



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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network. After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed.

What type of response is the IDS giving?

- A. False Negative
- B. False Positive
- C. True Positive
- D. True Negative

Correct Answer: A

QUESTION 2

Paul works as a Technical Representative in a CSIRT for ABC Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Paul wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis.

Which of the following is the correct order for searching data on a Windows based system?

- A. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system.
- B. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces.
- C. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces.
- D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps.

Correct Answer: C

QUESTION 3

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled.

Which of the following attacks is John performing?

- A. Replay attack
- B. ARP spoofing
- C. DoS attack



D. Rainbow attack

Correct Answer: C

QUESTION 4

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 5

Which of the following firewalls operates at three layers - Layer3, Layer4, and Layer5?

A. Dynamic packet-filtering firewall

B. Application layer firewall

C. Proxy firewall

D. Circuit-level firewall

Correct Answer: A

[GPPA Practice Test](#)

[GPPA Study Guide](#)

[GPPA Exam Questions](#)