642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

QUESTION 1

You are tasked to create a custom IPS signature using the IDM Custom Signature Wizard to detect a network reconnaissance attack in which one system makes connections to multiple hosts on multiple TCP ports. Which Cisco IPS signature engine should be selected to configure this custom IPS signature?

A. Atomic IP

B. Atomic IP Advanced

C. String TCP

D. Sweep

E. Meta

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_signature_wizard.ht ml

QUESTION 2

Which two interface modes can be implemented with a single physical sensing interface on the Cisco IPS 4200 Series appliance? (Choose two.)

A. inline interface pair

B. inline VLAN groups

C. inline VLAN pair

D. promiscuous

E. hardware bypass

Correct Answer: CD

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

QUESTION 3

Which IPS alert action is available only in inline mode?

A. produce verbose alert

B. request rate limit

C. reset TCP connection

D. log attacker/victim pair packets

E. deny-packet-inline

F. request block connection

Correct Answer: E

http://www.cisco.com/web/about/security/intelligence/ipsmit.html

Inline Mode Event Actions

The following actions require the device to be deployed in Inline mode and are in affect for a user- configurable default time of 3600 seconds (60 minutes). Deny attacker inline: This action is the most severe and effectively blocks all

communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.

Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another

port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This

event action is appropriate when the likelihood of a false alarm or spoofing is minimal. Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could

communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not

deny further communication. Deny packet inline: This action prevents the specific offending packet from reaching its intended destination.

Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.

Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as

TCP segmentation and IP fragmentation re-ordering.

QUESTION 4

Which two configurations are required on the Cisco IPS appliance to allow Cisco Security Manager to log into the Cisco IPS appliance? (Choose two.)

A. Enable SNMPv2.

B. Enable SSH access.

C. Enable TLS/SSL to allow HTTPS access.

D. Enable NTP.

E. Enable Telnet access.

F. Enable the IP address of the Cisco Security Manager server as an allowed host.

Correct Answer: CF

Explanation: : Obvious standard config but needs confirmation
http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliTasks.html#wp1056053

QUESTION 5

Which of these depicts the correct process order of the Cisco IPS reputation filters and global correlation operations?

A. IPS reputation filters > signature inspection > global correlation

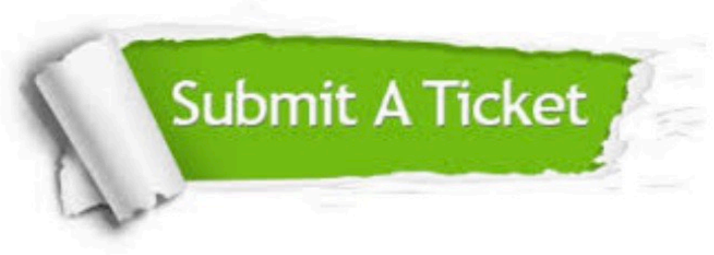
B. IPS reputation filters > global correlation > signature inspection

C. global correlation > IPS reputation filters > signature inspection

D. signature inspection > IPS reputation filters > global correlation

Correct Answer: A

http://www.cisco.com/en/US/prod/collateral/modules/ps2641/solution_overview_cisco_ips_aim.ht ml


Submit A Ticket

100%