EDUSUM

#1 Online Certification Guide

GIAC GCIA

GIAC Intrusion Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCIA

GIAC Certified Intrusion Analyst (GCIA)

100-150 Questions Exam – 68% Cut Score – Duration of 240 minutes

Table of Contents:

Know Your GCIA Certification Well:

The GCIA is best suitable for candidates who want to gain knowledge in the GIAC Cyber Defense. Before you start your GCIA preparation you may struggle to get all the crucial Intrusion Analyst materials like GCIA syllabus, sample questions, study guide.

But don't worry the GCIA 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 GCIA syllabus?
- How many questions are there in the GCIA exam?
- Which Practice test would help me to pass the GCIA exam at the first attempt?

Passing the GCIA exam makes you GIAC Certified Intrusion Analyst (GCIA). Having the Intrusion Analyst 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 GCIA Intrusion Analyst Certification Details:

Exam Name	GIAC Certified Intrusion Analyst (GCIA)
Exam Code	GCIA
Exam Price	$1999 (USD)
Duration	240 mins
Number of Questions	100-150
Passing Score	68%
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.
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.

GIAC GCIA Sample Questions:

Question: 1

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: 2

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: 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 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: 6

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: 7

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: 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 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: 10

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

Study Guide to Crack GIAC Intrusion Analyst GCIA Exam:

- Getting details of the GCIA 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 GCIA 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 GCIA 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 GCIA 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 GCIA practice tests is must. Continuous practice will make you an expert in all syllabus areas.