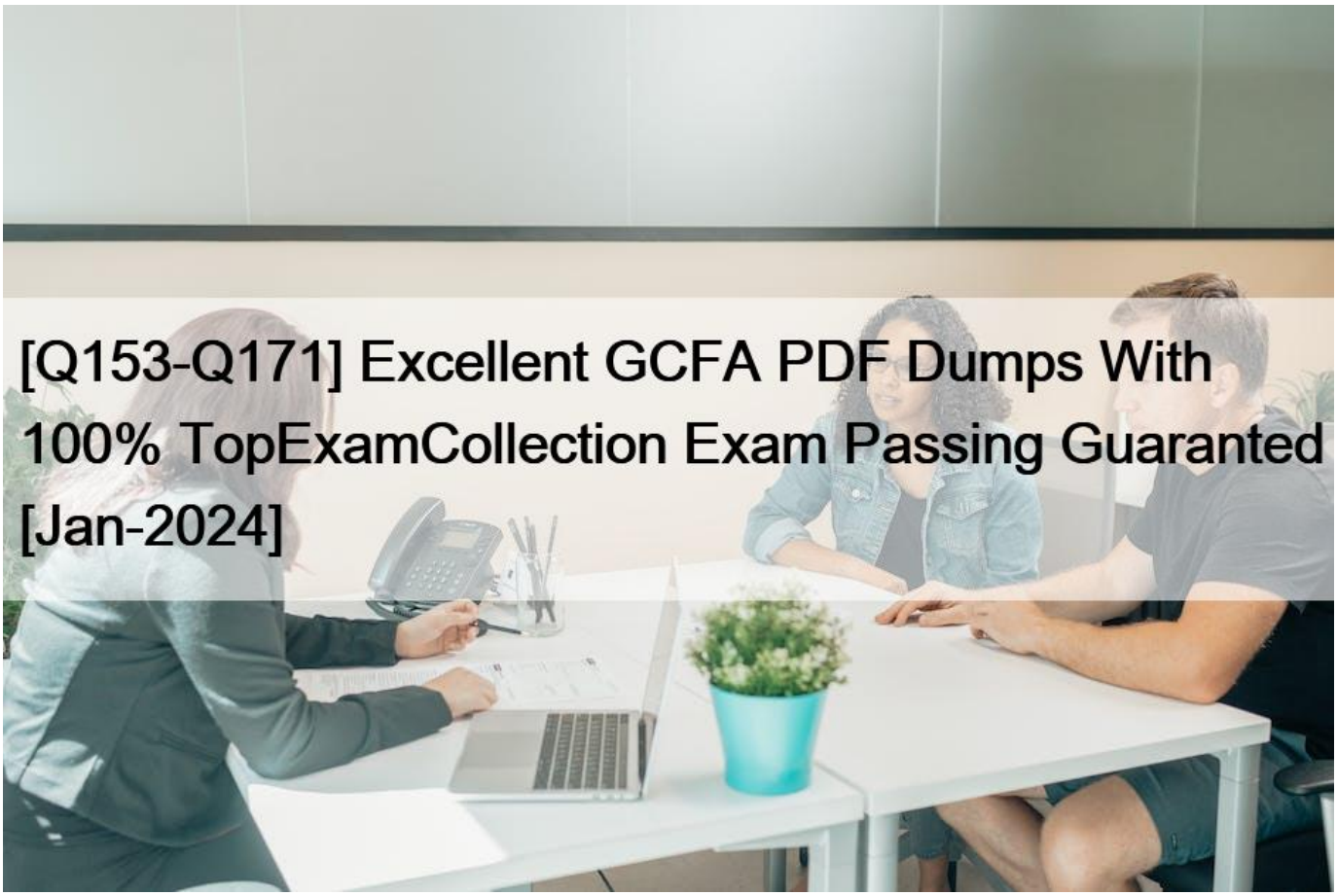
# [Q153-Q171 Excellent GCFA PDF Dumps With 100% TopExamCollection Exam Passing Guaranted [Jan-2024




**Excellent GCFA PDF Dumps With 100% TopExamCollection Exam Passing Guaranted** [**Jan-2024**]
**100% Pass Your GCFA** GIAC Certified Forensics Analyst at First Attempt with TopExamCollection

## How to book GCFA Exams

In order to apply for the NET, You have to follow these steps
Go to the GCFA Official Site- Read the instruction Carefully- Follow the given steps- Apply for the GCFA

## Candidates for GCFA

The GIAC GCFA certification exam is suitable for specialists who want to get specialized in Digital Forensics and Advanced Incident Response topics. This test, in particular, is dedicated to Incident Response team members or threat hunters. Also, it is on the certification list of SOC analysts, experienced digital forensic analysts, or Information Security professionals. Another category of candidates interested in taking the GCFA evaluation is formed of GCIH or GCFE certification holders, penetration testers, red team members, or exploit developers. Besides, law enforcement professionals or federal agents are part of the group of candidates who are usually interested in leveraging their skills with the GCFA certification test.

**QUESTION 153**

Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?
* Group Policy
* System registry
* System control
* Application virtualization

Section: Volume B

**QUESTION 154**

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e-mailing company’s secrets to an opponent?
* Electronic surveillance
* Civil investigation
* Physical surveillance
* Criminal investigation

**QUESTION 155**

Based on the case study, to implement more security, which of the following additional technologies should you implement for laptop computers?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.
* PAP authentication
* Encrypting File System (EFS)
* Digital certificates
* Two-factor authentication
* Encrypted Data Transmissions

Section: Volume C

**QUESTION 156**

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the main server of SecureEnet Inc. The server runs on Debian Linux operating system.

Adam wants to investigate and review the GRUB configuration file of the server system.

Which of the following files will Adam investigate to accomplish the task?
* /boot/grub/menu.lst
* /boot/grub/grub.conf
* /boot/boot.conf
* /grub/grub.com

**QUESTION 157**

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows

or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.
* System logs
* Event logs
* Web server logs
* Program logs
Section: Volume B

**QUESTION 158**

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?
* Copyright
* Utility model
* Cookie
* Trade secret

**QUESTION 159**

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?
* Corroborating
* Circumstantial
* Incontrovertible
* Direct

**QUESTION 160**

You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross-Site Scripting attack on your company’s Website. Which of the following methods of investigation can you use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.
* Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company’s site.
* Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.
* Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.
* Look at the Web servers logs and normal traffic logging.
Section: Volume B

**QUESTION 161**

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. While performing some security investigation, you want to see the hostname and IP address from where users logged in.

Which of the following commands will you use to accomplish the task?
* Dig
* Netstat

* Nslookup
* Last

**QUESTION 162**

In which of the following security tests does the security testing team simulate as an employee or other person with an authorized connection to the organization’s network?
* Remote network
* Remote dial-up network
* Stolen equipment
* Local network

**QUESTION 163**

Which of the following are the two different file formats in which Microsoft Outlook saves e-mail messages based on system configuration?

Each correct answer represents a complete solution. Choose two.
* .pst
* .xst
* .txt
* .ost

Section: Volume C

**QUESTION 164**

Which of the following tools is used to modify registry permissions in Windows?
* POLEDIT
* REGEDIT
* REGEDT32
* SECEDIT

**QUESTION 165**

Which of the following data is NOT listed as a volatile data in RFC 3227 list for Windows based system?
* Kernel statistics
* Temporary file system
* Data on a hard disk
* Routing table

**QUESTION 166**

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?
* Web ripping
* TCP FTP proxy scanning
* Fingerprinting
* Eavesdropping

**QUESTION 167**

Which of the following cryptographic methods are used in EnCase to ensure the integrity of the data, which is acquired for the investigation?

Each correct answer represents a complete solution. Choose two.
* MD5
* CRC
* HAVAL
* Twofish

**QUESTION 168**

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?
* WinHex
* Device Seizure
* FAR system
* Vedit

Section: Volume C

**QUESTION 169**

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?
* Artistic license
* Phishing
* Spam
* Patent

**QUESTION 170**

Which of the following files starts the initialization process in booting sequence of the Linux operating system?
* /etc/sbin/init
* /etc/inittab
* /etc/rc/rc.local
* /etc/rc/rc.sysinit

**QUESTION 171**

Which of the following file systems provides file-level security?
* CDFS
* FAT
* FAT32
* NTFS

Achieving the GCFA certification demonstrates a level of expertise in digital forensics that is recognized by industry professionals and employers worldwide. GIAC Certified Forensics Analyst certification is highly respected and can open up new career opportunities for professionals in the digital forensics field. Additionally, maintaining the certification requires continuing education and staying up-to-date with the latest trends and techniques in digital forensics.

**Trend for GCFA pdf dumps before actual exam:** https://www.topexamcollection.com/GCFA-vce-collection.html]