GCIH$^{Q\&As}$

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.pass4itsure.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Why should you inform incident handling team members in advance of their joining the team that they may be required to testify in a court of law?

A. Because most cases eventually end up in court

B. To make sure they understand that it is a requirement that could follow them for several years

C. To verify their abilities to hold up under cross-examination

D. Because US Code Section 1030 requires that all incident handlers receive such notification

Correct Answer: B

Inform them that they may be required to testify. This may scare them, but that is OK, sometimes it takes a long time to bring an incident to closure.

QUESTION 2

Maria works as the Chief Security Officer for PassGuide Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides \\'security through obscurity\\'. What technique is Maria using?

A. Steganography

B. Public-key cryptography

C. RSA algorithm

D. Encryption

Correct Answer: A

QUESTION 3

Which of the following is a technique that can be used to reduce the amount of data to examine during an investigation?

A. Ignore files with known good hashes

B. Ignore malicious file hashes

C. Create file hashes for all directories on the system

D. Request management recommendation for file hashes of interest

Correct Answer: A

QUESTION 4

Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

A. Demon dialing

B. Warkitting

C. War driving

D. Wardialing

Correct Answer: D

QUESTION 5

Detecting Virtual Machine Environments (VMEs) is the purpose of which of the following pieces of software?

A. Red Pill

B. White Pill

C. Green Pill

D. Black Pill

Correct Answer: A

To detect a virtual machine, an attacker has numerous options. There are several categories of local VME detection used today. One method includes looking for VME artifacts in memory, which is a technique used by Joanna Rutkowska\\'s Red Pill to look for a shifted Interrupt Descriptor Table, a critical data structure in the operating system.