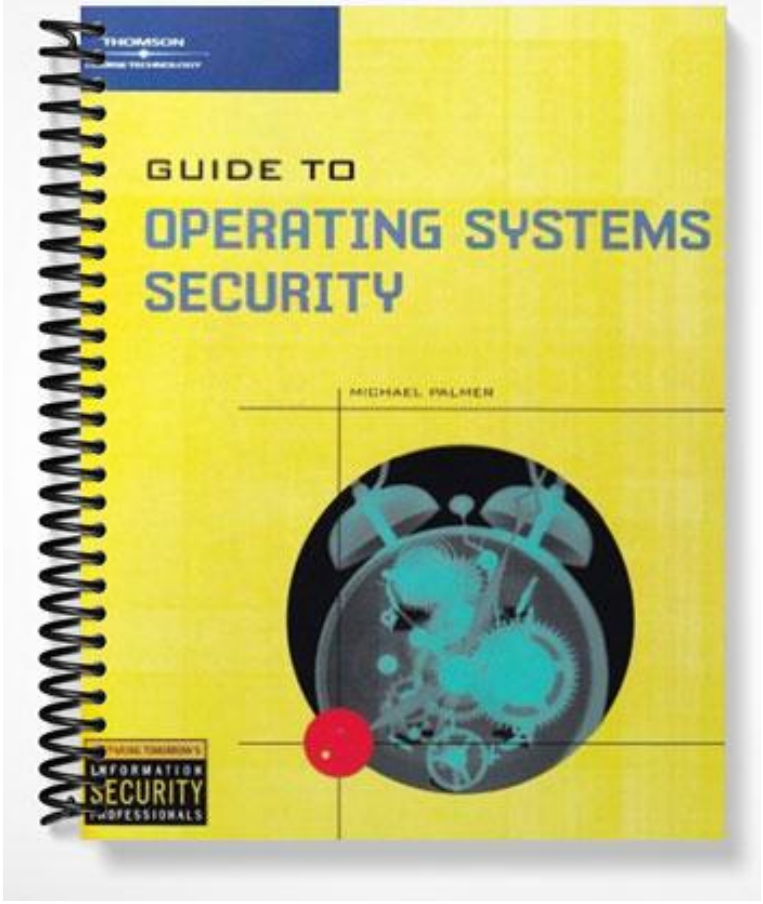
TEST BANK


THOMSON
GUIDE TO
OPERATING SYSTEMS SECURITY
MICHAEL PALMER
INFORMATION SECURITY

ch02

True/False
Indicate whether the statement is true or false.

____ 1. The W32.Pinfi virus is an example of a destructive virus that can infect Mac OS systems.

____ 2. A benign virus is one that replicates but does not inflict harm on a computer.

____ 3. Backdoor.Egghead is an example of a worm that is spread by buffer overflows.

____ 4. In Netware, the startup.ncf file contains commands used by the server.exe startup program.

____ 5. Boot or partition sector viruses particularly affect Windows and Netware systems.

____ 6. Cookie snarfing is an attack where a spyware operator can reconstruct a user's every move on the Internet by capturing cookies or the information contained in the cookies.

____ 7. The Netware 6.x operating system has a software update tool that connects to the Internet to obtain patches.

____ 8. Windows 2000 Server allows you to create an ERD, which enables you to fix problems that may arise with the server, such as corrupted system files.

____ 9. The Windows 2003 Server ASR set backs up all system files, system settings, and application data files.

____ 10. Organizational policy works best when users are included in the process, so that they know the importance of security.

Modified True/False
Indicate whether the statement is true or false. If false, change the identified word or phrase to make the statement true.

____ 11. The first stage of virus spread that occurs is replication within the infected system.
_____

____ 12. File infector viruses can infect systems through multiple means, particularly through boot or partition sectors and through executable files. _____

____ 13. A(n) stealth virus uses defenses to make itself hard to find and detect. _____

____ 14. The Code Red worm replicates for the first 23 days of the month and then stops.
_____

____ 15. The Digispid.B.Worm targets systems running the SQL Server database on Windows-based workstations and servers. _____

____ 16. A(n) macro virus, worm, or Trojan horse is a file that contains lines of computer code that can be run.
_____

____ 17. Batch files and scripts are files that contain code or instructions that are run by a(n) interpreter.
_____

____ 18. A(n) boot sector virus typically infects or replaces the instructions in the MBR or the Partition Boot Sector.
_____

____ 19. Software exploitation is particularly aimed at new software and new software versions.
_____

____ 20. Mac OS and NetWare automatically display the boot load information to the screen each time one of these systems is booted. _____

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 21. Which of the following virus programs is available for purchase on a Windows-based workstation?
a. AntiVir Personal Edition
b. Handybits Viruscan
c. VCatch Basic
d. Sophos Anti-virus
e. Both b and d

____ 22. Which anti-virus software is available for use on only Windows and Mac OS systems?
a. Central Command Vexira AntiVirus
b. F-Prot AV
c. Norton AntiVirus
d. McAfee VirusScan
e. Both c and d

____ 23. Which anti-virus software is available for use on Macintosh, NetWare, UNIX/Linux, and Windows-based systems?
a. AntiVir Personal Edition
b. HandyBits VirusScan
c. McAfee VirusScan
d. Sophos Anti-Virus

____ 24. Which of the following Microsoft operating systems uses driver signing?
a. Windows XP
b. Windows ME
c. Windows 98
d. Windows 95
e. Both a and c

____ 25. Which of the following operating systems uses an emergency repair disk?
a. Windows 2000 Server
b. Windows 2000 Pro
c. Windows XP Pro
d. Windows 2003 Server
e. Both a and b

____ 26. How many copies of the ASR set should you have for a server?
a. 1
b. 2
c. 3
d. 4

____ 27. What do you need to have for Red Hat Linux if a system file on the hard disk is corrupted?
a. An ERD
b. An ASR set
c. A boot disk
d. An MBR

____ 28. In Red Hat Linux, what command do you need to use to create a boot disk?
a. mkboot
b. makebootdisk
c. mkbootdisk
d. makebtdsk

____ 29. What is another name for malicious software?
a. malsoft
b. malware
c. scriptware
d. scriptsoft

____ 30. _____ is designed so that it does not infect all of these file types at once, but only a limited number each time Windows Explorer runs.
a. INIT 1984
b. Code Red
c. Slammer worm
d. W32.Pinfi

____ 31. The _____ virus can only become destructive if the user executes an infected file on a Friday the thirteenth.
a. Linux.Millen.Worm
b. INIT 1984
c. W32.Pinfi
d. Code Red II

____ 32. A _____ virus appends to program files such as system files, executable files, driver files, and supplementary files, including .dlls.
a. partition sector
c. macro

b. file infector
d. multipartite

____ 33. A _____ virus spreads to instruction set files typically used by word processors, spreadsheets, databases, and other programs.
a. boot sector
c. macro
b. file infector
d. multipartite

____ 34. A _____ virus can infect systems through multiple means, particularly through boot or partition sectors and through executable files.
a. boot sector
c. macro
b. multipartite
d. file infector

____ 35. A(n) _____ virus changes each time it is replicated, making it more difficult to create a defense against it.
a. armored
c. polymorphic
b. multipartite
d. heuristic

____ 36. A(n) _____ virus appears to run from a file other than the one to which it is actually appended.
a. stealth
c. polymorphic
b. armored
d. companion

____ 37. A(n) _____ virus uses defenses to make itself hard to find and detect.
a. polymorphic
c. companion
b. stealth
d. heuristic

____ 38. Which of the following worms uses buffer overflows to do damage?
a. Code Red
d. Both a and b
b. Code Red II
e. a, b, and c
c. Linux.Millen.Worm

____ 39. How many days of the month does the Code Red worm replicate?
a. 15
c. 23
b. 19
d. 29

____ 40. What process does the Linux.Millen.Worm use on the attacked operating system?
a. Telnet
c. DNS
b. FTP
d. SMTP

____ 41. The _____ targets systems running the SQL Server database on Windows-based workstations and servers.
a. Digispid.B.Worm
c. Linux.Lion.Worm
b. Linux.Millen.Worm
d. Code Red II Worm

____ 42. Which of the following is an example of a Trojan horse on a Mac OS system?
a. Simpsons AppleScript Virus
c. Backdoor.Egghead
b. AOL4FREE
d. Code Red

____ 43. Which of the following is an example of a Red Hat Linux file that can be the target of a virus?
a. autoexec.bat
c. startup.ncf
b. inittab
d. win.ini

____ 44. Which of the following is an example of a Netware 6.x file that can be the target of a virus?
a. autoexec.bat
c. win.ini
b. startup.ncf
d. Both a and b

____ 45. Which file on a Windows-based system is run when a system is booted, and can be used to rename specific files at startup?
a. win.ini
c. wininit.ini
b. autoexec.bat
d. winstart.bat

____ 46. Which of the following executable file extensions can be found on a Netware 6.x system?
a. .pl
c. .wsf
b. .msi
d. .bin

____ 47. Which of the following executable file extensions is found only on Windows-based systems?

a. .mst
b. .msi
c. .msp
d. .btm
e. All of the above

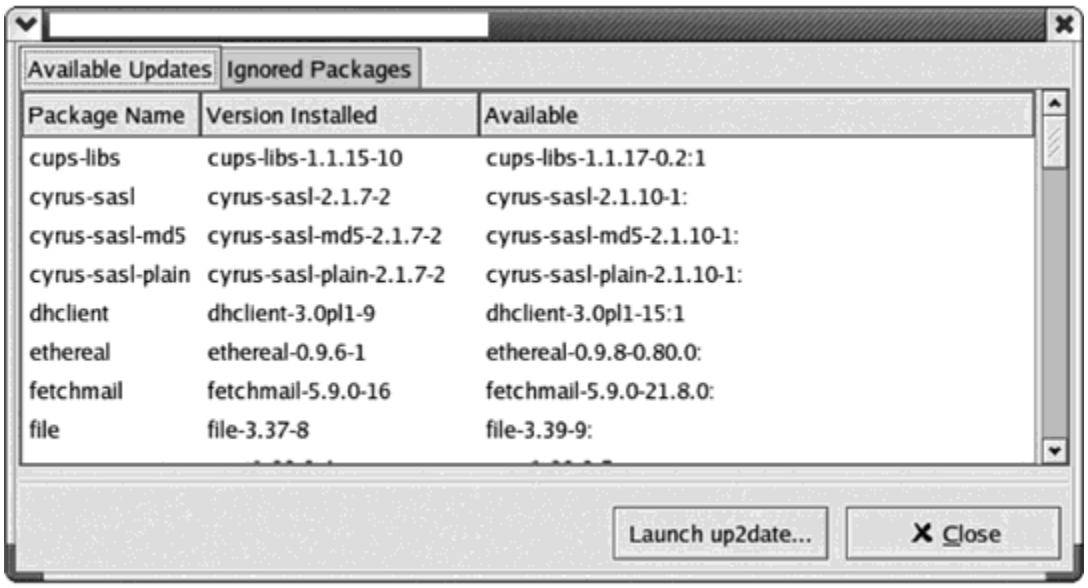
____ 48. In Red Hat Linux, what mode do you need to be in to run the fdisk/mbr utility which replaces the MBR?
a. Safe
b. Rescue
c. Recovery
d. MBR

____ 49. How was the Melissa virus transported?
a. File sharing
b. Floppy disk
c. Buffer overflow
d. E-mail

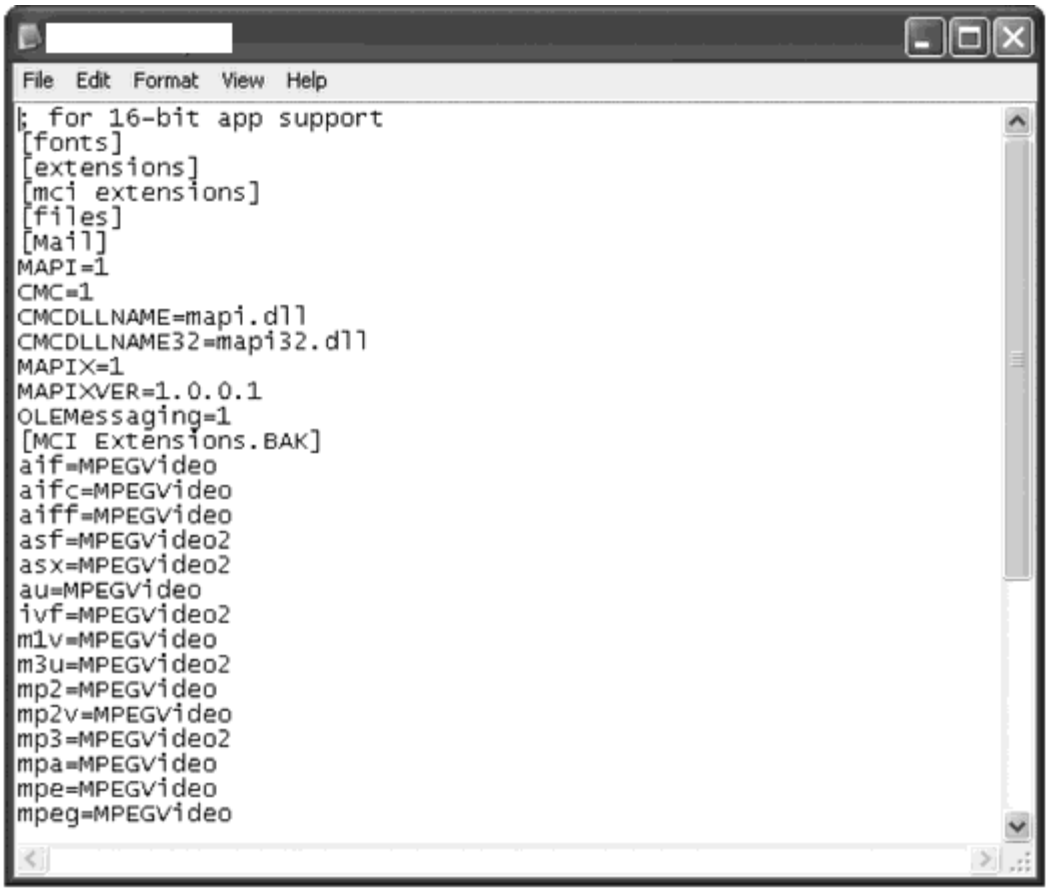
____ 50. With which attachment was the Resume virus associated?
a. Explorer.exe
b. Explorer.msi
c. Explorer.doc
d. Explorer.com

____ 51. Which of the following is notorious for enabling cookie snarfing?
a. SpyNet
b. PeepNet
c. Cookienet
d. Both a and b
e. a, b, and c

____ 52. What was one reason the Slammer worm was successful against SQL Server database servers in early 2003?
a. It gained access through a previously unknown vulnerability in SQL server
b. Many administrators had not installed new patches designed to block this attack
c. It was a polymorphic worm that rapidly changed signatures
d. It was a stealth worm that was difficult to detect

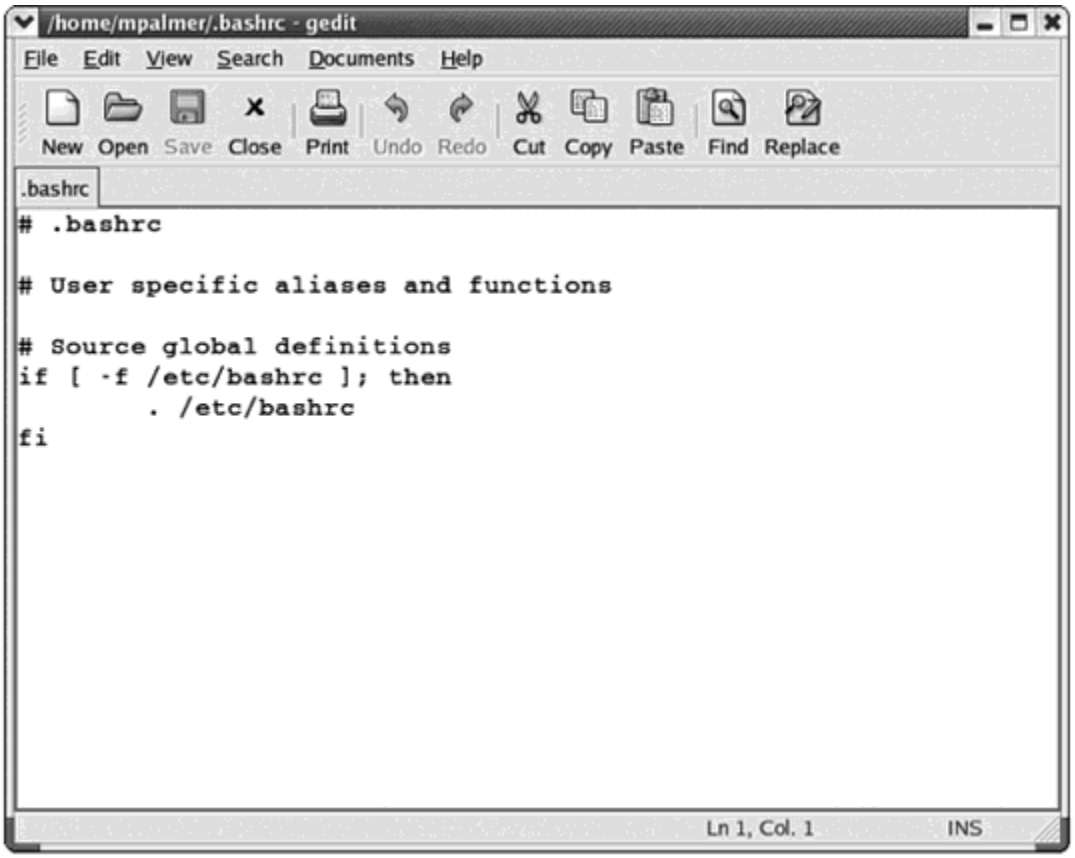


____ 53. What is displayed in the figure above?
a. Windows Update Setup Wizard
b. Red Hat Network Alert Notification Tool
c. Mac OS X Software Update Tool
d. None of the above



____ 54. What is displayed in the figure above?

a. A bashrc file in Red Hat Linux
b. A win.ini file in Windows XP
c. A startup.ncf file in Netware
d. The kernel file in Mac OS X



____ 55. Which of the following operating systems would use the commands listed in the figure above?

a. Windows XP
b. Netware 6.x
c. Red Hat Linux
d. Mac OS X

Yes/No

Indicate whether you agree with the statement.

____ 56. Can the VCatch Basic Anti-virus program be used both in Windows and Linux environments?

____ 57. Is Sophos Anti-virus free software that can be used in Macintosh, Netware, UNIX/Linux, and Windows-based systems?

____ 58. Is one advantage of a digital signature that it helps ensure the security of your system by allowing only drivers and system files that have been verified by Microsoft?

____ 59. Does Windows 2000 use an ASR set to recover from a system failure?

____ 60. Should you create a new ASR set each time you add a protocol or install a new driver for a network interface card?

____ 61. Does an organizational policy work best if users are not included in the policy creation process?

____ 62. In its destructive mode, will the INIT 1984 virus rename files using random characters and delete files on hard drives?

____ 63. Is Windows the only operating system that is vulnerable to a macro virus?

____ 64. Does the AOL4FREE e-mail hoax contain the AOL4FREE.com attachment?

____ 65. Can a boot or partition sector virus corrupt the address of the primary partition that is specified in the partition table of a disk?

Completion
Complete each statement.

66. Typically, eradicating boot or partition sector viruses involves recreating the _____ and Partition Boot Sector instructions.

67. One way to spread a(n) _____ virus is to attach it to a template that many users share, enabling it to spread each time the template is opened in a new document.

68. The _____ virus did not destroy data, but instead inserted the following line in the virus-carrying document when it was opened: "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

69. Viruses, worms, and Trojan horses all represent malicious software that use _____ to find weaknesses or holes in operating systems and networks.

70. Code Red and Code Red II use a buffer overflow to attack weaknesses in _____ Services on Microsoft servers.

71. _____ may operate without being installed on a user's computer by capturing information related to the user's Internet communications.

72. Windows XP Professional and Windows Server 2003 come with the _____ Setup Wizard which is designed to help you remember to obtain new updates, or even to obtain them for you.

73. In the _____ operating system, you can display the boot process by booting into either single user mode or verbose mode.

74. _____ are one of the most vulnerable points of attack in an organization.

75. A(n) _____ is a program that replicates and replicates on the same computer, or one that sends itself to many other computers on a network or the Internet.

Matching

Match the following terms to the appropriate definitions.

a. ASR Set	f. digital signature
b. back door	g. driver signing
c. boot disk	h. ERD
d. boot sector	i. MBR
e. cookie	j. spyware

____ 76. A removable disk used to boot an operating system
____ 77. The process of placing a digital signature in a device driver
____ 78. A code that is placed in a file to verify its authenticity
____ 79. A set of instructions used to find and load the operating system
____ 80. A secret avenue into an operating system that bypasses normal security
____ 81. In Windows 2000, a disk that contains repair and backup information
____ 82. Information that a Web server stores on a client computer

____ 83. Captures information about cookies sent between a Web server and a client
____ 84. Backup media needed to start a failed Windows XP Pro system
____ 85. The beginning of a disk where code to start up the operating system is stored

Short Answer

86. One way to classify viruses is by how they infect systems. List the four different classifications.
87. Viruses can be classified by the way they protect themselves from detection or from a virus scanner. List the four classifications.
88. What is a destructive virus?
89. What is a benign virus?
90. What are the six typical methods used in malicious software attacks?
91. List eight examples of executable-type file extensions and the operating systems that use them..
92. List the three steps in the process of the initial bootup from a disk.
93. List five of the services, applications, systems, or functions that are known to be vulnerable in which attackers may look for problems.
94. What basic steps should be taken to protect an operating system from malicious software?
95. List seven features should you look for when you purchase virus scanning software.

ch02
Answer Section

TRUE/FALSE

1. ANS: F PTS: 1 REF: 48
2. ANS: T PTS: 1 REF: 50
3. ANS: F PTS: 1 REF: 51
4. ANS: T PTS: 1 REF: 53
5. ANS: F PTS: 1 REF: 56
6. ANS: T PTS: 1 REF: 59
7. ANS: F PTS: 1 REF: 65
8. ANS: T PTS: 1 REF: 70
9. ANS: F PTS: 1 REF: 72
10. ANS: T PTS: 1 REF: 74

MODIFIED TRUE/FALSE

11. ANS: F, second

    PTS: 1 REF: 49
12. ANS: F, Multipartite

    PTS: 1 REF: 49
13. ANS: T PTS: 1 REF: 50
14. ANS: F, 19

    PTS: 1 REF: 50
15. ANS: T PTS: 1 REF: 51
16. ANS: F, executable

    PTS: 1 REF: 55
17. ANS: T PTS: 1 REF: 55
18. ANS: T PTS: 1 REF: 56
19. ANS: T PTS: 1 REF: 58
20. ANS: F, Red Hat Linux

    PTS: 1 REF: 66

MULTIPLE CHOICE

21. ANS: D PTS: 1 REF: 69
22. ANS: C PTS: 1 REF: 69
23. ANS: D PTS: 1 REF: 69
24. ANS: A PTS: 1 REF: 69

25. ANS: E PTS: 1 REF: 70
26. ANS: B PTS: 1 REF: 72
27. ANS: C PTS: 1 REF: 73
28. ANS: C PTS: 1 REF: 74
29. ANS: B PTS: 1 REF: 48
30. ANS: D PTS: 1 REF: 48
31. ANS: B PTS: 1 REF: 48
32. ANS: B PTS: 1 REF: 49
33. ANS: C PTS: 1 REF: 49
34. ANS: B PTS: 1 REF: 49
35. ANS: C PTS: 1 REF: 49
36. ANS: D PTS: 1 REF: 50
37. ANS: B PTS: 1 REF: 50
38. ANS: E PTS: 1 REF: 50
39. ANS: B PTS: 1 REF: 50
40. ANS: B PTS: 1 REF: 51
41. ANS: A PTS: 1 REF: 51
42. ANS: A PTS: 1 REF: 52
43. ANS: B PTS: 1 REF: 52
44. ANS: D PTS: 1 REF: 52
45. ANS: C PTS: 1 REF: 53
46. ANS: D PTS: 1 REF: 55
47. ANS: E PTS: 1 REF: 55
48. ANS: B PTS: 1 REF: 56
49. ANS: D PTS: 1 REF: 57
50. ANS: C PTS: 1 REF: 57
51. ANS: D PTS: 1 REF: 59
52. ANS: B PTS: 1 REF: 60
53. ANS: B PTS: 1 REF: 64
54. ANS: B PTS: 1 REF: 54
55. ANS: C PTS: 1 REF: 53

YES/NO

56. ANS: N PTS: 1 REF: 69
57. ANS: Y PTS: 1 REF: 69
58. ANS: Y PTS: 1 REF: 69
59. ANS: N PTS: 1 REF: 70
60. ANS: Y PTS: 1 REF: 72
61. ANS: N PTS: 1 REF: 74
62. ANS: Y PTS: 1 REF: 48
63. ANS: N PTS: 1 REF: 49
64. ANS: N PTS: 1 REF: 52
65. ANS: Y PTS: 1 REF: 56

COMPLETION

66. ANS:
Master Boot Record
MBR

PTS: 1 REF: 56

67. ANS: macro

PTS: 1 REF: 57

68. ANS: Melissa

PTS: 1 REF: 57

69. ANS: software exploitation

PTS: 1 REF: 58

70. ANS: Internet Information

PTS: 1 REF: 59

71. ANS: Spyware

PTS: 1 REF: 59

72. ANS: Automatic Updates

PTS: 1 REF: 61

73. ANS: Mac OS X

PTS: 1 REF: 66

74. ANS: Users

PTS: 1 REF: 74

75. ANS: worm

PTS: 1 REF: 50

MATCHING

76.	ANS: C	PTS: 1	REF: 76
77.	ANS: G	PTS: 1	REF: 76
78.	ANS: F	PTS: 1	REF: 76
79.	ANS: I	PTS: 1	REF: 76
80.	ANS: B	PTS: 1	REF: 76
81.	ANS: H	PTS: 1	REF: 76
82.	ANS: E	PTS: 1	REF: 76
83.	ANS: J	PTS: 1	REF: 77
84.	ANS: A	PTS: 1	REF: 76
85.	ANS: D	PTS: 1	REF: 76

SHORT ANSWER

86. ANS:
    1. Boot or partition sector
    2. File infector
    3. Macro
    4. Multipartite

    PTS: 1 REF: 49
87. ANS:
    1. Armored
    2. Polymorphic
    3. Stealth
    4. Companion

    PTS: 1 REF: 49
88. ANS:
    A virus that is designed to delete or damage files, stop normal workflow, or cause problems for users of computer or network systems.

    PTS: 1 REF: 50
89. ANS:
    A virus that replicates but does not inflict harm on a computer. Some benign viruses actually start as a test to determine the ability of a program or executable code block to replicate. These viruses are sometimes used by attackers to test a certain aspect of their program code before unleashing an actual attack. Benign viruses may also start when test code goes beyond the laboratory is used by those learning to write or test software intended to stop viruses. Even though a benign virus does no physical harm, it still may disturb or concern the user.

    PTS: 1 REF: 50
90. ANS:
    1. Executable methods
    2. Boot and partition sector methods
    3. Macro methods
    4. E-mail methods
    5. Software exploitation
    6. Spyware

    PTS: 1 REF: 54
91. ANS:
    Any eight of the following:
    1. .exe (for Windows and NetWare systems)
    2. .com (for Windows and NetWare systems)
    3. .bat (for Windows and NetWare systems)
    4. .bin (for Windows, NetWare, and Mac OS systems)
    5. .btm (for Windows systems)
    6. .cgi (for Windows, UNIX/Linux, NetWare, and Mac OS systems)
    7. .pl (for UNIX/Linux systems, including Mac OS)
    8. .cmd (for Windows and NetWare systems)
    9. .msi (for Windows systems)
    10. .msp (for Windows systems)

11. .mst (for Windows systems)
12. .vb and .vbe (for Windows and NetWare systems)
13. .wsf (for Windows systems)

PTS: 1 REF: 55

92. ANS:
1. The computer finds the MBR.
2. The instructions in the MBR enable it to locate the Master Partition Boot Sector of the active partition (the partition from which a system boots).
3. Instructions, sometimes called the boot loader, in the Master Partition Boot Sector locate and start the computer's operating system.

PTS: 1 REF: 56

93. ANS:
Any five of the following:
1. DNS services
2. Newly developed or enhanced services
3. Network services and applications
4. E-mail and messaging services and applications
5. Internet services and applications
6. Remote access services
7. Database systems
8. Buffer overflow handling

PTS: 1 REF: 58

94. ANS:
1. Installing updates
2. Viewing what is loaded when a system is booted
3. Using malicious software scanners
4. Using digital signatures for system and driver files
5. Backing up systems and creating repair disks
6. Creating and implementing organizational policies

PTS: 1 REF: 60

95. ANS:
Any seven of the following:
1. Scans memory and removes viruses
2. Continuous memory scanning
3. Scans hard and floppy disks and removes viruses
4. Scans all known file formats, including zipped or compressed files
5. Scans HTML documents and e-mail attachments
6. Automatically runs at a scheduled time you specify
7. Manual run option
8. Detects known and unknown malicious software
9. Updates for new malicious software
10. Scans files that are downloaded from a network or the Internet
11. Use of protected or quarantined zones for downloaded files so that they can be automatically scanned in a safe location before they are used

PTS: 1 REF: 67