EDUSUM

#1 Online Certification Guide

GIAC GCIH

GIAC Incident Handler Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCIH

GIAC Certified Incident Handler (GCIH)

100-150 Questions Exam – 70% Cut Score – Duration of 240 minutes

Table of Contents:

Know Your GCIH Certification Well: 2

GIAC GCIH Incident Handler Certification Details: 2

GCIH Syllabus: 3

GIAC GCIH Sample Questions: 4

Study Guide to Crack GIAC Incident Handler GCIH Exam: 7

Know Your GCIH Certification Well:

The GCIH is best suitable for candidates who want to gain knowledge in the GIAC Penetration Testing. Before you start your GCIH preparation you may struggle to get all the crucial Incident Handler materials like GCIH syllabus, sample questions, study guide.

But don't worry the GCIH PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the GCIH syllabus?
- How many questions are there in the GCIH exam?
- Which Practice test would help me to pass the GCIH exam at the first attempt?

Passing the GCIH exam makes you GIAC Certified Incident Handler (GCIH). Having the Incident Handler certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GIAC GCIH Incident Handler Certification Details:

Exam Name	GIAC Certified Incident Handler (GCIH)
Exam Code	GCIH
Exam Price	$2499 (USD)
Duration	240 mins
Number of Questions	100-150
Passing Score	70%
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCIH Sample Questions**
Practice Exam	**GIAC GCIH Certification Practice Exam**

GCIH Syllabus:

Topic	Details
Covering Tracks on Hosts	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against methods attackers use to remove evidence of compromise on hosts.
Covering Tracks on the Network	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against methods attackers use to remove evidence of compromise on the network.
Domain Attacks	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against Domain attacks in Windows environments.
Drive-By Attacks	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against drive-by attacks in modern environments.
Endpoint Attacks and Pivoting	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against attacks against endpoints and attack pivoting.
Incident Handling and Digital Investigations	- The candidate will demonstrate an understanding of what Incident Handling is, why it is important, an understanding of the PICERL incident handling process, and industry best practices in Incident Handling and Digital Investigations.
Memory and Malware Investigations	- The candidate will demonstrate an understanding of the steps necessary to perform basic memory forensics, including collection and analysis of processes and network connections and basic malware analysis.
Metasploit	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of Metasploit.
Netcat	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of covert tools such as netcat.
Network Investigations	- The candidate will demonstrate an understanding of the steps necessary to perform effective digital investigations of network data.
Password Attacks	- The candidate will demonstrate a detailed understanding of the three methods of password cracking.
Physical Access Attacks	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against physical access attacks.
Reconnaissance and Open-Source Intelligence	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate public and open source reconnaissance techniques.
Scanning and Mapping	- The candidate will demonstrate an understanding the fundamentals of how to identify, defend against, and mitigate against scanning; to discover and map networks and hosts, and reveal services and vulnerabilities.

Topic	Details
SMB Scanning	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate reconnaissance and scanning of SMB services.
Web App Attacks	- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against Web Application Attacks.

GIAC GCIH Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 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

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: 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

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: 9

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: 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

Study Guide to Crack GIAC Incident Handler GCIH Exam:

- Getting details of the GCIH syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GCIH exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GCIH exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GCIH sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GCIH practice tests is must. Continuous practice will make you an expert in all syllabus areas.