread are:
    a. Viruses and trojans b. Rootkits and worms
    c. Trojans and worms d. Rootkits and Trojans

15. Which of the following is not one of the four methods for classifying the various types of malware?
    a. Circulation
    b. Infection
    c. Concealment
    d. Source

16. A series of instructions that can be grouped together as a single command and are often used to automate a complex set of tasks or a repeated series of tasks are known as:
    a. A rootkit b. A macro
    c. A program d. A process

17. A virus that infects an executable program file is known as?
    a. macro virus b. program virus
    c. companion virus d. boot sector virus

18. What type of malware is heavily dependent on a user in order to spread?
    a. Trojan b. worm
    c. rootkit d. virus

19. What type of attack is targeted against a smaller group of specific individuals, such as the major executives working for a manufacturing company?

Chapter 2

a. Spam
b. Adware
c. Watering Hole
d. Typo Squatting

20. Select below the type of malware that appears to have a legitimate use, but actually contains or does something malicious:
a. script b. virus
c. Trojan d. worm

21. What type of system security malware allows for access to a computer, program, or service without authorization?
a. Botnet
b. Zombie
c. Backdoor
d. Command and Control

22. The physical procedure whereby an unauthorized person gains access to a location by following an authorized user is known as?
a. Dumpster diving
b. Tailgating
c. Stalking
d. Shadowing

23. Malware that locks or prevents a device from functioning properly until a fee has been paid is known as:
a. Lockware
b. Ransomware
c. Stealware
d. Hostageware

24. What kind of software program delivers advertising content in a manner that is unexpected and unwanted by the user, and is typically included in malware?
a. Adware b. Keylogger
c. Spam d. Trojan

25. What type of undocumented yet benign hidden feature launches after a special set of commands, key combinations, or mouse clicks, and was no longer included in Microsoft software after the start of their Trustworthy Computing initiative?
a. Trojan horse b. virus
c. bug d. Easter egg

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

26. A macro virus takes advantage of the "_____" relationship between the application and the operating system.

27. A(n) _____ is either a small hardware device or a program that monitors each keystroke a user types on the computer's keyboard.

Chapter 2

28. In the _____ technique, the virus is divided into several parts and the parts are placed at random positions throughout the host program, overwriting the original contents of the host.

29. Malicious software, or _____, silently infiltrate computers with the intent to do harm.

30. _____ is a general term used to describe software that secretly spies on users by collecting information without their consent.

Match the following terms to the appropriate definitions.

a. Adware b. Backdoor
c. Botnet d. Computer virus
e. Hoax f. Keylogger
g. Logic bomb h. Macro virus
i. Spear phishing j. Vishing

31. A software program that delivers advertising content in a manner that is unexpected and unwanted by the user.

32. Computer code that lies dormant until it is triggered by a specific logical event

33. A logical computer network of zombies under the control of an attacker.

34. A false warning designed to trick users into changing security settings on their computer

35. A phishing attack that uses telephone calls instead of e-mails.

36. Software code that gives access to a program or a service that circumvents normal security protections.

37. A computer virus that is written in a script known as a macro

38. Software or a hardware device that captures and stores each keystroke that a user types on the computer's keyboard.

39. A phishing attack that targets only specific users

40. Malicious computer code that, like its biological counterpart, reproduces itself on the same computer.

41. What is a worm?

42. Describe adware.

43. How does a rootkit work?

44. What is a backdoor and what is it used for?

45. What are some of the functions performed by viruses?

46. What is malware?

Name:_____ Class:_____ Date:_____

Chapter 2

47. Explain how an appender infection works.

48. Describe a macro virus.

49. Due to the prevalence of text filters for filtering spam, how have spammers modified their attacks?

50. What are botnets?

Name:_____ Class:_____ Date:_____

Chapter 2

Answer Key

1. True

2. False

3. False

4. True

5. True

6. a

7. a

8. c

9. a

10. c

11. c

12. b

13. b

14. a

15. d

16. b

17. b

18. d

19. c

20. c

21. c

22. b

23. b

24. a

25. d

Chapter 2

26. trust

27. keylogger

28. split infection

29. malware

30. Spyware

31. a

32. g

33. c

34. e

35. j

36. b

37. h

38. f

39. i

40. d

41. A worm is a malicious program that uses a computer network to replicate, and is designed to enter a computer through the network then take advantage of vulnerability in an application or an operating system on the host computer.

42. Adware delivers advertising content in a manner that is unexpected and unwanted by the user. Once it becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals.

43. One approach used by rootkits is to alter or replace operating system files with modified versions that are specifically designed to ignore malicious activity. For example, on a computer the anti-malware software may be instructed to scan all files in a specific directory and in order to do this, the software will receive a list of those files from the operating system. A rootkit will replace the operating system's ability to retrieve a list of files with its own modified version that ignores specific malicious files. The anti-malware software assumes that the computer will willingly carry out those instructions and retrieve all files; it does not know that the computer is only displaying files that the rootkit has approved.

44. A backdoor gives access to a computer, program, or service that circumvents any normal security protections. Backdoors that are installed on a computer allow th attacker to return at a later time and bypass security settings.

45. Viruses have performed the following functions:
• Caused a computer to crash repeatedly
• Erased files from a hard drive
• Made multiple copies of itself and consumed all of the free space in a hard drive
• Turned off the computer's security settings

Name:_____ Class:_____ Date:_____

Chapter 2

• Reformatted the hard disk drive

46. Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted—and usually harmful—action. Malware is a general term that refers to a wide variety of damaging or annoying software programs. One way to classify malware is by its primary objective. Some malware has the primary goal of rapidly spreading its infection, while other malware has the goal of concealing its purpose. Another category of malware has the goal of making a profit for its creators.

47. The virus first appends itself to the end of a file. It then moves the first three bytes of the original file to the virus code and replaces them with a "jump" instruction pointing to the virus code. When the program is launched, the jump instruction redirects control to the virus.

48. A macro virus is written in a script known as a macro. A macro is a series of commands and instructions that can be grouped together as a single command. Macros often are used to automate a complex set of tasks or a repeated series of tasks. Macros can be written by using a macro language, such as Visual Basic for Applications (VBA), and are stored within the user document (such as in an Excel .XLSX worksheet). A macro virus takes advantage of the "trust" relationship between the application (Excel) and the operating system (Microsoft Windows). Once the user document is opened, the macro virus instructions execute and infect the computer.

49. Spammers have turned to image spam, which uses graphical images of text in order to circumvent text-based filters.

50. Botnets are collections of thousands or even hundreds of thousands of zombie computers are gathered into a logical computer network under the control of an attacker, or bot herder.