GIAC GCIA

GIAC Intrusion Analyst Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

GCIA

GIAC Certified Intrusion Analyst (GCIA)

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

Table of Contents:

Discover More about the GCIA Certification

Are you interested in passing the GIAC GCIA exam? First discover, who benefits from the GCIA certification. The GCIA is suitable for a candidate if he wants to learn about Cyber Defense. Passing the GCIA exam earns you the GIAC Certified Intrusion Analyst (GCIA) title.

While preparing for the GCIA exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The GCIA PDF contains some of the most valuable preparation tips and the details and instant access to useful **GCIA study materials just at one click**.

GCIA GIAC Intrusion Analyst Certification Details:

Exam Name	GIAC Certified Intrusion Analyst (GCIA)
Exam Code	GCIA
Exam Price	$2499 (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**

GCIA Syllabus:

Topic	**Details**
Advanced Analysis and Network Forensics	- The candidate will demonstrate competence in analyzing data from multiple sources (e.g. full packet capture, netflow, log files) as part of a forensic investigation.
Advanced IDS Concepts	- The candidate will demonstrate an understanding of IDS tuning methods and correlation issues.
Application Protocols	- The candidate will demonstrate knowledge and skill relating to application layer protocol dissection and analysis.

Topic	Details
Concepts of TCP/IP and the Link Layer	- The candidate will demonstrate understanding of the TCP/IP communications model and link layer operations.
DNS	- The candidate will demonstrate an understanding of how DNS works for both legitimate and malicious purposes.
Fragmentation	- The candidate will demonstrate understanding of how fragmentation works, and how to identify fragmentation and fragmentation-based attacks in packet captures.
IDS Fundamentals and Network Architecture	- The candidate will demonstrate knowledge of fundamental IDS concepts, such as network architecture options and benefits/weaknesses of common IDS systems.
IDS Rules	- The candidate will create effective IDS rules to detect varied types of malicious activity.
IP Headers	- The candidate will demonstrate the ability to dissect IP packet headers and analyze them for normal and anomalous values that may point to security issues.
IPv6	- The candidate will demonstrate knowledge of IPv6 and how it differs from IPv4.
Network Traffic Analysis	- The candidate will demonstrate the ability to analyze network and application traffic to identify both normal and malicious behaviors.
Packet Engineering	- The candidate will demonstrate knowledge relating to packet crafting and manipulation.
Silk and Other Traffic Analysis Tools	- The candidate will demonstrate an understanding of SiLK and other tools to perform network traffic and flow analysis.
TCP	- The candidate will demonstrate understanding of the TCP protocol and the ability to discern between typical and anomalous behavior.
Tcpdump Filters	- The candidate will demonstrate ability to craft tcpdump filters that match on given criteria.
UDP and ICMP	- The candidate will demonstrate understanding of the UDP and ICMP protocols and the ability to discern between typical and anomalous behavior.
Wireshark Fundamentals	- The candidate will demonstrate skill associated with traffic analysis using Wireshark with an intermediate degree of proficiency.

Broaden Your Knowledge with GIAC 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 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: 3

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

Question: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

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

Avail the Study Guide to Pass GCIA GIAC Intrusion Analyst Exam:

- Find out about the GCIA syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **GCIA syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the GCIA training. Joining the GIAC provided training for GCIA exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **GCIA sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. GCIA practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the GCIA exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the GCIA Certification

EduSum.Com is here with all the necessary details regarding the GCIA exam. We provide authentic practice tests for the GCIA exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **GCIA practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the GIAC Certified Intrusion Analyst (GCIA).

Start Online Practice of GCIA Exam by visiting URL
https://www.edusum.com/giac/gcia-giac-intrusion-analyst