Vendor: Juniper

Exam Code:JN0-541

Exam Name:IDP, Associate(JNCIA-IDP)

Version: Demo

QUESTION 1

Which two tasks can be performed using the ACM? (Choose two.)

A. Upgrade the firmware on the IDP sensor.

B. Install a policy on the IDP sensor.

C. Change the mode in which the sensor is operating.

D. Change the management IP address for the IDP sensor.

Correct Answer: CD

QUESTION 2

What two statements are true about the attack object database update process? (Choose two.)

A. Attack objects are downloaded from the Juniper web site over TCP port 443 and are stored on Security Manager.

B. Attack object database update can be scheduled using the commands guiSvrCli.sh and cron.

C. Attack object database update can be scheduled using the two commands idpSvrCli.sh andcron.

D. The administrator is given the choice of which static groups to update.

Correct Answer: AB

QUESTION 3

How can you monitor real-time IP flows through the IDP Sensor?

A. use the IDP UI Dashboard

B. use the CLI utilitysctop

C. use the IDP UI Traffic Logs

D. enable "debug flow basic" on the IDP Sensor

Correct Answer: B

QUESTION 4

Which three fields in a packet must match an IDP rule before that packet is examined for an attack? (Choose three.)

A. destination address

B. service

C. terminate match

D. source address

E. attack object

Correct Answer: ABD

QUESTION 5

What does a Drop Connection action do?

A. drops all packets from the attacker\\'s IP

B. drops any packet matching thissrc/dst/protocol

C. drops the specific session containing the attack pattern

D. drops only the specific packet matching the attack pattern

Correct Answer: C

QUESTION 6

Which two statements are true as they relate to a sniffer mode IDP Sensor deployment? (Choose two.)

A. An IP address must be assigned to the sniffer interface.

B. It does not affect the performance or availability of the network.

C. It provides passive monitoring only with limited attack prevention.

D. IDP Sensor cannot be managed by the IDP Management Server Sniffer mode.

Correct Answer: BC

QUESTION 7

Which two statements are true about quick reports? (Choose two.)

A. Maximum duration is restricted to 12 hours.

B. Quick reports are ideal for zero day investigation.

C. Quick reports can be created only from the Log Viewer.

D. Once a quick report is created, the report options cannot be modified.

Correct Answer: BC

QUESTION 8

Exhibit:

```
id policy-name  n_sess  memory   detector  nref s/o module-name

 0 june21_policy   181  86580104 4.0.90383    1   0 detector115143465
```

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which command would have produced this output?

A. sctop "p" option

B. scio agentstats policy list

C. scio policy list vr0

D. scio policy list s0

Correct Answer: D

QUESTION 9

Which field(s) can be filtered on in the Log Investigator?

A. Protocol

B. any field in the Log Viewer

C. Time

D. Source IP and Destination IP

Correct Answer: B

QUESTION 10

Which type of cable do you use for a console connection to an IDP sensor?

A. straight-through serial cable

B. null-modem cable

C. CAT 5 cable

D. Juniper proprietary cable

Correct Answer: B

QUESTION 11

Which statement about the Enterprise Security Profiler (ESP) is true?

A. The ESP must be configured and started using the IDP sensor CLI before it is used.

B. The administrator must manually initiate Security Manager to sensor polling to retrieve ESP data.

C. The ESP must be configured and started on each IDP sensor manually, using the Security Manager GUI.

D. The ESP is started by default in IDP version 4.0 or newer.

Correct Answer: C

QUESTION 12

Exhibit:

Time Received	Src Addr	Dst Addr	Protocol	Dst Port	Subcategory
8/29/06 10:20:08 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded
8/29/06 10:20:48 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which rule base would have generated the log message?

A. traffic anomaly

B. networkhoneypot

C. backdoor

D. SYN protector

Correct Answer: A