GCIA Q&As

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

https://www.pass4itsure.com/gcia.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 proxy servers is also referred to as transparent proxies or forced proxies?

A. Tunneling proxy server

B. Reverse proxy server

C. Anonymous proxy server

D. Intercepting proxy server

Correct Answer: D

QUESTION 2

Adam works on a Linux system. He is using Sendmail as the primary application to transmit e-mails. 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. /var/log/logmail

C. /var/log/mailog

D. /log/var/logd

Correct Answer: C

QUESTION 3

Which of the following intrusion detection systems (IDS) produces the false alarm because of the abnormal behavior of users and network?

A. Application protocol-based intrusion detection system (APIDS)

B. Protocol-based intrusion detection system (PIDS)

C. Network intrusion detection system (NIDS)

D. Host-based intrusion detection system (HIDS)

Correct Answer: D

QUESTION 4

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. DOS boot disk

B. EnCase with a hardware write blocker

C. Linux Live CD

D. Secure Authentication for EnCase (SAFE)

Correct Answer: D

QUESTION 5

Which of the following programs is used to add words to spam e-mails so that the e-mail is not considered spam and therefore is delivered as if it were a normal message?

A. Adler-32

B. Hash filtrer

C. Hash buster

D. Checksum

Correct Answer: C