

GCIH Reliable Test Simulator & GCIH Valid Exam Tutorial



P.S. Free & New GCIH dumps are available on Google Drive shared by PassSureExam: https://drive.google.com/open?id=1VRsHGKyk_yNrjrGHj9Ejh535KTk8PZh

PassSureExam offers authentic and up-to-date GCIH study material that every candidate can rely on for good preparation. Our top priority is to help you pass the GIAC Certified Incident Handler (GCIH) exam on the first try. The cost of registering for a certification GIAC Certified Incident Handler (GCIH) exam is quite expensive, ranging between \$100 and \$1000. After paying such an amount, the candidate is sure to be on a tight budget. PassSureExam provides GIAC Certified Incident Handler (GCIH) preparation material at very low prices compared to other platforms. We also assure you that the amount will not be wasted and you will not have to pay for the GIAC Certified Incident Handler (GCIH) certification test for a second time.

GIAC GCIH exam is intended for security professionals who are responsible for detecting, responding to, and preventing security incidents in their organizations. It covers a wide range of topics such as incident handling processes, network protocols, malware analysis, and forensic analysis. GCIH exam is designed to test the candidate's ability to identify, analyze, and respond to security incidents in a timely and effective manner.

To prepare for the GCIH Exam, candidates should have a solid understanding of computer networks, operating systems, and security principles. They should also have experience with incident response, either through work experience or through training courses. GIAC offers a variety of training options for candidates, including self-paced study guides, online courses, and in-person training sessions. Candidates should plan to study for several months before taking the exam.

>> GCIH Reliable Test Simulator <<

GIAC GCIH Valid Exam Tutorial & GCIH Dumps Questions

If you are worried about your exam, and want to pass the exam just one time, we can do that for you. GCIH exam materials are compiled by experienced experts, and they are quite familiar with the exam center, and therefore the quality can be guaranteed. In addition, you can receive the downloading link and password within ten minutes, so that you can begin your learning immediately. We provide you with free update for one year and the update version for GCIH Exam Torrent will be sent to your email automatically.

The GCIH exam is a challenging certification program that requires candidates to have a strong background in information security and incident handling. GCIH exam consists of 150 multiple-choice questions that test the candidate's knowledge and skills in various areas of incident handling. Candidates are required to achieve a passing score of 70% or higher to earn the certification. The GCIH Certification program is a valuable investment for professionals who want to advance their careers in the information security field and demonstrate their skills and expertise in incident handling.

GIAC Certified Incident Handler Sample Questions (Q77-Q82):

NEW QUESTION # 77

Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

- A. rkhunter
- **B. chkrootkit**
- C. OSSEC
- D. Blue Pill

Answer: B

Explanation:

Section: Volume B

NEW QUESTION # 78

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

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

- A. Perceptual masking
- B. Technical steganography
- **C. Text Semagrams**
- **D. Linguistic steganography**

Answer: C,D

NEW QUESTION # 79

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.

□ Which of the following attacks is John using?

- A. Eavesdropping
- B. War driving
- C. Sniffing
- **D. Banner grabbing**

Answer: D

NEW QUESTION # 80

Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

- A. Dictionary attack
- B. Hybrid attack
- **C. Rainbow attack**
- D. Brute Force attack

Answer: C

Explanation:

Section: Volume A

NEW QUESTION # 81

Which of the following tools is used to download the Web pages of a Website on the local system?

- A. jplag
- B. Ettercap
- C. wget
- D. Nessus

Answer: C

Explanation:

Section: Volume A

NEW QUESTION # 82

• • • • •

GCIH Valid Exam Tutorial: <https://www.passsureexam.com/GCIH-pass4sure-exam-dumps.html>

BONUS!!! Download part of PassSureExam GCIH dumps for free: https://drive.google.com/open?id=1VRsHGKyk_yNjrjGHj9Ejh535KTk8PZhm