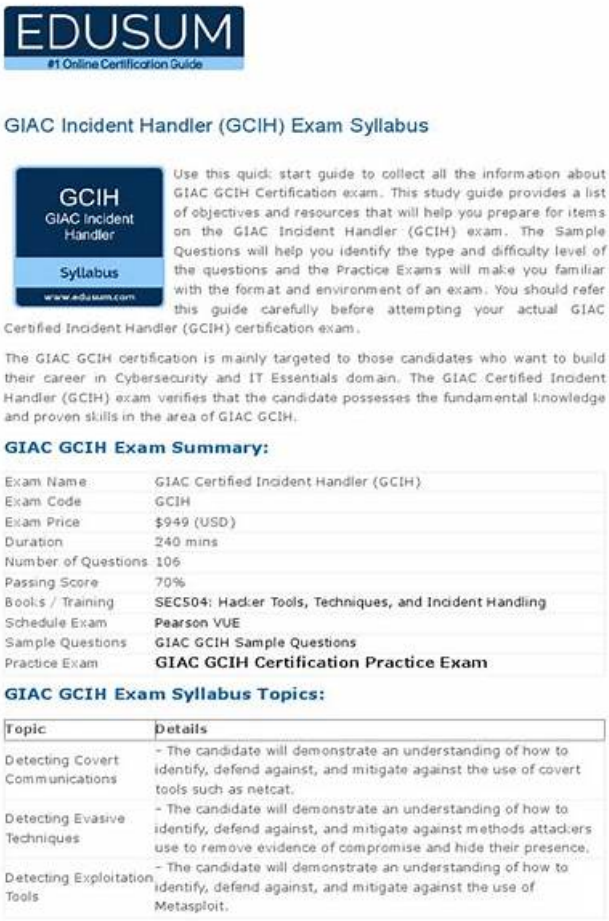
Latest GIAC GCIH Learning Materials | GCIH Test Simulator Online



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.

BONUS!!! Download part of CramPDF GCIH dumps for free: https://drive.google.com/open?id=1fMN_OLQoXS5xMuoIE-ZZ8iNlw2g9QsXn

CramPDF is a reliable site offering the GCIH valid study material supported by 100% pass rate and full money back guarantee. Besides, our GCIH training material is with the high quality and can simulate the actual test environment, which make you feel in the real test situation. You can get the latest information about the GCIH real test, because our CramPDF will give you one year free update. You can be confident to face any difficulties in the GCIH actual test no matter any changes.

Our GCIH study materials can help you achieve your original goal and help your work career to be smoother and your family life quality to be better and better. There is no exaggeration to say that you will be confident to take part in you GCIH exam with only studying our GCIH practice torrent for 20 to 30 hours. And we can ensure your success for we have been professional in this career for over 10 years. And thousands of candidates have achieved their dreams and ambitions with the help of our outstanding GCIH training materials.

>> Latest GIAC GCIH Learning Materials <<

GCIH Test Simulator Online & Real GCIH Torrent

Some people are inclined to read paper materials. Do not worry. Our company has already taken your thoughts into consideration. Our PDF version of the GCIH practice materials support printing on papers. All contents of our GCIH Exam Questions are arranged reasonably and logically. In addition, the word size of the GCIH study guide is suitable for you to read. And you can take it

conveniently.

GIAC Certified Incident Handler (GCIH) certification exam is a highly respected and recognized certification in the field of incident handling and response. It is designed for professionals who are responsible for detecting, responding to, and remedying security incidents in their organizations. The GCIH Certification is offered by the Global Information Assurance Certification (GIAC), which is a leading provider of cybersecurity certifications.

GIAC Certified Incident Handler Sample Questions (Q39-Q44):

NEW QUESTION # 39
Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.
Which of the following are the techniques used for network mapping by large organizations?
Each correct answer represents a complete solution. Choose three.

- A. Route analytics
- B. SNMP-based approaches
- C. Active Probing
- D. Packet crafting

Answer: A,B,C

NEW QUESTION # 40
Which of the following are types of access control attacks?
Each correct answer represents a complete solution. Choose all that apply.

- A. Brute force attack
- B. Mail bombing
- C. Spoofing
- D. Dictionary attack

Answer: A,C,D

NEW QUESTION # 41
Which of the following attacks are examples of Denial-of-service attacks (DoS)?
Each correct answer represents a complete solution. Choose all that apply.

- A. Fraggle attack
- B. Birthday attack
- C. Ping flood attack
- D. Smurf attack

Answer: A,C,D

NEW QUESTION # 42
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host.
Which of the following steps can you use to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

- A. Add the copied virtual machine to a protection group.
- B. Run consistency check.
- C. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
- D. Copy the virtual machine to the new server.

Answer: A,C,D

Explanation:

Section: Volume B

NEW QUESTION # 43
Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether.
The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?
Each correct answer represents a complete solution. Choose all that apply.

- A. Using ARP Guard utility
- B. Using smash guard utility
- C. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets
- D. Using ARP watch utility
- E. Using static ARP entries on servers, workstation and routers

Answer: A,C,D,E

NEW QUESTION # 44
.....

To help people pass exam easily, we bring you the latest GCIH exam prep for the actual test which enable you get high passing score easily in test. Our study materials are the up-to-dated and all GCIH Test Answers you practiced are tested by our professional experts. Once you have well prepared with our GCIH dumps collection, you will go through the formal test without any difficulty.

2026 Latest CramPDF GCIH PDF Dumps and GCIH Exam Engine Free Share: https://drive.google.com/open?id=1fMN_OLQoXS5xMuoIE-ZZ8iNlw2g9QsXn