DUMPSBOSS.COM

SCNS Tactical Perimeter Defense

Exin SCNS

Version Demo

Total Demo Questions: 15

Total Premium Questions: 238

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	115
Topic 2, Volume B	123
Total	238

QUESTION NO: 1

You have discovered that your Bastion host has been compromised but cannot determine when the compromise occurred. The best course of action for you to take would be:

A. Boot to the "Last Known Good Configuration".

B. Format the disk and re-install everything from scratch.

C. Restore from your most recent tape back-up.

D. Run an Anti-Virus scan on the Bastion host and clean any infected files.

E. Download and run the patch for the exploit that was used in the attack.

ANSWER: B

QUESTION NO: 2

In the command ipchains -N chain , what will the -N accomplish in the chain?

A. Calls up the next sequential chain

B. Create a new chain named "chain"

C. Calls up the chain named "chain"

D. Negate the current chain

E. Commit the new changes in the present chain

ANSWER: B

QUESTION NO: 3

The organization you work for has recently decided to have a greater focus on security issues. You run the network, and are called in the meeting to discuss these changes. After the initial meeting you are asked to research and summarize the major issues of network security that you believe the organization should address. What are Network Securitys five major issues?

A. Authorization and Availability

B. Administration

C. Integrity

D. Confidentiality

E. Encapsulation

F. Encryption

G. Non-Repudiation

H. Authentication

ANSWER: A C D G H

QUESTION NO: 4

You are evaluating the security of different wireless media, and are considering the use of microwave technology. What are the two types of microwave transmissions used in commercial wireless networking?

A. Terrestrial

B. Line of sight

C. Diffused

D. Integrated

E. Satellite

ANSWER: A E

QUESTION NO: 5

As Intrusion Detection Systems become more sophisticated, the software manufacturers develop different methods of detection. If an IDS uses the process of matching known attacks against data collected in your network, what is this known as?

A. Signature analysis

B. Packet filter matching

C. Statistical analysis

D. Analysis engine engagement

E. Packet match and alarming

ANSWER: A

QUESTION NO: 6

You are building the rules of your new firewall. You wish to allow only (Internal) access to smtp email on the Internet (External). You wish for all other traffic to be disallowed. Which of the following rules will you have to implement to make this happen?

A. Direction: Inbound, Protocol: TCP, Source IP: Internal, Destination IP: External, Source Port: 25, Destination Port: >=1024, Action: Allow.

B. Direction: Outbound, Protocol: TCP, Source IP: External, Destination IP: Internal, Source Port: 25, Destination Port: >=1024, Action: Allow.

C. Direction: Outbound, Protocol: TCP, Source IP: Internal, Destination IP: External, Source Port: >=1024, Destination Port: 25, Action: Allow.

D. Direction: Inbound, Protocol: TCP, Source IP: External, Destination IP: Internal, Source Port: 25, Destination Port: >=1024, Action: Allow.

E. Direction: Inbound, Protocol: SMTP, Source IP: Internal, Destination IP: External, Source Port: 25, Destination Port: >=1024, Action: Allow

ANSWER: C D

QUESTION NO: 7

You have just installed a new Intrusion Detection System in your network. You are concerned that there are functions this system will not be able to perform. What is a reason an IDS cannot manage hardware failures?

A. The IDS can only manage RAID 5 failures.

B. The IDS cannot be programmed to receive SNMP alert messages.

C. The IDS cannot be programmed to receive SNMP trap messages.

D. The IDS cannot be programmed to respond to hardware failures.

E. The IDS can only inform you that an event happened.

ANSWER: E

QUESTION NO: 8

You have recently been contracted to implement a new firewall solution at a client site.

What are the two basic forms of firewall implementations?

A. Chaining

B. Stateful

C. DMZ

D. Stateless

E. KMZ

ANSWER: B D

QUESTION NO: 9

You are configuring your new IDS machine, where you have recently installed Snort. While you are working with this machine, you wish to create some basic rules to test the ability to log traffic as you desire.

Which of the following Snort rules will log any tcp traffic from any IP address to any port between 1 and 1024 on any host in the 10.0.10.0/24 network?

A. log tcp 0.0.0.0/24 -> 10.0.10.0/24 1<>1024

B. log tcp any any -> 10.0.10.0/24 1<>1024

C. log tcp any any -> 10.0.10.0/24 1:1024

D. log tcp 0.0.0.0/24 -> 10.0.10.0/24 1:1024

E. log udp any any -> 10.0.10.0/24 1:1024

ANSWER: C

QUESTION NO: 10

If you are configuring your WLAN for security, and you configure the access points with a security feature that the clients do not support, what can you add to the clients to have them participate in the WLAN?

A. Protocol Analyzers

B. WLAN Support

C. The correct SSID

D. New access points

E. Supplicants

ANSWER: E

QUESTION NO: 11

You are configuring the Access Lists for your new Cisco Router. The following are the commands that are entered into the router for the list configuration.

Router(config)#access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 80

Router(config)#access-list 171 deny tcp 0.0.0.0 255.255.255.255 10.10.0.0 0.0.255.255 eq

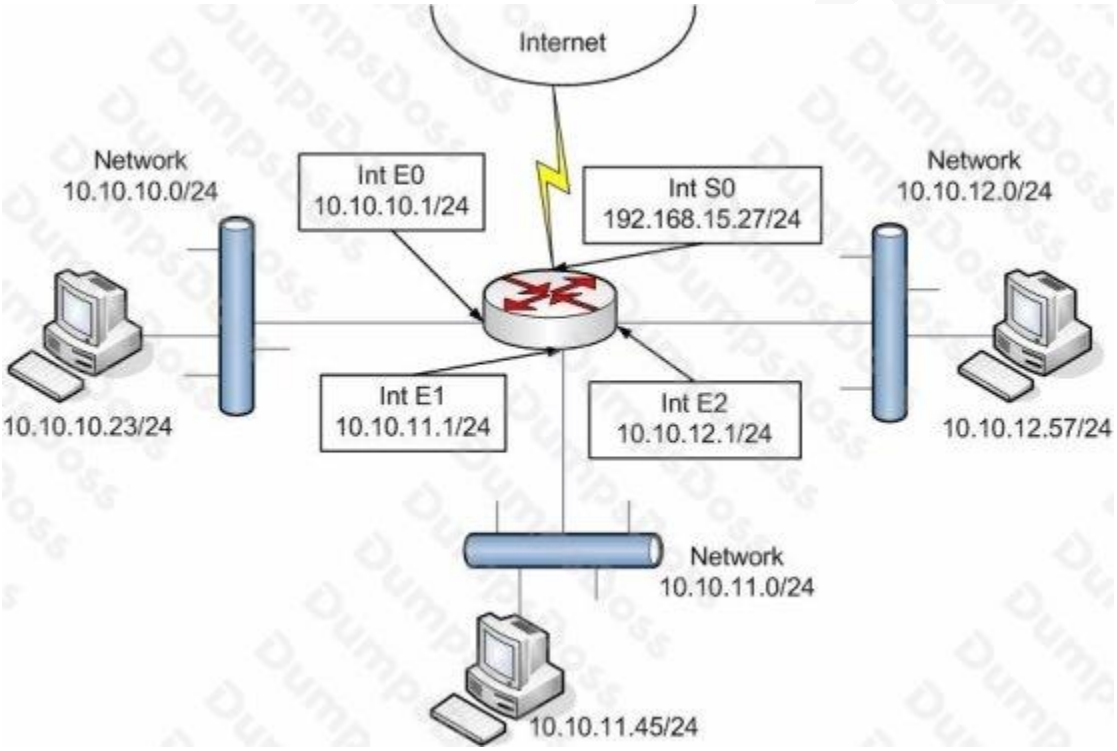
80

Router(config)#access-list 171 deny tcp any any eq 23

Router(config)#access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 20

Router(config)# access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 21

Based on this configuration, and using the exhibit, select the answers that identify how the router will deal with network traffic.



A. Permit WWW traffic to the Internet

B. Deny WWW traffic to the internal networks

C. Deny all Telnet traffic

D. Permit FTP traffic to the Internet

E. Permit FTP traffic to the internal networks

ANSWER: A D E

QUESTION NO: 12

What is the function of the following configuration fragment?

Router#configure terminal

Router(config)#line vty 0 4

Router(config-line)#transport input ssh telnet

Router(config-line)#^Z

Router#

A. The router will attempt to use SSH first, then use Telnet

B. The router will attempt to use Telnet first, then use SSH

C. The router will accept only SSH on VTY 0 4

D. The router will accept both Telnet and SSH connections

E. The router will accept only Telnet on VTY 0 4

ANSWER: D

QUESTION NO: 13

What tool used in wireless network analysis has the ability to output its findings to

MapPoint?

A. Netstumbler

B. AirSnort

C. Wireshark

D. Network Monitor

E. AirSniffer

ANSWER: A

QUESTION NO: 14

You are configuring a new custom IPSec policy on your Windows Server 2003 machine. On the rules tab, you find the three default options under the IP Filter List. What are these three default options?

A. All TCP Traffic

B. All UDP Traffic

C. All IP Traffic

D. All ICMP Traffic

ANSWER: C D

QUESTION NO: 15

You are building the rules of your new firewall. You wish to allow only (Internal) access to standard www sites on the Internet (External). You wish for all other traffic to be disallowed.

Which of the following rules will you have to implement to make this happen?

A. Direction: Inbound, Protocol: TCP, Source IP: Internal, Destination IP: External, Source Port: 80, Destination Port: >=1024, Action: Allow.

B. Direction: Outbound, Protocol: TCP, Source IP: External, Destination IP: Internal, Source Port: 80, Destination Port: >=1024, Action: Allow.

C. Direction: Outbound, Protocol: TCP, Source IP: Internal, Destination IP: External,
Source Port: >=1024,
Destination Port: 80, Action: Allow.

D. Direction: Inbound, Protocol: TCP, Source IP: External, Destination IP: Internal, Source Port: 80, Destination Port: >=1024, Action: Allow.

E. Direction: Inbound, Protocol: WWW, Source IP: Internal, Destination IP: External, Source Port: 80, Destination Port: >=1024, Action: Allow

ANSWER: C D