JN0-541 Q&As

IDP, Associate(JNCIA-IDP)

Pass Juniper JN0-541 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/jn0-541.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

On a sensor in transparent mode, how many virtual circuits are assigned to a virtual router?

A. 2

B. 1

C. 1 or 2

D. 3 or more

Correct Answer: A

QUESTION 2

Which three statements are true about exporting logs? (Choose three.)

A. Logs can be exported to XML, CSV, SNMP,SMTP, Syslog or PostgreSQL database from the CLI of the Management Server.

B. Logs can be exported to PDF or PostScript from the IDP User Interface.

C. Logs can be printed from the IDP User Interface.

D. Logs can be exported to HTML format.

Correct Answer: ABC

QUESTION 3

When migrating from Sniffer mode to Inline mode, what three changes need to be made so that the IDP can effectively prevent attacks? (Choose three.)

A. reconnect the IDP Sensors forwarding interfaces appropriately

B. from the ACM, change the IDP Sensor mode from Sniffer to Inline

C. reconfigure management interface IP

D. modify the rule action to drop or close

Correct Answer: ABD

QUESTION 4

Which three Profiler tables does ESP use to store data? (Choose three.)

A. Value

B. User

C. Peer

D. Host

Correct Answer: ACD

QUESTION 5

What should you do to view the attack and policy that triggered a specific Log Event?

A. sort through all fields of that log entry, and sort for the policy name and ID

B. right-click on that event, choose Show - Attack

C. right-click on that event, select Show - Attack in Security Policy

D. right-click on that event, choose Show - Security Policy

Correct Answer: C

QUESTION 6

What is the process for enabling packet logging?

A. in the notification column of a rule in the mainrulebase, select Enable logging and check "log packets" option

B. in the actions column of arulebase, select "log packets"

C. in the action column of arulebase, select logging and choose "log packets"

D. in the notification column of a rule in the mainrulebase check "log packets" option

Correct Answer: A

QUESTION 7

On a sensor, which command will list the status of the IDP processes?

A. scio getsystem

B. scio agentconfig list

C. scio vr list

D. sctop "s" option

E. serviceidp status

Correct Answer: E

QUESTION 8

Which two statements are true about packet logging? (Choose two.)

A. Packets captured are stored inpcap format.

B. IDP senor will tag all replayed packets are offline.

C. Packets logged can be replayed back into the IDP Sensor.

D. Packets captured cannot be replayed back into the IDP Sensor

Correct Answer: AC

QUESTION 9

How can you see a "view all ESP events" for Violation Objects?

A. You must define a custom filter to view only Violation Objects.

B. You select Violation Objects in the Log Viewer screen.

C. You select the Violation view in the Profiler.

D. Violation Objects are not used in ESP.

Correct Answer: C

QUESTION 10

What are two limitations of traditional IDS systems? (Choose two.)

A. do not detect internal attacks

B. do not use signatures for known attacks

C. do not operate inline so they cannot effectively block all attacks

D. frequentlyhave false positives due to less accurate packet signatures

Correct Answer: CD

QUESTION 11

Which sensor process handles all communication between the sensor and Security Manager?

A. agent

B. idp

C. sciod

D. profiler

Correct Answer: A

QUESTION 12

What is one use of an IP action?

A. It modifies the IP header to prevent the attack.

B. It blocks subsequent connections from specific IP addresses.

C. It permits or denies the traffic, based on the IP header.

D. It modifies the IP header to redirect the attack.

Correct Answer: B

QUESTION 13

You have a false positive in the Log Viewer that you want to exclude from further detection. What should you do?

A. right-click on that event, selectExempt

B. go to the Exempt rules and add that Attack Object

C. right-click on that event, choose Filter - Not this Value

D. create a policy in the top of the rulebase that ignores that event and make it a Terminal rule

Correct Answer: A

QUESTION 14

What does a Drop Packet action do?

A. drops any packet matching thissrc/dst/protocol

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

C. drops only the specific packet matching the attack

D. drops the specific session containing the attack pattern

Correct Answer: C

QUESTION 15

Which context value do you filter on to identify all webservers in a network?

A. HTTP Request Method

B. HTTP Server IP

C. HTTP Header Server

D. HTTP Header User Agent

Correct Answer: C