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.pass2lead.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

Which of the following types of IP actions are supported by an IDP rulebase? (Choose three.)

A. Initiate rules of the rulebase

B. Notify

C. Drop/block session

D. Close connection

Correct Answer: BCD

QUESTION 2

Which of the following attacks sends false ICMP packets in an attempt to cripple a system using random fake Internet source addresses?

A. Twinge attack

B. SYN attack

C. Replay attack

D. Land attack

Correct Answer: A

QUESTION 3

Passive OS fingerprinting (POSFP) is configured in an organization\\'s network in order to improve the alert

output by reporting some information.

Which of the following information does it include?

Each correct answer represents a part of the solution. (Choose all that apply.)

A. Network security device

B. Source of the OS identification

C. Victim OS

D. Relevancy to the victim in the alert

Correct Answer: BCD

QUESTION 4

Which of the following tools allows an attacker to intentionally craft the packets to gain unauthorized access?

Each correct answer represents a complete solution. (Choose two.)

A. Tcpdump

B. Ettercap

C. Fragroute

D. Mendax

Correct Answer: CD

QUESTION 5

Which of the following is the default port for POP3?

A. 80

B. 25

C. 21

D. 110

Correct Answer: D

QUESTION 6

A packet filtering firewall inspects each packet passing through the network and accepts or rejects it based

on user-defined rules.

Based on which of the following information are these rules set to filter the packets?

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

A. Source and destination Layer 3 address

B. Actual data in the packet

C. Layer 4 protocol information

D. Interface of sent or received traffic

Correct Answer: ACD

QUESTION 7

What is the function of baseline audit?

A. Packet filtering

B. Packet sniffing

C. ARP spoofing

D. Data capturing

Correct Answer: D

QUESTION 8

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes.

On the basis of above information, which of the following types of attack is Adam attempting to perform?

A. Ping of death attack

B. SYN Flood attack

C. Fraggle attack

D. Land attack

Correct Answer: A

QUESTION 9

Which of the following vulnerability scanners detects vulnerabilities by actually performing attacks?

A. Port scanner

B. Computer worm

C. Network enumerator

D. Web application security scanner

Correct Answer: D

QUESTION 10

Which of the following are packet filtering tools for the Linux operating system?

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

A. IPTables

B. IPFilter

C. Zone Alarm

D. BlackICE

Correct Answer: AB

QUESTION 11

Which of the following is the function of the editcap utility of Wireshark?

A. To analyze data packets.

B. To remove duplicate packets.

C. To transfer data packets.

D. To check data packets.

Correct Answer: B

QUESTION 12

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 13

Which of the following TShark options is used to set capture buffer size in MB?

A. -F

B. -B

C. -G

D. -C

Correct Answer: B

QUESTION 14

Which of the following commands is recommended by Cisco for latest switches and routers to erase the contents of NVRAM?

A. reload

B. erase startup-config

C. erase nvram:

D. write erase

Correct Answer: C

QUESTION 15

Sam works as a Security Manager for ABC Inc. The company has a Windows-based network. Sam wants to prevent specific traffic from IDP processing in order to reduce false positives.

Which of the following rulebases will he use to accomplish the task?

A. Network Honeypot rulebase

B. Backdoor rulebase

C. SYN Protector rulebase

D. Exempt rulebase

Correct Answer: D