

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam : **642-531**

Title : Cisco Secure Intrusion
Detection Systems Exam

Version : DEMO

1. When using IDS MC, which four actions can you configure a Cisco IDS Sensor to take when a signature is fired? (Choose four.)

- A. log
- B. alarm
- C. block host
- D. reset
- E. trigger
- F. block connection

Answer: ACDF

2. IDS MC version 2.0 communicates with a sensor using which two methods? Choose two.

- A. HTTP
- B. SSH
- C. RDEP
- D. Telnet
- E. FTP

Answer: BC

3. What are the two basic types of Cisco IDS signature parameters? (Choose two.)

- A. protected
- B. master
- C. sub-signature
- D. local
- E. required

Answer: BD

4. What is the function of the mls ip ids command when used for traffic capture?

- A. applies the IDS ACL to an interface
- B. assigns a port to receive capture traffic
- C. selects all IP traffic for IDS monitoring

- D. processes capture in hardware versus software
- E. used with keywords to define interesting traffic

Answer: A

5. Which two can a blocking Sensor use to manage a Cisco IOS router for shunning? (Choose two.)

- A. SSL
- B. SSH
- C. RDEP
- D. Telnet
- E. serial console

Answer: BD

6. Which command initiates the IDSM2 system configuration dialog?

- A. sysconfig-sensor
- B. setup
- C. configure terminal
- D. session
- E. initialize

Answer: B

7. When creating custom signatures with IDS MC, which two fields are you required to populate? (Choose two.)

- A. engine description
- B. engine name
- C. SubSigID
- D. signature name
- E. signature string

Answer: BD

8. Which Cisco IOS command is used to enable the forwarding of packets from the router to the NM-CIDS?

- A. ip cef
- B. ip inspect
- C. service-module
- D. ip cef linecard ipc memory

Answer: A

9. What does an attacker require to perform a Denial of Service attack?

- A. a means of network access
- B. prior access to the target
- C. previously installed root kit
- D. username and password

Answer: A

10. What is the maximum number of command and control interfaces on an IDS Sensor appliance?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: A