SCP SC0-451

SC0-451 Tactical Perimeter Defense

Practice Test

Version 1.4

QUESTION NO: 1

You are introducing a co-worker to the security systems in place in your organization. During the discussion you begin talking about the network, and how it is implemented. You mention something in RFC 791, and are asked what that is. What does RFC 791 specify the standards for?

A. IP
B. TCP
C. udp
d. ICMP
E. Ethernet

Answer: A

QUESTION NO: 2

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: 3

You have recently taken over the security of a mid-sized network. You are reviewing the current configuration of the IPTables firewall, and notice the following rule:

ipchains -A output -p TCP -d 172.168.35.40 ! www

What is the function of this rule?

A. This rule for the output chain states that all www traffic on 172.168.35.40 from any IP address is allowed.
B. This rule for the input chain states that all TCP packets are allowed to the 172.168.35.40 IP address to any port other than 80.
C. This rule for the input chain states that all TCP packets are able to get to the www service on any IP address except for 172.168.35.40.

D. This rule for the output chain states that all TCP packets are able to get to the www service on any IP address except for 172.168.35.40.
E. This rule for the output chain states that all TCP packets are allowed to the 172.168.35.40 IP address to any port other than 80.

Answer: E

QUESTION NO: 4

You are configuring the rules on your firewall, and need to take into consideration that some clients in the network are using automatic addressing. What is the IP address range reserved for internal use for APIPA in Microsoft networks?

A. 169.254.0.0/4
B. 169.254.0.0/16
C. 169.254.0.0/8
D. 169.254.0.0/0
E. 168.255.0.0/16

Answer: B

QUESTION NO: 5

You need to install a new antenna for the wireless network available on your company property. Which antenna type is best for extending theYou need to install a new antenna for the wireless network available on your company? property. Which antenna type is best for extending the local range of an Access Point?

A. Yagi
B. Omni-directional
C. Di-polar
D. Parabolic
E. Mono-polar

Answer: B

QUESTION NO: 6

You have decided to install Snort on your Windows Server 2003 and are making changes to the default configuration file. You see the following two lines:

include classification.config

include reference.config

What should these two lines read, after you make your changes, on a default installation?

A. include C:\Snort\etc\classification.config
B. include
C. \Snort\etc\reference.config
D. include \classification.config
E. include \reference.config
F. include //classification.config
G. include //reference.config

Answer: A,B

QUESTION NO: 7

In your organization a decision has been made to implement a multicasting application. You are configuring your firewall to allow this application to flow through in both directions. What address range are you going to address on the firewall?

A. 10.0.0.0/8
B. 172.16.0.0/12
C. Multicast addresses use APIPA's 169.254.0.0/16
D. 224.0.0.0/4
E. Addresses are negotiated at the time of the multicast. The nearest router assigns a public IP address assigned by ARIN.

Answer: D

QUESTION NO: 8

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: 9

Your company has created it's security policy and it's time to get the firewall in place. Your group is trying to decide whether to build a firewall or buy one. What are some of the benefits to purchasing a firewall rather than building one?

A. They usually have a good management GUI.
B. They offer good logging and alerting.
C. You do not need to configure them.
D. The OS doesn't need to be hardened before installing the vendor's firewall on it.
E. They often do real time monitoring.

Answer: A,B,E

QUESTION NO: 10

You have been given the task of adding some new wireless equipment to the existing wireless network in your office. What wireless standard allows for up to 54 Mbps transmission rates and is compatible with 802.11b?

A. 802.1a
B. 802.11e
C. 802.11c
D. 802.11g
E. 802.11i

Answer: D

QUESTION NO: 11

During an analysis of your IPSec implementation, you capture traffic with Network Monitor. You are verifying that IP is properly identifying AH. When you look into IP, what protocol ID would IP identify with AH?

A. Protocol ID 0x800 (800)
B. Protocol ID 0x6 (6)
C. Protocol ID 0x15 (21)
D. Protocol ID 0x33 (51)
E. Protocol ID 0x1 (1)

Answer: D

QUESTION NO: 12

You are concerned about attacks against your network, and have decided to implement some defensive measure on your routers. If you have 3 interfaces, SI, SO, and EO, and you implement the following configuration, what attack will you be defending against?

Router#config terminal
Router(config)# Interface Ethernet 0
Router(config-if)#no ip directed broadcast
Router(config-if)#Interface Serial 0
Router(config-if)#no ip directed broadcast
Router(config-if)#Interface Serial 1
Router(config-if)#no ip directed broadcast
Routerjconfig#^Z
Router#

A. Smurf
B. B02K
C. SubSeven
D. Any Trojan
E. Any Worm

Answer: A

QUESTION NO: 13

After installing Snort on your Windows machine that is destined to be your IDS, you need to edit the configuration file to customize it to your needs. What is the name of that configuration file?

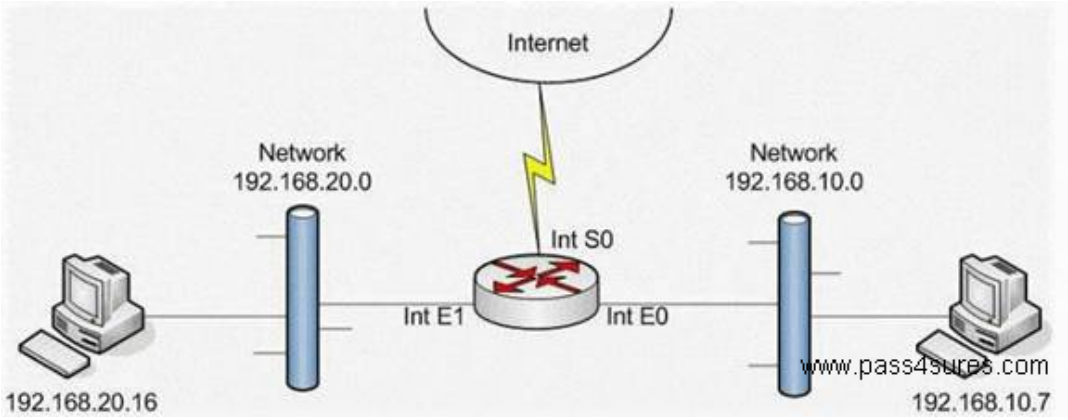
A. Snort.cfg
B. Config.snt
C. Snortconfig
D. Snort.conf
E. Config.snort

Answer: D

QUESTION NO: 14

The exhibit shows a router with three interfaces EO, E1 and SO. Interfaces EO and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface SO is connected to the Internet.

The objective is to allow host 192.168.10.7 access to the Internet via ftp and deny access to the Internet to everyone else while allowing them to access resources amongst themselves. From the following, select all the access list statements that are required to make this possible.



A. access-list 153permit tcp 192.168.10.7 0.0.0.0 any eq ftp
B. access-list 21permit ip 192.168.10.7 0.0.0.0 any eq ftp
C. access-list 21 deny 0.0.0.0 255.255.255.255
D. int SO, ip access-group 21 out
E. int SO, ip access-group 153 out
F. int E1, ip access-group 153 in

Answer: A,E

QUESTION NO: 15

After you implemented your IPSec solution, you wish to run some tests to verify functionality. Which of the following provides confidentiality and authentication when implementing IPSec?

A. Authentication Header
B. Encapsulating Security Payload
C. Security Associations
D. Security Authentications
E. Encapsulating Delimiters

Answer: B

QUESTION NO: 16

In your organization a decision has been made to implement a multicasting application. You are configuring your firewall to allow this application to flow through in both directions. What address range are you going to address on the firewall?

A. 10.0.0.0/8
B. 172.16.0.0/12
C. Multicast addresses use APIPA's 169.254.0.0/16
D. 224.0.0.0/4
E. Addresses are negotiated at the time of the multicast. The nearest router assigns a public IP address assigned by ARIN.

Answer: D

QUESTION NO: 17

Your company has recently become security conscious and wishes to protect it's electronic assets. What is the first thing you should have in place before configuring rules for your company's firewall?

A. A Security Policy
B. AN IDS
C. A DNS server
D. An Email server
E. A WINS server

Answer: A

QUESTION NO: 18

A router has two active Ethernet interfaces. Interface EO is connected to network 10.10.0.0/16 while Interface E1 is connected to network 10.11.0.0/16. You are configuring access control lists to manage specific access, which is disallowed on these segments. The configuration of the lists are as follows:

router(config)#access-list 123 deny tcp 10.11.0.0 0.0.255.255 10.10.0.0 0.0.255.255 eq 20
router(config)#access-list 123 deny tcp 10.11.0.0 0.0.255.255 10.10.0.0 0.0.255.255 eq 21
router(config)#access-list 123 deny tcp 10.10.0.0 0.0.255.255 10.11.0.0 0.0.255.255 eq 20
router(config)#access-list 123 deny tcp 10.10.0.0 0.0.255.255 10.11.0.0 0.0.255.255 eq 21
router(config)#access-list 123 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
router(config)#Interface Ethernet 0
router(config-if)#ip access-group 123 in
router(config-if)#Interface Ethernet 1

router(config-it)#ip access-group 123 in

Based on the above list configuration, which of the following statements is true on the router?

A. All packets will be dropped
B. All packets that match the deny statements will be forwarded to the console port
C. All packets that do not match the deny statements will be allowed
D. An Access List cannot simultaneously be implemented upon two or more interfaces
E. We do not know if this is a standard or extended access list, therefore there is not enough information.

Answer: A

QUESTION NO: 19

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: 20

During a training presentation, that you are delivering, you are asked how wireless networks function, compared to the OSI Model. What two layers of the OSI Model are addressed by the 802.11 standards?

A. Physical
B. Data Link
C. Network
D. Transport
E. Session

Answer: A,B

QUESTION NO: 21

You are configuring your new IDS machine, and are creating new rules. You enter the following rule:

Alert tcp any any -> any 23 (msg: "Telnet Connection Attempt";)

What is the effect of this rule?

A. This is a logging rule, designed to capture any telnet attempts
B. This is an alert rule, designed to notify you of the use of telnet in either direction
C. This is an alert rule, designed to notify you of the use of telnet in one direction
D. This is a logging rule, designed to notify you of telnet connection attempts
E. This is an alert rule, designed to notify you of attempts to connect from any IP address on port 23 to any IP address and any port on a remote host.

Answer: C

QUESTION NO: 22

Recently, you have made many changes to your ISA Server 2006 firewall. You are concerned about saving these changes. What is the part of ISA Server used for saving your configuration changes?

A. The built-in feature to export your configuration to an XLS file.
B. The Copy Configuration to CD feature.
C. The built-in feature to export your configuration to an XML file.
D. The image burning feature set.
E. The option to configure the server to utilize RAID 5.

Answer: C

QUESTION NO: 23

You need to add a line to your IPTables Firewall input chain that will stop any attempts to use the default install of Back Orifice against hosts on your network (the 10.10.10.0 network). Which of the following would be the correct command to use?

A. ipchains -A input TCP -d 0.0.0.0/0 -s 10.10.10.0/24 31337-J DENY
B. ipchains -A input UDP-s0.0.0.0/0 -d 10.10.10.0/24 p:31337-j DENY
C. ipchains -A input -s 0.0.0.0/0 -d 10.10.10.0/24 -p 31337 -j DENY
D. ipchains -A input TCP -s 0.0.0.0/0 -d 10.10.10.0/24 31337 -j DENY
E. ipchains -A input -s 0.0.0.0/0 -d 10.10.10.0/24 31337 -j deny