642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

QUESTION 1

From which three sources does the Cisco IPS appliance obtain OS mapping information? (Choose three.)

A. from manually configured OS mappings

B. imported OS mappings from Management Center for Cisco Security Agent

C. imported OS mappings from Cisco Security Manager

D. learned OS mappings from passive OS fingerprinting

E. learned OS mappings from Cisco SensorBase input

F. from Cisco IPS signature updates

Correct Answer: ABD

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/ipsevact.html#wp707692

There are three sources of OS information. The sensor ranks the sources of OS information in the following order:

1.

Configured OS mappings--OS mappings that you enter on the OS Identification tab of the Event Actions

Network Information policy. You can configure different mappings for each virtual sensor. For more information, see Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only). We recommend configuring OS mappings to define the

identity of the OS running on critical systems. It is best to configure OS mappings when the OS and IP address of the critical systems are unlikely to change.

2.

Imported OS mappings--OS mappings imported from Management Center for Cisco Security Agents (CSA MC).

Imported OS mappings are global and apply to all virtual sensors. For information on configuring the sensor to use CSA MC, see Configuring the External Product Interface, page 32-23.

3.

Learned OS mappings--OS mappings observed by the sensor through the fingerprinting of TCP packets with the SYN control bit set.

Learned OS mappings are local to the virtual sensor that sees the traffic. When the sensor needs to determine the OS for a target IP address, it consults the configured OS mappings. If the target IP address is not in the configured OS mappings, the sensor looks in the imported OS mappings. If the target IP address is not in the imported OS mappings, the sensor looks in the learned OS mappings. If it cannot find it there, the sensor treats the OS of the target IP address as unknown.

QUESTION 2

Which Cisco IPS appliance feature has the following three potential settings: off, partial, and full?

A. anomaly detection

B. POSFP

C. reputation filtering

D. global correlation network participation

E. event action overrides

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_collaboration.html

QUESTION 3

Which four features are supported on the Cisco ASA AIP-SSM but are not supported on the Cisco ASA AIP-SSC? (Choose four.)

A. multiple virtual sensors

B. anomaly detection

C. promiscuous mode

D. custom signatures

E. fail open

F. global correlation

Correct Answer: ABDF

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/ps6825/product_data_sheet0900aecd80404916_ps6120_Products_Data_Sheet.html

QUESTION 4

What about this configuration command is true: ips inline fail-open sensor sensor_name?

A. will enable fail-open hardware bypass on the Cisco IPS 4200 Series appliance

B. will enable inline operation on the Cisco IPS 4200 Series appliance

C. will enable inline operation on the Cisco IDSM-2, IPS AIM, or IPS NME

D. will enable the desired traffic to be diverted from the Cisco ASA to one of the Cisco ASA AIP- SSM virtual sensors

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/clissm.html

QUESTION 5

Which Cisco IPS feature is most likely to respond to a zero-day attack?

A. reputation filtering

B. botnet filtering

C. anomaly detection

D. meta-engine

E. de-obfuscation

F. threat detection

Correct Answer: C

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/anomaly_detector/v5.0/configuration/guide/Intro.html#wp1046115