IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **JN0-540**

Title : Juniper networks Certified internet associate.idp(jncia-idp)

Version : Demo

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
Answer: 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.
Answer: 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
Answer: 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
Answer: ACD

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
Answer: CD

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
Answer: BD

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
Answer: ACD

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
Answer: 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
Answer: ABD

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
Answer: AD

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

A. 128 MB

B. 256 MB

C. 512 MB

D. 1024 MB
Answer: D

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

A. IDP-10

B. IDP-100

C. IDP-500

D. IDP-1000
Answer: 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
Answer: AC

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
Answer: BD

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
Answer: CD

16. Which IDP Sensors support High-Availability? (Choose three.)

A. IDP-10

B. NetScreen IDP-100

C. NetScreen IDP-500

D. NetScreen IDP-1000
Answer: BCD

17. What does the Host Watch List monitor?

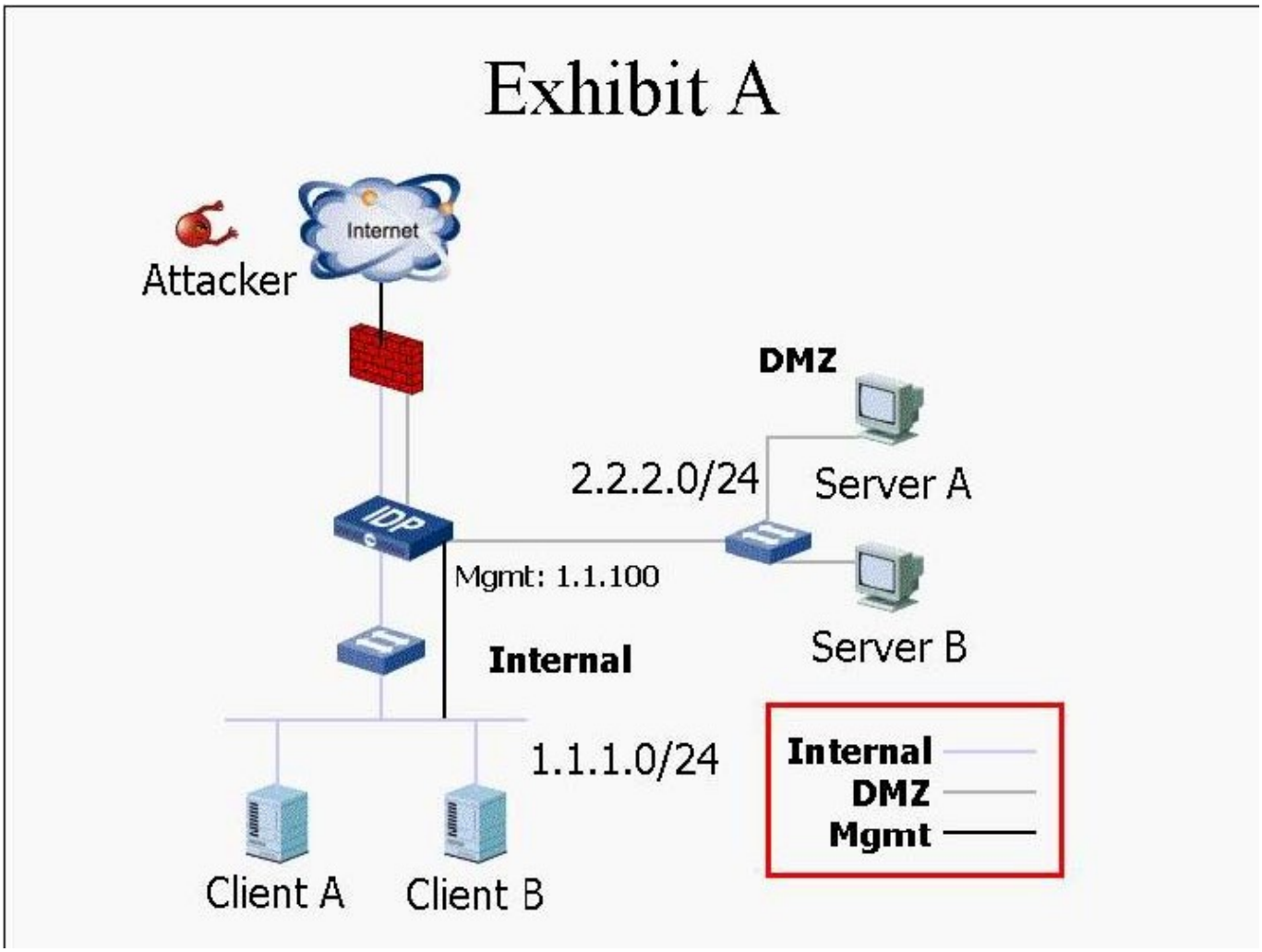
A. the status of specified hosts

B. all sessions directed to specified hosts

C. the number of attacks targeted to specified hosts

D. the number of attacks initiated from specified hosts
Answer: C

18. Click the Exhibit button. In the mode shown in the exhibit, IDP Sensor can protect Server A against attacks being initiated from which three hosts? (Choose three.)



A. Client A

B. Client B

C. Attacker

D. Server B
Answer: ABC

19. Which three actions must be taken prior to deploying an IDP Sensor in a network? (Choose three.)

A. A Security Policy must be configured for this IDP Sensor.

B. An IP address must be defined on all forwarding interfaces.

C. The IDP Sensor object must be configured in the IDP Management Server.

D. IDP Sensor must be configured with the ACM and assigned a Management IP address.
Answer: ACD

20. When a security policy is installed on a IDP Sensor, which statement is true? (Choose two.)

A. A Security policy must first be verified before it is installed.

B. A policy version is created when is successfully installed.

C. The policy.set file is deleted and a new file is created.

D. IDP Sensor stops processing traffic when policy is being installed.
Answer: AB

21. What is the function of the Log Packets notification action?

A. logs all packets the IDP Sensor sees

B. logs the packets containing the attack only

C. logs a specific number of packets before, after and during an attack

D. logs the packets used to give notification about a specific event (e.g. Syslog Traffic)
Answer: C

22. 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

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

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

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

23. You implement Traffic Anomaly detection and you find numerous alerts of portscans from your Security Auditing team that you want to ignore. What is the appropriate action to take?

A. create an Exempt rule for the Security Audit team in the Exempt to ignore Traffic Anomalies

B. create a rule on top of Traffic Anomaly rulebase to ignore traffic from "Security Audit Team"

C. create a rule on top of Main rulebase to ignore traffic with "from the Security Audit Team" and make this a Terminal rule

D. create a rule on top of Traffic Anomaly rulebase to ignore traffic with a "from the Security Audit Team" and make this a Terminal rule

Answer: B

24. What are two ways to verify that your rules in the Security Policies are not being shadowed? (Choose two.)

A. You can verify your security policy from the CLI of the Sensor.

B. You can verify your security policy from the IDP User Interface.

C. IDP Management Server can verify your Security policy automatically from the CLI of the Management Server.

D. You must manually verify your rules by hand to ensure they do not shadow each other.
Answer: AB

25. What should you do to build effective security policies?

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

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

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

D. create specific rules for critical servers first, which look for attacks that are relevant to those servers (such as HTTP attacks on Webservers); DO NOT make these rules Terminate Match
Answer: C

26. Which three actions can be taken on a rule when deployed in inline mode? (Choose three.)

A. drop stream

B. drop packet

C. drop connection

D. close server and client
Answer: BCD

27. What is the function of a Compound Attack Object?

A. combines multiple attacks in a single rulebase

B. looks for multiple occurrences of the same attack

C. allows you to take custom actions based on combinations of attacks

D. combines multiple attack signatures objects or anomalies objects into a single attack object
Answer: D 28. 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. reconfigure management interface IP

B. modify the rule action to drop or close

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

D. reconnect the IDP Sensors forwarding interfaces appropriately
Answer: BCD

29. You update your Attack Object database from the IDP User Interface. What must you do before the new signature attack objects become active on your IDP S ensor?

A. You restart the IDP Sensor.

B. You restart the IDP Service on the IDP Sensor (IDP restart).

C. No changes are required other than saving the policy changes.

D. You install the updated Security policy on that IDP Sensor from the IDP User Interface.
Answer: D

30. What does a Drop Packet action do?

A. drops all packets from the attacker's IP

B. drops any packet matching this src/dst/protocol

C. drops only the specific packet matching the attack

D. drops the specific session containing the attack pattern
Answer: C