

## CIT-15 Chapter 9 Study Guide

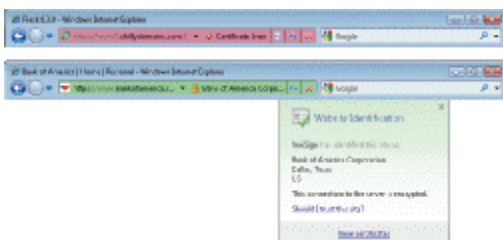
### Multiple Choice

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

- \_\_\_ 1. Computer crime is sometimes referred to as \_\_\_\_.
- a. hacking
  - b. cybercrime
  - c. cyberstalking
  - d. spoofing
- \_\_\_ 2. \_\_\_\_ occurs whenever an individual gains access to a computer, network, file, or other resource without permission.
- a. Spoofing
  - b. Unauthorized Access
  - c. Phishing
  - d. Vandalizing
- \_\_\_ 3. \_\_\_\_ refers to the act of breaking into a computer or network.
- a. Spamming
  - b. Phishing
  - c. Hacking
  - d. Spoofing
- \_\_\_ 4. \_\_\_\_ are sets of tools that allow hackers to access a system.
- a. Toolkits
  - b. Hackkits
  - c. Crimekits
  - d. Rootkits
- \_\_\_ 5. Advocates of \_\_\_\_ state that, unless individuals or businesses protect their access points, they are welcoming others to use them.
- a. spoofing
  - b. phishing
  - c. spamming
  - d. war driving
- \_\_\_ 6. The term \_\_\_\_ refers to accessing someone else's unsecured Wi-Fi network from the hacker's current location (such as inside his or her home, outside a Wi-Fi hotspot location, or near a local business).
- a. war driving
  - b. Wi-Fi piggybacking
  - c. Wi-Fi worming
  - d. denial of service
- \_\_\_ 7. \_\_\_\_, the most commonly used type of possessed knowledge, are secret words or character combinations associated with an individual.
- a. Usernames
  - b. PINs
  - c. Passwords
  - d. Codes
- \_\_\_ 8. \_\_\_\_ access systems use physical objects for identification purposes and they are frequently used to control access to facilities and computer systems.
- a. Touch object
  - b. Possessed object
  - c. Two-factor
  - d. Biometric
- \_\_\_ 9. Increasingly, USB security keys, also called USB security \_\_\_\_—USB flash drives that are inserted into a computer to grant access to a network, to supply Web site usernames and passwords, or to provide other security features—are being used.
- a. botherders
  - b. botnets
  - c. passes
  - d. tokens
- \_\_\_ 10. \_\_\_\_ identify users by a particular unique biological characteristic.
- a. Possessed object access systems
  - b. Password access systems
  - c. Possessed knowledge access systems
  - d. Biometric access systems
- \_\_\_ 11. A \_\_\_\_ is a security system that essentially creates a wall between a computer or network and the Internet in order to protect against unauthorized access.
- a. Trojan horse
  - b. firewall
  - c. hub
  - d. bridge
- \_\_\_ 12. \_\_\_\_ uses a single secret key to both encrypt and decrypt the file or message.
- a. Private key encryption
  - b. Public key encryption



- \_\_\_ 21. A \_\_\_ is a malicious program that masquerades as something else—usually as some type of application program.
- Trojan horse
  - computer worm
  - computer insect
  - computer bug
- \_\_\_ 22. A computer \_\_\_ spreads by creating copies of its code and sending those copies to other computers via a network.
- virus
  - software
  - worm
  - hacker
- \_\_\_ 23. One emerging type of Trojan horse is called a \_\_\_-Access Trojan.
- Demote
  - Remote
  - Control
  - Hacker
- \_\_\_ 24. Antivirus programs are usually set up to automatically download new \_\_\_ from their associated Web site on a regular basis.
- virus definitions
  - upgrades
  - software versions
  - virus reports
- \_\_\_ 25. A booming area of computer crime involves online fraud, theft, scams, and related activities collectively referred to as \_\_\_.
- e-cons
  - e-scams
  - dot frauds
  - dot cons
- \_\_\_ 26. \_\_\_ occurs when someone obtains enough information about a person to be able to masquerade as that person for a variety of activities—usually to buy products or services in that person’s name.
- Data theft
  - Information theft
  - Identity theft
  - Database theft
- \_\_\_ 27. \_\_\_ can be extremely distressing for victims, can take years to straighten out, and can be very expensive.
- Spams
  - Identity theft
  - Remote access
  - Software theft
- \_\_\_ 28. Phishing schemes may use a technique called \_\_\_, which is setting up spoofed Web sites with addresses slightly different from legitimate sites.
- typosquatting
  - spamming
  - DoS attacks
  - identity theft
- \_\_\_ 29. \_\_\_ is a type of scam that uses spoofed domain names to obtain personal information for use in fraudulent activities.
- Framing
  - Fishing
  - Pharming
  - Farming
- \_\_\_ 30. The best protection against many dot cons is \_\_\_.
- your ISP
  - updated operating systems
  - antivirus programs
  - common sense
- \_\_\_ 31. When a digitally signed document is received, the recipient’s computer uses the sender’s \_\_\_ key to verify the digital signature.
- private
  - public
  - organizational
  - token



- \_\_\_ 32. The green color of the Address bar in the accompanying figure indicates that the site is using a valid \_\_\_ SSL certificate.
- |       |          |
|-------|----------|
| a. EV | c. SQL   |
| b. SK | d. HTTPS |
- \_\_\_ 33. Repeated threats or other harassment carried out online between adults is referred to as \_\_\_\_.
- |                      |                   |
|----------------------|-------------------|
| a. cyberstalking     | c. cyberterrorism |
| b. computer sabotage | d. phishing       |
- \_\_\_ 34. The \_\_\_\_, implemented in 2001, grants federal authorities expanded surveillance and intelligence-gathering powers, such as broadening their ability to obtain the real identity of Internet users and to intercept Internet communications.
- |   |
|---|
| a. Sarbanes-Oxley Act                                   |
| b. USA Patriot Act                                      |
| c. Identity Theft and Assumption Deterrence Act of 1998 |
| d. No Electronic Theft (NET) Act                        |
- \_\_\_ 35. The \_\_\_ includes provisions to combat cyberterrorism, including protecting ISPs against lawsuits from customers for revealing private information to law enforcement agencies.
- |   |
|---|
| a. Heath Insurance Portability and Accountability Act (HIPAA) |
| b. PROTECT Act  |
| c. Homeland Security Act of 2002                              |
| d. National Information Infrastructure Protection Act         |

### Case-Based Critical Thinking Questions

#### Case 9-1

Melissa is the network administrator for a small publishing company. As network administrator, she is in charge of maintaining the security of all the computers that are part of the company's network.

- \_\_\_ 36. Melissa has set up procedures so that every user using a computer connected to the network needs to enter his or her \_\_\_\_, which appears as asterisks on the screen as it is being entered.
- |                   |               |
|-------------------|---------------|
| a. private key    | c. public key |
| b. e-mail address | d. password   |
- \_\_\_ 37. One of the first items that Melissa installed was a(n) \_\_\_\_, which checks all incoming and outgoing traffic and only allows authorized traffic to pass through.
- |             |                         |
|-------------|-------------------------|
| a. botnet   | c. IPS                  |
| b. firewall | d. encryption algorithm |
- \_\_\_ 38. Melissa also decided to use a(n) \_\_\_\_, which continuously monitors and analyzes the traffic allowed to and from the network to detect possible attacks as they are occurring and block them.
- |             |                       |
|-------------|-----------------------|
| a. IPS      | c. antivirus software |
| b. firewall | d. RAM                |

### Case-Based Critical Thinking Questions

#### Case 9-2

Fernando has been having problems with his computer. He takes it to his local computer repair shop to be checked and finds out that his computer has a number of malware that he was not even aware of.

- \_\_\_ 39. The technician tells Fernando that his computer has a \_\_\_\_, which might have gotten into Fernando's computer when he downloaded a free computer game from the Internet.
- |           |          |
|-----------|----------|
| a. spider | c. virus |
|-----------|----------|

