Testpassport Q&A

La meilleure qualité le meilleur service

http://www.testpassport.fr

Service de mise à jour gratuit pendant un an

Exam : **600-199**

Title : Securing Cisco Networks with Threat Detection and Analysis

Version : Demo

1.Which network management protocol relies on multiple connections between a managed device and the management station where such connections can be independently initiated by either side?
A. SSH
B. SNMP
C. Telnet
D. NetFlow
Answer: B

2.When an IDS generates an alert for a correctly detected network attack, what is this event called?
A. false positive
B. true negative
C. true positive
D. false negative
Answer: C

3.When is it recommended to establish a traffic profile baseline for your network?
A. outside of normal production hours
B. during a DDoS attack
C. during normal production hours
D. during monthly file server backup
Answer: C

4.Which two activities would you typically be expected to perform as a Network Security Analyst? (Choose two.)
A. Verify user login credentials.
B. Troubleshoot firewall performance.
C. Monitor database applications.
D. Create security policies on routers.
Answer: B,D

5.Which protocol is typically considered critical for LAN operation?
A. BGP
B. ARP
C. SMTP
D. GRE
Answer: B

6.Which two measures would you recommend to reduce the likelihood of a successfully executed network attack from the Internet? (Choose two.)
A. Completely disconnect the network from the Internet.
B. Deploy a stateful edge firewall.
C. Buy an insurance policy A. against attack-related business losses.
D. Implement a password management policy for remote users.
Answer: B,D

7.Which attack exploits incorrect boundary checking in network software?
A. Slowloris
B. buffer overflow
C. man-in-the-middle
D. Smurf
Answer: B

8.Where should you report suspected security vulnerability in Cisco router software?
A. Cisco TAC
B. Cisco IOS Engineering
C. Cisco PSIRT
D. Cisco SIO
Answer: C

9.When investigating potential network security issues, which two pieces of useful information would be found in a syslog message? (Choose two.)
A. product serial number
B. MAC address
C. IP address
D. product model number
E. broadcast address
Answer: B,C

10.Which command would provide you with interface status information on a Cisco IOS router?
A. show status interface
B. show running-config
C. show ip interface brief
D. show interface snmp
Answer: C