EDUSUM

#1 Online Certification Guide

GIAC GCIH STUDY GUIDE PDF

Grab the GIAC Incident Handler Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

GCIH

GIAC Certified Incident Handler (GCIH)

106 Questions Exam – 70% Cut Score – Duration of 240 minutes

Table of Contents:

Get an Overview of the GCIH Certification:

Who should take the **GCIH exam**? This is the first question that comes to a candidate's mind when preparing for the Incident Handler certification. The GCIH certification is suitable for candidates who are keen to earn knowledge on the Penetration Testing and grab their GIAC Certified Incident Handler (GCIH) certification. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But GCIH study guide PDF is here to solve the problem. GCIH PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the GIAC GCIH Certification?

There are several reasons why one should grab the GCIH certification.

- The Incident Handler certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential employers.
- Thus earning the **GIAC Certified Incident Handler (GCIH)** is a powerful qualification for a prosperous career.

What is the GIAC GCIH Incident Handler Certification Exam Structure?

Exam Name	GIAC Certified Incident Handler (GCIH)
Exam Code	GCIH
Exam Price	$2499 (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**

Enhance Knowledge with GCIH Sample Questions:

Question: 1

You enter the netstat -an command in the command prompt and you receive intimation that port number 7777 is open on your computer.

Which of the following Trojans may be installed on your computer?

a) NetBus
b) QAZ
c) Donald Dick
d) Tini

Answer: d

Question: 2

Which of the following statements about Ping of Death attack is true?

a) In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
b) This type of attack uses common words in either upper or lower case to find a password.
c) In this type of attack, a hacker maliciously cuts a network cable.
d) In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

Answer: d

Question: 3

Which of the following statements are true about tcp wrappers?

a) tcp wrapper provides access control, host address spoofing, client username lookups, etc.
b) When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
c) tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
d) tcp wrapper protects a Linux server from IP address spoofing.

Answer: a, b, c

Question: 4

What is the major difference between a worm and a Trojan horse?

a) A worm spreads via e-mail, while a Trojan horse does not.
b) A worm is a form of malicious program, while a Trojan horse is a utility.
c) A worm is self replicating, while a Trojan horse is not.
d) A Trojan horse is a malicious program, while a worm is an anti-virus software.

Answer: c

Question: 5

In which of the following attacking methods does an attacker distribute incorrect IP address?

a) IP spoofing
b) Mac flooding
c) DNS poisoning
d) Man-in-the-middle

Answer: c

Question: 6

Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

a) Evasion attack
b) Denial-of-Service (DoS) attack
c) Ping of death attack
d) Buffer overflow attack

Answer: d

Question: 7

A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

a) Vulnerability attack
b) Impersonation attack
c) Social Engineering attack
d) Denial-of-Service attack

Answer: d

Question: 8

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

a) Denial of Service attack
b) Replay attack
c) Teardrop attack
d) Land attack

Answer: a

Question: 9

What is the purpose of configuring a password protected screen saver on a computer?

a) For preventing unauthorized access to a system.
b) For preventing a system from a Denial of Service (DoS) attack.
c) For preventing a system from a social engineering attack.
d) For preventing a system from a back door attack.

Answer: a

Question: 10

In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

a) Ping of death
b) Jolt
c) Fraggle
d) Teardrop

Answer: a

What Study Guide Works Best in Acing the GIAC GCIH Incident Handler Certification?

The GCIH study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Incident Handler exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your study schedule must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

If there is related GIAC training, don't miss out the chance to join. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the GIAC GCIH Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, GCIH practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven GCIH Practice Test for Success!!!

Do you want to pass the GCIH exam on your first attempt? Stop worrying; EduSum.com is here to provide you the best experience during your GIAC Incident Handler preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **GCIH practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.