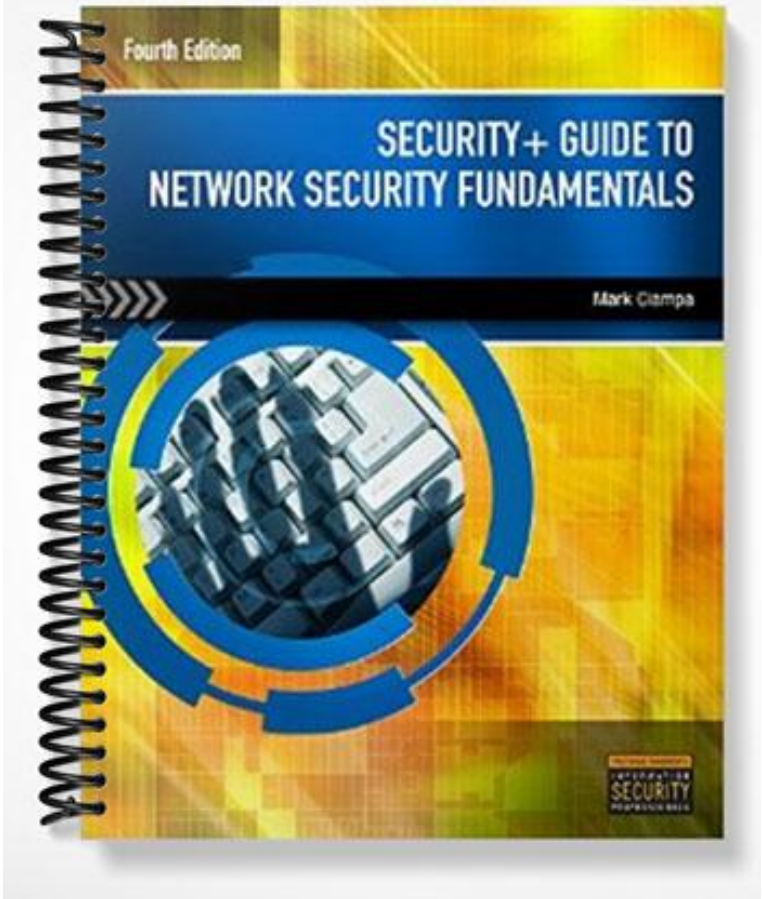
TEST BANK


Fourth Edition
SECURITY+ GUIDE TO
NETWORK SECURITY FUNDAMENTALS
Mark Ciampa
SECURITY

TRUE/FALSE

1. Approximately two out of three malicious Web attacks have been developed using one of four popular attack toolkits.

   ANS: F PTS: 1 REF: 42

2. Attack toolkits range in price from only $400 to as much as $8,000.

   ANS: F PTS: 1 REF: 42

3. Like a virus, a worm needs the user to perform an action such as starting a program or opening an e-mail attachment to start the infection.

   ANS: F PTS: 1 REF: 48

4. Removing a rootkit from an infected computer is extremely difficult.

   ANS: T PTS: 1 REF: 51

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

   ANS: T PTS: 1 REF: 56

MULTIPLE CHOICE

1. The most popular attack toolkit, which has almost half of the attacker toolkit market is ____.
   a. SpyEye
   b. NeoSploit
   c. ZeuS
   d. MPack

   ANS: D PTS: 1 REF: 42

2. ____ is when an attacker tricks users into giving out information or performing a compromising action.
   a. Phreaking
   b. Hacking
   c. Social engineering
   d. Reverse engineering

   ANS: C PTS: 1 REF: 43

3. The two types of malware that have the primary objective of spreading are ____.
   a. viruses and worms
   b. rootkits and worms
   c. Trojans and worms
   d. rootkits and Trojans

   ANS: A PTS: 1 REF: 43

4. A computer ____ is malicious computer code that reproduces itself on the same computer.
   a. virus
   b. worm
   c. adware
   d. spyware

   ANS: A PTS: 1 REF: 44

5. In a(n) ____ infection, a virus injects itself into the program's executable code instead of at the end of the file.
   a. stealth
   b. appender
   c. Swiss cheese
   d. split

   ANS: C PTS: 1 REF: 44

6. Unlike other malware, a ____ is heavily dependent upon the user for its survival.
   a. Trojan
   b. worm
   c. rootkit
   d. virus

   ANS: D PTS: 1 REF: 46

7. A ____ virus is loaded into random access memory (RAM) each time the computer is turned on and infects files that are opened by the user or the operating system.
   a. companion
   b. file infector
   c. resident
   d. boot

   ANS: C PTS: 1 REF: 47

8. A ____ virus infects the Master Boot Record of a hard disk drive.
   a. file infector
   b. companion
   c. resident
   d. boot

   ANS: D PTS: 1 REF: 47

9. A ____ virus infects program executable files.
   a. macro
   b. program
   c. companion
   d. boot sector

   ANS: B PTS: 1 REF: 47

10. There are almost ____ different Microsoft Windows file extensions that could contain a virus.
    a. 50
    b. 60
    c. 70
    d. 80

    ANS: C PTS: 1 REF: 47

11. A ____ is 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.
    a. rootkit
    b. macro
    c. program
    d. process

    ANS: B PTS: 1 REF: 47

12. A(n) ____ virus adds a program to the operating system that is a malicious copycat version to a legitimate program.
    a. macro
    b. metamorphic
    c. boot
    d. companion

    ANS: D PTS: 1 REF: 47

13. Viruses and worms are said to be self-____.
    a. duplicating
    b. updating
    c. copying
    d. replicating

ANS: D PTS: 1 REF: 48

14. A ____ is a program advertised as performing one activity but actually does something else.
    a. script
    b. virus
    c. Trojan
    d. worm

    ANS: C PTS: 1 REF: 49

15. A ____ is 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

    ANS: A PTS: 1 REF: 49

16. A ____ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event.
    a. Trojan
    b. logic bomb
    c. macro virus
    d. metamorphic virus

    ANS: B PTS: 1 REF: 51

17. A(n) ____ refers to an undocumented, yet benign, hidden feature, that launches by entering a set of special commands, key combinations, or mouse clicks.
    a. Trojan horse
    b. virus
    c. bug
    d. Easter egg

    ANS: D PTS: 1 REF: 52

18. ____ is a software program that delivers advertising content in a manner that is unexpected and unwanted by the user.
    a. Adware
    b. Keylogger
    c. Spam
    d. Trojan

    ANS: A PTS: 1 REF: 55

19. ____ is an image spam that is divided into multiple images.
    a. Word splitting
    b. Geometric variance
    c. Layer variance
    d. GIF layering

    ANS: D PTS: 1 REF: 63

20. ____ involves horizontally separating words, although it is still readable by the human eye.
    a. Word splitting
    b. GIF layering
    c. Geometric variance
    d. Layer variance

    ANS: A PTS: 1 REF: 63

21. ____ uses “speckling” and different colors so that no two spam e-mails appear to be the same.
    a. GIF layering
    b. Geometric variance
    c. Word splitting
    d. Layer variance

    ANS: B PTS: 1 REF: 63

COMPLETION

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

   ANS: malware

   PTS: 1 REF: 42

2. 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.

   ANS: split infection

   PTS: 1 REF: 44

3. The _____ contains the program necessary for the computer to start up and a description of how the hard drive is organized (the partition table).

   ANS:
   Master Boot Record (MBR)
   Master Boot Record
   MBR

   PTS: 1 REF: 47

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

   ANS: trust

   PTS: 1 REF: 47

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

   ANS: keylogger

   PTS: 1 REF: 56

MATCHING

Match each item with a statement below:

a. Trojan
b. Macro virus
c. Companion virus
d. Worm
e. Rootkit
f. Image spam
g. Spyware
h. Malware
i. Hoax

1. executable program advertised as performing one activity, but actually does something else
2. hides or removes traces of log-in records, log entries, and related processes
3. general term used to describe software that violates a user's personal security
4. adds a program to the operating system that is a malicious copycat version to a legitimate program
5. uses graphical images of text in order to circumvent text-based filters
6. false warning, often contained in an e-mail message claiming to come from the IT department

7. general term that refers to a wide variety of damaging or annoying software programs
8. a program designed to take advantage of a vulnerability in an application or an operating system in order to enter a system
9. series of instructions that can be grouped together as a single command

1. ANS: A PTS: 1 REF: 49
2. ANS: E PTS: 1 REF: 49
3. ANS: G PTS: 1 REF: 54
4. ANS: C PTS: 1 REF: 47
5. ANS: F PTS: 1 REF: 62
6. ANS: I PTS: 1 REF: 63
7. ANS: H PTS: 1 REF: 43
8. ANS: D PTS: 1 REF: 48
9. ANS: B PTS: 1 REF: 47

SHORT ANSWER

1. What is malware?

   ANS:
   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.

   PTS: 1 REF: 43

2. Explain how an appender infection works.

   ANS:
   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.

   PTS: 1 REF: 44

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

   ANS:
   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
   • Reformatted the hard disk drive

   PTS: 1 REF: 45

4. Describe a macro virus.

ANS:
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.

PTS: 1 REF: 47

5. What is a worm?

ANS:
A worm is a malicious program designed to take advantage of a vulnerability in an application or an operating system in order to enter a computer. Once the worm has exploited the vulnerability on one system, it immediately searches for another computer that has the same vulnerability. A worm uses a network to send copies of itself to other devices also connected to the network.

PTS: 1 REF: 48

6. How does a rootkit work?

ANS:
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.

PTS: 1 REF: 50

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

ANS:
A backdoor is software code that gives access to a program or service that circumvents any normal security protections. Creating a legitimate backdoor is a common practice by a developer, who may need to access a program or device on a regular basis, yet does not want to be hindered by continual requests for passwords or other security approvals. The intent is for the backdoor to be removed once the application is finalized. However, in some instances backdoors have been left installed, and attackers have used them to bypass security. In addition, malware from attackers can also install backdoors on a computer. This allows the attacker to return at a later time and bypass any security settings.

PTS: 1 REF: 52

8. What are botnets?

ANS:

One of the popular payloads of malware today that is carried by Trojan horses, worms, and viruses is a program that will allow the infected computer to be placed under the remote control of an attacker. This infected "robot" computer is known as a zombie. When hundreds, thousands, or even tens of thousands of zombie computers are under the control of an attacker, this creates a botnet.

Early botnets under the control of the attacker, known as a bot herder, used Internet Relay Chat (IRC) to remotely control the zombies. IRC is an open communication protocol that is used for real-time "chatting" with other IRC users over the Internet. It is mainly designed for group or one-to-many communication in discussion forums. Users access IRC networks by connecting a local IRC client to a remote IRC server, and multiple IRC servers can connect to other IRC servers to create large IRC networks. After infecting a computer to turn it into a zombie, bot herders would secretly connect it to a remote IRC server using its built-in client program and instruct it to wait for instructions, known as command and control (C&C). The bot herder could then remotely direct the zombies to steal information from the victims' computers and to launch attacks against other computers.

PTS: 1 REF: 52-53

9. Describe adware.

ANS:
Adware is a software program that delivers advertising content in a manner that is unexpected and unwanted by the user. Adware typically displays advertising banners, popup ads, or opens new Web browser windows while the user is accessing the Internet. Almost all users resist adware because:
• Adware may display objectionable content, such as gambling sites or pornography.
• Frequent pop-up ads can interfere with a user's productivity.
• Pop-up ads can slow a computer or even cause crashes and the loss of data.
• Unwanted advertisements can be a nuisance.

Some adware goes beyond affecting the user's computer. This is because adware programs can also perform a tracking function, which monitors and tracks a user's online activities and then sends a log of these activities to third parties without the user's authorization or knowledge. For example, a user who visits online automobile sites to view specific types of cars can be tracked by adware and classified as someone interested in buying a new car. Based on the order and type of Web sites visited, the adware can also determine whether the surfers' behavior suggests they are close to making a purchase or are also looking at competitors' cars. This information is gathered by adware and then sold to automobile advertisers, who send the users regular mail advertisements about their cars or even call the user on the telephone.

PTS: 1 REF: 55

10. What are some of the costs involved for spamming?

ANS:
Consider the following costs involved for spamming:
• E-mail addresses—Spammers often build their own lists of e-mail addresses using special software that rapidly generates millions of random e-mail addresses from well-known Internet Service Providers (ISPs) and then sends messages to these addresses. Because an invalid e-mail account returns the message to the sender, the software can automatically delete the invalid accounts leaving a list of valid e-mail addresses to send the actual spam. If a spammer wants to save time by purchasing a list of valid e-mail addresses to spam, the cost is relatively inexpensive ($100 for 10 million addresses).

• Equipment and Internet connection—Spammers typically purchase an inexpensive laptop computer ($500) and rent a motel room with a high-speed Internet connection ($85 per day) as a base for launching attacks. Sometimes spammers actually lease time from other attackers ($40 per hour) to use a network of 10,000 to 100,000 infected computers to launch an attack.

PTS: 1 REF: 62