Latest Version: 6

Question: 1

You are concerned about attacks against your network, and have decided to implement some defensive measure on your routers. If you have 3 interfaces, S1, S0, and E0, 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 Router(config)#^Z Router#

A. Smurf
B. BO2K
C. SubSeven
D. Any Trojan
E. Any Worm

Answer: A

Question: 2

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: 3

It has been decided that you must implement new security on your wireless networks. What wireless protection system is defined as: MIC + TKIP + EAP + 802.1x?

A. WTLS
B. WEP

C. WPA
D. W3DES
E. WPKI

Answer: C

Question: 4

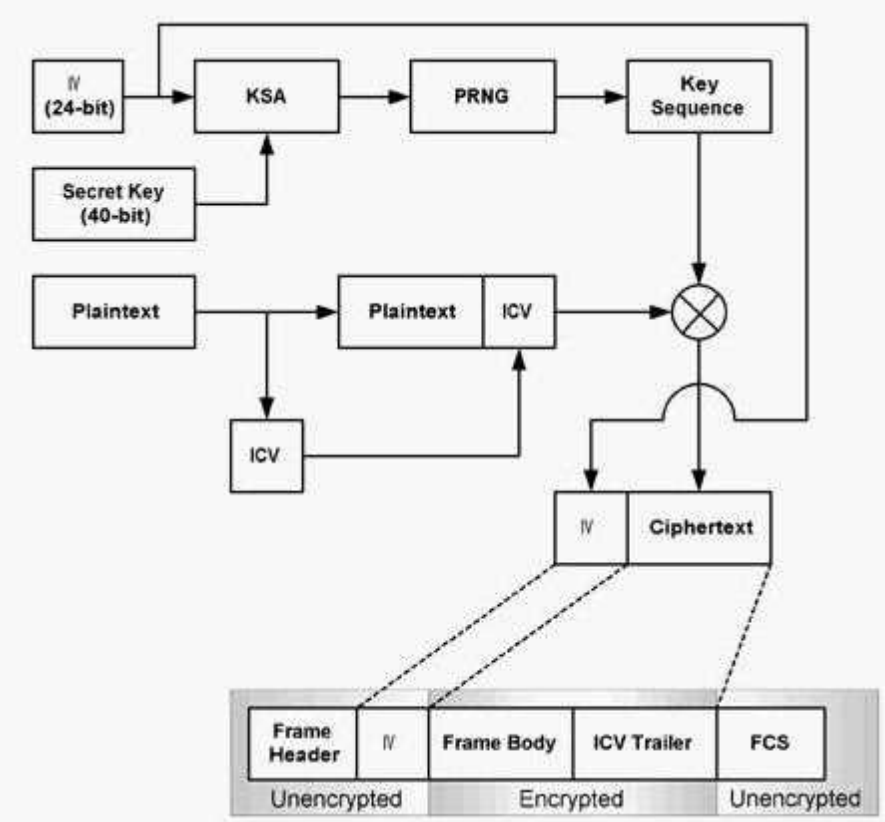
You are in the process of configuring your network firewall policy. As you begin building the content of the policy you start to organize the document into sections. Which of the following are sections found in the firewall policy?

A. The Acceptable Use Statement
B. The Firewall Administrator Statement
C. The Network Connection Statement
D. The Incident Handling Statement
E. The Escalation Procedures Statement

Answer: A, B, C

Question: 5

You need to diagram wireless security options for your team during a planning meeting. What wireless



A. WPA
B. WEP
C. WTLS
D. WPKI
E. W3DES

Answer: B

Question: 6

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: 7

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 -s 0.0.0.0/0 -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

Answer: D

Question: 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: 9

You have been given the task of building the new wireless networks for your office, and you need to verify that your equipment will not interfere with other wireless equipment frequencies. What wireless standard allows for up to 11 Mbps transmission rates and operates in the 2.4GHz range?

A. 802.11b
B. 802.11e
C. 802.11a
D. 802.11i
E. 802.11g

Answer: A

Question: 10

You are configuring the IP addressing for your network. One of the subnets has been defined with addresses already. You run ifconfig on a host and determine that it has an address of 10.12.32.18/14. What is the broadcast address for this network?

A. 0.0.0.0
B. 10.255.255.255
C. 10.12.0.0
D. 10.12.255.255
E. 10.15.255.255

Answer: E

Question: 11

At a policy meeting you have been given the task of creating the firewall policy. What are the two basic positions you can take when creating the policy?

A. To deny all traffic and permit only that which is required.
B. To permit only IP traffic and filter TCP traffic
C. To permit only TCP traffic and filter IP traffic
D. To permit all traffic and deny that which is required.
E. To include your internal IP address as blocked from incoming to prevent spoofing.

Answer: A, D

Question: 12

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