JN0-540

juniper networks certified internet associate.idp(jncia-idp)

DEMO

QUESTION NO: 1

How do you access the WebUI ACM Interface on a IDP Sensor?

A. https://&lt;IP Address of Sensor&gt;
B. through the SSH Interface
C. through the IDP User Interface
D. http://&lt;IP Address of Sensor&gt;

Answer: A

QUESTION NO: 2

You want ESP to alert on abnormal activities in a network. Which two actions should you take to accomplish this? (Choose two.)

A. from the Profiler configuration, select the Alert tab and select all options
B. create rule in the Profiler rulebase to log traffic from any internal source
C. create a filter in the Profiler to show only tracked hosts
D. create a Violation Object

Answer: A,D

QUESTION NO: 3

Which three functions can the IDP Sensor perform? (Choose three.)

A. forwards logs and status messages to the IDP Management Server
B. collects and presents logs to the IDP User Interface
C. performs attack detection and prevention
D. store logs locally when the IDP Management Server is unreachable

Answer: A,C,D

QUESTION NO: 4

You implement Backdoor Detection and you notice that an alert is generated each time an SSH session is established with the protected servers. What must you do to correct the situation?

A. You modify the Main rulebase to include the SSH Protocol in the top Ignore rule.
B. You create an Exempt rule for SSH in the Exempt rulebase.
C. There is no way to disable alerting on SSH if you have Backdoor Detection enabled.

D. You modify the Backdoor Detection rulebase to include the SSH Protocol ports in the top Ignore rule.

Answer: D

QUESTION NO: 5

What is the function of the IDP User Interface?

A. It stores Security Policies and Attack Objects
B. It supplements the Command-Line Interface on the Sensor, but is not required.
C. It provides an interface for the administrator to view Logs/Reports and define Security Policies.
D. It downloads logs from various Sensors and displays them to the administrator.

Answer: C

QUESTION NO: 6

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

A. ESP provides a summary of protocols and contexts on each host.
B. ESP indicates which hosts are talking with each other, and which protocols are being used.
C. ESP indicates when a specific machine has been attacked.
D. ESP indicates when new hosts or protocols are being used.

Answer: A,B,D

QUESTION NO: 7

Which two statements about disk management on the IDP Sensor are true?

A. If the IDP Management Server disk is full, the oldest packet captures are purged first, and the log messages are purged second.
B. If the IDP Sensor disk is full, the IDP Sensor will not store any additional logs or packet captures.
C. IDP Management Server can be configured to send disk space alerts.
D. If the IDP Sensor disk is full IDP Sensor starts oldest log entries first, and packet captures second.

Answer: A,C

QUESTION NO: 8

Which method of detection does IDP Sensor use to detect an invalid IP address entering an external interface?

A. Spoofing Detection
B. Backdoor Detection
C. DOS Detection
D. Layer2 Detection

Answer: A

QUESTION NO: 9

Which two attack detection methods are unique to Juniper NetScreenIDP? (Choose two.)

A. Packet Signatures
B. Statefull Signatures
C. Protocol Anomaly
D. Backdoor Detection

Answer: B,D

QUESTION NO: 10

Which three best describe denial-of-service attacks? (Choose three.)

A. disabling or corrupting networks, systems, or services with the intent to deny the service to intended users
B. transmission of TCP SYN requests from a spoofed IP address to exhaust the resources of a victim
C. the unauthorized discovery and mapping of systems, services, or vulnerabilities
D. transmission of ping packets of a certain size to crash a remote host

Answer: A,B,D

QUESTION NO: 11

Which layers of the OSI Model does IDP look into when inspecting a packet?

A. Layers 3-7
B. Layers 2-4 only