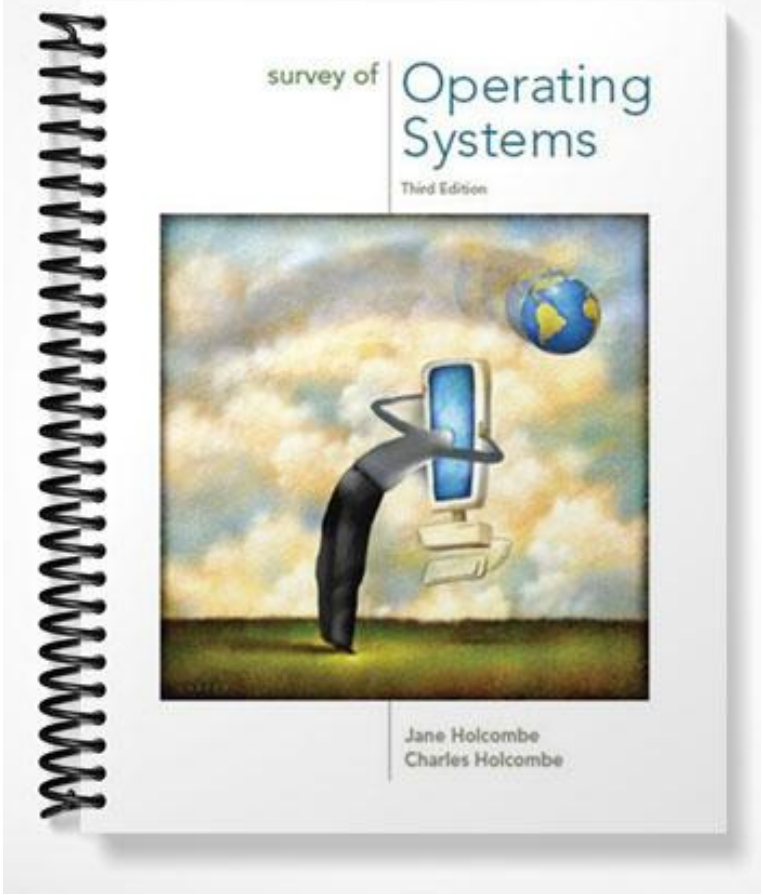
TEST BANK


survey of
Operating Systems
Third Edition
Jane Holcombe
Charles Holcombe

Multiple Choice Questions

1. The generic term for a mode of malware infection is
A. firewall
B. virus
C. DMZ
D. vector

2. This type of malware and mode of infection gets its name from one of Homer's tales of the ancient Greeks.
A. botnet
B. Trojan horse
C. backdoor
D. DMZ

3. This is the oldest mode of malware infection.
A. sneakernet
B. back door
C. war driving
D. bluesnarfing

4. A password cracker that tries a huge number of permutations of possible passwords is called a/an _____ password cracker.
A. keylogger
B. cracker
C. zombie
D. brute-force

5. This type of malware replicates itself on a computer or throughout a network.
A. Trojan horse
B. worm
C. botnet
D. zombie

6. This term describes a group of networked computers infected with programs that forward information to other computers.
A. Trojan horse
B. worm
C. botnet
D. zombie

7. A computer that belongs to a group of network computers, working mindlessly to serve whomever installed the program on the computers.
A. Trojan horse
B. worm
C. botnet
D. zombie

8. This form of malware is spyware that collects information about the user in order to display targeted advertisements to the user.
A. zombie
B. browser hijacking
C. adware
D. worm

9. Some unscrupulous people do this so that their Web site will register more visitors.
A. bluesnarfing
B. phishing
C. browser hijacking
D. key logging

10. This term describes unsolicited instant messages.
A. spam
B. browser hijacking
C. phishing
D. spim

11. This term describes a fraudulent method of obtaining personal financial information through Web page pop-us, e-mail, and letters mailed via the postal service.
A. phishing
B. browser hijacking
C. spim
D. bluesnarfing

12. You receive an e-mail message from a friend's e-mail address 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.
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 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, accepting or rejecting traffic 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. At home or in a small office, you probably connect to the Internet through one of these multi-function hardware devices.
A. keylogger
B. VPN
C. DMZ
D. broadband router, cable/DSL router

20. This type of software protects against unsolicited e-mail, filtering out those that have certain characteristics.
A. antivirus
B. anti-spam
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 your servers that keeps 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 there must be at least one existing standard account.
A. content filtering
B. Parental Controls
C. certificates
D. cookies

25. This content ratings organization is used by Internet Explorer.
A. EFS
B. ICRA
C. SSL
D. DMZ

26. This special file holds a secret key.
A. cookie
B. token
C. vector
D. digital certificate

27. A classic example of this type of social engineering is an e-mail claiming to be from a legitimate organization asking you for your social security number and/or other personal identifying information.
A. phishing
B. hoax
C. fraud
D. worm

28. Which of the following is among the symptoms of a possible malware attack?
A. browser hijacking
B. unsolicited e-mail
C. sudden computer slowdown
D. an error when you enter your username and 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 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 only encrypts entire drives.
True False

34. FileVault is a data encryption feature in Mac OS X.
True False

35. When you access a Web page where you will 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 Vista and Windows 7, allows you to encrypt an entire drive.
True False

39. Windows 7 will warn you if you try to log on with the Caps Lock key turned on.
True False

40. A Windows 7 computer that is a member of a domain will have a local account named Administrator that, by default has no password and can easily be accessed when your computer starts up in Safe Mode.
True False

Short Answer Questions

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

42. Briefly describe FileVault.

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. You keep confidential and personal information on your laptop. You configured your laptop to require a user name and password at logon and you have a comprehensive security program installed, including protection against a variety of malware and a personal firewall. Describe another step you should take to secure your data.

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 a logon error message indicating that your user name or password is incorrect. What should you check before attempting to enter it again?

49. After returning to work from an extended absence, you try several times to log on, only to receive an error message stating that your account is locked out. What does this message mean and what should you do about it?

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

Multiple Choice Questions

1. *(p. 40)* The generic term for a mode of malware infection is
A. firewall
B. virus
C. DMZ
D. vector

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

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

2. *(p. 40)* This type of malware and mode of infection gets its name from one of Homer's tales of the ancient Greeks.
A. botnet
B. Trojan horse
C. backdoor
D. DMZ

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

3. *(p. 40, 41)* This is the oldest mode of malware infection.
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: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

4. *(p. 43)* A password cracker that tries a huge number of permutations of possible passwords is called a/an _____ password cracker.
A. keylogger
B. cracker
C. zombie
D. brute-force

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

5. *(p. 44)* This type of malware replicates itself on a computer or throughout a network.
A. Trojan horse
B. worm
C. botnet
D. zombie

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

6. *(p. 44)* This term describes a group of networked computers infected with programs that forward information to other computers.
A. Trojan horse
B. worm
C. botnet
D. zombie

Botnets can be created for either good or evil.

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

7. *(p. 44)* A computer that belongs to a group of network computers, working mindlessly to serve whomever installed the program on the computers.
A. Trojan horse
B. worm
C. botnet
D. zombie

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

8. *(p. 44)* This form of malware is spyware that collects information about the user in order to display targeted advertisements to the user.
A. zombie
B. browser hijacking
C. adware
D. worm

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

9. *(p. 44 45)* Some unscrupulous people do this so that their Web site will register more visitors.
A. bluesnarfing
B. phishing
C. browser hijacking
D. key logging

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

10. *(p. 45)* This term describes unsolicited instant messages.
A. spam
B. browser hijacking
C. phishing
D. spim

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

11. *(p. 45)* This term describes a fraudulent method of obtaining personal financial information through Web page pop-us, e-mail, and letters mailed via the postal service.
A. phishing
B. browser hijacking
C. spim
D. bluesnarfing

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

12. *(p. 46)* You receive an e-mail message from a friend's e-mail address 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

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

13. *(p. 41)* This method of malware infection installs malware through use of a separate browser window that opens uninvited from a Web page.
A. rootkit
B. pop-up download
C. drive-by download
D. hoax

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

14. *(p. 41)* 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

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

15. *(p. 45, 46)* An e-mail containing enticements to open attachments is a form of what type of threat?
A. phishing
B. hoax
C. social engineering
D. worm

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

16. *(p. 54)* This software or hardware device examines network traffic, accepting or rejecting traffic based on predefined rules.
A. proxy service
B. DMZ
C. firewall
D. VPN

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

17. *(p. 55)* 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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

18. *(p. 55)* 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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

19. *(p. 54, 55)* At home or in a small office, you probably connect to the Internet through one of these multi-function hardware devices.
A. keylogger
B. VPN
C. DMZ
D. broadband router, cable/DSL router

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

20. *(p. 57)* This type of software protects against unsolicited e-mail, filtering out those that have certain characteristics.
A. antivirus
B. anti-spam
C. firewall
D. proxy service

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

21. *(p. 53)* 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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

22. *(p. 56)* 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 your servers that keeps 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: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

23. *(p. 58)* 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: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

24. *(p. 60)* To enable and configure this security feature in Windows Internet Options, you must use a password-protected administrator type account and there must be at least one existing standard account.
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: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

25. *(p. 60)* This content ratings organization is used by Internet Explorer.
A. EFS
B. ICRA
C. SSL
D. DMZ

ICRA is the Internet Content Rating Association.

Difficulty: Hard
Learning Outcome: 2.2 Identify methods for protecting against security threats

26. *(p. 70)* This special file holds a secret key.
A. cookie
B. token
C. vector
D. digital certificate

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

27. *(p. 45, 46)* A classic example of this type of social engineering is an e-mail claiming to be from a legitimate organization asking you for your social security number and/or other personal identifying information.
A. phishing
B. hoax
C. fraud
D. worm

Difficulty: Easy
Learning Outcome: 2.2 Identify methods for protecting against security threats

28. *(p. 53)* Which of the following is among the symptoms of a possible malware attack?
A. browser hijacking
B. unsolicited e-mail
C. sudden computer slowdown
D. an error when you enter your username and password

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

29. *(p. 67)* 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

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

30. *(p. 74)* 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 account can you log on with?
A. Guest
B. standard user
C. root
D. Administrator

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

True / False Questions

31. *(p. 70)* HTTPS uses a private key to encrypt data between a client and an e-commerce server.
FALSE

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

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

32. *(p. 48)* Cookies are always a threat.
FALSE

Cookies can be useful to you.

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

33. *(p. 70)* Windows EFS only encrypts entire drives.
FALSE

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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

34. *(p. 71)* FileVault is a data encryption feature in Mac OS X.
TRUE

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

35. *(p. 70)* When you access a Web page where you will pay for an online purchase, it should show HTTPS as the protocol in the address line.
TRUE

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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

36. *(p. 59)* We recommend that you block first-party cookies and allow third-party cookies.
FALSE

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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

37. *(p. 71)* You must use data wiping software on a hard drive before installing a new operating system.
FALSE

Difficulty: Hard
Learning Outcome: 2.2 Identify methods for protecting against security threats

38. *(p. 70, 71)* FileVault, a feature of some editions of Windows Vista and Windows 7, allows you to encrypt an entire drive.
FALSE

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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

39. *(p. 72, 73)* Windows 7 will warn you if you try to log on with the Caps Lock key turned on.
TRUE

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

40. *(p. 74)* A Windows 7 computer that is a member of a domain will have a local account named Administrator that, by default has no password and can easily be accessed when your computer starts up in Safe Mode.
FALSE

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

Short Answer Questions

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

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

Difficulty: Easy
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

42. *(p. 70, 71)* Briefly describe FileVault.

This feature of OS X will encrypt all the files in your Home folder.

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

43. *(p. 70)* Define EFS.

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

Difficulty: Medium
Learning Outcome: 2.1 Describe security threats and vulnerabilities to desktop PCs and users

44. *(p. 71)* What should you do before donating an old computer to your favorite charity?

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

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

45. *(p. 53)* Provide at least two common symptoms of a malware infection.

Strange screen messages, sudden computer slowdown, missing data, inability to access the hard drive.

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

46. *(p. 72)* You keep confidential and personal information on your laptop. You configured your laptop to require a user name and password at logon and you have a comprehensive security program installed, including protection against a variety of malware and a personal firewall. Describe another step you should take to secure your data.

You should encrypt the data on the hard drive, using the data encryption available through your operating system.

Difficulty: Medium
Learning Outcome: 2.2 Identify methods for protecting against security threats

47. *(p. 74)* 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?

Connect to the site of a reputable source of malware protection and run an online scan of your computer.

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

48. *(p. 72)* After typing in your password, you are greeted with a logon 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: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

49. *(p. 73)* After returning to work from an extended absence, you try several times to log on, only to receive an error message stating that your account is locked out. What does this message mean and what should you do about it?

The message means that you have made too many failed attempts to logon—probably because you have forgotten your password. You should call an administrator or simply wait and eventually the time-out period will expire and you can try again.

Difficulty: Medium
Learning Outcome: 2.3 Troubleshoot common security problems

50. *(p. 73, 74)* 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: Medium
Learning Outcome: 2.3 Troubleshoot common security problems