[Q165-Q182 Best Quality GCFA Exam Questions GIAC Test To Gain Brilliante Result!

Best Quality GCFA Exam Questions GIAC Test To Gain Brilliante Result!
Preparations of GCFA Exam 2022 GIAC Information Security Unlimited 318 Questions

NEW QUESTION 165

Which of the following file attributes are not available on a FAT32 partition?

Each correct answer represents a complete solution. Choose two.
* Compression
* Encryption
* Read Only
* Hidden
* Archive

NEW QUESTION 166

Sandra wants to create a full system state backup of her computer, which is running on Microsoft Windows XP operating system.

Which of the following is saved in full state system backup?

Each correct answer represents a complete solution. Choose all that apply.
* file system information
* Registry
* Windows boot files
* Active Directory (NTDS)

Section: Volume B

NEW QUESTION 167

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

NEW QUESTION 168

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to allow direct access to the filesystems data structure. Which of the following Unix commands can you use to accomplish the task?
* du
* debugfs
* df
* dosfsck

NEW QUESTION 169

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 170

Which of the following files in LILO booting process of Linux operating system stores the location of Kernel on the hard drive?
* /boot/map
* /boot/boot.b
* /etc/lilo.conf
* /sbin/lilo

NEW QUESTION 171

Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?
* Stalking by Electronic Communications Act (2001)
* Malicious Communications Act (1998)
* Anti-Cyber-Stalking law (1999)
* Stalking Amendment Act (1999)

NEW QUESTION 172

Which of the following encryption methods uses AES technology?
* Dynamic WEP
* Static WEP
* TKIP
* CCMP

NEW QUESTION 173

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?

Each correct answer represents a complete solution. Choose all that apply.
* The mutation engine of the virus is generating a new encrypted code.
* The virus, used by John, is not in the database of the antivirus program installed on the server.
* John has created a new virus.
* John has changed the signature of the virus.

NEW QUESTION 174

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.

NEW QUESTION 175

Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS X.

He wants to boot his system from the Network Interface Controller (NIC). Which of the following snag keys will Mark use to perform the required function?
* N
* D
* C
* Z

NEW QUESTION 176

Which of the following is NOT an example of passive footprinting?
* Querying the search engine.
* Analyzing job requirements.
* Scanning ports.
* Performing the whois query.

NEW QUESTION 177

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 178

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?
* 132.298.1.23
* A3-07-B9-E3-BC-F9
* F936.28A1.5BCD.DEFA
* 1011-0011-1010-1110-1100-0001
Section: Volume C

NEW QUESTION 179

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a compromised system of a cyber criminal, who hides some information in his computer.

This computer runs on Linux operating system. Adam wants to extract the data units of a file, which is specified by its meta-data address. He is using the Sleuth Kit for this purpose. Which of the following commands in the Sleuth kit will he use to accomplish the task?
* dcat
* ifind
* icat
* istat

NEW QUESTION 180

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.

NEW QUESTION 181

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

NEW QUESTION 182

You are the Security Consultant working with a client who uses a lot of outdated systems. Many of their clients PC’s still have Windows 98. You are concerned about the security of passwords on a Windows 98 machine.

What algorithm is used in Windows 98 to hash passwords?
* DES
* SHA
* LANMAN
* MD5

Section: Volume C