[Jan 12, 2024 Dumpleader GCFA dumps & GIAC Information Security sure practice dumps [Q133-Q148

[Jan 12, 2024] Dumpleader GCFA dumps & GIAC Information Security sure practice dumps
GIAC GCFA Actual Questions and Braindumps

GIAC Certified Forensics Analyst (GCFA) exam is a certification offered by the Global Information Assurance Certification (GIAC). The GCFA certification is designed to validate the skills and knowledge of professionals who work in the digital forensics field. GIAC Certified Forensics Analyst certification is particularly useful for individuals who want to demonstrate their expertise in conducting digital forensics investigations, analyzing evidence, and presenting findings in a clear and concise manner.

How to Prepare For GCFA Exam **Preparation Guide for GCFA Exam GCFA: Tips to survive if you don't have time to read all the page**

The GCFA certifies that the individual possesses the knowledge, skills, and abilities necessary to use advanced forensic analysis techniques to solve complex investigations based on Windows and Linux. GCFA specialists can articulate complex forensic ideas such as file system structures, business acquisition, complex media analysis, and memory analysis.
GCFAs are leading researchers during violations of computer intrusion in the company. They can help identify and protect compromised systems even if the opponent uses forensic techniques. Through the use of advanced techniques such as file system timeline analysis, log analysis, and memory inspection, GCFAs can find malware, rootkits and unknown data that intruders believed they had removed from the system.

GCFA certification will ensure that you possess a solid understanding of high-level accident response and forensic computer tools and techniques for investigating data breaches, dishonest employees, advanced persistent threats and complex forensic cases.
The GCFA certification verifies knowledge that is not intended only for law enforcement personnel, but also for investigation and response teams to corporate and organizational incidents that have different legal or legal requirements compared to a standard forensic investigation for law enforcement.
The GCFA certification is aimed at professionals working in the fields of information security, forensic information technology, and accident response. The certification focuses on the basic skills necessary to collect and analyze data from Windows and Linux computer systems. The Global Information Assurance Certification Forensic Analyst certifies that applicants have the experience, talents, and abilities to conduct formal incident investigations and handle advanced incident management scenarios, including inner and external data breach intrusions, advanced persistent threats and anti-forensic methods. used by attackers and complex digital court cases.

QUESTION 133

Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?
* Reconnaissance
* gaining access
* Scanning
* Preparation

QUESTION 134

Which of the following is used for remote file access by UNIX/Linux systems?
* NetWare Core Protocol (NCP)
* Common Internet File System (CIFS)
* Server Message Block (SMB)
* Network File System (NFS)

QUESTION 135

Which of the following command line tools are available in Helix Live acquisition tool on Windows?

Each correct answer represents a complete solution. Choose all that apply.
* .cab extractors
* ipconfig
* netstat
* whois

QUESTION 136

Which of the following commands can you use to create an ext3 file system?

Each correct answer represents a complete solution. Choose two.
* mke2fs
* mkfs.ext3
* mke2fs -j
* mkfs.ext2

QUESTION 137

Which of the following uses hard disk drive space to provide extra memory for a computer?
* Virtual memory
* File system
* Cluster
* RAM

Section: Volume B

QUESTION 138

Adam works as a Computer Hacking Forensic Investigator. He has been assigned a project to investigate child pornography. As the first step, Adam found that the accused is using a Peer-to-peer application to network different computers together over the internet and sharing pornographic materials of children with others. Which of the following are Peer-to-Peer applications?

Each correct answer represents a complete solution. Choose all that apply.
* Gnutella
* Kismet
* Hamachi
* Freenet

Section: Volume B

Explanation

QUESTION 139

Which of the following IP addresses are private addresses?

Each correct answer represents a complete solution. Choose all that apply.
* 19.3.22.17
* 192.168.15.2
* 192.166.54.32
* 10.0.0.3

QUESTION 140

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?
* Chain of evidence
* Chain of custody
* Incident response policy
* Evidence access policy

QUESTION 141

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?
* Wiretap Act
* Computer Fraud and Abuse Act
* Economic Espionage Act of 1996
* Electronic Communications Privacy Act of 1986

QUESTION 142

Which of the following provides high availability of data?
* RAID
* Anti-virus software
* EFS
* Backup

QUESTION 143

Which utility enables you to access files from a Windows .CAB file?
* ACCESS.EXE
* WINZIP.EXE
* XCOPY.EXE
* EXTRACT.EXE

QUESTION 144

Which of the following types of computers is used for attracting potential intruders?
* Bastion host
* Data pot
* Files pot
* Honey pot

Section: Volume A

QUESTION 145

Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?

Each correct answer represents a complete solution. Choose all that apply.
* All ideas present in the investigative report should flow logically from facts to conclusions.
* There should not be any assumptions made about any facts while writing the investigative report.
* Opinion of a lay witness should be included in the investigative report.
* The investigative report should be understandable by any reader.

QUESTION 146

Which of the following sections of an investigative report covers the background and summary of the report including the outcome of the case and the list of allegations?
* Section 2
* Section 4
* Section 3
* Section 1

Section: Volume A

QUESTION 147

What is the name of the Secondary IDE slave, fourth partition in Linux operating system according to the Linux naming convention?
* SDB3
* HDC4
* HDA4
* HDD4

QUESTION 148

Which of the following file systems is used by both CD and DVD?
* Network File System (NFS)
* New Technology File System (NTFS)
* Compact Disk File System (CDFS)
* Universal Disk Format (UDF)