Hands-On Ethical Hacking and Network Defense 3rd edition Simpson Test Bank

SKU: 9781285454610-TEST-BANK

TRUE/FALSE

1 : No matter what medium connects computers on 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.
A : true
B : false

Correct Answer : A

2 : In the TCP/IP stack, the Transport layer includes network services and client software.
A : true
B : false

Correct Answer : B

3 : To retrieve e-mail from a mail server, you most likely access port 119.
A : true
B : false

Correct Answer : B

4 : An octal digit can be represented with only three bits because the largest digit in octal is seven.
A : true
B : false

Correct Answer : A

5 : A hex number is written with two characters, each representing a byte.
A : true
B : false

Correct Answer : B

SHORT RESPONSE

6 : What is the binary numbering system and why was it chosen by computer engineers to be used in computers?

Correct Answer : The binary system uses the number two as its base. Each binary digit, or bit, is represented by a one or zero. 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.

7 : Why should a security professional fully understand the TCP header components?

Correct Answer : As a security professional, you should know the critical components of a TCP

header; hackers leverage knowledge of these TCP header components. You need to understand these components before learning how they can be abused. Then, and only then, can you check whether your network has vulnerabilities in these areas. Remember, to protect a network, you need to know the basic methods of hacking into networks.

8 : What steps are involved in TCP's "three-way handshake"?

Correct Answer : 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).

9 : What are the critical components of a TCP header?

Correct Answer : The critical components of a TCP header are TCP flags, the initial sequence number (ISN), 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.

10 : What is the Domain Name System (DNS) used for?

Correct Answer : 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.

11 : Often technical personnel who are not familiar with security techniques think that restricting access to ports on a router or firewall can protect a network from attack. Why is this solution ?

Correct Answer : When a firewall prevents any traffic from entering or exiting a network on any well-known port, such as 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.

12 : UDP is an unreliable data delivery protocol. Why is UDP widely used on the Internet?

Correct Answer : 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.

13 : What is ICMP used for?

Correct Answer : 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 using 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.

14 : What is a Class B IP address?

Correct Answer : 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".

15 : How many host addresses can be assigned with a subnet mask of 255.255.255.0? Explain how you calculated the result.

Correct Answer : 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:28 - 2 = 254You must subtract two in the formula because the network portion and host portion of an IP address can't contain all ones or all zeros.

MULTIPLE CHOICE

16 : What protocol is the most widely used and allows all computers on a network to communicate and functioncorrectly?
A : IPX/SPX
B : ATM
C : TCP/IP
D : NetBIOS

Correct Answer : C

17 : What does the acronym TCP represent?
A : Transfer Control Protocol
B : Transmission Control Protocol
C : Transfer Congestion Protocol
D : The Control Protocol

Correct Answer : B

18 : In the TCP/IP stack, what layer is concerned with physically moving bits across the network's medium?
A : Internet
B : Network
C : Transport
D : Application

Correct Answer : B

19 : In the TCP/IP stack, what 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

Correct Answer : C

20 : What layer, in the TCP/IP stack, do applications and protocols, such as HTTP and Telnet, operate?
A : Internet
B : Network
C : Transport
D : Application

Correct Answer : D

21 : What layer, in the TCP/IP stack, is responsible for routing a packet to a destination address?
A : Internet
B : Network
C : Transport
D : Application

Correct Answer : A

22 : What layer protocols operate as the front end to the lower-layer protocols in the TCP/IP stack?
A : Internet
B : Network
C : Transport
D : Application

Correct Answer : D

23 : What type of network attack relies on guessing a TCP header's initial sequence number, or ISN?
A : ARP spoofing
B : Session hijacking
C : DoS
D : Man-in-the-middle

Correct Answer : B

24 : What is the logical component of a TCP connection that can be assigned to a process that requires network connectivity?
A : ISN
B : IP
C : port
D : SYN

Correct Answer : C

25 : What port does the Hypertext Transfer Protocol, or HTTP service use?
A : 25
B : 53
C : 69
D : 80

Correct Answer : D

26 : What port does the Simple Mail Transfer Protocol, or SMTP service use?
A : 25
B : 53
C : 69
D : 80

Correct Answer : A

27 : What port does the Trivial File Transfer Protocol, or TFTP service use?
A : 25
B : 53
C : 69
D : 80

Correct Answer : C

28 : What port does the Domain Name System, or DNS service use?
A : 25
B : 53
C : 69
D : 80

Correct Answer : B

29 : What port is typically reserved and utilized by the Secure Hypertext Transfer Protocol to create a secure connection to a Web server?
A : 443
B : 80
C : 434
D : 408

Correct Answer : A

30 : What layer, in the TCP/IP protocol stack, is responsible for encapsulating data into segments?
A : Transport layer
B : Internet layer
C : Application layer
D : Network layer

Correct Answer : A

31 : What connection-oriented protocol is utilized by the Transport layer?
A : HTTPS
B : UDP
C : TCP
D : SSL

Correct Answer : C

32 : What TCP flag is responsible for synchronizing the beginning of a session?
A : URG flag

B : ACK flag
C : PSH flag
D : SYN flag

Correct Answer : D

33 : What TCP flag is responsible for delivering data directly and immediately to an application?
A : ACK flag
B : PSH flag
C : RST flag
D : SYN flag

Correct Answer : B

34 : What 32-bit number tracks packets received by a node and allows the reassembling of large packets that have been broken up into smaller packets?
A : IP
B : TCP
C : UDP
D : ISN

Correct Answer : D

35 : What TCP/IP protocol is fast, unreliable, and operates at the Transport layer?
A : TCP
B : UDP
C : FTP
D : POP3

Correct Answer : B

36 : What TCP/IP protocol is used to send messages related to network operations and can be used to troubleshoot network connectivity?
A : ICMP
B : UDP
C : TCP
D : ARP

Correct Answer : A

37 : What IP address is used as a loopback address and is not a valid IP address that can be assigned to a network?
A : 128 address
B : 127 address
C : 224 address
D : 255 address

Correct Answer : B

38 : What IPv4 address class has the IP address 221.1.2.3?
A : Class A
B : Class B
C : Class C

D : Class D

Correct Answer : C

39 : How many host computers can be assigned a valid IPv4 address when using a CIDR /24 prefix?
A : 254
B : 512
C : 65,000
D : 16 million

Correct Answer : A

40 : What is the decimal equivalent of the binary number 11000001?
A : 128
B : 164
C : 193
D : 201

Correct Answer : C

MATCHING

41 : Match each item with a statement below.

A : Protocol used to send messages related to network operations	A : ICMP
B : Attack that relies on guessing the ISNs of TCP packets	B : network session hijacking
C : Occupies one bit of the TCP segment and can be set to 0 (off) or 1 (on)	C : TCP flag
D : A logical component of a TCP connection that can be assigned to a process that requires network connectivity	D : port
E : Fast but unreliable delivery protocol that operates at the Transport layer	E : UDP
F : A protocol where the sender doesn't send any data to the destination node until the destination node acknowledges that it's listening to the sender	F : connection-oriented protocol
G : A 32-bit number that tracks packets received by a node and allows reassembling large packets that have been broken up into smaller packets	G : ISN
H : A protocol that does not need to verify whether the receiver is listening or ready to accept the packets	H : connectionless protocol
I : A common language used so computers can communicate with one another	I : protocol
J : A TCP/IP process that is used to establish a connection before data is sent	J : three-way handshake

Correct Answer :
A : A

B : B

C : C

D : D

E : E

F : F

G : G

H : H

I : I

J : J