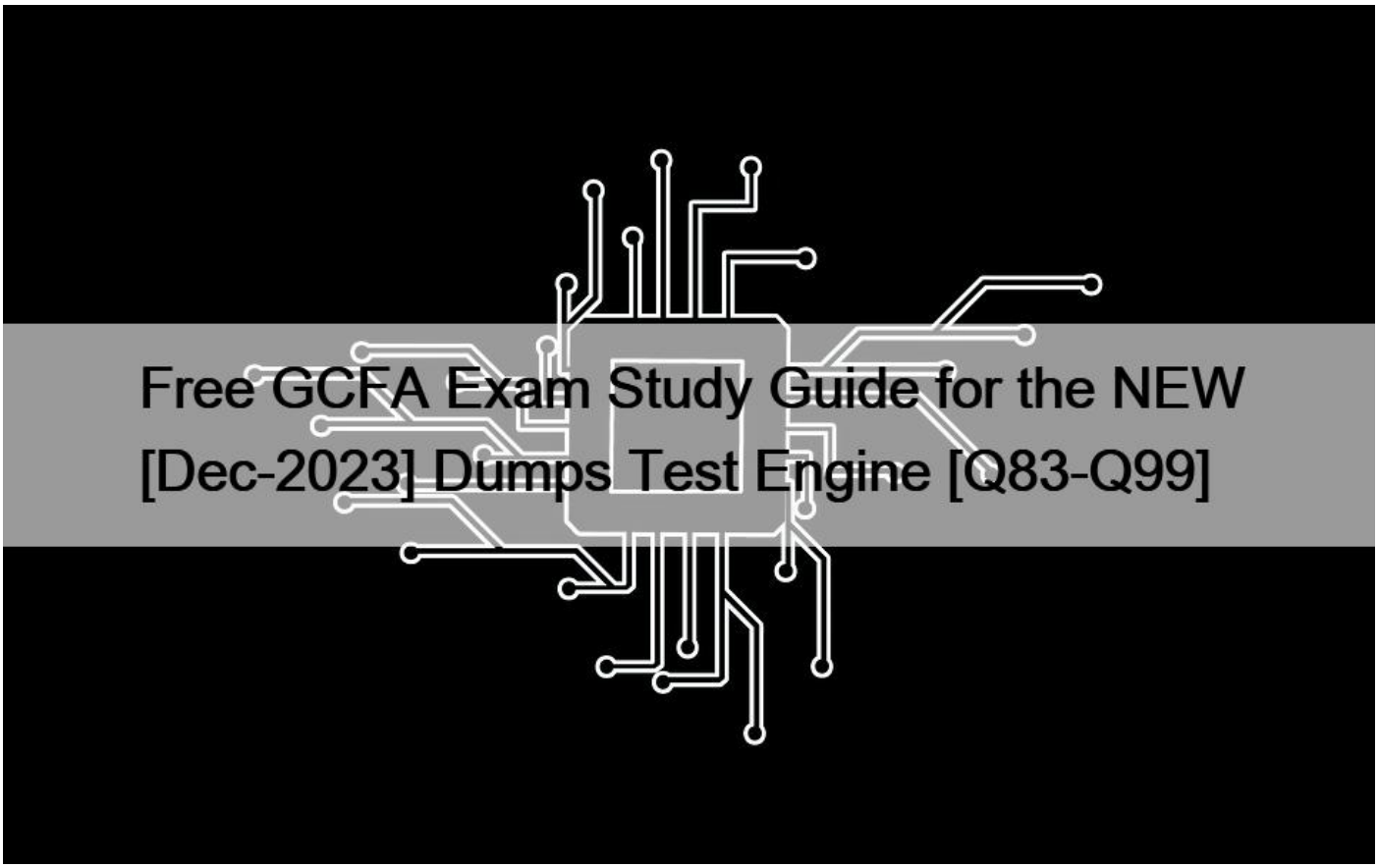
Free GCFA Exam Study Guide for the NEW [Dec-2023 Dumps Test Engine [Q83-Q99



Free GCFA Exam Study Guide for the NEW [Dec-2023 Dumps Test Engine GCFA PDF Dumps Extremely Quick Way Of Preparation

GIAC Certified Forensic Analyst (GCFA) is a professional certification that is awarded by the Global Information Assurance Certification (GIAC). The GCFA exam is designed for individuals who are interested in pursuing a career in digital forensics or incident response. GIAC Certified Forensics Analyst certification is globally recognized and is highly valued by employers in the information security industry.

NO.83 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

NO.84 The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook’s preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?
* HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun
* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRunServices
* HKEY_CURRENT_USERSoftwareMicrosoftWABWAB4Wab File Name = “file and pathname of the WAB file”
* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun
Section: Volume C

NO.85 John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we- are-secure.com. John wants to redirect all TCP port 80 traffic to UDP port 40, so that he can bypass the firewall of the We-are-secure server. Which of the following tools will John use to accomplish his task?
* Fpipe
* PsList
* Cain
* PsExec
Section: Volume C

NO.86 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

NO.87 Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe.

The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:

C:WINDOWS>netstat -an | find “UDP”

UDP IP_Address:31337 *:*

Now you check the following registry address:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunServices In the above address, you notice a ‘default’ key in the ‘Name’ field having ” .exe” value in the corresponding ‘Data’ field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?
* Tini

* Qaz
* Donald Dick
* Back Orifice

Section: Volume C

NO.88 Which of the following file systems contains hardware settings of a Linux computer?
* /var
* /etc
* /proc
* /home

NO.89 Which of the following components are usually found in an Intrusion detection system (IDS)?

Each correct answer represents a complete solution. Choose two.
* Sensor
* Firewall
* Modem
* Gateway
* Console

Section: Volume C

NO.90 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

NO.91 You want to upgrade a partition in your computer’s hard disk drive from FAT to NTFS. Which of the following DOS commands will you use to accomplish this?
* FORMAT C: /s
* CONVERT C: /fs:ntfs
* SYS C:
* FDISK /mbr

Section: Volume A

NO.92 Trinity wants to send an email to her friend. She uses the MD5 generator to calculate cryptographic hash of her email to ensure the security and integrity of the email. MD5 generator, which Trinity is using operates in two steps:

Creates check file

Verifies the check file

Which of the following MD5 generators is Trinity using?
* MD5 Checksum Verifier
* Mat-MD5
* Chaos MD5
* Secure Hash Signature Generator

NO.93 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

Section: Volume A

NO.94 You are the Network Administrator and your company has recently implemented encryption for all emails.

You want to check to make sure that the email packages are being encrypted. What tool would you use to accomplish this?
* Password cracker
* Packet sniffer
* Performance Monitor
* Vulnerability analyzer

NO.95 Jason, a game lover, owns an Apple’s iPod nano. He wants to play games on his iPod. He also wants to improve the quality of the audio recording of his iPod. Which of the following steps can Jason take to accomplish the task?
* Install iPodLinux.
* Install third party software.
* Upgrade Apple’s firmware.
* Buy external add-ons.

NO.96 Which two technologies should research groups use for secure VPN access while traveling? (Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.
* SSL
* PPTP
* Encrypting File System (EFS)
* Kerberos authentication
* Smart cards

NO.97 In 2001, the Council of Europe passed a convention on cybercrime. It was the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. On 1 March 2006, the Additional Protocol to the Convention on Cybercrime came into force. Which of the following statements clearly describes this protocol?
* The convention of cybercrime is only applied within Europe.
* It requires participating states to criminalize the dissemination of racist and xenophobic material through computer systems.
* The convention of cybercrime should immediately be put on hold until there is an inclusion of a new or amended article.
* English speaking states in Europe such as Ireland and the United Kingdom should sign the convention.

NO.98 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

NO.99 Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual

harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

Each correct answer represents a complete solution. Choose all that apply.
* Names of the victims
* Date and time of incident
* Nature of harassment
* Location of each incident

Section: Volume A