Exam Code: 642-532

Exam Name: Securing Networks Using Intrusion Prevention Systems Exam (IPS)

Vendor: CISCO

Version: DEMO

Part: A

1: Which three steps must you perform to prepare sensor interfaces for inline operations? (Choose three.)
A.Disable all interfaces except the inline pair.
B.Add the inline pair to the default virtual sensor.
C.Enable two interfaces for the pair.
D.Disable any interfaces that are operating in promiscuous mode.
E.Create the interface pair.
F.Configure an alternate TCP-reset interface
Correct Answers: B C E

2: Your Cisco router is hosting an NM-CIDS. The router configuration contains an inbound ACL. Which action does the router take when it receives a packet that should be dropped, according to the inbound ACL?
A.The router forwards the packet to the NM-CIDS for inspection, then drops the packet.
B.The router drops the packet and does not forward it to the NM-CIDS for inspection.
C.The router filters the packet through the inbound ACL, tags it for drop action, and forwards the packet to the NM-CIDS. Then the router drops it if it triggers any signature, even a signature with no action configured.
D.The router filters the packet through the inbound ACL, forwards the packet to the NM-CIDS for inspection only if it is an ICMP packet, and then drops the packet.
Correct Answers: B

3: Which action is available only to signatures supported by the Normalizer engine
A.Produce Verbose Alert
B.Modify Packet Inline
C.Deny Packet Inline
D.Log Pair Packets
E.Request SNMP Trap
F.Reset TCP Connection
Correct Answers: B

4: You would like to have your inline sensor deny attackers inline when events occur that have Risk Ratings over 85. Which two actions will accomplish this? (Choose two.)
A.Create Target Value Ratings of 85 to 100.
B.Create an Event Variable for the protected network.
C.Enable Event Action Overrides.
D.Create an Event Action Filter, and assign the Risk Rating range of 85 to 100 to the filter.
E.Enable Event Action Filters.
F.Assign the Risk Rating range of 85 to 100 to the Deny Attacker Inline event action.
Correct Answers: C F

5: Which two are appropriate installation points for a Cisco IPS sensor? (Choose two.)

A.on publicly accessible servers
B.on critical network servers
C.at network entry points
D.on user desktops
E.on corporate mail servers
F.on critical network segments
Correct Answers: C F

6: Which command displays the statistics for Fast Ethernet interface 0/1?
A.show interfaces FastEthernet0/1
B.show interface int1
C.show statistics FastEthernet0/1
D.show statistics virtual-sensor
E.packet capture FastEthernet0/1
F.show statistics event-store
Correct Answers: A

8: What is a configurable weight that is associated with the perceived importance of a network asset?
A.Risk Rating
B.parameter value
C.Target Value Rating
D.severity level
E.storage key
F.rate parameter
Correct Answers: C

9: You are using multiple monitoring interfaces on a sensor appliance running software version 5.0. Which statement is true?
A.You can have the simultaneous protection of multiple network subnets, which is like having multiple sensors in a single appliance.
B.You can use different sensing configurations for each monitoring interface.
C.You can enable an interface only if the interface belongs to an interface group.
D.Multiple monitoring interfaces can be assigned to Group 0 at any given time.
E.All interfaces must operate in a single mode; you cannot mix inline- and promiscuous-mode operations.
Correct Answers: A

10: Which two protocols can be used for automatic signature and service pack updates? (Choose two.)
A.SCP
B.SSH
C.FTP

D.HTTP
E.HTTPS
Correct Answers: A C

11: Which statement is true about viewing sensor events?
A.You can view events from the CLI, but you cannot filter them.
B.You can use the Events panel in the Cisco IDM to filter and view events.
C.In the Cisco IDM, you can filter events based on type or time but not both.
D.The Cisco IDM does not limit the number of events that you can view at one time.
E.To view events with high- and medium-severity levels in the Cisco IDM, you must select only the High check box from the Show alert events check boxes.
Correct Answers: B

12: How would you copy packets that have been captured from the data interfaces to a location off the Cisco IDS or IPS sensor?
A.Use the copy command with the packet-file keyword
B.Use the copy command with the capture keyword.
C.Press Ctrl-C when the capture is complete and paste the capture to your local host.
D.Use the packet display command.
Correct Answers: A

13: By manipulating the TTL on a TCP packet, an attacker could desynchronize inspection. Signature 1308 (TTL evasion) fires when the TTL for any packet in a TCP session is higher than the lowest-observed TTL for that session. Signature 1308 rewrites all TTLs to the lowest-observed TTL, and produces an alert. You would like to have the signature continue to modify packets inline but avoid generating alerts.
How could this be done?
A.This cannot be done; an alert is always generated when a signature fires.
B.Remove the Produce Alert action from the signature.
C.Create an Event Variable.
D.Create an Event Action Override that is based on the Produce Alert action.
E.Create a custom signature with the Meta engine.
Correct Answers: B

14: You recently noticed a large volume of alerts generated by attacks against your web servers. Because these are mission-critical servers, you keep them up to date on patches. As a result, the attacks fail and your inline sensor generates numerous false positives. Your assistant, who monitors the alerts, is overwhelmed.
Which two actions will help your assistant manage the false positives? (Choose two.)
A.Create a policy that denies attackers inline and filters alerts for events with high Risk Ratings.
B.Lower the severity level of signatures that are generating the false positives.
C.Lower the fidelity ratings of signatures that are generating the false positives.
D.Raise the Target Value Ratings for your web servers.
E.Create a filter that filters out any alert whose target address is that of one of your web servers.

Correct Answers: A D

15: In which file format are IP logs stored?
A.Microsoft Word
B.Microsoft Excel
C.text
D.libpcap
Correct Answers: D