DumpsHero

GIAC

GPPA Exam

GIAC Certified Perimeter Protection Analyst Exam

Questions & Answers
(Demo Version – Limited Content)

Thank you for Downloading GPPA exam PDF Demo

Version: 6.0

Question: 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

Question: 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

Question: 3

Which of the following are open-source vulnerability scanners? (Choose three.)

A. Nessus
B. Hackbot
C. Nikto
D. NetRecon

Answer: A,B,C

Question: 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

Question: 5

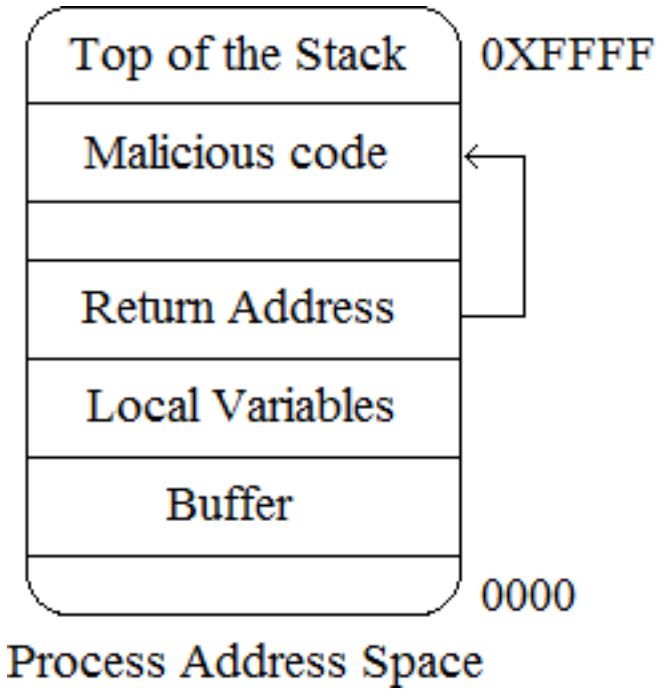
Which of the following techniques is used to identify attacks originating from a botnet?

A. Recipient filtering
B. BPF-based filter
C. IFilter
D. Passive OS fingerprinting

Answer: D

Question: 6

An attacker changes the address of a sub-routine in such a manner that it begins to point to the address of the malicious code. As a result, when the function has been exited, the application can be forced to shift to the malicious code. The image given below explains this phenomenon:



Which of the following tools can be used as a countermeasure to such an attack?

A. SmashGuard
B. Obiwan
C. Kismet
D. Absinthe

Answer: A

Question: 7

Which of the following protocols is used by TFTP as a file transfer protocol?

A. SMTP
B. UDP
C. TCP
D. SNMP

Answer: B

Question: 8

Which of the following steps are generally followed in computer forensic examinations?
Each correct answer represents a complete solution. (Choose three.)

A. Analyze
B. Acquire
C. Authenticate
D. Encrypt

Answer: A,B,C

Question: 9

Which of the following monitors program activities and modifies malicious activities on a system?

A. HIDS
B. Back door
C. NIDS
D. RADIUS

Answer: A

Question: 10

Which of the following wireless security features provides the best wireless security mechanism?

A. WPA with Pre Shared Key
B. WPA
C. WPA with 802.1X authentication
D. WEP

Answer: C

Thank You for trying GPPA PDF Demo