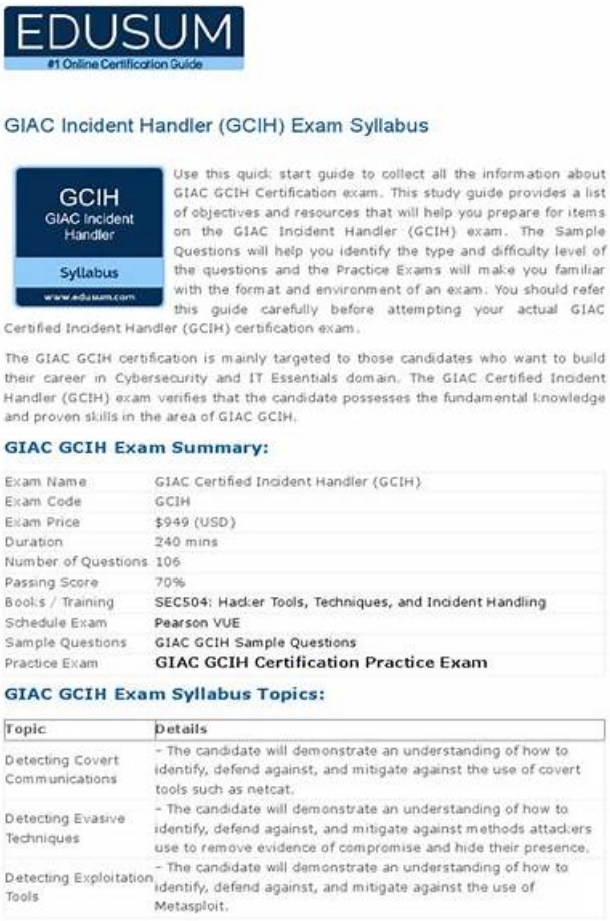
# GCIH Exam Guide - GCIH Study Tools & GCIH Exam Torrent


EDUSUM

#1 Online Certification Guide

GIAC Incident Handler (GCIH) Exam Syllabus

GCIH
GIAC Incident Handler
Syllabus
www.edusum.com

Use this quick start guide to collect all the information about GIAC GCIH Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the GIAC Incident Handler (GCIH) exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual GIAC Certified Incident Handler (GCIH) certification exam.

The GIAC GCIH certification is mainly targeted to those candidates who want to build their career in Cybersecurity and IT Essentials domain. The GIAC Certified Incident Handler (GCIH) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of GIAC GCIH.

GIAC GCIH Exam Summary:

| | |
|---|---|
| Exam Name | GIAC Certified Incident Handler (GCIH) |
| Exam Code | GCIH |
| Exam Price | $949 (USD) |
| Duration | 240 mins |
| Number of Questions | 106 |
| Passing Score | 70% |
| Books / Training | SEC504: Hacker Tools, Techniques, and Incident Handling |
| Schedule Exam | Pearson VUE |
| Sample Questions | GIAC GCIH Sample Questions |
| Practice Exam | GIAC GCIH Certification Practice Exam |

GIAC GCIH Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Detecting Covert Communications | - The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of covert tools such as netcat. |
| Detecting Evasive Techniques | - The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against methods attackers use to remove evidence of compromise and hide their presence. |
| Detecting Exploitation Tools | - The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of Metasploit. |

BTW, DOWNLOAD part of Braindumpsqa GCIH dumps from Cloud Storage: https://drive.google.com/open?id=1c6XLbLbUveGfyEz2_zmRYffVnH7vFrDw

If you have been very panic sitting in the examination room, our GCIH actual exam allows you to pass the exam more calmly and calmly. After you use our products, our GCIH study materials will provide you with a real test environment before the GCIH Exam. After the simulation, you will have a clearer understanding of the exam environment, examination process, and exam outline. And our GCIH learning guide will be your best choice.

GIAC GCIH exam covers a wide range of topics related to incident handling and response, including incident response techniques, malware analysis, network forensics, and cyber threat intelligence. GCIH exam is designed to test candidates' knowledge and skills in these areas and to ensure that they have the necessary expertise to handle security incidents effectively. Candidates who pass the GCIH Exam are considered to have a deep understanding of incident handling and response and are well-prepared to respond to security incidents in real-world situations.

**>> GCIH Valid Practice Materials <<**

## Reliable GCIH Mock Test | GCIH Valid Exam Topics

Once you get the GCIH certificate, you can quickly quit your current job and then change a desirable job. The GCIH certificate can prove that you are a competent person. So it is easy for you to pass the interview and get the job. The assistance of our GCIH practice quiz will change your life a lot. As we can claim that if you study with our GCIH exam braindumps for 20 to 30 hours, you

can pass the exam and get the certification with ease.

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.

GIAC GCIH (GIAC Certified Incident Handler) exam is a certification program designed to validate the skills and knowledge of professionals in the field of incident handling and response. GCIH Exam is developed and administered by the Global Information Assurance Certification (GIAC) organization, which is a leading provider of information security certifications. The GCIH certification is highly respected in the information security industry and is recognized as a benchmark for incident handlers.

## GIAC Certified Incident Handler Sample Questions (Q269-Q274):

**NEW QUESTION # 269**
Which of the following functions in c/c++ can be the cause of buffer overflow?
Each correct answer represents a complete solution. Choose two.

- A. strlength()
- B. printf()
- C. strcat()
- D. strcpy()

**Answer: C,D**

**NEW QUESTION # 270**
Which of the following statements are true about session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

- A. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
- B. It is used to slow the working of victim's network resources.
- C. TCP session hijacking is when a hacker takes over a TCP session between two machines.
- D. Use of a long random number or string as the session key reduces session hijacking.

**Answer: A,C,D**

**NEW QUESTION # 271**
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. OSSEC
- B. Blue Pill
- C. rkhunter
- D. chkrootkit

**Answer: D**

**NEW QUESTION # 272**
Which of the following viruses/worms uses the buffer overflow attack?

- A. Nimda virus
- B. Code red worm
- C. Klez worm
- D. Chernobyl (CIH) virus

**Answer: B**

**NEW QUESTION # 273**
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network.
The company uses Check Point SmartDefense to provide security to the network of the company. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.
Which of the following attacks will be blocked by defining this limitation?
Each correct answer represents a complete solution. Choose all that apply.

- A. Code red worm
- B. User-defined worm
- C. Land attack
- D. Backdoor attack

**Answer: A,B**

**NEW QUESTION # 274**
.....