**Chapter 7 Review Questions**

1. The TCP/IP architecture uses how many layers?

a. Seven

b. Six

c. Five

d. Four – PG252

2. Which of the following would not be a valid Internet Control Message Protocol (ICMP) error message?

a. Network Unreachable

b. Host Unreachable

c. Router Delay – PG253

d. Destination Network Unknown

3. Each of the following attacks use Internet Control Message Protocol (ICMP) except .

a. Smurf DoS attack

b. ICMP Redirect attack

c. Ping of Death

d. ICMP poisoning – PG254

4. Which version of Simple Network Management Protocol (SNMP) is considered the most secure?

a. SNMPv2

b. SNMPv3 – PG254

c. SNMPv4

d. SNMPv5

5. Which of the following Domain Name System (DNS) attacks substitutes a fraudulent IP address for a symbolic name?

a. DNS replay

b. DNS poisoning – PG256

c. DNS masking

d. DNS forwarding

6. Which of the following is the most secure protocol for transferring files?

a. SCP

b. FTPS

c. SFTP – PG258

d. FTP

7. The address space in an IPv6 header is \_\_\_\_ bits in length.

a. 32

b. 64

c. 128 – PG259

d. 256

8. Each of the following is a technique for securing a router except .

a. make all configuration changes remotely – PG261

b. secure all ports

c. use a meaningful router name

d. set a strong administrator password

9. Which of the following is true regarding a flood guard?

a. It is a separate hardware appliance that is located inside the DMZ.

b. It can be used on either local host systems or network devices.

c. It protects a router from password intrusions.

d. It prevents DoS or DDoS attacks. – PG263

10. Each of the following is a type of a network security hardware log except \_\_\_\_\_\_\_.

a. local host anti-virus log – PG263

b. NIDS and NIPS logs

c. proxy server log

d. firewall log

11. Each of the following is an entry in a firewall log that should be investigated except .

a. IP addresses that are being rejected and dropped

b. suspicious outbound connections

c. IP addresses that are being rejected and dropped

d. successful logins – PG265

12. If a group of users must be separated from other users, which is the most secure network design?

a. Use a VLAN.

b. Connect them to different switches and routers. – PG265

c. Use a subnet mask.

d. It is impossible to separate users on a network.

13. Why is loop protection necessary?

a. It denies attackers from launching DDoS attacks.

b. It prevents a broadcast storm that can cripple a network. – PG267

c. It must be installed before IEEE 802.1d can be implemented.

d. It makes a DMZ more secure.

14. What does MAC limiting and filtering do?

a. It limits devices that can connect to a switch. – PG268

b. It prevents Address Resolution Protocol spoofing.

c. It provides security for a router.

d. It allows only approved wireless devices to connect to a network.

15. In a network using IEEE 802.1x, a supplicant .

a. makes a request to the authenticator – PG269

b. contacts the authentication server directly

c. can only be a wireless device

d. must use IEEE 802.11d to connect to the network

16. Which of the following is true regarding security for a computer that boots to Apple Mac OS X and then runs a Windows 7 virtual machine?

a. The security of the Apple Mac OS X completely protects the Windows 7 virtual machine.

b. The security of the Windows 7 virtual machine completely protects the Apple Mac OS X.

c. The Windows 7 virtual machine needs its own security.

d. The hypervisor protects both the Apple Mac OS X and Windows 7 operating systems. – PG270

17. Which of the following is not an advantage of host virtualization?

a. Penetration testing can be performed using a simulated network environment on a computer using multiple virtual machines.

b. Only one copy of anti-virus software is needed. – PG270

c. Security patches can be tested.

d. Host operating system virtualization can be used for training purposes.

18. Which of the following is not a security concern of virtualized environments?

a. Virtual machines must be protected from both the outside world and also from other virtual machines on the same physical computer.

b. Virtual servers are less expensive than their physical counterparts. – PG271

c. Live migration can immediately move one virtualized server to another hypervisor.

d. Physical security appliances are not always designed to protect virtual systems.

19. \_\_\_\_\_\_\_ is adding digital voice clients and new voice applications onto the IP network.

a. VoIP

b. IP telephony – PG272

c. TCP/IP convergence

d. Voice packet consolidation (VPC)

20. Which of the following is not a characteristic of cloud computing?

a. Limited client support – PG274

b. On-demand self-service

c. Immediate elasticity

d. Metered services

**Chapter 8 Review Questions**

1. Bluetooth falls under the category of \_\_\_\_\_\_.

a. local area network (LAN)

b. short area network (SAN)

c. paired-device network (PDN)

d. personal area network (PAN) – PG294

2. A Bluetooth network that contains one master and at least one slave using the same RF channel forms a \_\_\_\_\_\_\_.

a. cluster

b. grouping

c. scatteringnet

d. piconet – PG294

3. \_\_\_\_\_ is the unauthorized access of information from a wireless device through a Bluetooth connection.

a. Bluejacking

b. Bluetooth snatching

c. Bluetooth spoofing

d. Bluesnarfing – PG296

4. The IEEE \_\_\_\_\_\_ standard specifies a maximum rated speed of 54 Mbps using the 5 GHz spectrum.

a. 802.11

b. 802.11a – PG296

c. 802.11b

d. 802.11g

5. Each of the following is an advantage of IEEE 802.11n except \_\_\_\_\_.

a. smaller coverage area – PG297

b. faster speed

c. less interference

d. stronger security

6. Which of the following is not found in a residential WLAN gateway?

a. intrusion detection system (IDS) – PG297

b. firewall

c. router

d. dynamic host configuration protocol (DHCP)

7. Which of the following is not a requirement for war driving?

a. Wireless NIC adapter

b. antennas

c. GPS receiver – PG299

d. mobile computer device

8. The primary design of a(n) is to capture the transmissions from legitimate users.

a. evil twin – PG301

b. Bluetooth grabber

c. WEP

d. rogue access point

9. Which of the following is a vulnerability of MAC address filtering?

a. The user must enter the MAC.

b. APs use IP addresses instead of MACs.

c. Not all operating systems support MACs.

d. MAC addresses are initially exchanged between wireless devices and the AP in an unencrypted format. – PG303

10. Each of the following is a limitation of turning off the SSID broadcast from an AP except \_\_\_\_\_\_.

a. the SSID can easily be discovered, even when it is not contained in beacon frames, because it still is transmitted in other management frames sent by the AP

b. turning off the SSID broadcast may prevent users from being able to freely roam from one AP coverage area to another

c. some versions of operating systems favor a network broadcasting an SSID over one that does not

d. users can more easily roam from one WLAN to another – PG304

11. The primary weakness of wired equivalent privacy (WEP) is \_\_\_\_\_\_\_.

a. its usage creates a detectable pattern – PG306

b. initialization vectors (IVs) are difficult for users to manage

c. it only functions on specific brands of APs

d. it slows down a WLAN from 104 Mbps to 16 Mbps

12. The two models for personal wireless security developed by the Wi-Fi Alliance are Wi-Fi Protected Access (WPA) and \_\_\_\_\_\_\_.

a. Protected Wireless Security (WPS)

b. IEEE 802.11ai

c. Postshared Key Protection (PKP)

d. Wi-Fi Protected Access 2 (WPA2) – PG308

13. WPA replaces WEP with \_\_\_\_\_.

a. Temporal Key Integrity Protocol (TKIP) – PG308

b. Cyclic Redundancy Check (CRC)

c. Message Integrity Check (MIC)

d. WPA2

14. A preshared key (PSK) of fewer than \_\_\_\_\_\_ characters may be subject to an attack if that key is a common dictionary word.

a. 6

b. 12

c. 16

d. 20 – PG309

15. WEP key that is 128 bits in length \_\_\_\_\_\_\_.

a. cannot be used on access points that use passphrases.

b. is less secure than a WEP key of 64 bits because shorter keys are stronger.

c. has an initialization vector (IV) that is the same length as a WEP key of 64 bits. – PG305

d. cannot be cracked because it is too long.

16. AES-CCMP is the encryption protocol standard used in \_\_\_\_\_\_\_.

a. WPA2 – PG310

b. IEEE 802.11

c. WPA

d. Bluetooth

17. What is the Extensible Authentication Protocol (EAP)?

a. A subset of WPA2

b. The protocol used in TCP/IP for authentication

c. A framework for transporting authentication protocols – PG311

d. A technology used by IEEE 802.11 for encryption

18. Which technology should be used instead of LEAP?

a. STREAK

b. LEAP-2

c. REAP

d. PEAP – PG311

19. Each of the following is a type of wireless AP probe except \_\_\_\_\_\_\_.

a. wireless device probe

b. dedicated probe

c. AP probe

d. WNIC probe – PG313

20. The most flexible approach for a wireless VLAN is to have which device separate the packets?

a. firewall

b. AP – PG314

c. NIC

d. router