HP

Exam HP2-Z09

HP HP2-Z09

Version: 3.0

[Total Questions: 76]

Question No : 1

A security administrator for a TippingPoint IPS suspects that an employee has logged into the IPS and altered its configuration. How can the security administrator analyze and undo all of the unauthorized changes?

A. by reviewing the IPS systemlog, searching for filter hits from the employee
B. by reviewing the IPS audit log, filtering by the employee's username and/or IP address
C. by reviewing the configuration changes listed in the IPS alert log
D. by reviewing the IPS block log (the employeewould have been blocked)

Answer: B

Question No : 2

Which statements about the Digital Vaccine are true? (Select three.)

A. Installing a new Digital Vaccine will reboot the IPS.
B. Some filters have a Recommended setting of Disabled.
C. Some filters have aRecommended setting of Enabled.
D. Digital Vaccines can be automatically down loaded and installed on the IPS.
E. New Digital Vaccines are released at 2 p.m. EST.

Answer: B,D,E

Question No : 3

How can the TippingPoint Threat Management Center (TMC) be accessed? (Select three.)

A. directly by your SMS, if your SMS has a valid TMC username/password
B. by anyone with a browser and valid TMC username/password
C. using an FTP client
D. directly by your IPS
E. directly by your SMS, as your SMS does not need a TMC username/password

Answer: B,D,E

Question No : 4

What does the Threat Management Center (TMC) allow you to do? (Select three.)

A. Download TOS images.
B. Access knowledgebase articles.
C. Remotely log in to your IPS.
D. Download Digital Vaccines.
E. Download custom Digital Vaccines.

Answer: A,B,D

Question No : 5

A security administrator at a university has been tasked with identifying the TippingPoint IPS that would best meet the university's needs. The university has a complex network, with a mixture of both fiber and copper wiring. IPS protection must be provided for three copper segments and two fiber segments. The aggregate bandwidth (with expansion capacity) is not expected to exceed 3Gbps over the next four years.

Which TippingPoint IPS solution should the security administrator recommend?

A. 2 TippingPoint 330s and 1 TippingPoint 600E
B. TippingPoint 5000E or TippingPoint 5100N
C. TippingPoint SMS
D. TippingPoint 5100N only

Answer: D

Question No : 6

By default, what is an IPS single super-user called?

A. By default, the single super-user is called root.
B. By default, the single super-user is called SuperUser.
C. By default, the single super-user is called admin.
D. There is no default user.

Answer: D

Question No : 7

Multiple user accounts can be created on an IPS device. Each can be assigned to one of three roles: super-user, administrator, or operator. Which statements are true about these roles? (Select two.)

A. An administrator can reset the audit log.
B. A super-user can create new accounts and edit existing account passwords.
C. An operator is a view-only role.
D. Only the super-user can reboot an IPS.

Answer: B,C

Question No : 8

What is the serial console speed of an IPS?

A. 9600
B. 19200
C. 115,200
D. user configurable

Answer: C

Question No : 9

An IPS can be managed and unmanaged from the SMS. How can you unmanage an IPS? (Select two.)

A. from the SMS Web interface
B. from the SMS client
C. from the IPS LSM Web interface
D. from the IPS CLI using conf t sms disable

Answer: B,C

Question No : 10

Jack, Kevin, and Louise are responsible for various administrative functions on the TippingPoint solution. Louise is the manager of the group and is defined on the SMS as a super-user. Jack and Kevin are both defined as administrators. Jack is responsible for network operations and uptime, and Kevin is responsible for security policy.

Which permissions should you grant? (Select two.)

A. Jack should only be granted permissions for the IPS devices.
B. Louise should be granted permissions to all segment groups, devices, and profiles.
C. Kevin should be granted permissions for the IPS devices.
D. Kevin should only be granted permissions to the appropriate profiles and segment groups.

Answer: A,D

Question No : 11

The SMS Event Viewer can query events based on which criteria? (Select three.)

A. IPS device and/or segment group that the event was generated by
B. time the event occurred
C. the attacker's MAC address
D. Microsoft exploits/vulnerabilities that have critical severity
E. the attacker's PC serial number

Answer: A,B,D

Question No : 12

When logging into the SMS Java GUI, which tab is always shown first?

A. the Events tab
B. the Profiles tab
C. the Devices tab
D. the Admin tab

Answer: A