Chapter 02

Computer Security Basics

Multiple Choice Questions

1. What is the generic term for a mode or method of malware infection?

   A. firewall
   B. virus
   C. DMZ
   D. vector

2. What type of malware is also a vector and gets its name from Virgil's famous epic poem, *The Aeneid*, which described how Greek warriors gained access to the City of Troy?

   A. botnet
   B. Trojan horse
   C. backdoor
   D. DMZ

3. What is the oldest malware vector?

   A. sneakernet
   B. back door
   C. war driving
   D. bluesnarfing

4. What term describes a password cracker that tries a huge number of possible passwords?

   A. keylogger
   B. cracker
   C. zombie
   D. brute-force

5. What type of malware replicates itself on a computer or throughout a network?

   A. zero-day exploit
   B. worm
   C. botnet
   D. zombie

6. What term describes a group of networked computers infected with malware that forward information to other computers?

   A. Trojan horse
   B. worm
   C. botnet
   D. zombie

7. What term is used for a computer that belongs to a group of networked computers, all working mindlessly to serve the person who installed the program on the computers?

   A. Trojan horse
   B. worm
   C. botnet
   D. zombie

8. What type of malware is spyware that collects information about the user's browsing habits in order to display advertisements in the browser targeted to that user?

A. zero-day exploit
B. browser hijacking
C. adware
D. worm

9. What type of threat points your browser's home page to a website you did not chose, and may even keep you from changing the default home page for the browser?

A. bluesnarfing
B. phishing
C. browser hijacking
D. key logging

10. What term describes unsolicited instant messages?

A. spam
B. browser hijacking
C. phishing
D. spim

11. What term describes malware that takes advantage of a vulnerability in an operating system or application that is (as yet) unknown to the publisher, leaving systems using that software vulnerable until the vulnerability is detected and patched?

A. zero-day exploit
B. browser hijacking
C. spim
D. bluesnarfing

12. You receive an e-mail message from a friend claiming that she is in another country, in trouble, and urgently needs money wired to her. You call the friend, and discover that she is safe at home and did not know about the message. This scenario is an example of a/an _____.

    A. spam
    B. browser hijacking
    C. hoax
    D. war driving

13. This method of malware infection installs malware through use of a separate browser window that opens uninvited from a Web page. If you click within the window, you may unknowingly agree to install malware.

    A. rootkit
    B. pop-up download
    C. drive-by download
    D. hoax

14. Once installed, this type of malware becomes a vector giving other malware administrative access to a computer.

    A. rootkit
    B. pop-up download
    C. drive-by download
    D. hoax

15. An e-mail containing enticements (often appealing to human weaknesses) to open attachments is a form of what type of threat?

A. phishing
B. hoax
C. social engineering
D. worm

16. This software or hardware device examines network traffic and allows or rejects traffic into a network or computer based on predefined rules.

A. proxy service
B. DMZ
C. firewall
D. VPN

17. Combine this technology with a firewall for a very safe way to connect two private networks over the Internet.

A. proxy service
B. DMZ
C. firewall
D. VPN

18. Also called an application-layer gateway, this software will watch for application-specific traffic, acting as a stand-in for internal computers.

A. proxy service
B. DMZ
C. firewall
D. VPN

19. It is a good idea to install or enable one of these on your computer, even if your network has similar protection between it and other networks.

A. Administrator
B. secret key
C. DMZ
D. personal firewall

20. This type of software protects against unsolicited e-mail, filtering out those that have certain characteristics.

A. antivirus
B. spam filter
C. firewall
D. proxy service

21. A set of these should exist in both document form and software form for any organization.

A. cookies
B. account lockout policy
C. anti-spyware
D. security policies

22. If your private network has both client computers needing Internet access and servers that must be available from the Internet, you should create this separate network for those servers in order to keep Internet-initiated traffic from entering the network containing your client computers. What is the term for the network where the servers are located?

A. back door
B. DMZ
C. botnet
D. firewall

23. What type of security software can you use to both protect from malware infections and also to scan disk space and RAM looking for installed malware?

A. antivirus
B. anti-spam
C. firewall
D. proxy service

24. To enable and configure this security feature in Windows Internet Options, you must use a password-protected administrator type account and apply this feature to an existing standard account.

A. content filtering
B. Parental Controls
C. certificates
D. cookies

25. After several failed attempts to log on/sign in to your Windows computer you see a message stating that your account has been locked out. What caused this problem?

A. Wrong password
B. Too many failed attempts
C. Wrong username
D. Incorrect version of Windows

26. This special file holds a secret key.

A. cookie
B. token
C. vector
D. digital certificate

27. Use this type of program to guard against an especially annoying type of adware that appears in your browser and blocks the content you want to see.

A. pop-up blocker
B. antivirus
C. spam filter
D. content filter

28. Which of the following is among the symptoms of a possible malware infection?

A. adware
B. unsolicited e-mail
C. sudden computer slowdown
D. an error message when you enter your password

29. You attempt to install software in Windows; and although you are logged on with a computer administrator type of account, your screen turns grey and you receive a message asking if you want to allow the program to make changes to the computer. What Windows feature is at work here?

A. HTTPS
B. UAC
C. EFS
D. authentication

30. Your computer has been showing signs of a malware infection, and today it started up in Safe Mode. Because your computer is not a member of an Active Directory domain, what all-powerful built-in account can you log on with?

A. Guest
B. standard user
C. root
D. Administrator

True / False Questions

31. HTTPS uses a private key to encrypt data between a client and an e-commerce server.

True False

32. Cookies are always a threat.

True False

33. Windows EFS encrypts entire drives.

True False

34. FileVault is a data encryption feature in OS X.

True False

35. When you access a Web page to pay for an online purchase, it should show HTTPS as the protocol in the address line.

True False

36. We recommend that you block first-party cookies and allow third-party cookies.

    True False

37. You must use data wiping software on a hard drive before installing a new operating system.

    True False

38. FileVault, a feature of some editions of Windows, allows you to encrypt an entire drive.

    True False

39. Windows will warn you if you try to log on with the Caps Lock key turned on.

    True False

40. A Windows computer that is a member of a domain will have a local account named Administrator that you can access when your computer starts up in Safe Mode.

    True False

Short Answer Questions

41. What does the term "malware" stand for?

42. Briefly define the security tool known as a honey pot.

43. Define EFS.

44. What should you do before donating an old computer to your favorite charity?

45. Provide at least two common symptoms of a malware infection.

46. After encrypting a file using the Windows Encrypting File System (EFS) you move the file to another NTFS-formatted volume. Is the file still encrypted? Explain your answer.

47. You believe your computer is infected by malware, but you have not kept your security software up-to-date. How can you quickly run an up-to-date scan for malware, providing you have an Internet connection?

48. After typing in your password, you are greeted with an error message indicating that your user name or password is incorrect. What should you check before attempting to enter it again?

49. Describe at least two symptoms that can mean that you are the victim of identity theft.

50. Briefly describe what you should do if you suspect that malware has infected your computer.

Chapter 02 Computer Security Basics Answer Key

Multiple Choice Questions

1. What is the generic term for a mode or method of malware infection?
(p. 40)

A. firewall
B. virus
C. DMZ
D. vector

Just as with viruses that infect humans, malware finds many modes for infecting computers.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

2. What type of malware is also a vector and gets its name from Virgil's famous epic poem, *The Aeneid*, which described how Greek warriors gained access to the City of Troy?
(p. 41)

A. botnet
B. Trojan horse
C. backdoor
D. DMZ

In Homer's epic poem, The Iliad, the ancient Greek warriors gained access to the city of Troy by hiding in a large wooden horse presented as a gift to the City.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

3. What is the oldest malware vector?

(p. 42)

A. sneakernet
B. back door
C. war driving
D. bluesnarfing

Today, most computers connect to the Internet, providing a path for a variety of malware to attack; but in the 1980s that was not true, and viruses were hand-carried from computer-to-computer on infected floppy disks.

Difficulty: 1 Easy
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

4. What term describes a password cracker that tries a huge number of possible passwords?

(p. 44)

A. keylogger
B. cracker
C. zombie
D. brute-force

In conventional warfare this type of attack is very violent and direct.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

5. What type of malware replicates itself on a computer or throughout a network?
(p. 45)

A. zero-day exploit
B. worm
C. botnet
D. zombie

Imagine this type of malware "worming" its way through your computer or network.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

6. What term describes a group of networked computers infected with malware that forward information to other computers?
(p. 45)

A. Trojan horse
B. worm
C. botnet
D. zombie

Botnets can be created for either good or evil.

Difficulty: 1 Easy
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

7. What term is used for a computer that belongs to a group of networked computers, all working mindlessly to serve the person who installed the program on the computers? *(p. 45)*

A. Trojan horse
B. worm
C. botnet
D. zombie

The person who controls these computers is referred to as a *botherder*.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

8. What type of malware is spyware that collects information about the user's browsing habits in order to display advertisements in the browser targeted to that user? *(p. 45)*

A. zero-day exploit
B. browser hijacking
C. adware
D. worm

This type of spyware may take the form of inline banners or pop-ups. Aside from being very annoying, clicking on one of these may trigger a pop-up download, installing malware.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

9. What type of threat points your browser's home page to a website you did not chose, and may even keep you from changing the default home page for the browser?
(p. 46)

A. bluesnarfing
B. phishing
C. browser hijacking
D. key logging

Some unscrupulous people do this so that their Website will register more visitors.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

10. What term describes unsolicited instant messages?
(p. 46)

A. spam
B. browser hijacking
C. phishing
D. spim

Rather than relating this to a meat product, this term includes the "im" of instant messages.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

11. *(p. 44-45)* What term describes malware that takes advantage of a vulnerability in an operating system or application that is (as yet) unknown to the publisher, leaving systems using that software vulnerable until the vulnerability is detected and patched?

A. zero-day exploit
B. browser hijacking
C. spim
D. bluesnarfing

It is a constant challenge to keep ahead of the bad guys, so when they know about and exploit a vulnerability before the publisher does, there is no time to fix it.

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

12. *(p. 47-48)* You receive an e-mail message from a friend claiming that she is in another country, in trouble, and urgently needs money wired to her. You call the friend, and discover that she is safe at home and did not know about the message. This scenario is an example of a/an _____.

A. spam
B. browser hijacking
C. hoax
D. war driving

If you receive a message from someone claiming they are in a situation that you know is out of character for that person, contact them using a means other than email. To perpetrate this hoax, someone had to hijack the user's email account.

Difficulty: 1 Easy
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

13. This method of malware infection installs malware through use of a separate browser window that opens uninvited from a Web page. If you click within the window, you may unknowingly agree to install malware. *(p. 42)*

A. rootkit
B. pop-up download
C. drive-by download
D. hoax

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

14. Once installed, this type of malware becomes a vector giving other malware administrative access to a computer. *(p. 42)*

A. rootkit
B. pop-up download
C. drive-by download
D. hoax

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

15. An e-mail containing enticements (often appealing to human weaknesses) to open attachments is a form of what type of threat? *(p. 46-48)*

A. phishing
B. hoax
C. social engineering
D. worm

Difficulty: 2 Medium
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

16. This software or hardware device examines network traffic and allows or rejects traffic into a network or computer based on predefined rules. *(p. 56)*

A. proxy service
B. DMZ
C. firewall
D. VPN

This software or hardware uses several technologies to accomplish its work.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

17. Combine this technology with a firewall for a very safe way to connect two private networks over the Internet. *(p. 57)*

A. proxy service
B. DMZ
C. firewall
D. VPN

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

18. Also called an application-layer gateway, this software will watch for application-specific traffic, acting as a stand-in for internal computers. *(p. 57)*

A. proxy service
B. DMZ
C. firewall
D. VPN

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

19. It is a good idea to install or enable one of these on your computer, even if your network has similar protection between it and other networks. *(p. 57-58)*

A. Administrator
B. secret key
C. DMZ
D. personal firewall

Threats can originate from other computers on your LAN, as well as from the Internet.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

20. This type of software protects against unsolicited e-mail, filtering out those that have certain characteristics. *(p. 60)*

A. antivirus
B. spam filter
C. firewall
D. proxy service

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

21. A set of these should exist in both document form and software form for any organization. *(p. 55)*

A. cookies
B. account lockout policy
C. anti-spyware
D. security policies

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

22. *(p. 57)* If your private network has both client computers needing Internet access and servers that must be available from the Internet, you should create this separate network for those servers in order to keep Internet-initiated traffic from entering the network containing your client computers. What is the term for the network where the servers are located?

A. back door
B. DMZ
C. botnet
D. firewall

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

23. *(p. 60-61)* What type of security software can you use to both protect from malware infections and also to scan disk space and RAM looking for installed malware?

A. antivirus
B. anti-spam
C. firewall
D. proxy service

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

24. To enable and configure this security feature in Windows Internet Options, you must use a password-protected administrator type account and apply this feature to an existing standard account. *(p. 61-62)*

A. content filtering
B. Parental Controls
C. certificates
D. cookies

There is no sense having Parental Controls unless there is a less-capable user account (standard account type) to protect.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

25. After several failed attempts to log on/sign in to your Windows computer you see a message stating that your account has been locked out. What caused this problem? *(p. 75)*

A. Wrong password
B. Too many failed attempts
C. Wrong username
D. Incorrect version of Windows

At work or at school, the account policy may be configured with an account lockout threshold, which is the maximum number of failed attempts before it locks the account. There is then usually an amount of time (account lockout duration) before it will accept another log on (sign in) attempt.

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

26. This special file holds a secret key.
(p. 72)

A. cookie
B. token
C. vector
D. digital certificate

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

27. Use this type of program to guard against an especially annoying type of adware that appears in your browser and blocks the content you want to see.
(p. 61)

A. pop-up blocker
B. antivirus
C. spam filter
D. content filter

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

28. Which of the following is among the symptoms of a possible malware infection?
(p. 55)

A. adware
B. unsolicited e-mail
C. sudden computer slowdown
D. an error message when you enter your password

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

29. *(p. 69)* You attempt to install software in Windows; and although you are logged on with a computer administrator type of account, your screen turns grey and you receive a message asking if you want to allow the program to make changes to the computer. What Windows feature is at work here?

A. HTTPS
B. UAC
C. EFS
D. authentication

This is an important security feature that you should not disable. The built-in Administrator account is not subject to this feature. A good reason to not enable and use the built-in Administrator account.

Difficulty: 3 Hard
Learning Objective: 02-03 Troubleshoot common security problems.

30. *(p. 76)* Your computer has been showing signs of a malware infection, and today it started up in Safe Mode. Because your computer is not a member of an Active Directory domain, what all-powerful built-in account can you log on with?

A. Guest
B. standard user
C. root
D. Administrator

Difficulty: 2 Medium
Learning Objective: 02-03 Troubleshoot common security problems.

True / False Questions

31. HTTPS uses a private key to encrypt data between a client and an e-commerce server. *(p. 72)*

FALSE

HTTPS uses the public key to encrypt data, and a private key to decrypt data.

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

32. Cookies are always a threat. *(p. 50-51)*

FALSE

Cookies can be useful to you by remembering user preferences and browsing activity for a site so that you do not have to repeat certain actions every time you go to that site.

Difficulty: 1 Easy
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

33. Windows EFS encrypts entire drives. *(p. 72)*

FALSE

Windows Encrypting File System encrypts files on an NTFS partition; it is not capable of encrypting entire drives.

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

34. FileVault is a data encryption feature in OS X. *(p. 73)*

TRUE

Use FileVault in OS X to ensure that your local data is available only by logging on with your user name and password.

Difficulty: 2 Medium

Learning Objective: 02-02 Identify methods for protecting against security threats.

35. When you access a Web page to pay for an online purchase, it should show HTTPS as the protocol in the address line. *(p. 72)*

TRUE

HTTPS is Secure HTTP, which encrypts the communications between you and the e-commerce server through which you pay for your purchases.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

36. We recommend that you block first-party cookies and allow third-party cookies. *(p. 61)*

FALSE

It is the other way around; you should allow first-party cookies *from trusted sites*, but block all third-party cookies.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

37. You must use data wiping software on a hard drive before installing a new operating system. *(p. 73-74)*

FALSE

Use data wiping software to permanently delete files from a hard drive. This is not a necessary task when installing a new operating system unless you are preparing the computer for someone else's use, as when you donate an old computer.

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

38. FileVault, a feature of some editions of Windows, allows you to encrypt an entire drive.
(p. 73)

FALSE

BitLocker Drive Encryption is the feature of Windows Vista, Windows 7, and Windows 8 that allows you to encrypt an entire drive, while FileVault is an encryption feature of OS X.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

39. Windows will warn you if you try to log on with the Caps Lock key turned on.
(p. 75)

TRUE

Difficulty: 2 Medium
Learning Objective: 02-03 Troubleshoot common security problems.

40. A Windows computer that is a member of a domain will have a local account named
(p. 76) Administrator that you can access when your computer starts up in Safe Mode.

FALSE

You can only access the built-in local Administrator account in Safe Mode when you are NOT a member of a domain.

Difficulty: 3 Hard
Learning Objective: 02-03 Troubleshoot common security problems.

Short Answer Questions

41. What does the term "malware" stand for?
(p. 40)

The term malware is short for **mal**icious soft**ware**.

Difficulty: 1 Easy
Learning Objective: 02-01 Describe security threats and vulnerabilities to computers and users.

42. Briefly define the security tool known as a honey pot.
(p. 57)

A honey pot is a server created as a decoy to draw malware attacks and gather information about attackers. It may be located outside a corporate firewall, within a DMZ, or inside a corporate network.

Difficulty: 3 Hard
Learning Objective: 02-02 Identify methods for protecting against security threats.

43. Define EFS.
(p. 72)

EFS is Microsoft's Encrypting File System, which is only available on Windows Computers on hard drives formatted with the NTFS file system.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

44. What should you do before donating an old computer to your favorite charity?
(p. 73)

You should use data wiping software to ensure that all personal data—even deleted data—is not recoverable.

Difficulty: 2 Medium

Learning Objective: 02-02 Identify methods for protecting against security threats.

45. Provide at least two common symptoms of a malware infection.
(p. 55)

Common symptoms of a malware infection include: strange screen messages, sudden computer slowdown, missing data, and inability to access the hard drive.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

46. After encrypting a file using the Windows Encrypting File System (EFS) you move the file to another NTFS-formatted volume. Is the file still encrypted? Explain your answer.
(p. 72)

The file is still encrypted after moving it to another NTFS-formatted volume. Encrypting File System (EFS) only works on an NTFS volume. Therefore, the encryption will be maintained when it is moved to another NTFS volume, but it will be lost if you move the file to a non-NTFS volume.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

47. You believe your computer is infected by malware, but you have not kept your security software up-to-date. How can you quickly run an up-to-date scan for malware, providing you have an Internet connection?
(p. 76)

Connect to the site of a reputable source of malware protection and run an online scan of your computer. One example is HouseCall, available at www.trendmicro.com.

Difficulty: 3 Hard
Learning Objective: 02-03 Troubleshoot common security problems.

48. *(p. 75)* After typing in your password, you are greeted with an error message indicating that your user name or password is incorrect. What should you check before attempting to enter it again?

Check that caps lock is not on, and check to ensure that you properly placed your hands on the keyboard.

Difficulty: 2 Medium
Learning Objective: 02-03 Troubleshoot common security problems.

49. *(p. 55)* Describe at least two symptoms that can mean that you are the victim of identity theft.

Indications that you may be a victim of identity theft include: 1) charges you are sure you or your family did not make appear on an account; 2) you receive collection calls for overdue payments on accounts you never opened; 3) you apply for new credit and are rejected for reasons you know are not true; and 4) a credit bureau reports existing credit accounts you never opened.

Difficulty: 2 Medium
Learning Objective: 02-02 Identify methods for protecting against security threats.

50. *(p. 76)* Briefly describe what you should do if you suspect that malware has infected your computer.

You should run a scan of all drives and memory using your installed antivirus program.

Difficulty: 2 Medium
Learning Objective: 02-03 Troubleshoot common security problems.