

# Approved GCIH Certified Information Systems Security Professional Exam Questions



## ISC CISSP Exam Answers (Certified Information Systems Security Professional Exam Answers)

Psst, You can use CTRL+F to search for question on site. Good luck!

### Question 1

Physical assets defined in an organization's business impact analysis (BIA) could include which of the following?

- A. Personal belongings of organizational staff members
- B. Disaster recovery (DR) line-item revenues
- C. Cloud-based applications
- D. Supplies kept off-site a remote facility

### Question 2

When assessing the audit capability of an application, which of the following activities is MOST important?

- A. Identify procedures to investigate suspicious activity.
- B. Determine if audit records contain sufficient information.
- C. Verify if sufficient storage is allocated for audit records.
- D. Review security plan for actions to be taken in the event of audit failure.

### Question 3

An organization would like to implement an authorization mechanism that would simplify the assignment of various system access permissions for many users with similar job responsibilities. Which type of authorization mechanism would be the BEST choice for the organization to implement?

- A. Role-based access control (RBAC)
- B. Discretionary access control (DAC)
- C. Content-dependent Access Control
- D. Rule-based Access Control

### Question 4

DOWNLOAD the newest ActualTestsIT GCIH PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1FV-4JF7og-EIVV9N\\_5zTp4fOysc6HA1v](https://drive.google.com/open?id=1FV-4JF7og-EIVV9N_5zTp4fOysc6HA1v)

The second format is a web-based format that can be accessed from browsers like Firefox, Microsoft Edge, Chrome, and Safari. It means you don't need to download or install any software or plugins to take the GIAC Certified Incident Handler practice test. The web-based format of the GIAC GCIH Certification Exams practice test supports all operating systems. The third and last format is desktop software format which can be accessed after installing the software on your GIAC Certified Incident Handler (GCIH) Windows Pc or Laptop. These formats are built especially for the students so they don't stop preparing for the GIAC Certified Incident Handler (GCIH) certification.

The GCIH certification program is designed to meet the needs of professionals who are responsible for managing and responding to security incidents within their organizations. This includes incident response teams, security engineers, security analysts, and security consultants. GIAC Certified Incident Handler certification helps candidates develop their skills in managing and responding to incidents, which is a critical aspect of cybersecurity.

GIAC GCIH (GIAC Certified Incident Handler) certification exam is designed to assess the knowledge and skills of individuals who are responsible for detecting, responding to, and resolving incidents within an organization. GCIH Exam is intended for professionals in the field of incident handling, including security analysts, incident responders, and security operations center (SOC) personnel.

To prepare for the GIAC GCIH certification exam, candidates can enroll in a training course or study on their own. GIAC offers an official course that covers all the topics on the exam and provides hands-on experience with incident handling tools and techniques.

Candidates can also purchase study materials, such as books, practice exams, and online courses, to supplement their learning.

>> Sample GCIH Test Online <<

## GIAC GCIH Reliable Practice Questions, GCIH Pdf Demo Download

One of the most significant parts of your GIAC GCIH certification exam preparation is consistent practice. ActualTestsIT has made sure that you get sufficient GCIH exam practice by adding GIAC GCIH desktop practice exam software to your study course. This GIAC GCIH desktop-based practice exam software is compatible with all windows-based devices.

### GIAC Certified Incident Handler Sample Questions (Q47-Q52):

#### NEW QUESTION # 47

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service, or unauthorized changes to system hardware, software, or data?

- A. Occupant Emergency Plan
- B. Cyber Incident Response Plan
- C. Crisis Communication Plan
- D. Disaster Recovery Plan

**Answer: B**

Explanation:

Section: Volume C

#### NEW QUESTION # 48

CORRECT TEXT

Fill in the blank with the appropriate name of the rootkit.

A \_\_\_\_\_ rootkit uses device or platform firmware to create a persistent malware image.

**Answer:**

Explanation:

firmware

#### NEW QUESTION # 49

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

**Answer: A,C**

#### NEW QUESTION # 50

John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.

Original cookie values:

ItemID1=2  
ItemPrice1=900  
ItemID2=1  
ItemPrice2=200  
Modified cookie values:  
ItemID1=2  
ItemPrice1=1  
ItemID2=1  
ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.  
Which of the following hacking techniques is John performing?

- A. Man-in-the-middle attack
- B. Cross site scripting
- C. Cookie poisoning
- D. Computer-based social engineering

**Answer: C**

### NEW QUESTION # 51

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.

Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

- A. `nmap -O -p`
- B. `nmap -sU -p`
- C. `nmap -sS`
- D. `nmap -sT`

**Answer: A**

### NEW QUESTION # 52

.....

The latest GCIH exam torrent covers all the qualification exam simulation questions in recent years, including the corresponding matching materials at the same time. Do not have enough valid GCIH practice materials, can bring inconvenience to the user, such as the delay progress, learning efficiency and to reduce the learning outcome was not significant, these are not conducive to the user persistent finish learning goals. Therefore, to solve these problems, the GCIH test material is specially designed for you to pass the GCIH exam.

**GCIH Reliable Practice Questions:** <https://www.actualtestsit.com/GIAC/GCIH-exam-prep-dumps.html>

- Desktop GIAC GCIH Practice Test Software  Search for > GCIH  on « [www.testkingpass.com](http://www.testkingpass.com) » immediately to obtain a free download  GCIH Valid Test Answers
- GCIH Valid Exam Prep  GCIH Reliable Test Preparation  GCIH Valid Braindumps Free  Easily obtain 【 GCIH 】 for free download through ➡ [www.pdfvce.com](http://www.pdfvce.com)   Test GCIH Simulator Free
- Get free updates with GIAC GCIH PDF Dumps  Search for “GCIH” and download it for free immediately on 「 [www.prep4sures.top](http://www.prep4sures.top) 」  Reliable GCIH Test Pattern
- Free PDF 2026 GCIH - Sample GIAC Certified Incident Handler Test Online  Search for  GCIH  and download exam materials for free through { [www.pdfvce.com](http://www.pdfvce.com) }  Test GCIH Quiz
- Test GCIH Simulator Free  GCIH Pass4sure  Test GCIH Questions Answers  Enter “[www.prep4away.com](http://www.prep4away.com)” and search for ( GCIH ) to download for free  GCIH Reliable Test Bootcamp
- Free PDF 2026 GCIH - Sample GIAC Certified Incident Handler Test Online  Simply search for  GCIH  for free download on “[www.pdfvce.com](http://www.pdfvce.com)”  GCIH Exam Tutorial
- Desktop GIAC GCIH Practice Test Software  Open ⇒ [www.practicevce.com](http://www.practicevce.com) ⇐ enter > GCIH < and obtain a free download  GCIH Pass4sure
- GCIH Valid Braindumps Free  GCIH Reliable Test Blueprint  GCIH Valid Exam Prep  Download  GCIH  for free by simply searching on ➡ [www.pdfvce.com](http://www.pdfvce.com)   GCIH Actual Tests

- Test GCIH Quiz | GCIH Reliable Test Preparation | GCIH Valid Exam Prep | Open > [www.verifiddumps.com](http://www.verifiddumps.com) < and search for ➡ GCIH | to download exam materials for free | GCIH Reliable Test Bootcamp
- Free PDF 2026 GCIH - Sample GIAC Certified Incident Handler Test Online | The page for free download of | GCIH | on | [www.pdfvce.com](http://www.pdfvce.com) | will open immediately | GCIH Actual Tests
- GCIH Valid Test Answers | GCIH Reliable Test Bootcamp | GCIH Exam Tutorial | Copy URL { [www.troytecdumps.com](http://www.troytecdumps.com) } open and search for | GCIH | to download for free | GCIH Exam Tutorial
- [paidforarticles.in](http://paidforarticles.in), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [lms.ait.edu.za](http://lms.ait.edu.za), [foodsgyan.com](http://foodsgyan.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), Disposable vapes

2026 Latest Actual Tests IT GCIH PDF Dumps and GCIH Exam Engine Free Share: [https://drive.google.com/open?id=1FV-4JF7og-EIVV9N\\_5zTp4fOysc6HAlv](https://drive.google.com/open?id=1FV-4JF7og-EIVV9N_5zTp4fOysc6HAlv)