642-627 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

Which four networking tools does Cisco IME include that can be invoked for specific events, to learn more about attackers and victims using basic network reconnaissance? (Choose four.)

A. ping

B. traceroute

C. packet tracer

D. nslookup

E. whois

F. nmap

Correct Answer: ABDE

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/ime/ime_getting_started.htm l IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events

QUESTION 2

The Cisco IPS appliance global correlation and reputation filtering features depend on which two of these? (Choose two.)

A. anomaly detection

B. OS fingerprinting

C. Cisco SensorBase

D. watch list ratings

E. event action overrides

F. DNS

Correct Answer: CF

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

QUESTION 3

What are the five possible values for the event count key parameter of an IPS signature? (Choose five.)

A. attacker address

B. victim address

C. attacker and victim address

D. victim address and port

E. attacker and victim addresses and ports

F. attacker address and victim port

G. attacker and victim port

Correct Answer: ABCEF

QUESTION 4

Numerous attacks using duplicate packets, changed packets, or out-of-order packets are able to successfully evade and pass through the Cisco IPS appliance when it is operating in inline mode. What could be causing this problem?

A. The IPS Application Inspection and Control is disabled.

B. All the DoS signatures are disabled.

C. All the reconnaissance signatures are disabled.

D. TCP state bypass is enabled.

E. The normalizer is set to asymmetric mode.

Correct Answer: E

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/white_paper_c11- 459025.html

QUESTION 5

A Cisco IPS appliance running in a network environment with asymmetrical traffic flow is experiencing many false positive alerts that are triggered by the 13000 signature ID. What can the IPS administrator tune on the IPS to reduce the false positives?

A. set the normalizer mode to strict mode

B. set the AD operational mode to inactive

C. enable TCP state bypass

D. increase the default scanner threshold

E. disable the uRPF check

Correct Answer: B

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

Anomaly Detection Modes

Anomaly detection initially conducts a "peacetime" learning process when the most normal state of the network is reflected. Anomaly detection then derives a set of policy thresholds that best fit the normal network. This is done in two phases:

an initial learning mode phase, followed by the ongoing operational detect mode phase.

Anomaly detection has the following modes:

?earning accept mode (initial setup)

Although anomaly detection is in detect mode by default, it conducts an initial learning accept mode for the default period of 24 hours. We assume that during this phase no attack is being carried out. Anomaly detection creates an initial

baseline, known as a knowledge base, of the network traffic. The default interval value for periodic schedules is 24 hours and the default action is rotate, meaning that a new knowledge base is saved and loaded, and then replaces the initial

knowledge base after 24 hours.

Keep the following in mind:

?nomaly detection does not detect attacks when working with the initial knowledge base, which is empty.

After the default of 24 hours, a knowledge base is saved and loaded and now anomaly detection also detects attacks.

?epending on your network complexity, you may want to have anomaly detection in learning accept mode for longer than the default 24 hours. You configure the mode in the Virtual Sensors policy; see Defining A Virtual Sensor, . After your

learning period has finished, edit the virtual sensor and change the mode to Detect.

?etect mode

For ongoing operation, the sensor should remain in detect mode. This is for 24 hours a day, 7 days a week.

Once a knowledge base is created and replaces the initial knowledge base, anomaly detection detects attacks based on it. It looks at the network traffic flows that violate thresholds in the knowledge base and sends alerts.

As anomaly detection looks for anomalies, it also records gradual changes to the knowledge base that do not violate the thresholds and thus creates a new knowledge base. The new knowledge base is periodically saved and takes the place

of the old one thus maintaining an up-to-date knowledge base.

?nactive mode

You can turn anomaly detection off by putting it in inactive mode. Under certain circumstances, anomaly detection should be in inactive mode, for example, if the sensor is running in an asymmetric environment.

Because anomaly detection assumes it gets traffic from both directions, if the sensor is configured to see only one direction of traffic, anomaly detection identifies all traffic as having incomplete connections, that is, as scanners, and sends

alerts for all traffic flows. The following example summarizes the default anomaly detection configuration. If you add a virtual sensor at 11:00 pm and do not change the default anomaly detection configuration, anomaly detection begins

working with the initial knowledge base and only performs learning. Although it is in detect mode, it cannot detect attacks until it has gathered information for 24 hours and replaced the initial knowledge base. At the first start time (10:00 am by

default), and the first interval (24 hours by default), the learning results are saved to a new knowledge base and this knowledge base is loaded and replaces the initial knowledge base. Because the anomaly detection is in detect mode by

default, now that anomaly detection has a new knowledge base, the anomaly detection begins to detect attacks.