Network Security Firewalls and VPNs 4th edition Kinsey Test Bank

SKU: 9781284302509-TEST-BANK

Multiple Choice

1. What is the primary purpose of using the ARP command in network security analysis?
a. To test network connectivity
b. To display IP configuration
c. To map IP addresses to MAC addresses
d. To detect potential ARP spoofing attacks

Ans: d
REF: Section 1, Part 1, Step 8 Note

2. Which tool is described as a "comprehensive graphical packet analyzer" in the lab overview?
a. Nmap
b. Hping3
c. Tcpdump
d. Wireshark

Ans: d
REF: Introduction, Tools and Software section

3. What does the command "ipconfig /all | findstr /i "ipv4 subnet mask physical"" do?
a. Displays all network adapter information
b. Clears the ARP cache
c. Filters output to show only IPv4 address, subnet mask, and MAC address
d. Pings all devices on the network

Ans: c
REF: Section 1, Part 1, Step 2c

4. In the lab topology, what is the IP address of the pfSense firewall's internal interface?
a. 172.30.0.2
b. 172.40.0.2
c. 172.30.0.1
d. 202.20.1.1

Ans: c
REF: Topology section

Network Security Firewalls and VPNs 4th edition Kinsey Test Bank

5. What is the primary difference between a Regular scan and an Intense scan in Nmap/Zenmap?
a. A Regular scan checks only for open ports.
b. An Intense scan works only on Linux systems.
c. An Intense scan uses more aggressive techniques to gather information.
d. A Regular scan provides more detailed information than an Intense scan.

Ans: c
REF: Section 1, Part 2, Step 21 Note

6. What protocol does hping3 use when executing the command "hping3 -1 -c 1 202.20.1.1"?
a. TCP
b. UDP
c. ICMP
d. ARP

Ans: c
REF: Section 2, Part 2, Step 4 Note

7. What doesn't the ipconfig command display?
a. Computer name
b. Default gateway
c. IP address
d. Subnet mask

Ans: a
REF: Section 1, Part 1, Step 2 Note

8. Which command is used to display and configure network interface parameters in Linux?
a. ipconfig
b. arp
c. ifconfig
d. ping

Ans: c

Network Security Firewalls and VPNs 4th edition Kinsey Test Bank

REF: Section 2, Part 1, Step 4

9. What does the "-n" option in the tcpdump command "tcpdump -i eth0 -n host 202.20.1.1" do?
a. Specifies the network interface to listen on
b. Limits the number of packets captured
c. Prevents conversion of addresses to names
d. Filters packets by host IP address

Ans: c
REF: Section 2, Part 2, Step 7 Note

10. What is the purpose of sending a TCP SYN packet to a specific port using hping3?
a. To establish a full TCP connection
b. To clear the ARP cache
c. To test firewall rules or identify how the firewall handles traffic from different sources
d. To perform a denial-of-service attack

Ans: c
REF: Section 2, Part 2, Step 11 Note

Network Security Firewalls and VPNs 4th edition Kinsey Test Bank