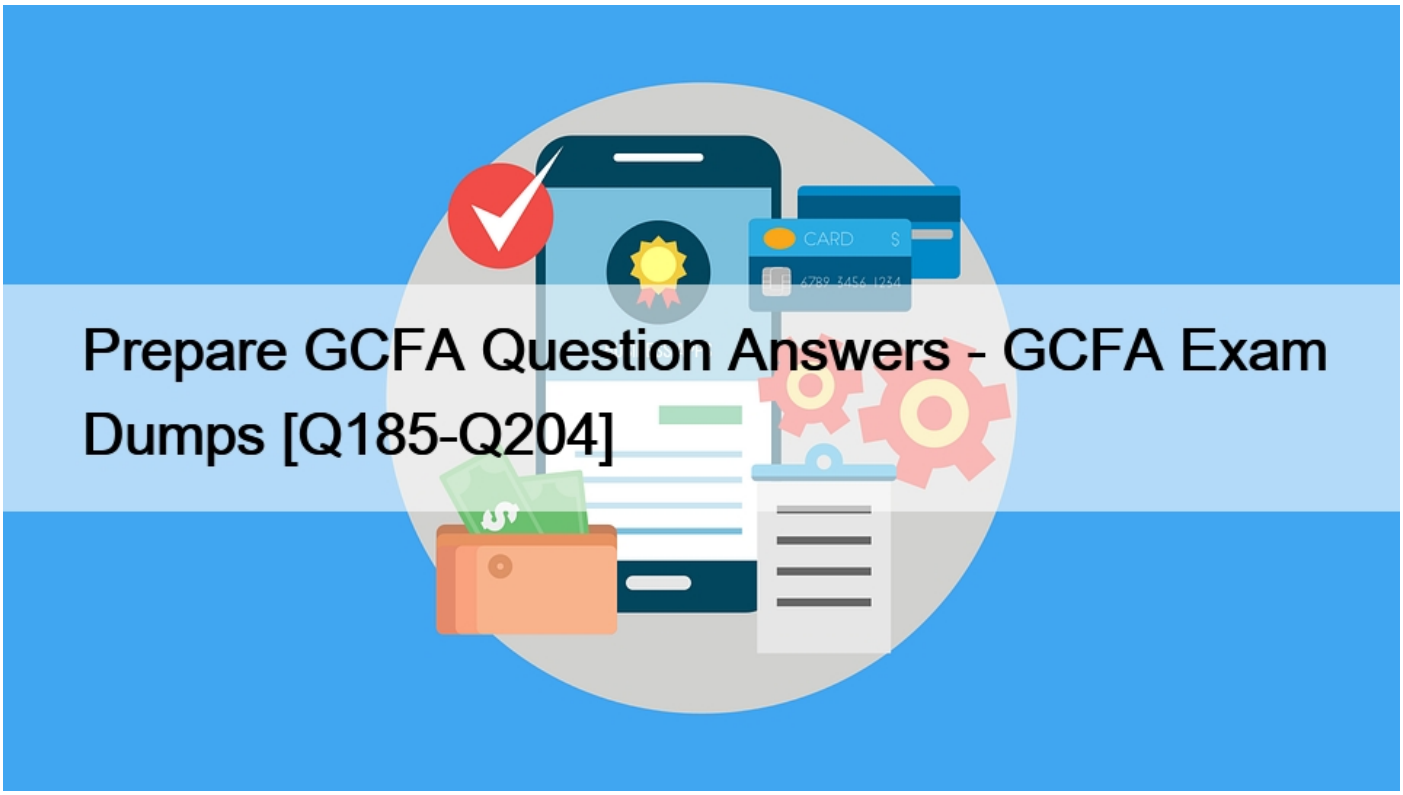
Prepare GCFA Question Answers - GCFA Exam Dumps [Q185-Q204



Prepare GCFA Question Answers - GCFA Exam Dumps
Real GIAC GCFA Exam Questions [Updated 2023]

NEW QUESTION 185

Which of the following statements best describes the consequences of the disaster recovery plan test?
* If no deficiencies were found during the test, then the plan is probably perfect.
* The results of the test should be kept secret.
* The plan should not be changed no matter what the results of the test would be.
* If no deficiencies were found during the test, then the test was probably flawed.

Section: Volume B

NEW QUESTION 186

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.

Section: Volume B

NEW QUESTION 187

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)

Section: Volume A

NEW QUESTION 188

Peter works as a Security Administrator for SecureEnet Inc. He observes that the database server of the company has been compromised and the data is stolen. Peter immediately wants to report this crime to the law enforcement authorities. Which of the following organizations looks after the computer crimes investigations in the United States?
* Federal Bureau of Investigation
* Local or National office of the US secret service
* Incident response team
* National Institute of Standards and Technology

Section: Volume C

NEW QUESTION 189

Which of the following commands is used to enforce checking of a file system even if the file system seems to be clean?
* e2fsck -f
* e2fsck -p
* e2fsck -b
* e2fsck -c

Section: Volume C

NEW QUESTION 190

Which of the following tools is an asterisk password revealer tool?
* Aircrack
* SnadBoy
* Cain and Abel
* Pwdump3

NEW QUESTION 191

Which of the following directories cannot be placed out of the root filesystem?

Each correct answer represents a complete solution. Choose all that apply.
* /sbin
* /etc
* /var
* /lib

NEW QUESTION 192

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

NEW QUESTION 193

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
Section: Volume B

NEW QUESTION 194

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

NEW QUESTION 195

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

NEW QUESTION 196

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

NEW QUESTION 197

John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?
* 18 U.S.C. 2701
* 18 U.S.C. 1030
* 18 U.S.C. 1362
* 18 U.S.C. 2510

NEW QUESTION 198

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

NEW QUESTION 199

Allen works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a computer, which is used by the suspect to sexually harass the victim using instant messenger program. Suspect’s computer runs on Windows operating system. Allen wants to recover password from instant messenger program, which suspect is using, to collect the evidence of the crime. Allen is using Helix Live for this purpose. Which of the following utilities of Helix will he use to accomplish the task?
* Mail Pass View
* MessenPass
* Asterisk Logger
* Access PassView

NEW QUESTION 200

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?
* CHKDSK /I
* CHKDSK /C /L
* CHKDSK /V /X

* CHKDSK /R /F

NEW QUESTION 201

What are the purposes of audit records on an information system?

Each correct answer represents a complete solution. Choose two.
* Backup
* Investigation
* Upgradation
* Troubleshooting

NEW QUESTION 202

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate an iphone, which is being seized from a criminal. The local police suspect that this iphone contains some sensitive information. Adam knows that the storage partition of the iphone is divided into two partitions. The first partition is used for the operating system. Other data of iphone is stored in the second partition. Which of the following is the name with which the second partition is mounted on the iphone?
* /private/var
* /var/data
* /var/private
* /data/var

NEW QUESTION 203

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

NEW QUESTION 204

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect’s computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?
* Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces
* Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps
* Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system
* Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

Section: Volume A

GCFA Exam Dumps Pass with Updated 2023: https://www.exams4sures.com/GIAC/GCFA-practice-exam-dumps.html]