EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **GPPA**

Title : GIAC Certified Perimeter Protection Analyst

Version : DEMO

1.Which of the following tools is an open source protocol analyzer that can capture traffic in real time?
A. Snort
B. NetWitness
C. Wireshark
D. Netresident
Answer: C

2.You are implementing a host based intrusion detection system on your web server. You feel that the best way to monitor the web server is to find your baseline of activity (connections, traffic, etc.) and to monitor for conditions above that baseline.
This type of IDS is called _____.
A. Signature Based
B. Reactive IDS
C. Anomaly Based
D. Passive IDS
Answer: C

3.Which of the following are open-source vulnerability scanners? (Choose three.)
A. Nessus
B. Hackbot
C. Nikto
D. NetRecon
Answer: A,B,C

4.Suppose you are working as a Security Administrator at ABC Inc. The company has a switched network. You have configured tcpdump in the network which can only see traffic addressed to itself and broadcast traffic.
What will you do when you are required to see all traffic of the network?
A. Connect the sniffer device to a Switched Port Analyzer (SPAN) port.
B. Connect the sniffer device to a Remote Switched Port Analyzer (RSPAN) port.
C. Configure Network Access Control (NAC).
D. Configure VLAN Access Control List (VACL).
Answer: A

5.Which of the following techniques is used to identify attacks originating from a botnet?
A. Recipient filtering
B. BPF-based filter
C. IFilter
D. Passive OS fingerprinting
Answer: D