642-627$^{\text{Q\&As}}$

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/642-627.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

You are working with Cisco TAC to troubleshoot a software problem on the Cisco IPS appliance. TAC suspects a fault with the NotificationApp software module in the Cisco IPS appliance. In this case, which Cisco IPS appliance operations may be most affected by the NotificationApp software module fault?

A. SNMP

B. IDM or IME

C. global correlation

D. remote blocking

E. anomaly detection

F. SDEE

Correct Answer: A

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_architecture.ht ml#wp1009053

NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in the Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

QUESTION 2

Which two statements accurately describe virtual sensor operations on the Cisco IPS appliance? (Choose two.)

A. You must create a new instance of a signature set for each new virtual sensor.

B. The packet processing policy is virtualized.

C. Creating a new virtual sensor creates a "virtual" machine on the Cisco IPS appliance.

D. vs0 can be cloned then deleted.

E. Each virtual sensor can have its own unique event action rules.

Correct Answer: BE

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_virtual_sensors.html# wp1029979

QUESTION 3

Which two are the functions of the learning feature of anomaly detection within a Cisco IPS appliance? (Choose two.)

A. observes actual traffic patterns to the zones

B. retrieves zero-day attack information from the Cisco SIO

C. dynamically populates the host operating system database

D. allows false-positive training by an IPS administrator

E. builds the host reputation histogram

F. learns which legitimate services have a scanning behavior

Correct Answer: AF

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_anomaly_detection.ht ml#wp1046814

QUESTION 4

Which two methods can be used together to configure a Cisco IPS signature set into detection mode when tuning the Cisco IPS appliance to reduce false positives? (Choose two.)

A. Subtract all aggressive actions using event action filters.

B. Enable anomaly detection learning mode.

C. Enable verbose alerts using event action overrides.

D. Decrease the number of events required to trigger the signature.

E. Increase the maximum inter-event interval of the signature.

Correct Answer: AC

1 > Remove all agressive actions from all signatures using event action filters 2 > Add verbose alerts using event action overrides 3 > Add logging packets between the attacker and the victim using event action overrides

QUESTION 5

What will happen if you try to recover the password on the Cisco IPS 4200 Series appliance on which password recovery is disabled?

A. The GRUB menu will be disabled.

B. The ROM monitor command to reset the password will be disabled.

C. The password recovery process will proceed with no errors or warnings; however, the password is not reset.

D. The Cisco IPS appliance will reboot immediately.

Correct Answer: C

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_troubleshooting.html# wp1139544

If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the

password, and password recovery is set to disabled, you must reimage your sensor.

You have the ability to disable password recovery if required (it is enabled by default). Follow these steps to disable password recovery from the CLI:

Step 1. Log in to the CLI using administrative privileges. Step 2. Enter global configuration mode followed by host mode:

```
sensor# configure terminal
```

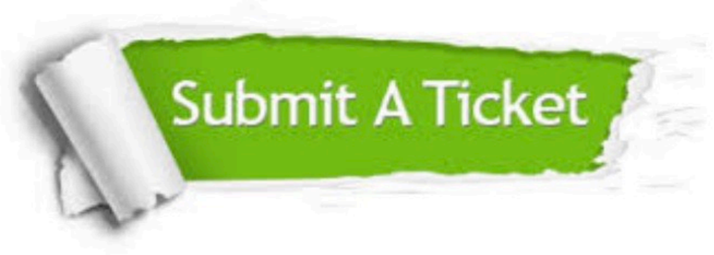
```
sensor(config)# service host
```

Step 3. Disable password recovery:

```
sensor(config-host)# password-recovery disallowed
```

Note: If an admin/user tries to recover the password on a sensor that is disabled, the process proceeds with no errors or warnings; however, the password is not reset. Follow these steps to disable password recovery from the Cisco IDM:

Step 1. Log in to the Cisco IDM using administrative privileges. Step 2. Navigate to Configuration > Sensor Setup > Network. Step 3. Disable password recovery by deselecting the Allow Password Recovery check box.


Submit A Ticket