GPPA Q&As

GIAC Certified Perimeter Protection Analyst

Pass GIAC GPPA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gppa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

- It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
- It is commonly used for the following purposes:

a) War driving b) Detecting unauthorized access points c) Detecting causes of interference on a WLAN d) WEP ICV error tracking e) Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as _____.

A. THC-Scan

B. Kismet

C. Absinthe

D. NetStumbler

Correct Answer: D

QUESTION 2

Which of the following well-known ports is used by BOOTP?

A. UDP 67

B. TCP 21

C. UDP 69

D. TCP 161

Correct Answer: A

QUESTION 3

You work as a Firewall Analyst in the ABC Inc. The company has a Linux-based environment. You have

installed and configured netfilter/iptables on all computer systems.

What are the main features of netfilter/iptables?

Each correct answer represents a complete solution. (Choose all that apply.)

A. It provides network address and port address translations with both IPv4 and IPv6 addressing schemes.

B. It offers stateless and stateful packet filtering with both IPv4 and IPv6 addressing schemes.

C. It includes a number of layers of API\\'s for third party extensions.

D. It includes many plug-ins or modules in \\'patch-o-matic\\' repository.

Correct Answer: BCD

QUESTION 4

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

A. Apache

B. Snort

C. SSH

D. SUDO

Correct Answer: D

QUESTION 5

Jain works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.abc.com.

He has successfully completed the following steps of the preattack phase:

>> Information gathering >> Determining network range >> Identifying active machines >> Finding open ports and applications >> OS fingerprinting >> Fingerprinting services

Now Jain wants to perform network mapping of the ABC network.

Which of the following tools can he use to accomplish his task?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Traceroute

B. Cheops

C. NeoTrace

D. Ettercap

Correct Answer: ABC

QUESTION 6

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Fragmentation overwrite attack

B. Fragmentation overlap attack

C. Evasion attack

D. Insertion attack

Correct Answer: D

QUESTION 7

Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails. Linux uses Syslog to maintain logs of what has occurred on the system.

Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

A. /log/var/mailog

B. /log/var/logd

C. /var/log/logmail

D. /var/log/mailog

Correct Answer: D

QUESTION 8

Which of the following types of firewall ensures that the packets are part of the established session?

A. Circuit-level firewall

B. Switch-level firewall

C. Application-level firewall

D. Stateful inspection firewall

Correct Answer: D

QUESTION 9

You work as a Network Administrator for NetTech Inc. You want to prevent your network from Ping flood attacks.

Which of the following protocols will you block to accomplish this task?

A. IP

B. FTP

C. PPP

D. ICMP

Correct Answer: D

QUESTION 10

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

Correct Answer: ABC

QUESTION 11

Which of the following IPv4 to IPv6 transition methods uses encapsulation of IPv6 packets to traverse IPv4 networks?

A. Translation

B. Stack

C. Tunneling

D. Dual-stack

Correct Answer: C

QUESTION 12

In which of the following attacks does an attacker change the MAC address on the sniffer to one that is the same in another system on the local subnet?

A. MAC duplicating

B. IP spoofing

C. ARP spoofing

D. MAC flooding

Correct Answer: A

QUESTION 13

Which of the following files is a Cisco IOS configuration file that resides in RAM?

A. temp-config

B. running-config

C. startup-config

D. ram-config

Correct Answer: B

QUESTION 14

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be most helpful against Denial of Service (DOS) attacks?

A. Honey pot

B. Network surveys

C. Stateful Packet Inspection (SPI) firewall

D. Packet filtering firewall

Correct Answer: C

QUESTION 15

Which of the following methods will allow data to be sent on the Internet in a secure format?

A. Browsing

B. Virtual Private Networks

C. Serial Line Interface Protocol

D. Point-to-Point Protocol

Correct Answer: B