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.pass4itsure.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

You run the tcpdump command line utility and get a report produced by tcpdump.

What information does this report include?

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

A. Packets captured

B. Packets dropped by kernel

C. Packets discarded

D. Packets received by filter

Correct Answer: ABD

QUESTION 2

Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively.

Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Mac OS

B. Windows XP

C. MINIX 3

D. Linux

Correct Answer: A

QUESTION 3

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 4

Which of the following security protocols uses a single, manually configured, static key for data encryption that is shared by the client and the WAP?

A. IPSec

B. WPA

C. WEP

D. L2TP

Correct Answer: C

QUESTION 5

You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -d

B. tcpdump -B

C. tcpdump -dd

D. tcpdump -w

Correct Answer: D