Exam Code: jn0-540

Exam Name: juniper networks certified internet

associate.idp(jncia-idp)

Vendor: Juniper Networks

Version: DEMO

Part: A

1: Which method of detection does IDP Sensor use to detect a known buffer overflow against a specific server?

A.Protocol Anomaly

B.Network Honeypot

C.Stateful Signatures

D.Backdoor Detection

Correct Answers: A

2: 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 downloads logs from various Sensors and displays them to the administrator.

D.It provides an interface for the administrator to view Logs/Reports and define Security Policies.

Correct Answers: D

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

A.DOS Detection

B.Layer2 Detection

C.Spoofing Detection

D.Backdoor Detection

Correct Answers: C

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

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

B.the unauthorized discovery and mapping of systems, services, or vulnerabilities

C.transmission of TCP SYN requests from a spoofed IP address to exhaust the resources of a victim

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

Correct Answers: A C D

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

A.Protocol Anomaly

B.Packet Signatures

C.Statefull Signatures

D.Backdoor Detection

Correct Answers: C D

6: What are two drawbacks of an IDS system blocking an IP address? (Choose two.)

A.works only on TCP traffic

B.might not block the attacker until the attack has already taken place

C.need to know the sequence number of the attacker's IP Header to successfully block the IP address

D.might lead to denial-of-service situation where attacker can intentionally block valid users from accessing a network

Correct Answers: B D

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

A.performs attack detection and prevention

B.collects and presents logs to the IDP User Interface

C.forwards logs and status messages to the IDP Management Server

D.store logs locally when the IDP Management Server is unreachable

Correct Answers: A C D

8: What best describes Reconnaissance attacks?

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

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

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

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

Correct Answers: C

9: What are the limitations of using TCP Reset to block connections in an IDS? (Choose three.)

A.only works on TCP traffic

B.does not reset the connection until the attack has already taken place

C.must know the correct packet size to successfully reset a connection

D.resets all connections from a certain source-IP, which could lead to denial-of-service

Correct Answers: A B D

10: You can remotely administer the IDP Sensor through _____. (Choose two.)

A.an SSH Console

B.a Telnet Console

C.the WebUI ACM over HTTP

D.the WebUI ACM over HTTPS

Correct Answers: A D

11: How much RAM is recommended for the IDP Management Server?

A.128 MB

B.256 MB

C.512 MB

D.1024 MB

Correct Answers: D

12: Which IDP Sensor is recommended to support onboard Management Server?

A.IDP-10

B.IDP-100

C.IDP-500

D.IDP-1000

Correct Answers: B

13: On which two operating systems can the IDP User Interface be installed? (Choose two.)

A.Linux

B.Solaris

C.Windows

D.any Java capable operating system

Correct Answers: A C

14: Which two steps are taken to change the management IP of an IDP Sensor? (Choose two.)

A.edit the existing IDP Sensor object from the UI and change the IP address

B.change the management interface IP of the IDP Sensor using the ACM

C.change the management interface IP of IDP Sensor using the ifconfig command

D.delete the Sensor object from the IDP Management Server and   add the IDP Sensor with the new IP address

Correct Answers: B D

15: Which two tasks can be performed from the IDP ACM? (Choose two.)

A.disable a Security Policy

B.disable Layer 2 Attack Detection

C.change the One-Time Password for IDP Management Server communication

D.enable or disable SSH Access, and restrict which networks can SSH to the IDP

Correct Answers: C D