Free Questions for SC0-451 by vceexamstest

Shared by Morrow on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- IP

B- TCP

C- UDP

D- ICMP

E- Ethernet

Answer:

A

Question 2

Question Type: MultipleChoice

You are configuring your new IDS machine, and are creating new rules. You enter the following rule: Alert tcp any any -> 10.0.10.0/24 any (msg: "NULL scan detected"; flags: 0;) What is the effect of this rule?

Options:

A- This is a logging rule, designed to capture NULL scans originating from the 10.0.10.0/24 network.

B- This is a logging rule, designed to capture NULL scans.

C- This is an alert rule, designed to notify you of NULL scans of the network in either direction.

D- This is an alert rule, designed to notify you of NULL scans of the network in one direction.

E- This is a logging rule, designed to notify you of NULL scans.

Answer:

D

Question 3

Question Type: MultipleChoice

You are designing a new IPSec implementation for your organization, and are trying to determine your security needs. You need to clearly understand the implementation choices, before you make any changes to the network. Which of the following describes what transport and tunnel modes protect using IPSec?

Options:

A- In transport mode, IPSec protects upper-layer protocols.

B- In transport mode, IPSec protects just the TCP header.

C- In tunnel mode, IPSec protects the upper-layer protocols.

D- In transport mode, IPSec protects the entire IP packet.

E- In tunnel mode, IPSec protects the entire IP packet.

F- In tunnel mode, IPSec protects just the IP header.

Answer:

A, E

Question 4

Question Type: **MultipleChoice**

You are configuring your new IDS machine, and are creating new rules. You enter the following rule: Alert tcp any any -> 10.0.10.0/24 any (msg: "SYN-FIN scan detected"; flags:SF;) What is the effect of this rule?

Options:

A- This is an alert rule, designed to notify you of SYN-FIN scans of the network in one direction.

B- This is an alert rule, designed to notify you of SYN-FIN scans of the network in either direction.

C- This is a logging rule, designed to capture SYN-FIN scans.

D- This is a logging rule, designed to notify you of SYN-FIN scans.

E- This is an alert rule, designed to notify you of SYN-FIN scans originating from the 10.0.10.0/24 network.

Answer:

A

Question 5

Question Type: **MultipleChoice**

You have just installed a new network-based IDS for your organization. You are in the middle of your initial configuration of the system, and are now configuring the response. What is the most common response of an IDS when an event happens?

Options:

A- To trace the origin of the event

B- To close the communication path to the hostile host

C- To page the security officer on call

D- To place an entry of the event in the log file

E- To reconfigure the service that is being exploited

Answer:

D

Question 6

Question Type: **MultipleChoice**

You are configuring your new Intrusion Detection System, and studying the true-false matrix. You read about the different types of alarms and events. Which of the following defines an event where an alarm does not occur and there is no actual intrusion?

Options:

A- True-negative

B- False-positive

C- True-positive

D- False-negative

E- Absolute-positive

Answer:

A

Question 7

Question Type: **MultipleChoice**

Your network is going to implement a new network security solution, and as part of this you are configuring IPSec on a Windows Server 2003 machine. Which of the following is the description of the Client (Respond Only) default IPSec Policy?

Options:

A- This policy is used for normal communications, and any system with this policy enabled will have the ability to communicate using IPSec if required, or requested.

B- This policy is used when all IP network traffic is to be secured. Any system with this policy enabled will always enforce secure communications using IPSec.

C- This policy is used when IP traffic is to be secured, and to allow unsecured communication with clients that do not respond to the request.

D- This policy is used when clients are the only machines on the network that need IP traffic to be secured. Any client with this policy enabled will initialize secure communications with other clients running this policy.

E- This policy is used when clients must respond to IPSec servers. If the client does not use IPSec, network communications will fail.

Answer:

A

Question 8

Question Type: MultipleChoice

You are working on your company's IPTables Firewall; you wish to create a rule to address traffic using ports 1024 through 2048. Which of the following would you use during the creation of your rule?

Options:

A- p:1024 P:2048

B- P:1024 p2048

C- p=1024-2048

D- 1024-2048

E- 1024:2048

Answer:

E

To Get Premium Files for SC0-451 Visit

https://www.p2pexams.com/products/sc0-451

For More Free Questions Visit

https://www.p2pexams.com/scp/pdf/sc0-451