

---

## Chapter 2 Solutions

### Review Questions

1. The Netstat command indicates that POP3 is in use on a remote server. Which port is the remote server most likely using?
  - a. port 110
2. At a Windows XP computer, what command can you enter to show all open ports being used?
  - a. Netstat
3. Which protocol uses UDP?
  - d. TFTP
4. Which protocol offers guaranteed delivery and is connection-oriented?
  - c. TCP
5. TCP communication could be likened to which of the following?
  - d. telephone conversation
6. Which of the following protocols is connectionless? (Choose all that apply.)
  - a. UDP
  - b. IP
7. Which command verifies the existence of a node on a network?
  - a. Ping
8. FTP offers more security than TFTP. True or False?

True
9. List the three components of the TCP/IP three-way handshake.

SYN, SYN-ACK, and ACK
10. What protocol is used for reporting or informational purposes?
  - c. ICMP
11. List the six flags of a TCP packet.

SYN, ACK, PSH, URG, RST, FIN
12. A UDP packet is usually smaller than a TCP packet. True or False?

True
13. What port, other than port 110, is used to retrieve e-mail?
  - b. port 143
14. What port does DNS use?
  - d. port 53
15. What command is used to log on to a remote server, computer, or router?
  - b. Telnet
16. Which of the following is not a valid octal number?

c. 3482

17. The initial sequence number (ISN) is set at what step of the TCP three-way handshake?

d. 1 and 2

18. A Ping command initially uses which ICMP type code?

b. type 8

19. "Destination Unreachable" is designated by which ICMP type code?

c. type 3

20. What is the hexadecimal equivalent of the binary number 1111 1111?

a. FF

## Activities

### Activity 2-4

1. Octal values are 4, 7, 5, 3, and 2.

2. You should have written the binary number 101, which converts to the octal number 5 (1 + 0 + 4).

3. You use 111 000 000 in binary and 700 in octal.

4. You use 111 110 100 in binary and 764 in octal.

5. Your calculation should be  $777 - 020 = 757$ . Converting octal 757 gives you the directory permissions `rw-r-xrwx`.

6. You should have done the following to solve this problem:

Default permission: 666

umask 022

Result: 644

Permissions: `rw-r--r--`

## Case Projects

### Case Project 2-1: Determining the Services Running on a Network

Answers may vary. The memo should include the most obvious services that would be running on a corporate network such as K.J. Williams. At the very least, the network would be running e-mail (POP3, IMAP4, SMTP) and Web services.

### Case Project 2-2: Investigating Possible E-mail Fraud

## **Hands-On Ethical Hacking and Network Defense 1st Edition Simpson Solutions Manual**

Full Download: <http://testbanklive.com/download/hands-on-ethical-hacking-and-network-defense-1st-edition-simpson-solutions-m>

*Hands-on Ethical Hacking and Network Defense*, 0619217081

Ch. 2

Solutions-3

Answers may vary. The memo should include the syntax for connecting to an e-mail server and sending an e-mail message to another student, using a different From address.