

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : **JN0-541**

Title : IDP, Associate(JNCIA-IDP)

Version : Demo

1.Which statement is true about the attack object database update process?

- A. Each sensor updates its own attack object database automatically; however they must be able to access the Juniper site on TCP port 443.
- B. The attack object database update must be manually performed by the administrator, and the administrator must manually install it on each sensor.
- C. The attack object database update can be initiated manually or automatically.
- D. The attack object database update can be automatically scheduled to occur using the Security Manager GUI.

Answer: C

2.On a sensor, which command will indicate if log messages are being sent to Security Manager.?

- A. scio vr list
- B. serviceidp status
- C. scio agentstats display
- D. scio getsystem

Answer: C

3.After you enable alerts for new hosts that are detected by the Enterprise Security Profiler, where do you look in Security Manager to see those alerts?

- A. Security Monitor > Profiler > Application Profiler tab
- B. Security Monitor > Profiler > Violation Viewer tab
- C. Security Monitor > Profiler > Network Profiler tab
- D. Log Viewer > Profiler Log

Answer: D

4.When connecting to a sensor using SSH, which account do you use to login?

- A. admin
- B. super
- C. netscreen
- D. root

Answer: A

5.Which OSI layer(s) of a packet does the IDP sensor examine?

- A. layers 2-7
- B. layers 2-4
- C. layer 7 only
- D. layers 4-7

Answer: A

6.Which two will change the management IP of an IDP sensor? (Choose two.)

- A. Edit the existing IDP sensor object in Security Manager GUI and change the IP address.
- B. Delete the IDP sensor object from Security Manager and re-add the sensor with the new IP address.
- C. Use ifconfig to change the management IP address.
- D. Use the ACM to change the management IP address.

Answer: B,D

7.Which rule base would detect netcat?

- A. SYN protector
- B. traffic anomalies
- C. backdoor
- D. exempt

Answer: C

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

- A. terminate match
- B. service
- C. destination address
- D. source address
- E. attack object

Answer: B,C,D

9.What is "a deviation from a protocol's expected behavior or packet format"?

- A. context
- B. compound attack object
- C. attack signature
- D. protocol anomaly

Answer: D

10.A newly re-imaged sensor is running IDP 4.0 code. You want to assign IP address 10.1.1.1 to the sensor. Which method do you use to do this?

- A. Connect to the sensor's console port, login as root, and answer theEasyConfig
- B. Use SSH to connect to the sensor at IP 192.168.1.1.Login as root, and run ipconfig.
- C. Connect to the sensor's console port, login as admin, and answer theEasyConfig
- D. Use SSH to connect to the sensor at IP 192.168.1.1.Login as admin, and run ipconfig.

Answer: A

11.Which rule base would detect the use of nmap on a network?

- A. SYN protector
- B. traffic anomalies
- C. backdoor
- D. exempt

Answer: B

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

- A. CAT 5 cable
- B. Juniper proprietary cable
- C. straight-through serial cable

D. null-modem cable

Answer: D

13.Which statement is true regarding IDP rule matching on a sensor?

- A. Each rule in the IDP rule base that matches on the source IP, destination IP, and service will be processed further.
- B. Each rule in the IDP rule base that matches on the source IP, destination IP, and service will be processed further, unless the particular rule is terminal.
- C. Each rule in the IDP rule base that matches on the source IP, destination IP, service, and attack object will be processed further.
- D. Each rule in the IDP rule base that matches on the source IP, destination IP, service, and attack object will be processed further, unless the particular rule is terminal.

Answer: B

14.Which TCP port is used for communication between Security Manager and an IDP sensor?

- A. 7801
- B. 7800
- C. 7803
- D. 443

Answer: C

15.Which command on the IDP sensor CLI can be used to display the sensor statistics, which policy is installed, and mode of sensor deployment?

- A. sctop "s" option
- B. sensor statistics can only be displayed from Security Manager GUI
- C. scio list s0 sensor stat
- D. scio sensor stat

Answer: A

16.Which statement is true about packet capture in the IDP sensor?

- A. The Log Viewer has no indication of whether a log message has associated packet captures.
- B. You can only log packets after an attack packet.
- C. You can configure a particular number of packets to capture before and after an attack.
- D. Packet capture records all packets flowing through the sensor.

Answer: C

17.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.

Answer: C

18.What is one use of an IP action?

- A. It blocks subsequent connections from specific IP addresses.
- B. It modifies the IP header to redirect the attack.
- C. It modifies the IP header to prevent the attack.
- D. It permits or denies the traffic, based on the IP header.

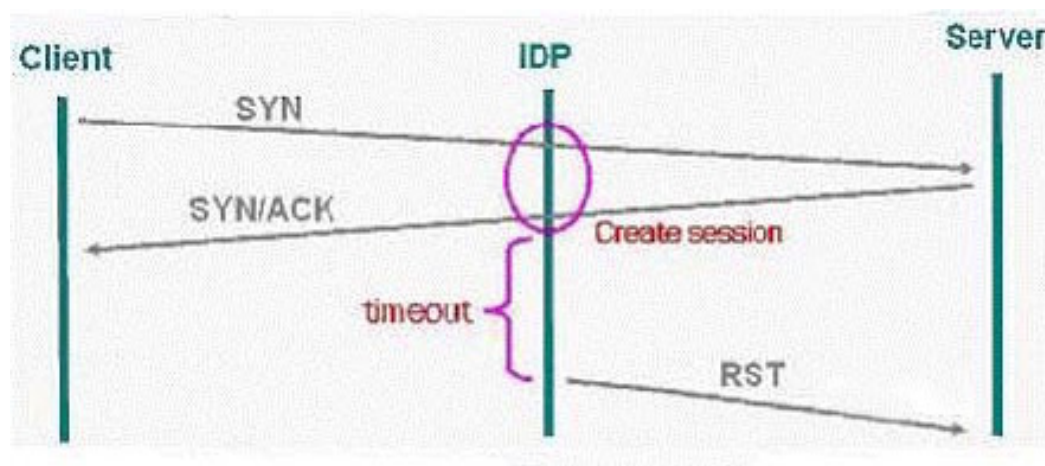
Answer: A

19.You update your attack object database on Security Manager. What must you do before the new attack objects become active on the IDP sensors?

- A. You install the updated security policy on the IDP sensor.
- B. No changes are required.
- C. You must restart the IDP sensor.
- D. You must restart the IDP processes on the IDP sensors.

Answer: A

20.Exhibit:



You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which SYN protector mode is the IDP using?

- A. passive
- B. handshake
- C. relay
- D. protective

Answer: A