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.pass4itsure.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

In which three fields does Log Investigator allow you to create reports and view logs? (Choose three.)

A. Time

B. Attack

C. Destination Port

D. Sensor IP Address

Correct Answer: ABC

QUESTION 2

You implement all HTTP Signatures for your Web Server and notice an alert is generated each time a web user accesses the SQL database with the default passwords. Your webmaster does not want to reprogram the page to use valid SQL passwords. How do you disable alerting on this False Positive?

A. create an Exempt rule for any traffic destined to your Web Server, include all HTTP:LOW level attacks; make this a Terminal rule

B. create an Exempt rule for any traffic destined to your Web Server, include only the specific HTTP SQL default password signature

C. create an Exempt rule for any traffic destined to your Web Server, include all HTTP:LOW level attacks

D. create an Exempt rule for any traffic generated by your Webserver, include only the specific HTTP SQL default password signature

Correct Answer: B

QUESTION 3

Which three statements are true about ESP? (Choose three.)

A. ESP indicates when new hosts or protocols are being used.

B. ESP provides a summary of protocols and contexts on each host.

C. ESP indicates when a specific machine has been attacked.

D. ESP indicates which hosts are talking with each other, and which protocols are being used.

Correct Answer: ABD

QUESTION 4

Which method of detection does IDP Sensor use to detect rootkits or Trojans present on internal systems?

A. Protocol Anomaly

B. NetworkHoneypot

C. Stateful Signatures

D. Backdoor Detection

Correct Answer: D

QUESTION 5

Which command is used to verify the license installed on the IDP Sensor?

A. scio lic list

B. sctop lic list

C. sctop -l

D. get license

Correct Answer: A

QUESTION 6

Which statement is true about the Attack Object Update process?

A. The Attack Update can be automatically scheduled by the administrator in control.

B. The Attack Update must be manually downloaded by the administrator from the Juniper site and installed on each Sensor.

C. The Administrator in control must initiate a signature update or the User Interface can be configured to check for updates on startup.

D. Each Sensor updates its own Attack Objectsautomatically, however they must be able to access the Jumper site on TCP/443 (SSL).

Correct Answer: C

QUESTION 7

Which three actions must be taken prior to deploying an IDP sensor (in transparent mode) in a network?

A. Assign an IP to all forwarding interfaces.

B. Establish communication between Security manager and the sensor.

C. Assign an IP to the management interface IP.

D. Configure the sensor mode.

Correct Answer: BCD

QUESTION 8

What should you do to build effective security policies?

A. create specific rules for critical servers first, which look for attacks that are relevant to those servers (such as HTTP attacks onWebservers); DO NOT make these rules Terminate Match

B. create specific rules for critical servers first, which look for attacks that are relevant to those servers (such as HTTP attacks onWebservers); make these rules Terminate Match

C. create an Any/Any rule to look for all attacks and make this rule#1; DO NOT select Terminate Match

D. create an Any/Any rule to look for all attacks and make this rule#1; select Terminate Match

Correct Answer: B

QUESTION 9

You want Enterprise Security Profiler (ESP) to capture layer 7 data of packets traversing the network. Which two steps must you perform? (Choose two.)

A. Configure ESP to enable application profiling, and select the contexts to profile.

B. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.

C. Start or restart the profiler process.

D. Create a filter in the ESP to show only tracked hosts.

Correct Answer: AC

QUESTION 10

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.

Correct Answer: C

QUESTION 11

Which two statements are true? (Choose two.)

A. In transparent mode, a virtual circuit maps one-to-one with a physical interface.

B. A virtual circuit is not a forwarding interface.

C. Virtual circuits on a sensor can be listed using the commandsctop vc list.

D. A virtual circuit is a communications path in and out of the sensor.

Correct Answer: AD

QUESTION 12

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 13

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.

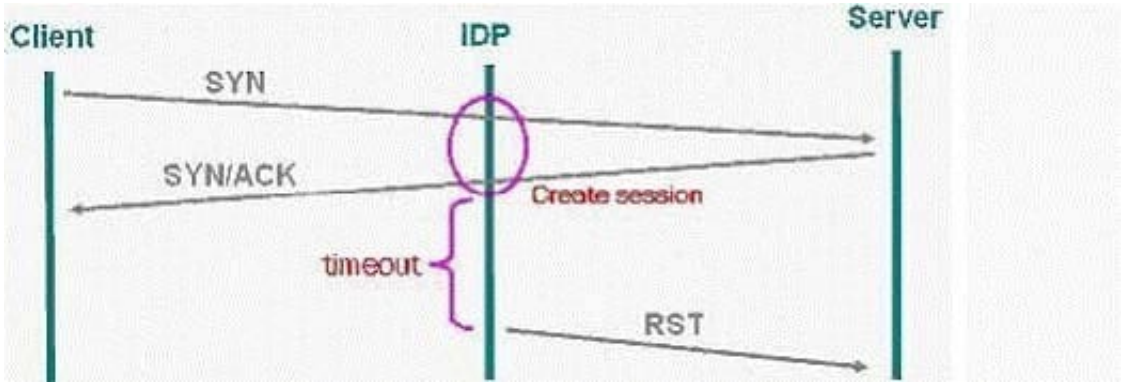
C. Logs can be printed from the IDP User Interface.

D. Logs can be exported to HTML format.

Correct Answer: ABC

QUESTION 14

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. protective

B. passive

C. handshake

D. relay

Correct Answer: B

QUESTION 15

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