ch02

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

____ 1. No matter what medium connects computers on a network—copper wires, fiber-optic cables, or a wireless setup—the same protocol must be running on all computers if communication is going to function correctly.

____ 2. In the TCP/IP stack, the transport layer includes network services and client software.

____ 3. To retrieve e-mail from a mail server, you most likely access port 119.

____ 4. An octal digit can be represented with only three bits because the largest digit in octal is 7.

____ 5. A hex number is written with two characters, each representing a byte.

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

____ 6. The most widely used is protocol is ____.
a. IPX/SPX
b. ATM
c. TCP/IP
d. NetBIOS

____ 7. TCP stands for ____.
a. Transfer Control Protocol
b. Transmission Control Protocol
c. Transfer Congestion Protocol
d. THE Control Protocol

____ 8. In the TCP/IP stack, the ____ layer is concerned with physically moving electrons across a media or wire.
a. Internet
b. network
c. transport
d. application

____ 9. In the TCP/IP stack, the ____ layer is concerned with controlling the flow of data, sequencing packets for reassembly, and encapsulating the segment with a TCP or UDP header.
a. Internet
b. network
c. transport
d. application

____ 10. In the TCP/IP stack, the ____ layer is where applications and protocols, such as HTTP and Telnet, operate.
a. Internet
b. network
c. transport
d. application

____ 11. In the TCP/IP stack, the ____ layer uses IP addresses to route packets to their appropriate destination network.
a. Internet
b. network
c. transport
d. application

____ 12. The ____ layer protocols are the front ends to the lower-layer protocols in the TCP/IP stack.
a. Internet
b. network
c. transport
d. application

____ 13. UDP stands for ____.
a. User Datagram Protocol
b. Universal Datagram Protocol
c. User Data Packet
d. Universal Data Packet

____ 14. ____ is an attack that relies on guessing the ISNs of TCP packets.
a. ARP spoofing
b. Session hijacking
c. DoS
d. Man-in-the-middle

____ 15. A(n) ____ is the logical, not physical, component of a TCP connection.

a. ISN
b. socket
c. port
d. SYN

____ 16. The HTTP service uses port ____.
a. 25
b. 53
c. 69
d. 80

____ 17. The SMTP service uses port ____.
a. 25
b. 53
c. 69
d. 80

____ 18. The TFTP service uses port ____.
a. 25
b. 53
c. 69
d. 80

____ 19. The DNS service uses port ____.
a. 25
b. 53
c. 69
d. 80

____ 20. ____ was the de facto standard for moving or copying large files and is still used today, although to a lesser extent because of the popularity of HTTP.
a. FTP
b. TFTP
c. SNMP
d. SMTP

____ 21. The POP3 service uses port ____.
a. 110
b. 119
c. 135
d. 139

____ 22. The Microsoft RPC service uses port ____.
a. 110
b. 119
c. 135
d. 139

____ 23. The NetBIOS service uses port ____.
a. 110
b. 119
c. 135
d. 139

____ 24. The Network News Transport Protocol service uses port ____.
a. 110
b. 119
c. 135
d. 139

____ 25. ____ is a fast but unreliable delivery protocol that operates on the transport layer.
a. IP
b. TCP
c. TFTP
d. UDP

____ 26. ____ is a connectionless protocol
a. TCP
b. UDP
c. FTP
d. POP3

____ 27. Based on the starting decimal number of the ____ byte, you can classify IP addresses as Class A, Class B, or Class C.
a. first
b. second
c. third
d. fourth

____ 28. What type of class has the IP address 193.1.2.3?
a. Class A
b. Class B
c. Class C
d. Class D

____ 29. Each Class C IP address supports up to ____ host computers.
a. 254
b. 512
c. 65,000
d. 16 million

____ 30. The binary number 11000001 converted to decimal is ____.
a. 128
c. 193

b. 164 d. 201

Completion
Complete each statement.

31. The IP in TCP/IP stands for _____.
32. In the TCP/IP stack, the _____ layer is responsible for getting data packets to and from the application layer by using port numbers.
33. In the TCP/IP stack, the _____ layer represents the physical network pathway and the network interface card.
34. TCP is a(n) _____ protocol, which means the sender doesn't send any data to the destination node until the destination node acknowledges that it's listening to the sender.
35. In TCP, the _____ is a 32-bit number that tracks the packets received by the node and enables the reassembly of large packets that have been broken up into smaller packets.
36. An octet is equal to _____ bits, which equals one byte.
37. In addition to a unique network address, each network must be assigned a(n) _____, which helps identify the network address bits from the host address bits.

Matching

Match each term with the correct statement below.

a. FTP
b. SMTP
c. SNMP
d. SSH
e. HTTP
f. IRC
g. URG
h. SYN
i. PSH

____ 38. the main protocol for transmitting e-mail messages across the Internet
____ 39. the primary protocol used to communicate over the World Wide Web
____ 40. TCP header flag used to deliver data directly to an application
____ 41. allows different operating systems to transfer files between one another
____ 42. primarily used to monitor devices on a network, such as remotely monitoring a router's state
____ 43. enables multiple users to communicate over the Internet in discussion forums
____ 44. TCP header flag that signifies the beginning of a session
____ 45. enables a remote user to log on to a server and issue commands
____ 46. TCP header flag that is used to signify urgent data

Short Answer

47. What is the "poor man's firewall"?
48. What steps are involved in TCP's "three-way handshake"?
49. What are the critical components of a TCP header? How may hackers abuse them?
50. What is DNS used for?

51. Often technical personnel who aren't familiar with security techniques think that restricting access to ports on a router or firewall can protect a network from attack. Is this a good solution?
52. UDP is an unreliable data delivery protocol. Why is it widely used on the Internet?
53. What is ICMP used for?
54. What is a Class B IP address?
55. How many host addresses can be assigned with a subnet mask of 255.255.255.0? Give a brief description of how you calculated the result.
56. What is the binary numbering system and why was it chosen by computer engineers to be used in computers?
57. How does the octal numbering system relate to network security? You may answer this question by providing an example.

ch02
Answer Section

TRUE/FALSE

1. ANS: T PTS: 1 REF: 20
2. ANS: F PTS: 1 REF: 20
3. ANS: F PTS: 1 REF: 25
4. ANS: T PTS: 1 REF: 33
5. ANS: F PTS: 1 REF: 34

MULTIPLE CHOICE

6. ANS: C PTS: 1 REF: 20
7. ANS: B PTS: 1 REF: 20
8. ANS: B PTS: 1 REF: 20
9. ANS: C PTS: 1 REF: 20
10. ANS: D PTS: 1 REF: 20
11. ANS: A PTS: 1 REF: 20
12. ANS: D PTS: 1 REF: 21
13. ANS: A PTS: 1 REF: 28
14. ANS: B PTS: 1 REF: 22
15. ANS: C PTS: 1 REF: 23
16. ANS: D PTS: 1 REF: 23
17. ANS: A PTS: 1 REF: 24
18. ANS: C PTS: 1 REF: 24
19. ANS: B PTS: 1 REF: 24
20. ANS: A PTS: 1 REF: 24
21. ANS: A PTS: 1 REF: 25
22. ANS: C PTS: 1 REF: 25
23. ANS: D PTS: 1 REF: 25
24. ANS: B PTS: 1 REF: 25
25. ANS: D PTS: 1 REF: 28
26. ANS: B PTS: 1 REF: 28
27. ANS: A PTS: 1 REF: 29
28. ANS: C PTS: 1 REF: 29
29. ANS: A PTS: 1 REF: 30
30. ANS: C PTS: 1 REF: 32

COMPLETION

31. ANS: Internet Protocol

    PTS: 1 REF: 20
32. ANS: transport

PTS: 1 REF: 20

33. ANS: network

PTS: 1 REF: 20

34. ANS: connection-oriented

PTS: 1 REF: 21

35. ANS: initial sequence number (ISN)

PTS: 1 REF: 22

36. ANS: eight

PTS: 1 REF: 29

37. ANS: subnet mask

PTS: 1 REF: 30

MATCHING

38. ANS: B PTS: 1 REF: 21
39. ANS: E PTS: 1 REF: 21
40. ANS: I PTS: 1 REF: 22
41. ANS: A PTS: 1 REF: 21
42. ANS: C PTS: 1 REF: 21
43. ANS: F PTS: 1 REF: 21
44. ANS: H PTS: 1 REF: 22
45. ANS: D PTS: 1 REF: 21
46. ANS: G PTS: 1 REF: 22

SHORT ANSWER

47. ANS:
Even though IPX/SPX is not widely used today, many corporations have legacy systems that rely on it. In fact, some users separate their internal networks from the outside world by running IPX/SPX internally. An intruder attempting to attack a network over the Internet would be blocked when the protocol changes from TCP/IP to IPX/SPX. This tactic is referred to as "the poor man's firewall." Of course, it's not a recommended solution for protecting a network, but as a network security professional, you might see it used.

PTS: 1 REF: 20

48. ANS:
1. Host A sends a TCP packet with the SYN flag set (that is, a SYN packet) to Host B.
2. After receiving the packet, Host B sends Host A its own SYN packet with an ACK flag (a SYN-ACK packet) set.
3. In response to the SYN-ACK packet from Host B, Host A sends Host B a TCP packet with the ACK flag set (an ACK packet).

PTS: 1 REF: 21

49. ANS:
As a security professional, you should know the critical components of a TCP header: TCP flags, the initial sequence number, and source and destination port numbers. Hackers abuse many of these TCP header components; for example, when port scanning,many hackers use the method of sending a packet with a SYN-ACK flag set even though a SYN packet was not sent first.

PTS: 1 REF: 21

50. ANS:
Most networks require a DNS server so that users can connect to Web sites with URLs instead of IP addresses. When a user enters a URL, such as *www.yahoo.com*, the DNS server resolves the name to an IP address. The DNS server might be internal to the company, or each computer might be configured to point to the IP address of a DNS server that's serviced by the company's ISP.

PTS: 1 REF: 24

51. ANS:
This is easier said than done. After all, if a firewall prevents any traffic from entering or exiting a network on port 80, you have indeed closed a vulnerable port to access from hackers. However, you have also closed the door to Internet access for your users, which probably isn't acceptable to your company. The tricky (and almost impossible) part for security personnel is attempting to keep out the bad guys while allowing the good guys to work and use the Internet.

PTS: 1 REF: 24

52. ANS:
UDP is a widely used protocol on the Internet because of its speed. UDP doesn't need to verify whether the receiver is listening or ready to accept the packets. The sender doesn't care—it just sends, even if the receiver isn't ready to accept the packet.

PTS: 1 REF: 28

53. ANS:
Internet Control Message Protocol (ICMP) is used to send messages that relate to network operations. For example, if a packet cannot reach its destination, you might see the "Destination Unreachable" error. ICMP makes it possible for network professionals to troubleshoot network connectivity problems (with the Ping command) and to track the route a packet traverses from a source IP address to a destination IP address (with the Traceroute command).

PTS: 1 REF: 28

54. ANS:
These address are evenly divided between a two-octet network and a two-octet host address, allowing more than 65,000 host computers per Class B network address. Large organizations and Internet service providers are often assigned Class B Internet addresses. Class B addresses have the format "network.network.node.node".

PTS: 1 REF: 30

55. ANS:
With a default subnet mask of 255.255.255.0, 254 host addresses can be assigned to each segment. You use the formula $2x - 2$ for this calculation. For this example, x equals 8 because there are eight bits in the fourth octet:

$2^8 - 2 = 254$

You must subtract 2 in the formula because the network portion and host portion of an IP address can't contain all 1s or all 0s.

PTS: 1 REF: 30

56. ANS:
The binary system, on the other hand, uses the number 2 as its base. Each binary digit, or bit, is represented by a 1 or 0. Bits are usually grouped by eight because a byte contains eight bits. Computer engineers chose this numbering system because logic chips make binary decisions based on true or false,on or off,and so forth. With eight bits, a computer programmer can represent 256 different colors for a video card, for example.(Two to the power of eight, or 28, equals 256.) Therefore, black can be represented by 00000000, white by 11111111, and so on.

PTS: 1 REF: 31

57. ANS:
To see how the octal numbering system relates to network security, take a look at UNIX permissions. Octal numbering is used to express the following permissions on a directory or a file: Owner permissions, Group permissions, and Other permissions. For a directory, (rwxrwxrwx) means that the owner of the directory, members of a group, and everyone else (Other) have read, write, and execute permissions for that directory.

Because each category has three unique permissions, and each permission can be expressed as true or false (on or off), three bits are used. You don't need all eight bits because three bits (rwx) are enough.Recall from binary numbering that 0 is counted as a number, so with three bits, there are eight possible occurrences: 000, 001, 010, 011, 100, 101, 110, and 111. Using octal numbering, 001 indicates that the execute (x) permission is granted, 010 indicates that the write (w) permission is granted, but not read and execute, and so on.

PTS: 1 REF: 33