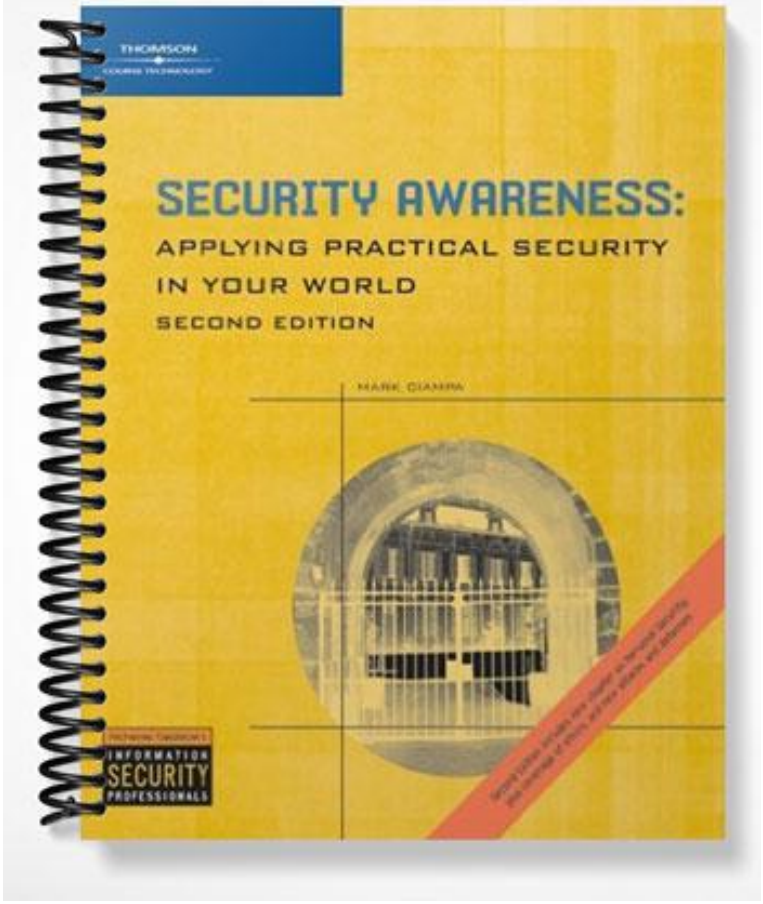
TEST BANK


THOMSON
COURSE TECHNOLOGY
SECURITY AWARENESS:
APPLYING PRACTICAL SECURITY
IN YOUR WORLD
SECOND EDITION
MARK OSWALD
INFORMATION
SECURITY
PROFESSIONALS

Chapter 2: Desktop Security

TRUE/FALSE

1. Viruses can spread through instant messaging (IM).

   ANS: T PTS: 1 REF: 45

2. A worm must attach itself to a computer document, such as an e-mail message, and is spread by traveling along with the document.

   ANS: F PTS: 1 REF: 46

3. Logic bombs are extremely difficult to detect before they are triggered.

   ANS: T PTS: 1 REF: 47

4. ERD bootable floppies can be created for Microsoft Windows Server 2003, Windows 2000, and Windows XP.

   ANS: F PTS: 1 REF: 68

5. If the hard drive of a stolen laptop computer that is equipped with a stealth signal transmitter is removed and installed on another computer, it will send a signal from the new computer.

   ANS: T PTS: 1 REF: 61

MULTIPLE CHOICE

1. A computer ____ is a program that secretly attaches itself to a document or another program and executes when that document or program is opened.
   a. biometric
   b. virus
   c. patch
   d. password

   ANS: B PTS: 1 REF: 44

2. A(n) ____ is a computer program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a person's rank in an organization dropped below a previous level.
   a. logic bomb
   b. biometric
   c. password
   d. public key

   ANS: A PTS: 1 REF: 47

3. ____ relies on tricking and deceiving someone to access a system.
   a. Encryption
   b. Hashing
   c. Dumpster diving
   d. Social engineering

   ANS: D PTS: 1 REF: 48

4. ____ involves digging through trash receptacles to find computer manuals, printouts, or password lists that have been thrown away.
   a. Hashing
   c. Encryption

b. Dumpster diving
d. Instant messaging

ANS: B PTS: 1 REF: 48

5. ____ can be performed based on what you have, what you know, or what you are.
a. Brute force attacks
c. Authentication
b. Biometrics
d. Decryption

ANS: C PTS: 1 REF: 49

6. A(n) ____ is a secret combination of letters and numbers that serves to validate or authenticate a user by what he knows.
a. digital signature
c. patch software
b. device lock
d. password

ANS: D PTS: 1 REF: 49

7. Attackers can exploit weak passwords by ____.
a. instant messaging
c. password guessing
b. using a device lock
d. hashing

ANS: C PTS: 1 REF: 50

8. A(n) ____ attack occurs when an attacker attempts to create every possible password combination by systematically changing one character at a time in a password, and then using each newly generated password to attempt to access the system.
a. brute force
c. dumpster diving
b. logic bomb
d. dictionary

ANS: A PTS: 1 REF: 50

9. ____ is generally configured to constantly monitor for viruses and automatically check for updated signature files.
a. Data backup software
c. Instant messaging software
b. Encryption
d. Antivirus software

ANS: D PTS: 1 REF: 56

10. ____ uses the unique human characteristics of a person for authentication.
a. Digital signatures
c. Digital certificates
b. Biometrics
d. Signature files

ANS: B PTS: 1 REF: 59

11. A(n) ____ consists of a steel cable and a lock.
a. device lock
c. antivirus software program
b. key
d. stealth signal transmitter

ANS: A PTS: 1 REF: 60

12. A(n) ____ is software installed on the laptop computer that cannot be detected.
a. patch
c. device lock
b. signature file
d. stealth signal transmitter

ANS: D PTS: 1 REF: 60

13. Changing the original text of a message to a secret message using cryptography is known as ____.

a. biometrics
b. encryption
c. social engineering
d. dumpster diving

ANS: B PTS: 1 REF: 61

14. ____ scrambles data so that it cannot be viewed by unauthorized users.
a. Cryptography
b. Instant messaging
c. Patch software
d. Network attached storage

ANS: A PTS: 1 REF: 61

15. Once the only means of backing up data, ____ today are usually found only on large networked file servers.
a. portable USB hard drives
b. NAS devices
c. tape backups
d. Internet services

ANS: C PTS: 1 REF: 67

16. With a(n) ____ system, the same key is used to both encrypt and decrypt the message.
a. public key
b. antivirus
c. biometric
d. private key

ANS: D PTS: 1 REF: 61

17. With a(n) ____ system, two mathematically related keys are used: a public key and a private key.
a. biometric
b. public key
c. antivirus
d. private key

ANS: B PTS: 1 REF: 61

18. A ____ is a code attached to an electronic message that helps to prove that the person sending the message with a public key is not an imposter, that the message was not altered, and that it cannot be denied that the message was sent.
a. digital signature
b. device lock
c. hash
d. digital certificate

ANS: A PTS: 1 REF: 62

19. A ____ creates encrypted text that is never intended to be decrypted; instead, it is used in a comparison for authentication purposes.
a. digital signature
b. public key
c. hash
d. private key

ANS: C PTS: 1 REF: 62

20. A ____ links or binds a specific person to a public key.
a. digital certificate
b. logic bomb
c. definition file
d. stealth signal transmitter

ANS: A PTS: 1 REF: 64

21. A ____ is similar to a portable USB hard drive, except it has additional “intelligence” that allows all devices connected to the computer network to access it (instead of unplugging it a computer and moving it from computer to computer).
a. device lock
b. patch
c. network attached storage device
d. private key

ANS: C PTS: 1 REF: 67

COMPLETION

1. A(n) _____ is an encrypted hash of a message that is transmitted along with the message.

   ANS: digital signature

   PTS: 1 REF: 62

2. A(n) _____ is an independent third-party organization that provides digital certificates.

   ANS:
   certification authority
   CA
   certification authority (CA)
   CA (certification authority)

   PTS: 1 REF: 64

3. Creating a(n) _____ involves copying data onto digital media and storing it in a secure location.

   ANS: data backup

   PTS: 1 REF: 66

4. _____ usually replicate themselves until they clog all available resources, such as the hard disk drive, computer memory, or the Internet network connection.

   ANS: Worms

   PTS: 1 REF: 47

5. A(n) _____ takes each word from a dictionary and encodes it in the same way the computer encodes a user's password for protection.

   ANS: dictionary attack

   PTS: 1 REF: 51

MATCHING

Match each item with a statement below.

a. Desktop computers
b. Malware
c. Viruses
d. Logic bombs
e. Username
f. Patch software
g. Cryptography
h. Instant messaging
i. Worms

1. Also referred to as malicious software.

2. Often used to ensure payment for software.
3. Can refer to either computers that sit on a user's desk or portable laptop computers.
4. General term used to describe software security updates that vendors provide for their programs and operating system.
5. The science of transforming information so that it is secure while it is being transmitted or stored.
6. Unique identifier.
7. Method of online communication.
8. Do not depend on the e-mail message for its survival.
9. Can be programmed to send themselves to all users listed in an e-mail address book.

1. ANS: B PTS: 1 REF: 44
2. ANS: D PTS: 1 REF: 47
3. ANS: A PTS: 1 REF: 44
4. ANS: F PTS: 1 REF: 53
5. ANS: G PTS: 1 REF: 61
6. ANS: E PTS: 1 REF: 49
7. ANS: H PTS: 1 REF: 45
8. ANS: I PTS: 1 REF: 46
9. ANS: C PTS: 1 REF: 45

SHORT ANSWER

1. What effect can a computer virus have on your computer?

   ANS:
   Viruses can:
   Cause a computer to continually crash
   Erase files from a hard drive
   Install hidden programs, such as stolen ("pirated") software, which is then secretly distributed or even sold to other users from the computer
   Make multiple copies of itself and consume all of the free space in a hard drive
   Reduce security settings and allow intruders to remotely access the computer
   Reformat the hard disk drive and erase its entire contents

   PTS: 1 REF: 45

2. List five symptoms that indicate that a virus has infected a computer.

   ANS:
   The symptoms include:
   An e-mail contact says that recently received e-mail messages from you contained unusual attachments.
   A program suddenly disappears from the computer.
   An e-mail message appears that has an unexpected attachment or the attachment has a double file extension, such as PICTURE.JPG.VPS or SUNSET.TIF.EXE.
   After opening the attachment, dialog boxes open or the computer slows significantly.
   New icons appear on the desktop that are not associated with any recently installed programs.
   New programs do not install properly.
   Out-of-memory error messages appear.
   Programs that used to function normally stop responding. If the software is removed and reinstalled, the problem continues.

Sometimes the computer starts normally, but at other times it stops responding before the desktop icons and taskbar appear.
Unusual dialog boxes or message boxes appear.
Sounds or music plays from the speakers unexpectedly.
The computer runs very slowly and takes a long time to start.
There is a significant amount of modem activity.
Windows restarts unexpectedly.
Windows error messages appear listing "critical system files" that are missing and refuse to load.

PTS: 1 REF: 46

3. List five characteristics of a weak password.

ANS:
Passwords that are short (such as ABCD)
A common word used as a password (such as Friday)
Personal information in a password (such as the name of a child)
Using the same password for all accounts
Writing the password down
Not changing passwords unless forced to do so

PTS: 1 REF: 50

4. Provide brief descriptions of each of the four Windows automatic update configuration options.

ANS:
Automatic - This option checks the Microsoft Web site every day at a user designated time and, if there are any patches, Windows automatically downloads and installs them onto the desktop computer.
Download - The Download option automatically downloads the patches but does not install them, allowing the user to review and choose which patches to install.
Notify - This option alerts the user that patches are available but does not download or install them. The user must go to the Microsoft Web site to review and install the patches.
Turn off - The Turn off option disables automatic updates.

PTS: 1 REF: 54-55

5. What are the basic rules for creating strong passwords?

ANS:
Passwords must have at least eight characters.
Passwords must contain a combination of letters, numbers, and special characters.
Passwords on Windows XP systems can be enhanced by using a space in the password or by using nonprintable characters.
Passwords should be replaced at least every 30 days.
Passwords should not be reused for 12 months.
The same password should not be used on two or more systems or accounts.

PTS: 1 REF: 57

6. What are the five basic questions that should be answered when creating a data backup?

ANS:
The questions are:

What information should be backed up?
How often should it be backed up?
What media should be used?
Where should the backup be stored?
How should the backup be performed?

PTS: 1 REF: 66-68

7. How would you recover from an attack using ASR?

ANS:
To recover from an attack using ASR:
1. Insert the original operating system installation CD into the CD drive.
2. Restart the computer. If prompted to press a key in order to start the computer from CD, press the appropriate key.
3. Press the F2 key when prompted during the text–only mode section of Setup.
4. Insert the ASR floppy disk when prompted.
5. Follow the remaining directions on the screen.

PTS: 1 REF: 69

8. What is the difference between a worm and a virus?

ANS:
Although similar to viruses, worms are different in two regards. First, a virus must attach itself to a computer document, such as an e-mail message, and is spread by traveling along with the document. A worm, on the other hand, does not attach to a document to spread, but can instead travel by itself.

A second difference between a worm and a virus is that a virus needs the user to perform an action, such as starting a program or reading an e-mail message, to start the infection. A worm does not always require action by the computer user to begin its execution.

PTS: 1 REF: 46

9. When selling or donating your computer, what files should you remove?

ANS:
The files that should be removed include:
E-mail contacts
E-mail messages
All personal documents
All files in the operating system recycle bin or trash folder
Internet files
All nontransferable software

PTS: 1 REF: 64-65

10. Microsoft classifies patches based on the level of vulnerability that the patch fixes. Briefly describe each level of vulnerability.

ANS:
Critical - A critical vulnerability could freely allow a worm to infect a computer even when other defense mechanisms are in place.

Important - An important vulnerability could result in the confidentiality, integrity, or availability of data or resources being compromised.
Moderate - Moderate vulnerabilities are those that are difficult for an attacker to exploit because of current configurations.
Low - Low vulnerability means that it would be very difficult for an attacker to take advantage of this weakness and whose impact would be minimal.

PTS: 1 REF: 54