GIAC.GCFA.v2022-05-19.q241

Exam Code:	GCFA
Exam Name:	GIAC Certified Forensics Analyst
Certification Provider:	GIAC
Free Question Number:	241
Version:	v2022-05-19
# of views:	4583
# of Questions views:	2410
https://www.exam-tests.com/GCFA-exam/GIAC.GCFA.v2022-05-19.q241.html	

NEW QUESTION: 1
You are reviewing a Service Level Agreement between your company and a Web development vendor.
Which of the following are security requirements you should look for in this SLA?
Each correct answer represents a complete solution. Choose all that apply.
A. Security Monitoring
B. Guarantees on known security flaws
C. Encryption standards
D. Time to respond to bug reports
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following directories contains administrative commands on a UNIX computer?
A. /sbin
B. /export
C. /bin
D. /usr/local
Answer: (SHOW ANSWER)

NEW QUESTION: 3
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare- secure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:
Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'
This error message shows that the We-are-secure Website is vulnerable to _____.
A. A buffer overflow
B. A Denial-of-Service attack

C. An XSS attack
D. A SQL injection attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following provides high availability of data?
A. RAID
B. Anti-virus software
C. EFS
D. Backup
Answer: A (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 5
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?
A. dump
B. dumpe2fs
C. e2fsck
D. e2label
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
You work as a Network Administrator for NetTech Inc. The company has a network that consists of 200 client computers and ten database servers. One morning, you find that an unauthorized user is accessing data on a database server on the network. Which of the following actions will you take to preserve the evidences?
Each correct answer represents a complete solution. Choose three.
A. Prevent the company employees from entering the server room.
B. Detach the network cable from the database server.
C. Prevent a forensics experts team from entering the server room.
D. Preserve the log files for a forensics expert.
Answer: A,B,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 7
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?
A. CHKDSK /I
B. CHKDSK /C /L
C. CHKDSK /V /X
D. CHKDSK /R /F
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 8
Peter, an expert computer user, attached a new sound card to his computer. He then restarts the computer, so that the BIOS can scan the hardware changes. What will be the memory range of ROM that the BIOS scan for additional code to be executed for proper working of soundcard?
A. hCA79 to hAC20
B. hDF80 to hFF80
C. hC800 to hDF80
D. hAA43 to hF345
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following is the Windows feature on which the file management can be performed by a PC user?
A. Activity Monitor
B. Windows Explorer
C. Task Manager
D. Finder
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?
A. Security law
B. Privacy law
C. Copyright law
D. Trademark law
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 11

Which of the following encryption methods use the RC4 technology?
Each correct answer represents a complete solution. Choose all that apply.
A. Dynamic WEP
B. TKIP
C. Static WEP
D. CCMP
Answer: A,B,C (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 12
Which of the following graphical tools is used to navigate through directory structures?
A. Disk Cleanup
B. System Information
C. Disk Management
D. Windows Explorer
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 13
Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?
A. 18 U.S.C. 1362
B. 18 U.S.C. 2510
C. 18 U.S.C. 2701
D. 18 U.S.C. 1029
E. 18 U.S.C. 1030
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Which utility enables you to access files from a Windows .CAB file?
A. EXTRACT.EXE
B. XCOPY.EXE
C. WINZIP.EXE
D. ACCESS.EXE
Answer: (SHOW ANSWER)

NEW QUESTION: 15
You want to change the attribute of a file named ACE.TXT to Hidden. Which command line will enable you to set the attribute?
A. ATTRIB ACE.TXT /H

B. ATTRIB ACE.TXT /HR
C. ATTRIB ACE.TXT +H
D. ATTRIB ACE.TXT -H
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Which of the following functionality within the Autopsy browser is specifically designed to aid in case management?
A. Keyword searches
B. File listing
C. Hash database
D. Image integrity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
Which of the following statements about registry is true?
Each correct answer represents a complete solution. Choose three.
A. It can be edited using SCANREG utility.
B. It is a centralized configuration database that stores information related to a Windows computer.
C. It is divided in many areas known as hives.
D. It was first introduced with Windows 95 operating system.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?
A. Melissa
B. Tequila
C. Brain
D. I love you
Answer: C (LEAVE A REPLY)

Section: Volume A

NEW QUESTION: 19
Which of the following is a file management tool?
A. MSCONFIG
B. Device Manager
C. Windows Explorer
D. Defrag
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following protocols allows computers on different operating systems to share files and disk storage?
A. Domain Name System (DNS)
B. Network File System (NFS)
C. Trivial File Transfer Protocol (TFTP)
D. Simple Network Management Protocol (SNMP)
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 21
Which of the following is used to authenticate asymmetric keys?
A. Password
B. Digital signature
C. MAC Address
D. Demilitarized zone (DMZ)
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 22
Which of the following is used for remote file access by UNIX/Linux systems?
A. NetWare Core Protocol (NCP)
B. Common Internet File System (CIFS)
C. Server Message Block (SMB)
D. Network File System (NFS)
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 23
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the

local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

A. Web ripping

B. Fingerprinting

C. Eavesdropping

D. TCP FTP proxy scanning

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Convention on Cybercrime, created by the Council of Europe, is the treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Which of the following chapters of Convention of Cybercrime contains the provisions for mutual assistances and extradition rules related to cybercrimes?

A. Chapter II

B. Chapter IV

C. Chapter III

D. Chapter I

Answer: (SHOW ANSWER)

Section: Volume B

NEW QUESTION: 25

You work as a Network Administrator for uCertify Inc. You want to edit the MSDOS.SYS file, in your computer, from the DOS prompt. You are unable to find the file. What is the most likely cause?

A. It is a built-in command in the COMMAND.COM file.

B. Someone has deleted the file.

C. It is a hidden file.

D. It is a read-only file.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 26

Which of the following Windows XP system files handles memory management, I/O operations, and interrupts?

A. Ntoskrnl.exe

B. Win32k.sys

C. Advapi32.dll

D. Kernel32.dll

Answer: D (LEAVE A REPLY)

Section: Volume B

NEW QUESTION: 27
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.
A. Hybrid attack
B. Dictionary attack
C. Brute Force attack
D. Rule based attack
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 28
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the BlackBerry, which is suspected to be used to hide some important information.
Which of the following is the first step taken to preserve the information in forensic investigation of the BlackBerry?
A. Remove the storage media.
B. Turn off the BlackBerry.
C. Keep BlackBerry in 'ON' state.
D. Eliminate the ability of the device to receive the push data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?
A. Device Seizure
B. Ontrack
C. DriveSpy
D. Forensic Sorter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
Nathan works as a professional Ethical Hacker. He wants to see all open TCP/IP and UDP ports of his computer. Nathan uses the netstat command for this purpose but he is still unable to map open ports to the running process with PID, process name, and path. Which of the following commands will Nathan use to accomplish the task?
A. Psloggedon
B. Pslist
C. fport
D. ping
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following directories contains administrative commands and daemon processes in the Linux operating system?
A. /etc
B. /dev
C. /usr
D. /sbin
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 32
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?
A. 18 U.S. 1362
B. 18 U.S.C. 1030
C. 18 U.S.C. 2510
D. 18 U.S.C. 2701
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?
A. Containment
B. Identification
C. Eradication

D. Recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 34
You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to run a command that forces all the unwritten blocks in the buffer cache to be written to the disk. Which of the following Unix commands can you use to accomplish the task?
A. tune2fs
B. sync
C. swapoff
D. swapon
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 35
Which of the following tools can be used by a user to hide his identity?
Each correct answer represents a complete solution. Choose all that apply.
A. Rootkit
B. Anonymizer
C. Proxy server
D. War dialer
E. IPchains
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following file systems is designed by Sun Microsystems?
A. NTFS
B. ext2
C. CIFS
D. ZFS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following statements is NOT true about the file slack spaces in Windows operating system?
A. It is possible to find user names, passwords, and other important information in slack.
B. Large cluster size will decrease the volume of the file slack.
C. File slack may contain data from the memory of the system.
D. File slack is the space, which exists between the end of the file and the end of the last cluster.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
In which of the following security tests does the security testing team simulate as an employee or other person with an authorized connection to the organization's network?
A. Remote network
B. Remote dial-up network
C. Stolen equipment
D. Local network
Answer: (SHOW ANSWER)

NEW QUESTION: 39
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are creating a user account by using the USERADD command. Which of the following entries cannot be used for specifying a user ID?
Each correct answer represents a complete solution. Choose all that apply.
A. 99
B. 0
C. -1
D. 100
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 40
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?
A. Innocent Images National Initiative (IINI)
B. Internet Crimes Against Children (ICAC)
C. Project Safe Childhood (PSC)
D. Anti-Child Porn.org (ACPO)
Answer: B (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 41
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?
A. 18 U.S.C. 2701
B. 18 U.S.C. 1030
C. 18 U.S.C. 1362
D. 18 U.S.C. 2510
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42

Which of the following cryptographic methods are used in EnCase to ensure the integrity of the data, which is acquired for the investigation?
Each correct answer represents a complete solution. Choose two.
A. MD5
B. CRC
C. HAVAL
D. Twofish
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following file attributes are not available on a FAT32 partition?
Each correct answer represents a complete solution. Choose two.
A. Compression
B. Encryption
C. Read Only
D. Hidden
E. Archive
Answer: A,B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 44
Which of the following file systems provides file-level security?
A. NTFS
B. FAT32
C. FAT
D. CDFS
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following diagnostic codes sent by POST to the internal port h80 refers to the system board error?
A. 200 to 299
B. 100 to 199
C. 300 to 399
D. 400 to 499
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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?
A. Windows XP
B. Linux
C. Mac OS
D. MINIX 3
Answer: (SHOW ANSWER)

NEW QUESTION: 47
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?
A. Performance Monitor
B. Vulnerability analyzer
C. Packet sniffer
D. Password cracker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?
A. Civil Rights Act of 1991
B. PROTECT Act
C. Sexual Predators Act
D. The USA Patriot Act of 2001
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
Your network has a Windows 2000 Server computer with FAT file system, shared by several users.
This system stores sensitive data. You decide to encrypt this data to protect it from unauthorized

access. You want to accomplish the following goals:
Data should be secure and encrypted.
Administrative efforts should be minimum.
You should have the ability to recover encrypted files in case the file owner leaves the company.
Other permissions on encrypted files should be unaffected.
File-level security is required on the disk where data is stored.
Encrypting or decrypting of files should not be the responsibility of the file owner.
You take the following steps to accomplish these goals :
Convert the FAT file system to Windows 2000 NTFS file system.
Use Encrypting File System (EFS) to encrypt data.
Which of the following goals will you be able to accomplish?
Each correct answer represents a complete solution. Choose all that apply.
A. Encrypting or decrypting of files is no longer the responsibility of the file owner.
B. Administrative efforts are minimum.
C. Other permissions on encrypted files are unaffected.
D. File-level security is available on the disk where data is stored.
E. Data are secured and encrypted.
F. You have the ability to recover encrypted files in case the file owner leaves the company.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?
A. Confidentiality
B. Authentication
C. Non-repudiation
D. Integrity
Answer: C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 51
Which of the following tools is used to locate lost files and partitions to restore data from a formatted, damaged, or lost partition in Windows and Apple Macintosh computers?
A. Easy-Undelete
B. File Scavenger
C. VirtualLab
D. Recover4all Professional
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e-mailing company's secrets to an opponent?

A. Physical surveillance

B. Civil investigation

C. Electronic surveillance

D. Criminal investigation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 53

Which of the following precautionary steps are taken by the supervisors or employers to avoid sexual harassment in workplace?

Each correct answer represents a complete solution. Choose all that apply.

A. Communicate to an employee who is indulging in such behavior.

B. Establish a complaint mechanism.

C. Immediately take action on the complaint.

D. Contact the police and take legal action.

Answer: (SHOW ANSWER)

NEW QUESTION: 54

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?

A. CONVERT C: /fs:ntfs

B. FDISK /mbr

C. FORMAT C: /s

D. SYS C:

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55

You are responsible for tech support at your company. You have been instructed to make certain that all desktops support file and folder encryption. Which file system should you use when installing Windows XP?

A. FAT32

B. FAT

C. EXT4

D. NTFS

Answer: D (LEAVE A REPLY)

NEW QUESTION: 56

Adrian, the Network Administrator for Peach Tree Inc., wants to install a new computer on the company's network. He asks his assistant to make a boot disk with minimum files. The boot disk will be used to boot the computer, which does not have an operating system installed, yet. Which of the following files will he include on the disk?

A. IO.SYS, MSDOS.SYS, COMMAND.COM, and AUTOEXEC.BAT.

B. IO.SYS, MSDOS.SYS, COMMANCOM, and FDISK.

C. IO.SYS, MSDOS.SYS, and COMMAND.COM.

D. IO.SYS, MSDOS.SYS, COMMAND.COM, and CONFIG.SYS.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 57

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?

A. MD5 Checksum Verifier

B. Mat-MD5

C. Chaos MD5

D. Secure Hash Signature Generator

Answer: (SHOW ANSWER)

Section: Volume B

NEW QUESTION: 58

You work as a Network Administrator for Peach Tree Inc. The company currently has a FAT-based Windows NT network. All client computers run Windows 98. The management wants all client computers to be able to boot in Windows XP Professional. You want to accomplish the following goals:

* The file system should support file compression and file level security.
* All the existing data and files can be used by the new file system.
* Users should be able to dual-boot their computers.

You take the following steps to accomplish these goals:

* Convert the FAT file system to NTFS using the CONVERT utility.
* Install Windows XP and choose to upgrade the existing operating system during setup.

Which of the following goals will you be able to accomplish?

Each correct answer represents a complete solution. Choose all that apply.

A. The file system supports file compression and file level security.

B. All the existing data and files can be used by the new file system.

C. Users are able to dual-boot their computers.

D. None of the goals are accomplished.

Answer: A,B (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 59
Which of the following file systems are supported by Windows 2000 operating systems?
Each correct answer represents a complete solution. Choose all that apply.
A. NTFS5
B. NTFS4
C. FAT32
D. HPFS
E. CDFS
Answer: A,B,C,E (LEAVE A REPLY)

NEW QUESTION: 60
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:
Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'
This error message shows that the We-are-secure Website is vulnerable to _____.
A. A Denial-of-Service attack
B. An XSS attack
C. A buffer overflow
D. A SQL injection attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following types of firewall functions at the Session layer of OSI model?
A. Application-level firewall
B. Switch-level firewall
C. Packet filtering firewall
D. Circuit-level firewall
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 62
Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?
A. WinHex
B. Device Seizure
C. FAR system
D. Vedit
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 63
Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature. Which of the following statements is true in context with the above scenario?
A. Adam is using NTFS file system.
B. Adam is using FAT file system.
C. Alternate Data Streams is a feature of Linux operating system.
D. Adam's system runs on Microsoft Windows 98 operating system.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following diagnostic codes sent by POST to the internal port h80 refers to the system board error?
A. 200 to 299
B. 100 to 199
C. 400 to 499
D. 300 to 399
Answer: (SHOW ANSWER)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 65
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?
A. Linux

B. MINIX 3
C. Windows XP
D. Mac OS
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 66
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the main server of SecureEnet Inc. The server runs on Debian Linux operating system. Adam wants to investigate and review the GRUB configuration file of the server system.
Which of the following files will Adam investigate to accomplish the task?
A. /boot/boot.conf
B. /boot/grub/menu.lst
C. /boot/grub/grub.conf
D. /grub/grub.com
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?
A. Spoofing
B. Eavesdropping
C. Data diddling
D. Wiretapping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.
What is the most likely cause?
A. The server's NIC is not working.
B. The switch device is not working.
C. The cable that connects the server to the switch is broken.
D. The server is configured with unspecified IP address.
E. Automatic IP addressing is not working.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
You work as a Network Administrator for Web World Inc. You want to host an e-commerce Web site on your network. You want to ensure that storage of credit card information is secure. Which of the following conditions should be met to accomplish this?
Each correct answer represents a complete solution. Choose all that apply.
A. NT authentication should be required for all customers before they provide their credit card numbers.
B. Strong encryption software should be used to store credit card information.
C. Only authorized access should be allowed to credit card information.
D. The NTFS file system should be implemented on a client computer.
Answer: B,C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 70
You use the FAT16 file system on your Windows 98 computer. You want to upgrade to the FAT32 file system. What is the advantage of the FAT32 file system over FAT16 file system?
Each correct answer represents a complete solution. Choose two.
A. On startup failure, you can start the computer by using an MS-DOS or Windows 95 bootable floppy disk.
B. It uses larger cluster sizes.
C. It supports drives up to 2 terabytes (TB) in size.
D. It allocates disk space more efficiently.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
You are responsible for maintaining and troubleshooting PC's at your company. The receptionist reports her screen has gone blue. When you get there you notice the 'blue screen of death' with an error message NTFS_FILE_SYSTEM. What is the most likely cause of this error?
A. Windows was installed improperly.
B. The hard disk is corrupt
C. A virus
D. Get the latest patch for Windows.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following is a type of intruder detection that involves logging network events to a file for an administrator to review later?
A. Event detection
B. Active detection

C. Packet detection
D. Passive detection
Answer: (SHOW ANSWER)

NEW QUESTION: 73
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?
A. /tmp
B. /mnt
C. /lib
D. /sbin
Answer: D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 74
Which of the following prevents malicious programs from attacking a system?
A. Smart cards
B. Firewall
C. Anti-virus program
D. Biometric devices
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following types of firewall ensures that the packets are part of the established session?
A. Application-level firewall
B. Circuit-level firewall
C. Stateful inspection firewall
D. Switch-level firewall
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 76
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?
A. Copyright
B. Utility model

C. Cookie
D. Trade secret
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with the project of investigating an iPod, which is suspected to contain some explicit material. Adam wants to connect the compromised iPod to his system, which is running on Windows XP (SP2) operating system. He doubts that connecting the iPod with his computer may change some evidences and settings in the iPod. He wants to set the iPod to read-only mode. This can be done by changing the registry key within the Windows XP (SP2) operating system. Which of the following registry keys will Adam change to accomplish the task?
A. HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies
B. HKEY_LOCAL_MACHINE\System\CurrentControlset\StorageDevicePolicies
C. HKEY_LOCAL_MACHINE\CurrentControlset\Control\StorageDevicePolicies
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following wireless network standards operates on the 5 GHz band and transfers data at a rate of 54 Mbps?
A. 802.11b
B. 802.11a
C. 802.11g
D. 802.11u
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which of the following file systems are supported by Windows 2000 operating systems?
Each correct answer represents a complete solution. Choose all that apply.
A. NTFS4
B. CDFS

C. FAT32
D. HPFS
E. NTFS5
Answer: A,B,C,E (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 80
Which of the following NIST RA process steps has the goal to identify the potential threat-sources and compile a threat statement listing the potential threat-sources that are applicable to the IT system being evaluated?
A. Threat Identification
B. Vulnerability Identification
C. Impact Analysis
D. Control Analysis
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 81
You are the Security Consultant and have been hired to check security for a client's network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server.
What should be your highest priority then in checking his network?
A. Vulnerability scanning
B. Setting up IDS
C. Port scanning
D. Setting up a honey pot
Answer: A (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 82
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?
A. FAU
B. Galleta
C. Device Seizure
D. FTK Imager
Answer: (SHOW ANSWER)

NEW QUESTION: 83
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?
A. Windows XP
B. Linux
C. MINIX 3
D. Mac OS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following needs to be documented to preserve evidences for presentation in court?
A. Separation of duties
B. Incident response policy
C. Chain of custody
D. Account lockout policy
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 85
You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.
What is the most likely cause?
A. The cable that connects the server to the switch is broken.
B. Automatic IP addressing is not working.
C. The switch device is not working.
D. The server is configured with unspecified IP address.
E. The server's NIC is not working.
Answer: (SHOW ANSWER)
Section: Volume A
Explanation

NEW QUESTION: 86

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?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces

B. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

D. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

Answer: D (LEAVE A REPLY)

Section: Volume A

NEW QUESTION: 87

Which of the following files contains the salted passwords in the Linux operating system?

A. /etc/shadow

B. /bin/passwd

C. /bin/shadow

D. /etc/passwd

Answer: A (LEAVE A REPLY)

NEW QUESTION: 88

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

A. Fingerprinting

B. Eavesdropping

C. TCP FTP proxy scanning

D. Web ripping

Answer: D (LEAVE A REPLY)

NEW QUESTION: 89

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be

ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?
A. Red Hat
B. Knoppix
C. Solaris
D. Windows
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?
A. Innocent Images National Imitative (IINI)
B. Anti-Child Porn.org
C. Project Safe Childhood (PSC)
D. Internet Crimes Against Children (ICAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following statements about the HKEY_LOCAL_MACHINE registry hive is true?
A. It contains the user profile for the user who is currently logged on to the computer.
B. 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.
C. It contains configuration data for the current hardware profile.
D. It contains data that associates file types with programs and configuration data for COM objects, Visual Basic programs, or other automation.
Answer: B (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 92
Which of the following file systems contains hardware settings of a Linux computer?
A. /proc

B. /home
C. /etc
D. /var
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?
A. Request for service, initial analysis, data collection, data analysis, data reporting
B. Initial analysis, request for service, data collection, data reporting, data analysis
C. Request for service, initial analysis, data collection, data reporting, data analysis
D. Initial analysis, request for service, data collection, data analysis, data reporting
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?
A. Digital certificates
B. Public key
C. Twofish
D. RSA
Answer: (SHOW ANSWER)

NEW QUESTION: 95
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?
A. White Hat
B. Black Hat
C. Gray Hat
D. Security providing organizations
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 96
Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?
A. Encouraging others to harass the victim
B. False accusations
C. False victimization
D. Attempts to gather information about the victim

Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
Adam works as a professional Computer Hacking Forensic Investigator, a project has been assigned to him to investigate and examine files present on suspect's computer. Adam uses a tool with the help of which he can examine recovered deleted files, fragmented files, and other corrupted data. He can also examine the data, which was captured from the network, and access the physical RAM, and any processes running in virtual memory with the help of this tool. Which of the following tools is Adam using?
A. HxD
B. Vedit
C. WinHex
D. Evidor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate and examine drive image of a compromised system, which is suspected to be used in cyber crime. Adam uses Forensic Sorter to sort the contents of hard drive in different categories. Which of the following type of image formats is NOT supported by Forensic Sorter?
A. RAW image file
B. PFR image file
C. EnCase image file
D. iso image file
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following are advantages of NTFS file system over FAT32 and FAT?
Each correct answer represents a part of the solution. Choose two.
A. Support for file and folder level permissions.
B. Support for audio files.
C. Support for Encrypting File System (EFS).
D. Support for dual-booting.
Answer: A,C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 100
Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

A. PROTECT Act
B. The USA Patriot Act of 2001
C. Sexual Predators Act
D. Civil Rights Act of 1991
Answer: D (LEAVE A REPLY)

NEW QUESTION: 101
You use the FAT16 file system on your Windows 98 computer. You want to upgrade to the FAT32 file system. What is the advantage of the FAT32 file system over FAT16 file system?
Each correct answer represents a complete solution. Choose two.
A. It uses larger cluster sizes.
B. It supports drives up to 2 terabytes (TB) in size.
C. On startup failure, you can start the computer by using an MS-DOS or Windows 95 bootable floppy disk.
D. It allocates disk space more efficiently.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 102
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?
A. 132.298.1.23
B. A3-07-B9-E3-BC-F9
C. F936.28A1.5BCD.DEFA
D. 1011-0011-1010-1110-1100-0001
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 103
Which of the following IP addresses are private addresses?
Each correct answer represents a complete solution. Choose all that apply.
A. 192.166.54.32
B. 19.3.22.17
C. 192.168.15.2
D. 10.0.0.3
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?
A. Anti-Child Porn.org

B. Project Safe Childhood (PSC)
C. Innocent Images National Imitative (IINI)
D. Internet Crimes Against Children (ICAC)
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 105
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?
A. 18 U.S.C. 2701
B. 18 U.S.C. 1030
C. 18 U.S.C. 1362
D. 18 U.S.C. 2510
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 106
You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step for you to take in preserving the chain of custody?
A. Place spyware on the employee's PC to confirm these activities.
B. Make copies of that employee's email.
C. Seize the employee's P
D. Preserve the email server including all logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
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?
A. Donald Dick
B. Back Orifice
C. Qaz
D. Tini
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?
A. False victimization
B. Encouraging others to harass the victim
C. False accusations
D. Attempts to gather information about the victim
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 109
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_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 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?

A. Tini

B. Qaz

C. Donald Dick

D. Back Orifice

Answer: D (LEAVE A REPLY)

Section: Volume C

NEW QUESTION: 110

In which of the following files does the Linux operating system store passwords?

A. SAM

B. Password

C. Passwd

D. Shadow

Answer: D (LEAVE A REPLY)

NEW QUESTION: 111

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

A. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer

B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer

C. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

D. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer

Answer: C (LEAVE A REPLY)

NEW QUESTION: 112

Which of the following Linux file systems is a journaled file system?

A. ext3

B. ext4

C. ext2

D. ext

Answer: A (LEAVE A REPLY)

Section: Volume C

NEW QUESTION: 113

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.
A. You falsely accuse an innocent employee.
B. Your company is unable to pursue the case against a perpetrator.
C. Your company is sued for defaming the character of an accused party.
D. You are charged with criminal acts.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 114
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone.
Which of the following tools is Adam using?
A. Galleta
B. FTK Imager
C. FAU
D. Device Seizure
Answer: D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 115
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?
A. Local or National office of the US secret service
B. Federal Bureau of Investigation
C. Incident response team
D. National Institute of Standards and Technology
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to

image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?
A. Recovery
B. Eradication
C. Identification
D. Containment
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 117
Which of the following file systems is used by both CD and DVD?
A. Universal Disk Format (UDF)
B. Compact Disk File System (CDFS)
C. Network File System (NFS)
D. New Technology File System (NTFS)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following sections of an investigative report covers the background and summary of the report including the outcome of the case and the list of allegations?
A. Section 1
B. Section 3
C. Section 2
D. Section 4
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
Rick works as a Network Administrator for uCertify Inc. He takes a backup of some important compressed files on an NTFS partition, using the Windows 2000 Backup utility. Rick restores these files in a FAT32 partition. He finds that the restored files do not have the compression attribute. What is the most likely cause?
A. A FAT32 partition does not support compression.
B. The FAT32 partition is corrupt and requires to be reformatted.
C. The Windows 2000 Backup utility decompresses compressed files while taking a backup.
D. The backup of files that are saved on an NTFS partition cannot be restored in a FAT32 partition.
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 120

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.
A. Your company is sued for defaming the character of an accused party.
B. You falsely accuse an innocent employee.
C. Your company is unable to pursue the case against a perpetrator.
D. You are charged with criminal acts.
Answer: A,B,C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 121
Which of the following registry hives contains information about all users who have logged on to the system?
A. HKEY_USERS
B. HKEY_CURRENT_USERS
C. HKEY_CURRENT_CONFIG
D. HKEY_CLASSES_ROOT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
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?
A. Title 18, U.S. 1831
B. Title 18, U.S.C. 1832
C. Title 18, U.S.C. 1834
D. Title 18, U.S.C. 1839
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Corroborating

B. Incontrovertible

C. Direct

D. Circumstantial

Answer: D (LEAVE A REPLY)

NEW QUESTION: 124

Which of the following is a file management tool?

A. Defrag

B. MSCONFIG

C. Device Manager

D. Windows Explorer

Answer: (SHOW ANSWER)

Section: Volume A

NEW QUESTION: 125

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. Which of the following commands will John use to display information about all mounted file systems? Each correct answer represents a complete solution. Choose all that apply.

A. df -m

B. df

C. du

D. ls

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 126

Which of the following is a password-cracking program?

A. L0phtcrack

B. NetSphere

C. SubSeven

D. Netcat

Answer: A (LEAVE A REPLY)

NEW QUESTION: 127

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Utility model

B. Copyright

C. Snooping
D. Patent
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?
Each correct answer represents a complete solution. Choose all that apply.
A. All ideas present in the investigative report should flow logically from facts to conclusions.
B. There should not be any assumptions made about any facts while writing the investigative report.
C. Opinion of a lay witness should be included in the investigative report.
D. The investigative report should be understandable by any reader.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 129
You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross- Site Scripting attack on your company's Website. Which of the following methods of investigation can you use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.
A. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.
B. Look at the Web servers logs and normal traffic logging.
C. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.
D. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 130
John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system and wants to install an Intrusion Detection System on the We-are-secure server so that he can receive alerts about any hacking attempts. Which of the following tools can John use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.
A. Snort
B. Tripwire
C. SARA

D. Samhain
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 131
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network.
John is working as a root user on the Linux operating system. Which of the following commands will John use to display information about all mounted file systems?
Each correct answer represents a complete solution. Choose all that apply.
A. du
B. ls
C. df
D. df -m
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 132
Which of the following hardware devices prevents broadcasts from crossing over subnets?
A. Bridge
B. Hub
C. Modem
D. Router
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 133
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He receives the following e-mail:


Hello Disney fans,

And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through a unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 13,000 people, 1,300 of the people on the list will receive $5,000, and the rest will receive a free trip for two to Disney World for one week during the summer of 1999 at our expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 13,000 people.

Your friends,
Walt Disney Jr., Disney, Bill Gates
& The Microsoft Development Team

The e-mail that John has received is an example of _____.
A. Virus hoaxes
B. Social engineering attacks
C. Spambots
D. Chain letters
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following articles defines illegal access to the computer or network in Chapter 2 of Section 1, i.e., Substantive criminal law of the Convention on Cybercrime passed by the Council of Europe?
A. Article 16
B. Article 3
C. Article 2
D. Article 5
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following commands can you use to create an ext3 file system?
Each correct answer represents a complete solution. Choose two.
A. mke2fs
B. mkfs.ext3
C. mke2fs -j
D. mkfs.ext2
Answer: B,C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 136
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?
A. Recovery
B. Containment
C. Identification
D. Eradication
Answer: (SHOW ANSWER)

NEW QUESTION: 137
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?
A. Local or National office of the US secret service
B. Federal Bureau of Investigation
C. Incident response team
D. National Institute of Standards and Technology
Answer: A (LEAVE A REPLY)

NEW QUESTION: 138
Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?
A. Chain of custody
B. Evidence access policy
C. Chain of evidence
D. Incident response policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139
Joseph works as a Web Designer for WebTech Inc. He creates a Web site and wants to protect it from lawsuits. Which of the following steps will he take to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.
A. Restrict customers according to their locations.
B. Restrict shipping in certain areas.
C. Restrict the transfer of information.
D. Restrict the access to the site.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 140
You work as a Network Administrator for Perfect Solutions Inc. You have to install Windows 2000 on a computer that will work as a file server. You have to format the hard disk of the computer, using a file system that supports encryption. Which of the following file systems will you use to accomplish this?
A. NTFS
B. FAT32

C. HPFS
D. FAT16
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 141
You want to retrieve information whether your system is in promiscuous mode or not. Which of the following commands will you use?
Each correct answer represents a complete solution. Choose all that apply.
A. ip link
B. show promisc
C. grep Promisc /var/log/messages
D. ifconfig | grep PROMISC
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 142
Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?
A. FAR system
B. WinHex
C. Vedit
D. Device Seizure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
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?
A. Web ripping
B. Social engineering
C. Steganography
D. Email spoofing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
You work as a Network Administrator for Net World International. Rick, a Sales Manager, complains that his Windows 98 computer is not displaying the taskbar. You reboot his computer and find that the taskbar is still missing. How will you resolve the issue?

A. Reinstall Windows 98 on Rick's computer.
B. Replace WIN.INI from backup.
C. Copy the registry from backup.
D. Use Registry Editor to delete the following registry key:
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorerStuckRects
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Your Windows XP hard drive has 2 partitions. The system partition is NTFS and the other is FAT. You wish to encrypt a folder created on the system partition for the purpose of data security. Which of the following statements is true about this situation?
A. Since the operating system is on the NTFS partition, you can encrypt files on both.
B. You can only encrypt files on the FAT partition.
C. You cannot encrypt files on either partition.
D. You can only encrypt files on the NTFS partition.
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which of the following statements best describes the consequences of the disaster recovery plan test?
A. If no deficiencies were found during the test, then the plan is probably perfect.
B. The results of the test should be kept secret.
C. The plan should not be changed no matter what the results of the test would be.
D. If no deficiencies were found during the test, then the test was probably flawed.
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 147
You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:

What is the IP address of the sender of this email?

A. 209.191.91.180

B. 141.1.1.1

C. 216.168.54.25

D. 172.16.10.90

Answer: (SHOW ANSWER)

NEW QUESTION: 148

Sandra, an expert computer user, hears five beeps while booting her computer that has AMI BIOS; and after that her computer stops responding. Sandra knows that during booting process POST produces different beep codes for different types of errors. Which of the following errors refers to this POST beep code?

A. Processor failure

B. Cache memory test failed

C. Mother board timer not operational

D. Display memory error

Answer: (SHOW ANSWER)

NEW QUESTION: 149

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?

A. Mail Pass View

B. MessenPass
C. Asterisk Logger
D. Access PassView
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 150
You work as a Network Administrator for Web World Inc. You want to host an e-commerce Web site on your network. You want to ensure that storage of credit card information is secure. Which of the following conditions should be met to accomplish this?
Each correct answer represents a complete solution. Choose all that apply.
A. The NTFS file system should be implemented on a client computer.
B. Strong encryption software should be used to store credit card information.
C. NT authentication should be required for all customers before they provide their credit card numbers.
D. Only authorized access should be allowed to credit card information.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which of the following steps are generally followed in computer forensic examinations?
Each correct answer represents a complete solution. Choose three.
A. Analyze
B. Authenticate
C. Encrypt
D. Acquire
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 152
Which of the following tools in Helix Windows Live is used to reveal the database password of password protected MDB files created using Microsoft Access or with Jet Database Engine?
A. Asterisk logger
B. FAU

C. Galleta
D. Access Pass View
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 153
By gaining full control of router, hackers often acquire full control of the network. Which of the following methods are commonly used to attack Routers?
Each correct answer represents a complete solution. Choose all that apply.
A. By launching Social Engineering attack
B. By launching Max Age attack
C. Route table poisoning
D. By launching Sequence++ attack
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 154
Which of the following switches of the XCOPY command copies attributes while copying files?
A. /o
B. /p
C. /k
D. /s
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 155
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we- are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?
A. Web ripping
B. TCP FTP proxy scanning
C. Fingerprinting
D. Eavesdropping
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 156
You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to query an image root device and RAM disk size. Which of the following Unix commands can you use to accomplish the task?

A. rdump
B. setfdprm
C. rdev
D. mount
Answer: (SHOW ANSWER)

NEW QUESTION: 157
Adam works as a professional Computer Hacking Forensic Investigator with the local police of his area. A project has been assigned to him to investigate a PDA seized from a local drug dealer. It is expected that many valuable and important information are stored in this PDA. Adam follows investigative methods, which are required to perform in a pre-defined sequential manner for the successful forensic investigation of the PDA. Which of the following is the correct order to perform forensic investigation of PDA?
A. Examination, Identification, Collection, Documentation
B. Examination, Collection, Identification, Documentation
C. Identification, Collection, Examination, Documentation
D. Documentation, Examination, Identification, Collection
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Mark is taking a data backup during non-working hours from a remote computer on the network by using the Backup utility. What will he do to ensure that the backup has no errors?
A. Log off all the users from the network.
B. Verify the backup.
C. Take an incremental backup.
D. Take a full backup.
Answer: (SHOW ANSWER)

NEW QUESTION: 159
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?
A. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
C. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
D. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
Answer: (SHOW ANSWER)

NEW QUESTION: 160

Which of the following wireless network standards operates on the 5 GHz band and transfers data at a rate of 54 Mbps?

A. 802.11a

B. 802.11g

C. 802.11u

D. 802.11b

Answer: A (LEAVE A REPLY)

NEW QUESTION: 161

Which of the following uses hard disk drive space to provide extra memory for a computer?

A. File system

B. RAM

C. Virtual memory

D. Cluster

Answer: (SHOW ANSWER)

NEW QUESTION: 162

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy

B. User password policy

C. Backup policy

D. Privacy policy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 163

What is the name of the group of blocks which contains information used by the operating system in Linux system?

A. Systemblock

B. logblock

C. Superblock

D. Bootblock

Answer: C (LEAVE A REPLY)

NEW QUESTION: 164

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?

A. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 165
Which of the following Windows Registry key contains the password file of the user?
A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIG
C. HKEY_DYN_DATA
D. HKEY_USER
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
Which of the following standard technologies is not used to interface hard disk with the computer?
A. USB
B. SCSI
C. IDE/ATA
D. PS/2
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 167
Which of the following Windows Registry key contains the password file of the user?
A. HKEY_CURRENT_CONFIG
B. HKEY_DYN_DATA
C. HKEY_USER
D. HKEY_LOCAL_MACHINE
Answer: D (LEAVE A REPLY)

NEW QUESTION: 168

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to set the hard disk geometry parameters, cylinders, heads, and sectors. Which of the following Unix commands can you use to accomplish the task?

A. mkswap

B. hdparm

C. mkfs

D. mke2fs

Answer: (SHOW ANSWER)

NEW QUESTION: 169

Which of the following is a password-cracking program?

A. NetSphere

B. SubSeven

C. L0phtcrack

D. Netcat

Answer: C (LEAVE A REPLY)

NEW QUESTION: 170

Which of the following is NOT an example of passive footprinting?

A. Analyzing job requirements.

B. Performing the whois query.

C. Querying the search engine.

D. Scanning ports.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 171

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate computer of an unfaithful employee of SecureEnet Inc. Suspect's computer runs on Windows operating system. Which of the following sources will Adam investigate on a Windows host to collect the electronic evidences?

Each correct answer represents a complete solution. Choose all that apply.

A. Swap files

B. Unused and hidden partition

C. Slack spaces

D. Allocated cluster

Answer: A,B,C (LEAVE A REPLY)

Section: Volume C

NEW QUESTION: 172

Which of the following statements about an extended partition are true?

Each correct answer represents a complete solution. Choose two.

A. It cannot contain more than one logical drive.
B. It cannot be formatted or assigned a drive letter.
C. A maximum of four extended partitions can exist on a single basic disk.
D. It can be sub-divided into logical drives.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following is used to authenticate asymmetric keys?
A. Demilitarized zone (DMZ)
B. Digital signature
C. MAC Address
D. Password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
Which of the following tools can be used to perform a whois query?
Each correct answer represents a complete solution. Choose all that apply.
A. Sam Spade
B. WsPingPro
C. Traceroute
D. SuperScan
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 175
Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?
A. Melissa
B. Brain
C. I love you
D. Tequila
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate the DoS attack on a computer network of SecureEnet Inc. Which of the following methods will you perform to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.
A. Seize all computers and transfer them to the Forensic lab.
B. Look for unusual traffic on Internet connections and network segments.
C. Look for core files or crash dumps on the affected systems.
D. Sniff network traffic to the failing machine.

Answer: (SHOW ANSWER)

NEW QUESTION: 177
Which of the following file systems supports the hot fixing feature?
A. FAT16
B. NTFS
C. FAT32
D. exFAT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
Which of the following directories contains administrative commands on a UNIX computer?
A. /sbin
B. /export
C. /usr/local
D. /bin
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which of the following steps should be performed in order to optimize a system performance? Each correct answer represents a complete solution. Choose three.
A. Run anti-spyware program regularly
B. Defragment the hard disk drive
C. Edit registry regularly
D. Delete the temporary files
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 180
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?
A. N
B. D
C. C
D. Z
Answer: A (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 181
Which of the following statements about the HKEY_LOCAL_MACHINE registry hive is true?

A. 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.
B. It contains configuration data for the current hardware profile.
C. It contains the user profile for the user who is currently logged on to the computer.
D. It contains data that associates file types with programs and configuration data for COM objects, Visual Basic programs, or other automation.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
In Linux, which of the following files describes the processes that are started up during boot up?
A. /etc/passwd
B. /etc/profile
C. /etc/inittab
D. /etc/shadow
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 183
Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?
A. Wiretap Act
B. Computer Fraud and Abuse Act
C. Economic Espionage Act of 1996
D. Electronic Communications Privacy Act of 1986
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 184
Which of the following protocols allows computers on different operating systems to share files and disk storage?
A. Domain Name System (DNS)

B. Simple Network Management Protocol (SNMP)
C. Network File System (NFS)
D. Trivial File Transfer Protocol (TFTP)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 185
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?
A. To prove that the data belongs to the company.
B. To present the evidences before the court.
C. To prove that the information has a value.
D. To submit investigative report to senior officials.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
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.
A. Windows NT file system (NTFS)
B. High Performance File System (HPFS)
C. Compact Disc File System (CDFS)
D. Novell Storage Services (NSS)
E. Log-structured file system (LFS)
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.
A. Routers act as protocol translators and bind dissimilar networks.
B. Routers do not limit physical broadcast traffic.
C. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.
D. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 188
Which of the following types of attack can guess a hashed password?

A. Evasion attack
B. Teardrop attack
C. Brute force attack
D. Denial of Service attack
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Adrian, the Network Administrator for Peach Tree Inc., wants to install a new computer on the company's network. He asks his assistant to make a boot disk with minimum files. The boot disk will be used to boot the computer, which does not have an operating system installed, yet. Which of the following files will he include on the disk?
A. IO.SYS, MSDOS.SYS, COMMAND.COM, and AUTOEXEC.BAT.
B. IO.SYS, MSDOS.SYS, COMMAND.COM, and FDISK.
C. IO.SYS, MSDOS.SYS, COMMAND.COM, and CONFIG.SYS.
D. IO.SYS, MSDOS.SYS, and COMMAND.COM.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 190
Which of the following tools is used to modify registry permissions in Windows?
A. POLEDIT
B. REGEDIT
C. REGEDT32
D. SECEDIT
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 191
On your dual booting computer, you want to set Windows 98 as the default operating system at startup. In which file will you define this?
A. NTBOOTDD.SYS
B. BOOT.INI
C. NTDETECT.COM
D. BOOTSECT.DOS
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 192
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?
A. Trademark laws

B. Code Security law
C. Patent laws
D. Copyright laws
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 193
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?
A. Fpipe
B. PsList
C. PsExec
D. Cain
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
SIMULATION
Fill in the blank with the appropriate file system.
Alternate Data Streams (ADS) is a feature of the_____ file system, which allows more than one data stream to be associated with a filename.
Answer:
NTFS

NEW QUESTION: 195
You work as a Network Administrator for Net World International. You want to configure a Windows 2000 computer to dual boot with Windows 98. The hard disk drive of the computer will be configured as a single partition drive. Which of the following file systems will you use to accomplish this?
A. HPFS
B. NTFS
C. FAT16
D. FAT32
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following tools are used for footprinting?
Each correct answer represents a complete solution. Choose all that apply.
A. Traceroute
B. Brutus

C. Sam spade
D. Whois
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 197
Which of the following methods can be used to start the Disk Defragmenter utility in Windows 9x? Each correct answer represents a complete solution. Choose two.
A. From Start menu > Programs, click Disk Defragmenter.
B. From Start menu > Programs > Windows Explorer, right-click on the drive to be defragmented > click Properties in the popup menu > Tools tab, then click the Defragment Now button.
C. From Start menu > Programs > Windows Explorer, right-click on the drive to be defragmented, then click the Disk Defragmenter in the popup window.
D. From Start menu > Programs > Accessories > System Tools, click Disk Defragmenter.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 198
Which of the following uses hard disk drive space to provide extra memory for a computer?
A. Virtual memory
B. File system
C. Cluster
D. RAM
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 199
Which of the following Windows XP system files handles memory management, I/O operations, and interrupts?
A. Ntoskrnl.exe
B. Win32k.sys
C. Advapi32.dll
D. Kernel32.dll
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
Which of the following files contains the salted passwords in the Linux operating system?
A. /bin/shadow
B. /bin/passwd
C. /etc/passwd
D. /etc/shadow
Answer: (SHOW ANSWER)

NEW QUESTION: 201
Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.
A. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.
B. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.
C. Routers do not limit physical broadcast traffic.
D. Routers act as protocol translators and bind dissimilar networks.
Answer: A,B,D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 202
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?
A. Shoulder surfing
B. File integrity auditing
C. Spoofing
D. Reconnaissance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203
Which of the following types of computers is used for attracting potential intruders?
A. Bastion host
B. Honey pot
C. Files pot
D. Data pot
Answer: (SHOW ANSWER)

NEW QUESTION: 204

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?

A. debugfs

B. du

C. dosfsck

D. df

Answer: (SHOW ANSWER)

NEW QUESTION: 205

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to forward all the kernel messages to the remote host having IP address 192.168.0.1. Which of the following changes will he perform in the syslog.conf file to accomplish the task?

A. kern.* @192.168.0.1

B. !kern.* @192.168.0.1

C. *.* @192.168.0.1

D. !*.* @192.168.0.1

Answer: A (LEAVE A REPLY)

NEW QUESTION: 206

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?

A. /mnt

B. /lib

C. /tmp

D. /sbin

Answer: D (LEAVE A REPLY)

NEW QUESTION: 207

Which of the following are the primary goals of the incident handling team?

Each correct answer represents a complete solution. Choose all that apply.

A. Prevent any further damage.

B. Inform higher authorities.

C. Freeze the scene.

D. Repair any damage caused by an incident.

Answer: (SHOW ANSWER)

NEW QUESTION: 208
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?
A. /data/var
B. /private/var
C. /var/data
D. /var/private
Answer: B (LEAVE A REPLY)

NEW QUESTION: 209
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.
A. ipconfig
B. whois
C. .cab extractors
D. netstat
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 210
Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?
A. Twofish
B. Digital certificates
C. Public key
D. RSA
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 211
Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?
A. Technical representative
B. Information security representative
C. Legal representative
D. Lead investigator
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 212

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He traceroutes the We-are-secure server and gets the following result:

Considering the above traceroute result, which of the following statements can be true? Each correct answer represents a complete solution. Choose all that apply.

A. While tracerouting, John's network connection has become slow.

B. Some router along the path is down.

C. The We-are-secure server is using a packet filtering firewall.

D. The IP address of the We-are-secure server is not valid.

Answer: A,B,C (LEAVE A REPLY)

Section: Volume B

NEW QUESTION: 213

Which of the following switches of the XCOPY command copies file ownerships and NTFS permissions on files while copying the files?

A. /o

B. /r

C. /p

D. /s

Answer: (SHOW ANSWER)

NEW QUESTION: 214

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?

A. DES

B. SHA

C. MD5

D. LANMAN

Answer: D (LEAVE A REPLY)

NEW QUESTION: 215

By gaining full control of router, hackers often acquire full control of the network. Which of the following methods are commonly used to attack Routers?

Each correct answer represents a complete solution. Choose all that apply.

A. By launching Social Engineering attack

B. By launching Max Age attack

C. By launching Sequence++ attack

D. Route table poisoning

Answer: (SHOW ANSWER)

NEW QUESTION: 216

Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

A. Device Seizure

B. Forensic Sorter

C. DriveSpy

D. Ontrack

Answer: (SHOW ANSWER)

NEW QUESTION: 217

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Eradication phase

B. Preparation phase

C. Identification phase

D. Recovery phase

E. Containment phase

Answer: B (LEAVE A REPLY)

NEW QUESTION: 218

Which of the following commands is used to enforce checking of a file system even if the file system seems to be clean?

A. e2fsck -f
B. e2fsck -p
C. e2fsck -b
D. e2fsck -c
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 219
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.
A. .xst
B. .txt
C. .ost
D. .pst
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 220
Which of the following attacks saturates network resources and disrupts services to a specific computer?
A. Polymorphic shell code attack
B. Replay attack
C. Teardrop attack
D. Denial-of-Service (DoS) attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 221
In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?
A. Access Control List (ACL)
B. Discretionary Access Control (DAC)
C. Role Based Access Control (RBAC)
D. Mandatory Access Control (MAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 222
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. While performing some security investigation, you want to see the hostname and IP address from where users logged in. Which of the following commands will you use to accomplish the task?

A. Nslookup
B. Dig
C. Netstat
D. Last
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
Which of the following steps are generally followed in computer forensic examinations?
Each correct answer represents a complete solution. Choose three.
A. Encrypt
B. Acquire
C. Authenticate
D. Analyze
Answer: B,C,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 224
You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step for you to take in preserving the chain of custody?
A. Seize the employee's PC.
B. Place spyware on the employee's PC to confirm these activities.
C. Preserve the email server including all logs.
D. Make copies of that employee's email.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
Which of the following uses hard disk drive space to provide extra memory for a computer?
A. Virtual memory
B. Cluster
C. RAM
D. File system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 226
Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property. The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN

network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge. The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.
Which of the following actions can Adam perform to prevent such attacks from occurring in future?
A. Apply different security policy to make passwords of employees more complex.
B. Disable VPN access to all employees of the company from home machines
C. Allow VPN access but replace the standard authentication with biometric authentication.
D. Replace the VPN access with dial-up modem access to the company's network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 227
Convention on Cybercrime, created by the Council of Europe, is the treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Which of the following chapters of Convention of Cybercrime contains the provisions for mutual assistances and extradition rules related to cybercrimes?
A. Chapter I
B. Chapter III
C. Chapter IV
D. Chapter II
Answer: B (LEAVE A REPLY)

NEW QUESTION: 228
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.

A. nc 208.100.2.25 23
B. nmap -v -O www.we-are-secure.com
C. nc -v -n 208.100.2.25 80
D. nmap -v -O 208.100.2.25
Answer: B,D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 229
Which of the following encryption methods use the RC4 technology?
Each correct answer represents a complete solution. Choose all that apply.
A. CCMP
B. Static WEP
C. Dynamic WEP
D. TKIP
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 230
You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to set the hard disk geometry parameters, cylinders, heads, and sectors. Which of the following Unix commands can you use to accomplish the task?
A. mkfs
B. mkswap
C. hdparm
D. mke2fs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 231
You work as a Network Administrator for uCertify Inc. You want to edit the MSDOS.SYS file, in your computer, from the DOS prompt. You are unable to find the file. What is the most likely cause?
A. It is a read-only file.
B. It is a built-in command in the COMMAND.COM file.
C. Someone has deleted the file.
D. It is a hidden file.
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 232
Which of the following are the benefits of information classification for an organization?
Each correct answer represents a complete solution. Choose two.
A. It helps identify which information is the most sensitive or vital to an organization.

B. It ensures that modifications are not made to data by unauthorized personnel or processes.
C. It helps reduce the Total Cost of Ownership (TCO).
D. It helps identify which protections apply to which information.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 233
Which of the following is a nonvolatile form of memory that can be reprogrammed by using a special programming device, and need not to be removed from the PC to be reprogrammed?
A. PROM
B. EEPROM
C. EPROM
D. SRAM
E. DRAM
Answer: (SHOW ANSWER)

NEW QUESTION: 234
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?
A. Shoulder surfing
B. File integrity auditing
C. Reconnaissance
D. Spoofing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 235
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?
A. The Sticky bit is set, but other users have no execute permission.
B. The SUID bit is set, but the owner has no execute permission.
C. The Sticky bit is set and other users have the execute permission.
D. The SGID bit is set, but the group execute permission is not set.
Answer: (SHOW ANSWER)

NEW QUESTION: 236
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare- secure.com. He is working on the Linux operating system. He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?
A. Hunt

B. Tripwire
C. IPChains
D. Ethercap
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Which of the following commands is used to create or delete partitions on Windows XP?
A. Part
B. fdisk
C. Active
D. DISKPART
Answer: D (LEAVE A REPLY)

NEW QUESTION: 238
The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement?
Each correct answer represents a complete solution. Choose all that apply.
A. Information dissemination policy
B. Electronic monitoring statement
C. Incident response plan
D. Additional personnel security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 239
Rick works as a Network Administrator for uCertify Inc. He takes a backup of some important compressed files on an NTFS partition, using the Windows 2000 Backup utility. Rick restores these files in a FAT32 partition. He finds that the restored files do not have the compression attribute. What is the most likely cause?
A. The backup of files that are saved on an NTFS partition cannot be restored in a FAT32 partition.
B. A FAT32 partition does not support compression.
C. The FAT32 partition is corrupt and requires to be reformatted.
D. The Windows 2000 Backup utility decompresses compressed files while taking a backup.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 240
Which of the following parameters is NOT used for calculating the capacity of the hard disk?
A. Bytes per sector
B. Number of heads
C. Total number of sectors

D. Number of platters
Answer: D (LEAVE A REPLY)
Section: Volume A
Explanation/Reference:

NEW QUESTION: 241
You work as a Network Administrator for McNeel Inc. You want to encrypt each user's MY DOCUMENTS folder. You decide to use Encrypting File System (EFS). You plan to write a script for encryption. Which of the following tools will you use to encrypt specified folders?
A. Windows Explorer
B. EFSINFO
C. CIPHER
D. SYSKEY
Answer: C (LEAVE A REPLY)

Valid GCFA Dumps shared by BraindumpsPass.com for Helping Passing GCFA Exam! BraindumpsPass.com now offer the **newest GCFA exam dumps**, the BraindumpsPass.com GCFA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com GCFA dumps with Test Engine here: https://www.braindumpspass.com/GIAC/GCFA-practice-exam-dumps.html (**318** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)