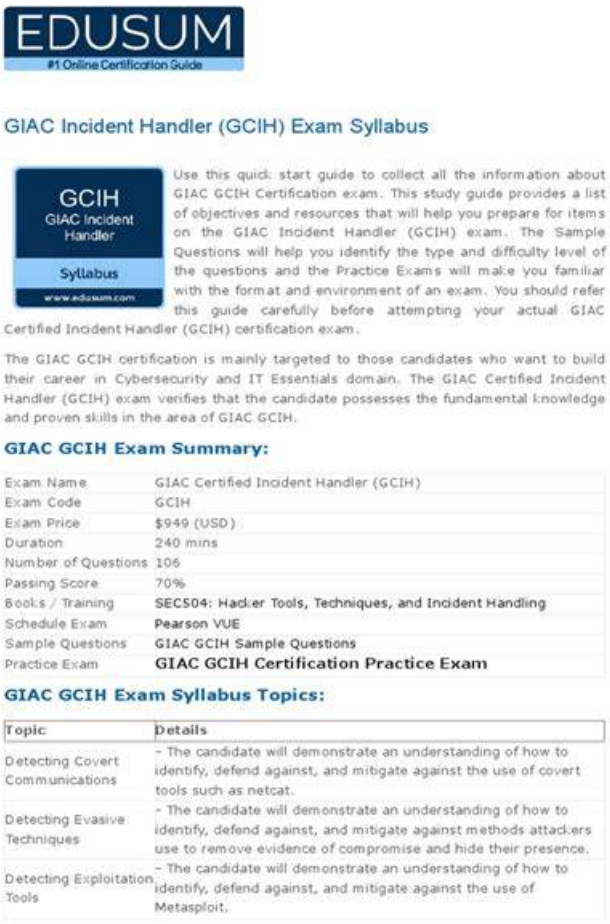
GCIH Valid Exam Answers - Latest GCIH Test Format



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 Actual4Dumps GCIH dumps from Cloud Storage: https://drive.google.com/open?id=1zYXwpge5huVUrToSZvXu8s2hgogWlriM

We don't just want to make profitable deals, but also to help our users pass the exams with the least amount of time to get GCIH certificate. Choosing our GCIH exam practice, you only need to spend 20-30 hours to prepare for the exam. Maybe you will ask whether such a short time can finish all the content, we want to tell you that you can rest assured ,because our GCIH Learning Materials are closely related to the exam outline and the questions of our GCIH guide questions are related to the latest and basic knowledge. You will pass the GCIH exam only with our GCIH exam questions.

The GCIH certification exam is intended for individuals who are responsible for incident handling and response, including network administrators, security analysts, incident responders, and other professionals who are involved in the detection and mitigation of security incidents. GCIH Exam covers a wide range of topics, including incident handling and response, network security, malware analysis, and forensic analysis.

>> GCIH Valid Exam Answers <<

Latest GIAC GCIH Test Format, Reliable GCIH Exam Answers

The three versions of our GCIH training materials each have its own advantage, now I would like to introduce the advantage of the software version for your reference. It is quite wonderful that the software version can simulate the real GCIH examination for all of the users in windows operation system. By actually simulating the real test environment, you will have the opportunity to learn and correct your weakness in the course of study on GCIH learning braindumps.

The GCIH exam covers a wide range of topics, including incident handling and response, network security principles, malware analysis, and forensic analysis. GCIH exam consists of 150 multiple-choice questions, and candidates are given four hours to

complete the exam. To pass the exam, candidates must score at least 71% or higher. Upon passing the exam, candidates receive the GCIH certification, which is valid for four years and can be renewed by passing a recertification exam or earning continuing education credits.

GCIH Structure

The test GCIH is the only benchmark necessary for obtaining the GIAC Certified Incident Handler designation. Also, it's a proctored exam and candidates should pay a registration fee of $1,999 to be eligible for it. To add more, the exam includes 100 to 150 inquiries with different levels of complexity and structure. The candidates should know that they will have only 4 hours to reply to as many questions as possible and get a passing score of 70%.

GIAC Certified Incident Handler Sample Questions (Q34-Q39):

NEW QUESTION # 34
Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two- factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Adam decides to implement smart cards but they are not cost effective.
Which of the following types of hardware devices will Adam use to implement two-factor authentication?

- A. One Time Password
- B. Security token
- C. Proximity cards
- D. Biometric device

Answer: B

NEW QUESTION # 35
You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?

- A. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
- B. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
- C. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP
- D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT

Answer: D

Explanation:
Section: Volume C

NEW QUESTION # 36
Which of the following protocol loggers is used to detect ping sweep?

- A. pitl
- B. ippl
- C. dpsl
- D. lppi

Answer: B

NEW QUESTION # 37
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage.
The firewall protects the network well and allows strict Internet access.
How was security compromised and how did the firewall respond?

- A. Security was not compromised as the webpage was hosted internally.
- B. The attack was Cross Site Scripting and the firewall blocked it.
- C. The attack was social engineering and the firewall did not detect it.
- D. Security was compromised as keylogger is invisible for firewall.

Answer: C

Explanation:
Section: Volume A

NEW QUESTION # 38
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

- A. Session hijacking
- B. ARP spoofing
- C. Man-in-the-middle
- D. Port scanning

Answer: B

NEW QUESTION # 39
.....