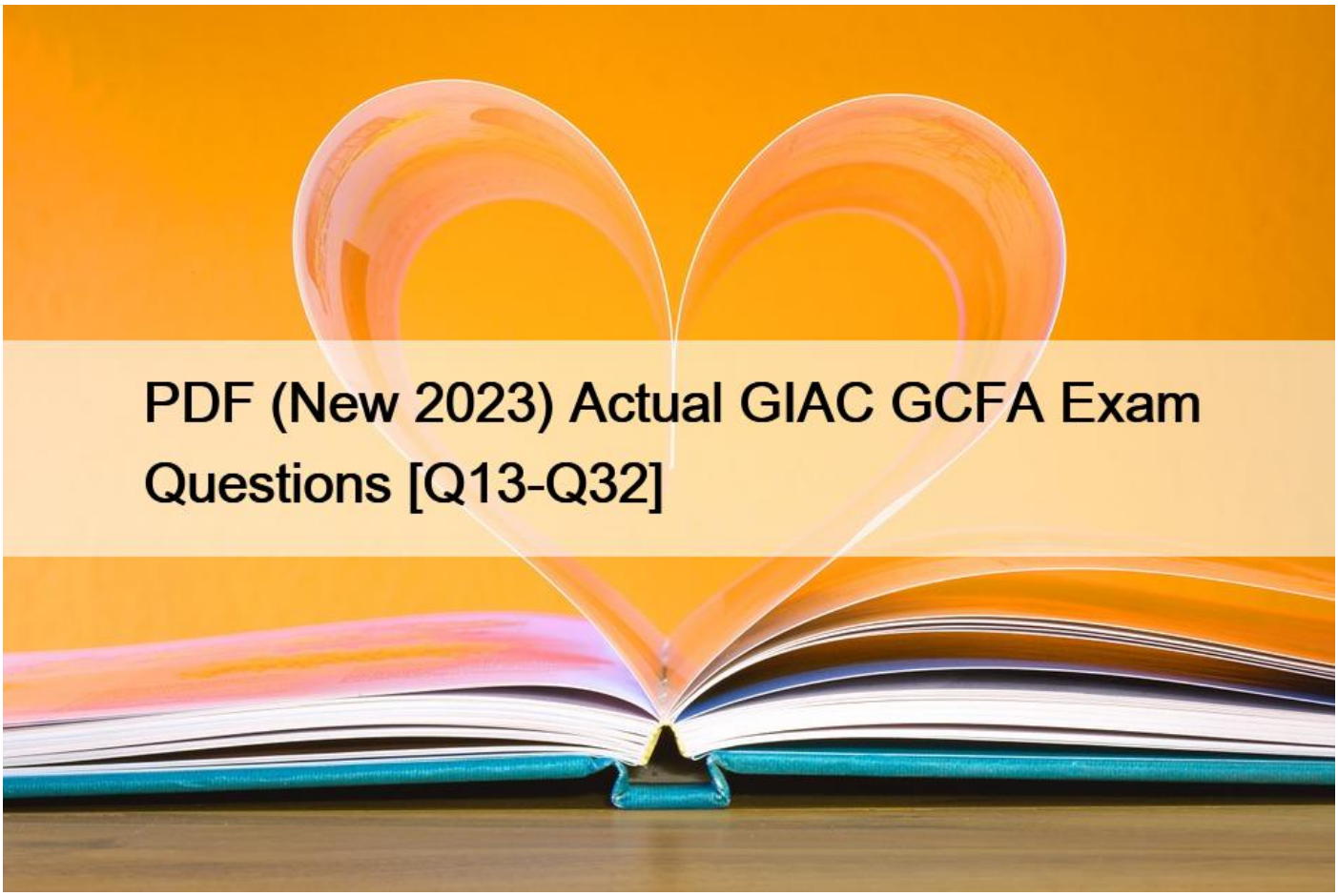
PDF (New 2023) Actual GIAC GCFA Exam Questions [Q13-Q32



PDF (New 2023) Actual GIAC GCFA Exam Questions
Dumps Moneyack Guarantee - GCFA Dumps UpTo 90% Off

The benefit in Obtaining the GCFA Exam Certification - Community awareness: GCFA-certified professionals actively strengthen the forensic community by encouraging members to participate in the popular GCFA computer forensics blog, which has led to the publication of more than 356 articles in the last two years.- Unique: GCFA is the largest neutral digital forensic certification in the market with more than 2,150 certified analysts. The Global Information Assurance Certification Forensic Analyst (GCFA) is also the only ANSI / 17024 accredited digital forensic certification offer. Together, this makes the GCFA a unique and desired certification among community professionals.- Skills: GCFAs can conduct investigations that regular auditors cannot resolve. Using techniques such as memory and log analysis, GCFA experts can answer questions that, several years ago, were believed to have no answer.- Legal: GCFA is the only neutral supplier certification that verifies the basic technical concepts and key legal knowledge required in the United States and the European Union. **Q13.** Sam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a compromised system, which runs on Linux operating system. Sam wants to investigate and review local software, system libraries, and other application installed on the system.

Which of the following directories in Linux will he review to accomplish the task?
* /tmp

* /mnt
* /lib
* /sbin

Section: Volume C

Q14. You are responsible for all computer security at your company. This includes initial investigation into alleged unauthorized activity. Which of the following are possible results of improperly gathering forensic evidence in an alleged computer crime by an employee?

Each correct answer represents a complete solution. Choose three.
* Your company is sued for defaming the character of an accused party.
* You falsely accuse an innocent employee.
* Your company is unable to pursue the case against a perpetrator.
* You are charged with criminal acts.

Q15. John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?
* Email spoofing
* Social engineering
* Steganography
* Web ripping

Q16. Which of the following sections of United States Economic Espionage Act of 1996 criminalizes the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret?
* Title 18, U.S.C. 1839
* Title 18, U.S.C. 1832
* Title 18, U.S. 1831
* Title 18, U.S.C. 1834

Q17. Which of the following file systems cannot be used to install an operating system on the hard disk drive?

Each correct answer represents a complete solution. Choose two.
* Windows NT file system (NTFS)
* High Performance File System (HPFS)
* Log-structured file system (LFS)
* Compact Disc File System (CDFS)
* Novell Storage Services (NSS)

Q18. Which of the following file systems supports the hot fixing feature?
* FAT16
* exFAT
* FAT32
* NTFS

Q19. Which of the following is a password-cracking program?
* Netcat

* L0phtcrack
* SubSeven
* NetSphere

Q20. Which of the following is the initiative of United States Department of Justice, which provides state and local law enforcement agencies the tools to prevent Internet crimes against children, and catches the distributors of child pornography on the Internet?
* Innocent Images National Initiative (IINI)
* Internet Crimes Against Children (ICAC)
* Project Safe Childhood (PSC)
* Anti-Child Porn.org (ACPO)

Q21. This type of virus infects programs that can execute and load into memory to perform predefined steps for infecting systems. It infects files with the extensions .EXE, .COM, .BIN, and .SYS. As it can replicate or destroy these types of files, the operating system becomes corrupted and needs reinstallation. This type of virus is known as _____.
* Polymorphic virus
* Stealth virus
* Boot sector virus
* File virus
* Multipartite virus

Section: Volume B

Q22. You work as a Network Administrator for NetTech Inc. The company’s network is connected to the Internet.

For security, you want to restrict unauthorized access to the network with minimum administrative effort.

You want to implement a hardware-based solution. What will you do to accomplish this?
* Connect a brouter to the network.
* Implement firewall on the network.
* Connect a router to the network.
* Implement a proxy server on the network.

Q23. Normally, RAM is used for temporary storage of data. But sometimes RAM data is stored in the hard disk, what is this method called?
* Cache memory
* Static memory
* Virtual memory
* Volatile memory

Q24. Which of the following statements about the HKEY_LOCAL_MACHINE registry hive is true?
* It contains the user profile for the user who is currently logged on to the computer.
* It contains information about the local computer system, including hardware and operating system data, such as bus type, system memory, device drivers, and startup control parameters.
* It contains configuration data for the current hardware profile.
* It contains data that associates file types with programs and configuration data for COM objects, Visual Basic programs, or other automation.

Section: Volume B

Explanation/Reference:

Q25. Nathan works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He uses Visual TimeAnalyzer software to

track all computer usage by logging into individual users account or specific projects and compile detailed accounts of time spent within each program. Which of the following functions are NOT performed by Visual TimeAnalyzer?

Each correct answer represents a complete solution. Choose all that apply.
* It monitors all user data such as passwords and personal documents.
* It gives parents control over their children’s use of the personal computer.
* It tracks work time, pauses, projects, costs, software, and internet usage.
* It records specific keystrokes and run screen captures as a background process.

Q26. John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task?

Each correct answer represents a complete solution. Choose two.
* nc 208.100.2.25 23
* nmap -v -O www.we-are-secure.com
* nc -v -n 208.100.2.25 80
* nmap -v -O 208.100.2.25

Explanation/Reference:

Q27. 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

Q28. Which of the following needs to be documented to preserve evidences for presentation in court?
* Separation of duties
* Incident response policy
* Chain of custody
* Account lockout policy

Section: Volume C

Explanation/Reference:

Q29. John, a novice web user, makes a new E-mail account and keeps his password as “apple”, his favorite fruit. John’s password is vulnerable to which of the following password cracking attacks?

Each correct answer represents a complete solution. Choose all that apply.
* Rule based attack
* Brute Force attack
* Dictionary attack
* Hybrid attack

Q30. You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to fix partitions on a hard drive. Which of the following Unix commands can you use to accomplish the task?
* fdformat

* exportfs
* fsck
* fdisk

Q31. Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?
* Linux
* MINIX 3
* Windows XP
* Mac OS

Q32. Which of the following file systems supports the hot fixing feature?
* FAT16
* exFAT
* FAT32
* NTFS

Section: Volume A