EDUSUM

#1 Online Certification Guide

GIAC GCIA STUDY GUIDE PDF

Grab the GIAC Intrusion Analyst Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

GCIA

GIAC Certified Intrusion Analyst (GCIA)

106 Questions Exam – 68% Cut Score – Duration of 240 minutes

Table of Contents:

Get an Overview of the GCIA Certification:

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

Why Should You Earn the GIAC GCIA Certification?

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

- The Intrusion Analyst 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 candidates.
- Thus earning the **GIAC Certified Intrusion Analyst (GCIA)** is a powerful qualification for a prosperous career.

What is the GIAC GCIA Intrusion Analyst Certification Exam Structure?

Exam Name	GIAC Certified Intrusion Analyst (GCIA)
Exam Code	GCIA
Exam Price	$949 (USD)
Duration	240 mins
Number of Questions	106
Passing Score	68%
Books / Training	**SEC503: Intrusion Detection In-Depth**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCIA Sample Questions**
Practice Exam	**GIAC GCIA Certification Practice Exam**

Enhance Knowledge with GCIA Sample Questions:

Question: 1

Which of the following statements are true about snort?

a) It develops a new signature to find vulnerabilities.
b) It detects and alerts a computer user when it finds threats such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, wellknown backdoors and system vulnerabilities, and DDoS clients.
c) It encrypts the log file using the 256 bit AES encryption scheme algorithm.
d) It is used as a passive trap to record the presence of traffic that should not be found on a network, such as NFS or Napster connections.

Answer: a, b, d

Question: 2

Which of the following tools can be used to check whether the network interface is in promiscuous mode or not?

a) IPTraf
b) MRTG
c) Chkrootkit
d) Ntop

Answer: c

Question: 3

Which of the following files in LILO booting process of Linux operating system stores the location of Kernel on the hard drive?

a) /boot/boot.b
b) /boot/map
c) /sbin/lilo
d) /etc/lilo.conf

Answer: b

Question: 4

Which of the following techniques allows probing firewall rule-sets and finding entry points into the targeted system or network?

a) Network enumerating
b) Packet collision
c) Distributed Checksum Clearinghouse
d) Packet crafting

Answer: d

Question: 5

At which layers of the OSI and TCP/IP models does IP addressing function?

a) OSI Layer 5 and TCP/IP Transport Layer
b) OSI Layer 2 and TCP/IP Network Layer
c) OSI Layer 4 and TCP/IP Application Layer
d) OSI Layer 3 and TCP/IP Internet Layer

Answer: d

Question: 6

What are the advantages of stateless autoconfigration in IPv6?

a) Ease of use.
b) It provides basic authentication to determine which systems can receive configuration data
c) No server is needed for stateless autoconfigration.
d) No host configuration is necessary.

Answer: a, c, d

Question: 7

Which of the following types of firewall ensures that the packets are part of the established session?

a) Switch-level firewall
b) Application-level firewall
c) Stateful inspection firewall
d) Circuit-level firewall

Answer: c

Question: 8

Which of the following commands in MQC tool matches IPv4 and IPv6 packets when IP parameter is missing?

a) Match access-group
b) Match fr-dlci
c) Match IP precedence
d) Match cos

Answer: c

Question: 9

Which of the following work as traffic monitoring tools in the Linux operating system?

a) MRTG
b) John the Ripper
c) IPTraf
d) Ntop

Answer: a, c, d

Question: 10

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft's Windows XP operating system?

a) NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
b) BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe
c) NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
d) NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe

Answer: d

What Study Guide Works Best in acing the GIAC GCIA Intrusion Analyst Certification?

The GCIA 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 Intrusion Analyst 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 syllabus 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:

Do not forget to join the GIAC GCIA training if it is providing any. 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 GCIA 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, GCIA practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven GCIA Practice Test for Success!!!

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