EDUSUM

#1 Online Certification Guide

GIAC GCFA

GIAC Forensic Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCFA

GIAC Certified Forensic Analyst (GCFA)

82-115 Questions Exam – 72% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GCFA Certification Well:

The GCFA is best suitable for candidates who want to gain knowledge in the GIAC Incident Response and Forensics. Before you start your GCFA preparation you may struggle to get all the crucial Forensic Analyst materials like GCFA syllabus, sample questions, study guide.

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

Passing the GCFA exam makes you GIAC Certified Forensic Analyst (GCFA). Having the Forensic 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 GCFA Forensic Analyst Certification Details:

Exam Name	GIAC Certified Forensic Analyst (GCFA)
Exam Code	GCFA
Exam Price	$2499 (USD)
Duration	180 mins
Number of Questions	82-115
Passing Score	72%
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCFA Sample Questions**
Practice Exam	**GIAC GCFA Certification Practice Exam**

GCFA Syllabus:

Topic	Details
Enterprise Environment Incident Response	- The candidate will demonstrate an understanding of the steps of the incident response process, attack progression, and adversary fundamentals and how to rapidly assess and analyze systems in an enterprise environment scaling tools to meet the demands of large investigations.
File System Timeline Artifact Analysis	- The candidate will demonstrate an understanding of the Windows filesystem time structure and how these artifacts are modified by system and user activity.
Identification of Malicious System and User Activity	- The candidate will demonstrate an understanding of the techniques required to identify and document indicators of compromise on a system, detect malware and attacker tools, attribute activity to events and accounts, and identify and compensate for anti-forensic actions using memory and disk resident artifacts.
Identification of Normal System and User Activity	- The candidate will demonstrate an understanding of the techniques required to identify, document, and differentiate normal and abnormal system and user activity using memory and disk resident artifacts.
Introduction to File System Timeline Forensics	- The candidate will demonstrate an understanding of the methodology required to collect and process timeline data from a Windows system.
Introduction to Volatile Data Forensics	- The candidate will demonstrate an understanding of how and when to collect volatile data from a system and how to document and preserve the integrity of volatile evidence.
NTFS Artifact Analysis	- The candidate will demonstrate an understanding of core structures of the Windows filesystems, and the ability to identify, recover, and analyze evidence from any file system layer, including the data storage layer, metadata layer, and filename layer.
Volatile Data Artifact Analysis of Malicious Events	- The candidate will demonstrate an understanding of abnormal activity within the structure of Windows memory and be able to identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits.
Volatile Data Artifact Analysis of Windows Events	- The candidate will demonstrate an understanding of abnormal activity within the structure of Windows memory and be able to identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits.
Windows Artifact Analysis	- The candidate will demonstrate an understanding of Windows system artifacts and how to collect and analyze data such as system back up and restore data and evidence of application execution.

GIAC GCFA Sample Questions:

Question: 1

Which of the following directories cannot be placed out of the root filesystem?

a) /sbin
b) /etc
c) /var
d) /lib

Answer: a, b, d

Question: 2

Which of the following are the benefits of information classification for an organization?

a) It ensures that modifications are not made to data by unauthorized personnel or processes.
b) It helps identify which information is the most sensitive or vital to an organization.
c) It helps reduce the Total Cost of Ownership (TCO).
d) It helps identify which protections apply to which information.

Answer: b, d

Question: 3

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

a) Netcraft
b) Ettercap
c) Ethereal
d) Nmap

Answer: a

Question: 4

What are the purposes of audit records on an information system?

a) Backup
b) Investigation
c) Upgradation
d) Troubleshooting

Answer: b, d

Question: 5

Which of the following types of virus makes changes to a file system of a disk?

a) Master boot record virus
b) Stealth virus
c) Cluster virus
d) Macro virus

Answer: c

Question: 6

In a Windows computer, which of the following utilities is used to convert a FAT16 partition to FAT32?

a) CVT16.EXE
b) CVT1.EXE
c) CONVERT16.EXE
d) CONVERT.EXE

Answer: b

Question: 7

Which of the following file systems supports the hot fixing feature?

a) FAT16
b) exFAT
c) FAT32
d) NTFS

Answer: d

Question: 8

Which of the following tools are used to determine the hop counts of an IP packet?

a) Netstat
b) TRACERT
c) IPCONFIG
d) Ping

Answer: b, d

Question: 9

Which of the following statements about SD cards are true?

a) It is used with mobile phones and digital cameras.
b) It is a type of non-volatile memory card.
c) It is a 184-pin memory module.
d) It is used as RAM on client computers and servers.

Answer: a, b

Question: 10

In which of the following files does the Linux operating system store passwords?

a) Password
b) Passwd
c) Shadow
d) SAM

Answer: c

Study Guide to Crack GIAC Forensic Analyst GCFA Exam:

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

Reliable Online Practice Test for GCFA Certification

Make EduSum.com your best friend during your GIAC Forensic Analyst exam preparation. We provide authentic practice tests for the GCFA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GCFA exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don’t bother if you don’t get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GCFA exam.

Start Online practice of GCFA Exam by visiting URL
https://www.edusum.com/giac/gcfa-giac-forensic-analyst