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.passapply.com/jn0-541.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which two statements describe action versus IP action? (Choose two.)

A. IP action responds to matching traffic by dropping or closing current attack packets or connection.

B. Action responds to matching traffic by dropping or closing current attacking packets or connection.

C. IP Action responds to future traffic based on a previous match by blocking or dropping future connections.

D. Action responds to future traffic based on a previous match by blocking or dropping future connections.

Correct Answer: BC

QUESTION 2

What is a Close Server action?

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

B. drops any packet matching thissrc/dst/protocol

C. drops only the specific packet matching the attack pattern

D. issues a TCP Reset to the server only

Correct Answer: D

QUESTION 3

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

A. admin

B. super

C. netscreen

D. root

Correct Answer: A

QUESTION 4

On a newly re-imaged sensor, which three TCP ports are open on its eth0 interface? (Choose three.)

A. 7801

B. 7803

C. 22

D. 443

E. 80

Correct Answer: BCD

QUESTION 5

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

Correct Answer: D

QUESTION 6

Which method of detection does IDP Sensor use to detect a network scan or portscan?

A. DOS Detection

B. Traffic Anomaly

C. Protocol Anomaly

D. Backdoor Detection

Correct Answer: B

QUESTION 7

In which two ways can you view the IP address of a sensor\\'s eth0 interface? (Choose two.)

A. ipconfig

B. ACM

C. the Security Manager GUI

D. tcpdump

Correct Answer: BC

QUESTION 8

Which three columns can be seen in the Application view of Profiler? (Choose three.)

A. Protocol

B. Context and Context Value

C. Source and Destination IPs

D. Date First Seen and Last Seen

Correct Answer: BCD

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 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 11

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

Correct Answer: C

QUESTION 12

What best describes Reconnaissance attacks?

A. disabling or corrupting networks, systems, or services with the intent to deny the service to intended users

B. transmission of ping packets of certain size to crash a remote host

C. unauthorized discovery and mapping of systems, services, or vulnerabilities

D. transmission of TCP SYN requests from a spoofed IP address

Correct Answer: C

QUESTION 13

Which statement is NOT true?

A. Target platform of idp-sos3.0 indicates the platform is software that runs on an ISG1000 or ISG 2000.

B. Target platform of sos.5.0.0 indicates the platform runs Screen OS software that supports Deep Inspection.

C. Target platform sos-av.5.0.0 indicates the platform is Screen OS software that supports the Anti-Virus feature.

D. Target platform of idp-4.0.0 indicates the platform is software that runs on an IDP sensor.

Correct Answer: C

QUESTION 14

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 15

Which two statements are true about Trojans? (Choose two.)

A. They are executables that infect only executable programs.

B. They are programs often used to gather information about a host.

C. They can secretly permit access to an infected computer from an outside host.

D. They are programs that target onlywebservers by overwhelming them with traffic.

Correct Answer: BC