EC-COUNCIL.312-49v9.v2022-11-21.q338

Exam Code:	312-49v9
Exam Name:	ECCouncil Computer Hacking Forensic Investigator (V9)
Certification Provider:	EC-COUNCIL
Free Question Number:	338
Version:	v2022-11-21
# of views:	3361
# of Questions views:	3380
https://www.freepdfdumps.com/EC-COUNCIL.312-49v9.v2022-11-21.q338.html	

NEW QUESTION: 1
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?
A. Resource Manager
B. Surface Manager
C. Application Framework
D. Media Framework
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
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. 203.218.39.50
B. 137.189.96.52
C. 203.218.39.20
D. 8.12.1.0
Answer: (SHOW ANSWER)

NEW QUESTION: 3

Which one of the following is not a first response procedure?

A. Fill forms

B. Crack passwords

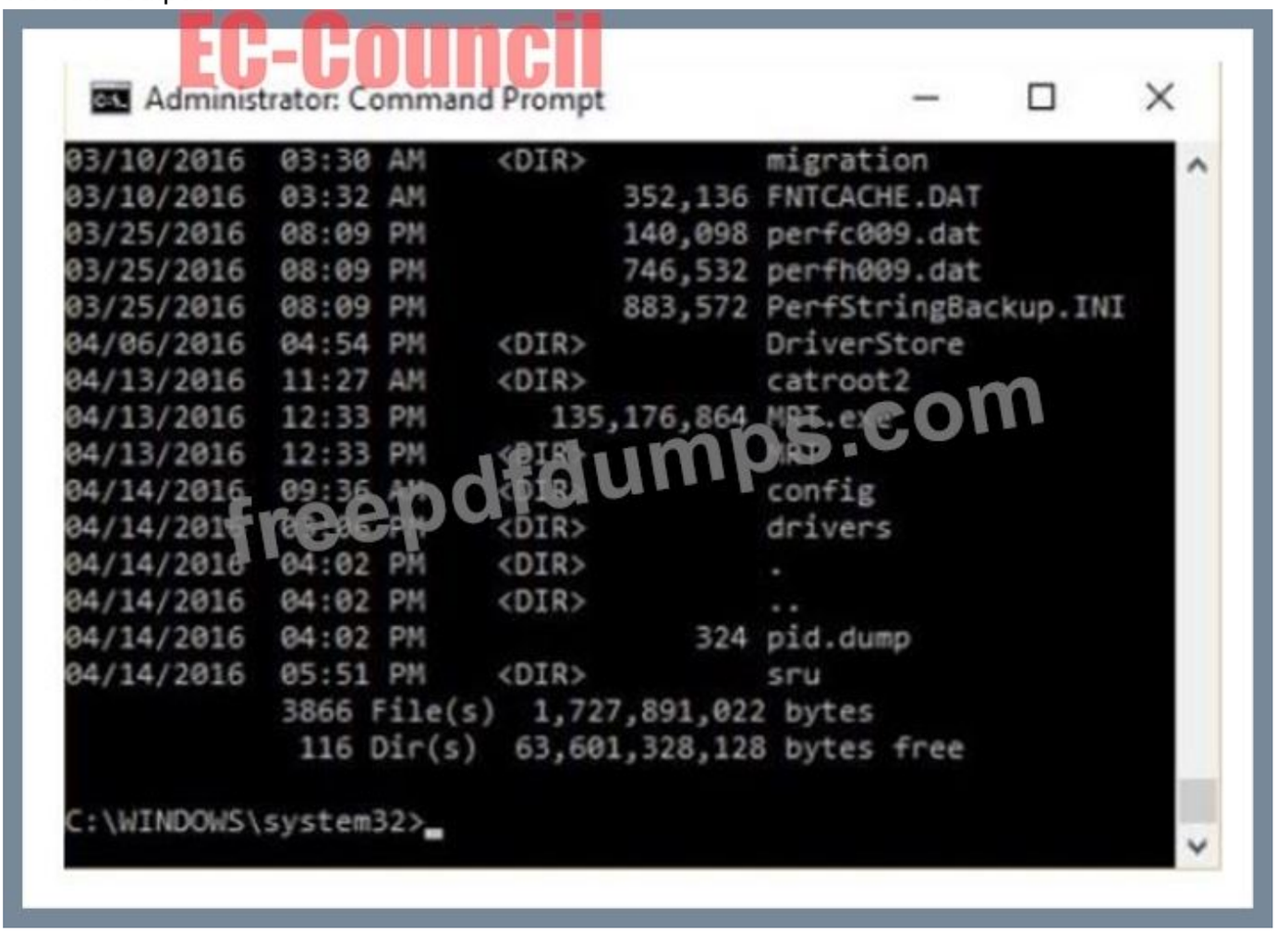
C. Preserve volatile data

D. Take photos

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

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:e

B. dir /o:s

C. dir /o:d

D. dir /o:n

Answer: (SHOW ANSWER)

NEW QUESTION: 5

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

A. Recover the evidence

B. Trace the IP address to its origin
C. Write a report
D. Determine whether a crime was actually committed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
What is one method of bypassing a system BIOS password?
A. Remove all the system memory
B. Removing the processor
C. Removing the CMOS battery
D. Login to Windows and disable the BIOS password
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?
A. Cross-platform correlation
B. Multiple-platform correlation
C. Same-platform correlation
D. Network-platform correlation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following stand true for BIOS Parameter Block?
A. The BIOS Partition Block always refers to the 512-byte boot sector
B. The BIOS Partition Block describes the physical layout of a data storage volume
C. The length of BIOS Partition Block remains the same across all the file systems
D. The BIOS Partition Block is the first sector of a data storage device
Answer: B (LEAVE A REPLY)

NEW QUESTION: 9
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?
A. Complete event analysis
B. End-to-end
C. Point-to-point
D. Thorough
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

C. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: (SHOW ANSWER)

NEW QUESTION: 11

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 those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?

A. Recuva

B. Xplico

C. Cain & Abel

D. Colasoft's Capsa

Answer: B (LEAVE A REPLY)

NEW QUESTION: 12

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89

44 represent?

A. Issuer Identifier Number and TAC

B. TAC and Industry Identifier

C. Industry Identifier and Country code

D. Individual Account Identification Number and Country Code

Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?
A. UTC
B. Time Protocol
C. PTP
D. NTP
Answer: (SHOW ANSWER)

NEW QUESTION: 14
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
A. Legal issues
B. Judging the character of defendants/victims
C. No particular field
D. Technical material related to forensics
Answer: C (LEAVE A REPLY)

NEW QUESTION: 15
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?
A. Physical
B. Data Link
C. Transport
D. Network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?
A. Netspionage
B. Spycrack
C. Hackspionage
D. Spynet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
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. Fill the disk with 4096 zeros
B. Low-level format
C. Copy files from the master disk to the slave disk on the secondary IDE controller
D. Fill the disk with zeros
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?
A. forensic duplication of hard drive
B. analysis of volatile data
C. comparison of MD5 checksums
D. review of SIDs in the Registry
Answer: (SHOW ANSWER)
Not MD5: MD5 checksums are used as integrity checks
User accounts are assigned a unique SID, and the SID are not reused.

NEW QUESTION: 19
When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?
A. Lsproc
B. DumpChk
C. EProcess
D. RegEdit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?
A. Rooting iPhone
B. Bypassing iPhone passcode
C. Copying contents of iPhone
D. Debugging iPhone
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves _____and waiting for responses from available wireless networks.
A. Scanning the network
B. Sniffing the packets from the airwave
C. Broadcasting a probe request frame
D. Inspecting WLAN and surrounding networks
Answer: (SHOW ANSWER)

NEW QUESTION: 23
During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?
A. C:\Exchsrvr\Message Tracking\servername.log
B. C:\Program Files\Microsoft Exchange\srvr\servername.log
C. C:\Program Files\Exchsrvr\servername.log
D. D:\Exchsrvr\Message Tracking\servername.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
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, to cause a denial-of-service attack?
A. Mail bombing
B. Email spoofing
C. Phishing
D. Email spamming
Answer: (SHOW ANSWER)

NEW QUESTION: 25
To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?
A. Reporting Phase
B. Pre-investigation Phase
C. Post-investigation Phase
D. Investigation Phase
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?
A. Model.lgf
B. Model.txt
C. Model.log
D. Model.ldf
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
%3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?
A. Base64
B. Unicode
C. Double encoding
D. Hex encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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 footer
B. the file header
C. the File Allocation Table
D. the sector map
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle
B. Smurf scan
C. SYN flood
D. Teardrop
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
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. Hard Drive Failure
C. Overzealous marketing
D. Unauthorized expenses
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which list contains the most recent actions performed by a Windows User?
A. Windows Error Log
B. Activity
C. MRU
D. Recents
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized access, as well as misuse.
Which of the following intrusion detection systems audit events that occur on a specific host?
A. Network-based intrusion detection
B. Log file monitoring
C. File integrity checking

D. Host-based intrusion detection
Answer: (SHOW ANSWER)

NEW QUESTION: 33
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as ow level? How long will the team have to respond to the incident?the investigation, the CEO informs them that the incident will be classified as ?ow level? How long will the team have to respond to the incident?
A. Immediately
B. One working day
C. Four hours
D. Two working days
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
What feature of Windows is the following command trying to utilize?

A. AFS
B. ADS
C. Slack file
D. White space
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?
A. One working day
B. Four hours
C. Immediately
D. Two working days
Answer: (SHOW ANSWER)

NEW QUESTION: 36

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers

B. Perform a zone transfer

C. Enumerate all the users in the domain

D. Perform DNS poisoning

Answer: B (LEAVE A REPLY)

NEW QUESTION: 37

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 Microsoft Virtual Machine Identifier

C. the Globally Unique ID

D. the Personal Application Protocol

Answer: (SHOW ANSWER)

NEW QUESTION: 38

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

What can the investigator infer from the screenshot seen below?

A. Network intrusion has occurred

B. Buffer overflow attempt on the firewall.
C. A smurf attack has been attempted
D. A denial of service has been attempted
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
Which MySQL log file contains information on server start and stop?
A. General query log file
B. Error log file
C. Binary log
D. Slow query log file
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which US law does the interstate or international transportation and receiving of child pornography fall under?
A. 18 U.S. Code § 2252
B. 18 U.S. Code § 1466A
C. 18 U.S. Code § 252
D. 18 U.S. Code § 146A
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

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

NEW QUESTION: 42
A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:
A. Harden organization network security
B. Take permission from all employees of the organization for investigation
C. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies
D. Create an image backup of the original evidence without tampering with potential evidence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
What does mactime, an essential part of the coroner's toolkit do?
A. It is too specific to the MAC OS and forms a core component of the toolkit
B. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps
C. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them
D. The tools scans for i-node information, which is used by other tools in the tool kit
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?
A. %systemroot%\system32\drivers\etc
B. %systemroot%\repair
C. %systemroot%\LSA
D. %systemroot%\system32\LSA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?
A. AES-CCMP
B. RC4-CCMP
C. AES-TKIP
D. RC4-TKIP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46

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. locate:"logon page"
C. allinurl:"exchange/logon.asp"
D. intitle:"exchange server"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
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 the company 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. Squatting
C. Phreaking
D. Pretexting
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following is NOT an anti-forensics technique?
A. Password Protection
B. Data Deduplication
C. Encryption
D. Steganography
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. All three servers need to face the Internet so that they can communicate between themselves
D. A web server and the database server facing the Internet, an application server on the internal network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?
A. Director of Administration
B. Security Administrator
C. Director of Information Technology
D. Network Administrator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?
A. Key escrow
B. Rootkit
C. Offset
D. Steganography
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?
A. config.db
B. sigstore.db
C. install.db
D. filecache.db
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Create a Separate partition of several hundred megabytes and place the swap file there
B. Use VMware to be able to capture the data in memory and examine it
C. Use intrusion forensic techniques to study memory resident infections
D. Give the Operating System a minimal amount of memory, forcing it to use a swap file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
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. EDoS Attack (Economic Denial of Service)
B. DDoS Attack (Distributed Denial of Service)
C. Man-in-the-cloud Attack
D. XSS Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 55
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. The life of the author plus 70 years
B. The life of the author
C. 70 years
D. Copyrights last forever
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which part of the Windows Registry contains the user's password file?
A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIGURATION
C. HKEY_USER
D. HKEY_CURRENT_USER
Answer: A,D (LEAVE A REPLY)
The answer is HKEY_CURRENT_USER\Identities\{VALUE}
Note the "user's" password file will be user specific, the Local Machine is the machine information

NEW QUESTION: 57
Which of the following statements is TRUE about SQL Server error logs?
A. SQL Server error logs record all the events occurred on the SQL Server and its databases

B. Error logs contain IP address of SQL Server client connections
C. Forensic investigator uses SQL Server Profiler to view error log files
D. Trace files record, user-defined events, and specific system events
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
A. Judging the character of defendants/victims
B. Legal issues
C. Technical material related to forensics
D. No particular field
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?
A. Inverse TCP flag scanning
B. ACK flag scanning
C. IP Fragment Scanning
D. TCP Scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 60
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?
A. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view themThe files are hidden and he must use ? switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which of the following is a MAC-based File Recovery Tool?
A. GetDataBack
B. Smart Undeleter
C. Cisdem DataRecovery 3

D. VirtualLab
Answer: (SHOW ANSWER)

NEW QUESTION: 62
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 called in the FBI without correlating with the fingerprint data
B. They examined the actual evidence on an unrelated system
C. They tampered with evidence by using it
D. They attempted to implicate personnel without proof
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Hard disk data addressing is a method of allotting addresses to each _____of data on a hard disk
A. Hard disk block
B. Logical block
C. Operating system block
D. Physical block
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following should a computer forensics lab used for investigations have?
A. isolation
B. restricted access
C. an entry log
D. open access

Answer: (SHOW ANSWER)

NEW QUESTION: 65
When NTFS Is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code
A. First 22
B. First 24
C. First 12
D. First 16
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
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. deltree command
D. Scandisk utility
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?
A. Slack Space
B. Virtual Memory
C. Sparse files
D. ESE Database
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?
A. NIPS

B. Active IDS
C. Progressive IDS
D. Passive IDS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
Consider that you are investigating a machine running an Windows OS released prior to Windows Vist a. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>\. You read an entry named "Dd5.exe". What does Dd5.exe mean?
A. D drive, fourth file deleted, a .exe file
B. D drive, fourth file restored, a .exe file
C. D drive. fifth file deleted, a .exe file
D. D drive, sixth file deleted, a .exe file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
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 creates cache files, which 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: 72
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?
A. Visual semagram
B. Text semagram
C. Grill cipher
D. Visual cipher

Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?
A. IOCE
B. SWGDE & SWGIT
C. Daubert
D. Frye
Answer: D (LEAVE A REPLY)

NEW QUESTION: 74
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 a honeypot is not illegal
C. Enticement
D. Entrapment
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which tool does the investigator use to extract artifacts left by Google Drive on the system?
A. RAM Capturer
B. PEBrowse Professional
C. RegScanner
D. Dependency Walker
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
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. LOGINFO2

C. INFO1
D. LOGINFO1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
A. OSPF
B. UDP
C. BPG
D. ATM
Answer: (SHOW ANSWER)

NEW QUESTION: 78
What must an investigator do before disconnecting an iPod from any type of computer?
A. Mount the iPod
B. Disjoin the iPod
C. Unmount the iPod
D. Join the iPod
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the
_____.
A. Drive name
B. Original file name
C. Sequential number
D. Original file name's extension
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
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. gwcheck.db
B. PUB.EDB
C. PRIV.STM
D. PRIV.EDB
Answer: (SHOW ANSWER)

NEW QUESTION: 81
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case.
How would you permanently erase the data on the hard disk?
A. Throw the hard disk into the fire
B. Run the powerful magnets over the hard disk
C. Format the hard disk multiple times using a low level disk utility
D. Overwrite the contents of the hard disk with Junk data
Answer: A,C (LEAVE A REPLY)
To be effective with throwing the hard drive into the fire, the fire would have to be hot enough to melt the platters into molten metal, which requires an industrial furnance. This requires special facilities.
Running powerful magnets over the disk, such as degaussing the disk, may destroy the data, but may also be ineffective. In some cases, the degaussing process for tape and disk may render the disk unusable for use again. (of course throwing the drives into a furnance also guarantee that as well).
Formatting the disk multiple times with a low level disk utility is the best way to go, and still beable to re-use the disk for later projects. The keys are "multiple" and "low level". A low level format is typicall a slow, thorough, format that is a wipe. Multiple - as opposed to once - is recommended. There is a theory on "how many times", some schools say at least three times. The problem with this answer is that with newer drives, such as ATA and SCSI, low level formats can destroy the volumes as well, and some BIOS may actually ignore the LLF directives.
Overwritting the disk with junk data would perform some form of wipe because the old data is wiped out, but still may be recoverd.
Note:
According to some websites:
Physical Methods that will not work to destroy data on a hard drive include:Throwing it in the water (this does not do much)Setting it on fire (the temperature is not going to be high enough at home)Throwing it out of the window. Hard drives can take quite a bit of G force.

They are not heavy so the impact of the hard drive on the ground is not likely to destroy the platters.Drive over the hard drive. A car, or even a tank, driving over a hard drive will do nothing, any more than they would driving over a book. Unless the drive is actually flattened, the platters are not going to be destroyed

NEW QUESTION: 82
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:
A. Acquire data from host-protected area on a disk
B. Prevent Contamination to the evidence drive
C. Avoiding copying data from the boot partition
D. Automate Collection from image files
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
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. Cause network congestion
B. Make you an agent of law enforcement
C. Write information to the subject's hard drive
D. Violate your contract
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?
A. Distributed network attack
B. Replay attack
C. Man-in-the-middle (MITM) attack
D. Rainbow attack
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion.

A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
If a suspect computer is located in an area that may have toxic chemicals, you must:
A. determine a way to obtain the suspect computer
B. do not enter alone
C. coordinate with the HAZMAT team
D. assume the suspect machine is contaminated
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?
A. 3 terabytes
B. 1 terabytes
C. 4 terabytes
D. 2 terabytes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
When a router receives an update for its routing table, what is the metric value change to that path?
A. Decreased by 1
B. Increased by 2
C. Decreased by 2
D. Increased by 1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?
A. Information about network connections
B. Status of network hardware
C. Status of users connected to the internet
D. Net status of computer usage
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90

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: 91
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 creates cache files, which would hinder the investigation
C. Searching for evidence themselves would not have any ill effects
D. Searching can change date/time stamps
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?
A. Enumerate all the users in the domain
B. Perform a zone transfer
C. Send DOS commands to crash the DNS servers
D. Perform DNS poisoning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
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. Universal Time Set

B. Network Time Protocol

C. Time-Sync Protocol

D. SyncTime Service

Answer: (SHOW ANSWER)

NEW QUESTION: 94

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. False

B. True

Answer: B (LEAVE A REPLY)

NEW QUESTION: 95

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

A. Password.conf

B. SAM

C. AMS

D. Shadow file

Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

Office Documents (Word, Excel and 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. Globally unique ID

B. Personal Application Protocol

C. Microsoft Virtual Machine Identifier

D. Individual ASCII string

Answer: (SHOW ANSWER)

NEW QUESTION: 97

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____

A. Drive name

B. Original file name

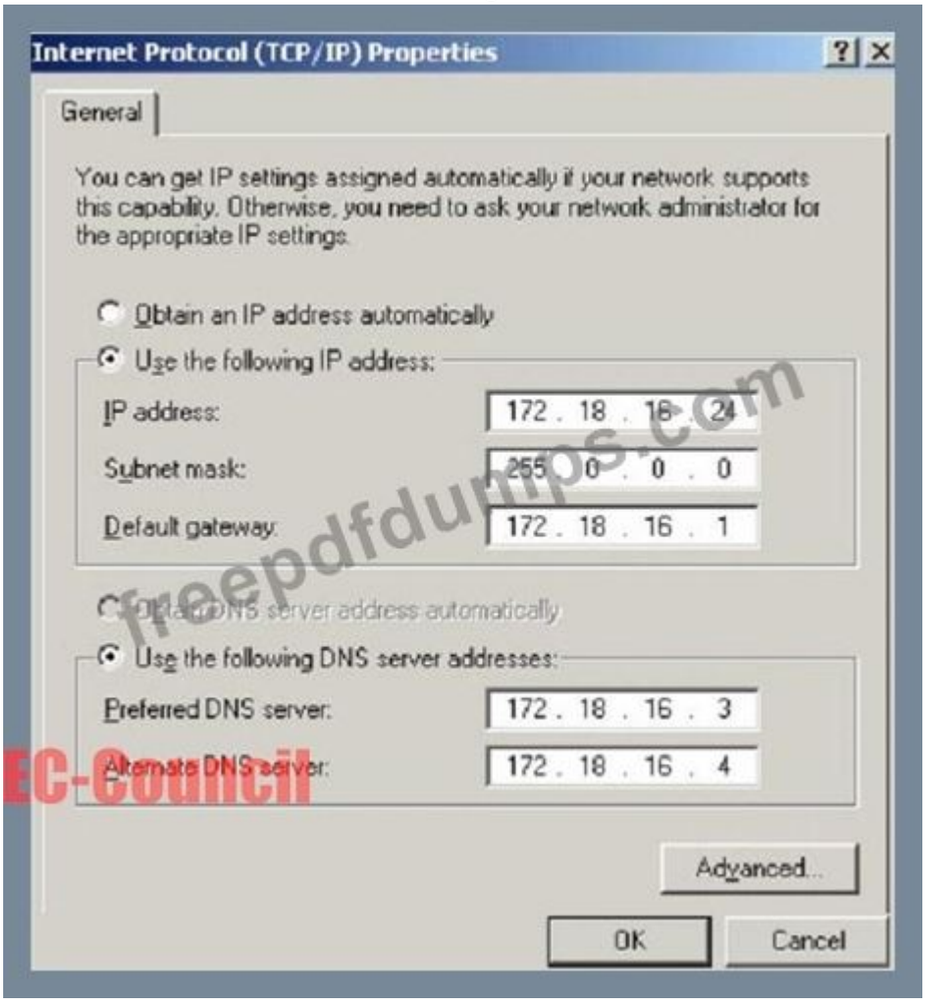
C. Sequential number

D. Original file name's extension

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98

What is the CIDR from the following screenshot?



A. /16 C./16 C./16

B. /32 B./32 B./32

C. /24A./24A./24

D. /8D./8D./8

Answer: D (LEAVE A REPLY)

NEW QUESTION: 99

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 disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum

C. A simple DOS copy will not include deleted files, file slack and other information

D. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence?
A. The American Forensics Laboratory Society (AFLS)
B. The American Forensics Laboratory for Computer Forensics (AFLCF)
C. International Society of Forensics Laboratory (ISFL)
D. The American Society of Crime Laboratory Directors (ASCLD)
Answer: (SHOW ANSWER)

NEW QUESTION: 101
A state department site was recently attacked, and all the servers had their hard disks erased. The incident response team sealed the area and commenced an investigation. During evidence collection, they came across a USB flash drive that did not have the standard labeling on it. The incident team inserted the flash drive into an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they shortlisted possible suspects including three summer interns. Where did the incident team go wrong?
A. They called in the FBI without correlating with the fingerprint data
B. They tampered with the evidence by using it
C. They examined the actual evidence on an unrelated system
D. They attempted to implicate personnel without proof
Answer: (SHOW ANSWER)

NEW QUESTION: 102
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?
A. NTDETECT.COM
B. NTOSKRNL.EXE
C. NTLDR
D. LSASS.EXE
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?
A. Injector
B. Packer
C. Obfuscator

D. Dropper
Answer: (SHOW ANSWER)

NEW QUESTION: 104
A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?
A. / /proc
B. /auth
C. /var/spool/cron/
D. /var/log/debug
Answer: A (LEAVE A REPLY)

NEW QUESTION: 105
E-mail logs contain which of the following information to help you in your investigation? (Choose four.)
A. user account that was used to send the account
B. attachments sent with the e-mail message
C. unique message identifier
D. contents of the e-mail message
E. date and time the message was sent
Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 106
What is the First Step required in preparing a computer for forensics investigation?
A. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination
B. Secure any relevant media
C. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
D. Do not turn the computer off or on, run any programs, or attempt to access data on a computer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
What hashing method is used to password protect Blackberry devices?
A. SHA-1
B. MD5
C. AES
D. RC5
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
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. Session Fixation Attack
B. Cookie Tampering
C. Cross Site Request Forgery
D. Parameter Tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?
A. Point-to-point
B. Thorough
C. Complete event analysis
D. End-to-end
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following standard is based on a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?
A. FERPA standard
B. Daubert Standard
C. Schneiderman Standard
D. Frye Standard
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

A. Every byte of the file(s) is encrypted using three different methods
B. Every byte of the file(s) is copied to three different hard drives
C. Every byte of the file(s) is verified using 32-bit CRC
D. Every byte of the file(s) is given an MD5 hash to match against a master file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 112
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:
A. Scan the suspect hard drive before beginning an investigation
B. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
C. Scan your Forensics workstation before beginning an investigation
D. Never run a scan on your forensics workstation because it could change your systems configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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 10
B. Windows 7
C. Windows 8
D. Windows 8.1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?
A. The wrong partition may be set to active
B. All virtual memory will be deleted
C. The computer will be set in a constant reboot state
D. This action can corrupt the disk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
What does the command "C:\>wevtutil gl <log name>" display?
A. Event log record structure
B. Configuration information of a specific Event Log
C. List of available Event Logs
D. Event logs are saved in .xml format
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
The police believe that Melvin 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 suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?
A. The Good Samaritan Laws
B. The Federal Rules of Evidence
C. The Fourth Amendment
D. The USA patriot Act
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
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. Search for disk errors within an image file
C. Backup a disk to an image file
D. Copy a partition to an image file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
An Expert witness gives an opinion if:
A. To define the issues of the case for determination by the finder of fact
B. To stimulate discussion between the consulting expert and the expert witness
C. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case
D. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119
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. Cain & Abel

B. Xplico
C. Colasoft's Capsa
D. Recuva
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
The MD5 program is used to:
A. view graphics files on an evidence drive
B. verify that a disk is not altered when you examine it
C. make directories on an evidence disk
D. wipe magnetic media before recycling it
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
Why should you note all cable connections for a computer you want to seize as evidence?
A. to know what outside connections existed
B. to know what peripheral devices exist
C. in case other devices were connected
D. to know what hardware existed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
Damaged portions of a disk on which no read/Write operation can be performed is known as _____.
A. Empty sector
B. Unused sector
C. Lost sector
D. Bad sector
Answer: (SHOW ANSWER)

NEW QUESTION: 123

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. Cross site scripting
B. SQL injection
C. Cookie Poisoning
D. Parameter tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 124
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. grep
C. pstree
D. pgrep
Answer: (SHOW ANSWER)

NEW QUESTION: 125
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. ARP redirect
B. Digital attack
C. Denial of service
D. Physical attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
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. Demonstrate that no system can be protected againstDoS attacks
C. Use attack as a launching point to penetrate deeper into the network
D. Show outdatedeQuipment so it can be replaced
Answer: A (LEAVE A REPLY)

NEW QUESTION: 127
Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system or device that holds electronic information.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
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. Lossless compression
B. Lossy compression
C. Lossful compression
D. Time-loss compression
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
Select the data that a virtual memory would store in a Windows-based system.
A. Information or metadata of the files
B. Application data
C. Documents and other files
D. Running processes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
One way to identify the presence of hidden partitions on a suspect's hard drive is to:
A. Examine the LILO and note an H in the partition Type field
B. Add up the total size of all known partitions and compare it to the total size of the hard drive

C. It is not possible to have hidden partitions on a hard drive
D. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
Answer: (SHOW ANSWER)

NEW QUESTION: 131
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
A. Title 18, Section Chapter 90
B. Title 18, Section 2703(d)
C. Title 18, Section 1030
D. Title 18, Section 2703(f)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
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: 133
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 positives
B. False negatives
C. False positives
D. True negatives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
In a Linux-based system, what does the command "Last -F" display?
A. Last run processes
B. Last functions performed

C. Login and logout times and dates of the system
D. Recently opened files
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
Where is the default location for Apache access logs on a Linux computer?
A. usr/local/apache/logs/access_log
B. bin/local/home/apache/logs/access_log
C. usr/logs/access_log
D. logs/usr/apache/access_log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 136
What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?
A. Disk cleaning
B. Disk magnetization
C. Disk deletion
D. Disk degaussing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
Digital evidence is not fragile in nature.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Cisco Discovery Protocol

B. Border Gateway Protocol

C. Broadcast System Protocol

D. Simple Network Management Protocol

Answer: A (LEAVE A REPLY)

NEW QUESTION: 139

File signature analysis involves collecting information from the _____ of a file to determine the type and function of the file

A. First 40 bytes

B. First 20 bytes

C. First 10 bytes

D. First 30 bytes

Answer: B (LEAVE A REPLY)

NEW QUESTION: 140

To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 25

B. 125

C. 143

D. 110

Answer: (SHOW ANSWER)

NEW QUESTION: 141

Which of the following tools will help the investigator to analyze web server logs?

A. LanWhois

B. Deep Log Analyzer

C. XRY LOGICAL

D. Deep Log Monitor

Answer: (SHOW ANSWER)

NEW QUESTION: 142

What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring

B. Host integrity Monitoring

C. System Baselining

D. Start-up Programs Monitoring

Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
The MD5 program is used to:
A. verify that a disk is not altered when you examine it
B. view graphics files on an evidence drive
C. wipe magnetic media before recycling it
D. make directories on a evidence disk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully.
Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices.
How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?
A. Two
B. One
C. Four
D. Three
Answer: (SHOW ANSWER)

NEW QUESTION: 145
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 free that you charge
C. Your Certifications
D. The correct, successful management of each and every case
Answer: D (LEAVE A REPLY)

NEW QUESTION: 146
A rogue/unauthorized access point is one that Is not authorized for operation by a particular firm or network
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 147
Which of the following information is displayed when Netstat is used with -ano switch?
A. Ethernet statistics
B. Details of TCP and UDP connections
C. Details of routing table
D. Contents of IP routing table
Answer: (SHOW ANSWER)

NEW QUESTION: 148
In a FAT32 system, a 123 KB file will use how many sectors?
A. 34
B. 25
C. 11
D. 56
E. 246
Answer: E (LEAVE A REPLY)
If you assume that we are using 512 bytes sectors, then 123x1024/512 = 246 sectors would be needed.

NEW QUESTION: 149
Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?
A. Google Chrome
B. Safari
C. Mozilla Firefox
D. Microsoft Edge
Answer: D (LEAVE A REPLY)

NEW QUESTION: 150
At what layer of the OSI model do routers function on?
A. 4
B. 1
C. 5
D. 3
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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?

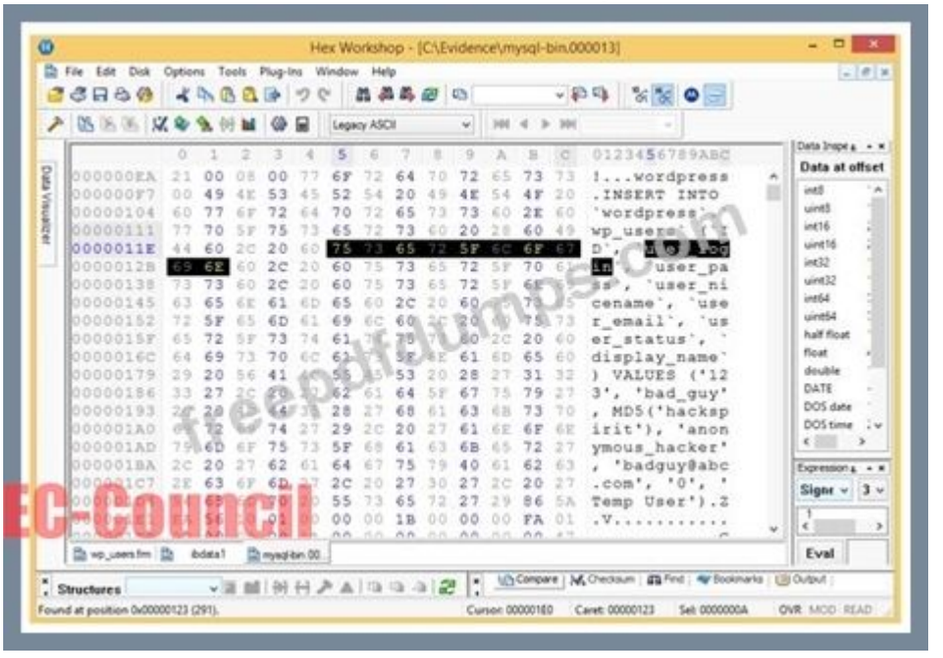
A. Nessus cannot perform wireless testing
B. Nessus is too loud
C. There are no ways of performing a "stealthy" wireless scan
D. Nessus is not a network scanner
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

What can the investigator infer from the screenshot seen below?
A. A smurf attack has been attempted
B. A denial of service has been attempted
C. Network intrusion has occurred
D. Buffer overflow attempt on the firewall.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 153
In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?
A. evidence in a civil case must be secured more tightly than in a criminal case
B. evidence must be handled in the same way regardless of the type of case
C. evidence procedures are not important unless you work for a law enforcement agency
D. evidence in a criminal case must be secured more tightly than in a civil case
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



A. A WordPress user has been created with the username bad_guy
B. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database
C. A WordPress user has been created with the username anonymous_hacker
D. A user with username bad_guy has logged into the WordPress web application
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155
Area density refers to:
A. the amount of data per disk
B. the amount of data per platter
C. the amount of data per square inch
D. the amount of data per partition
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 156
This organization maintains a database of hash signatures for known software.
A. American National standards Institute
B. International Standards Organization
C. National Software Reference Library
D. Institute of Electrical and Electronics Engineers
Answer: (SHOW ANSWER)

NEW QUESTION: 157
Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?
A. Tokenmon
B. Process Monitor
C. PSLoggedon
D. TCPView
Answer: C (LEAVE A REPLY)

NEW QUESTION: 158
MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network
A. 48-bit address
B. 24-bit address
C. 16-bit address
D. 32-bit address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
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 -b
B. netstat -r
C. netstat -s
D. netstat -ano
Answer: (SHOW ANSWER)

NEW QUESTION: 160

Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?
A. Hybrid Password Guessing Attack
B. Rule-Based Attack
C. Brute-Forcing Attack
D. Dictionary Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks.
Which of the following would that be?
A. The /tmp directory will be flushed
B. Power interruption will corrupt the pagefile
C. Any data not yet flushed to the system will be lost
D. All running processes will be lost
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?
A. If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer
B. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence
C. If the device's display is ON. the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons
D. To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
Which among the following U.S. laws requires financial institutions/companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance to protect their customers' information against security threats?
A. GLBA
B. SOX
C. FISMA
D. HIPAA

Answer: (SHOW ANSWER)

NEW QUESTION: 164
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. Violate your contract
B. Make you an agent of law enforcement
C. Write information to the subject's hard drive
D. Cause network congestion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
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. An email was marked as potential spam
B. The firewall rejected a connection
C. A virus was detected in an email
D. The firewall dropped a connection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as
http://www.juggyDoy.corn/GET/process.php././././././././etc/passwd.
Identify the attack referred.
A. File injection
B. SQL Injection
C. XSS attack
D. Directory traversal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 167
companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.
A. Reviewing the firewalls configuration
B. Data items and vulnerability scanning
C. Source code review
D. Interviewing employees and network engineers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
Which of the following reports are delivered under oath to a board of directors/managers/panel of jury?
A. Written Formal Report
B. Written informal Report
C. Verbal Informal Report
D. Verbal Formal Report
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
When should an MD5 hash check be performed when processing evidence?
A. Before and after evidence examination
B. After the evidence examination has been completed
C. Before the evidence examination has been completed
D. On an hourly basis during the evidence examination
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?
A. dir
B. grep
C. vim
D. Stringsearch

Answer: B (LEAVE A REPLY)

NEW QUESTION: 171
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen.
The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?
A. National Infrastructure Protection Center
B. Internet Fraud Complaint Center
C. CERT Coordination Center
D. Local or national office of the U.S. Secret Service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 172
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?
A. BootROM Stage
B. BIOS Stage
C. Bootloader Stage
D. Kernel Stage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 173
You should make at least how many bit-stream copies of a suspect drive?
A. 4
B. 1
C. 3
D. 2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
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. Buffer Overflow

D. Man-in-the-Middle Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by
_____of the compromised system.
A. Analyzing SAM file
B. Analyzing log files
C. Analyzing hard disk boot records
D. Analyzing rainbow tables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
What type of attack sends SYN requests to a target system with spoofed IP addresses?
A. SYN flood
B. Cross site scripting
C. Ping of death
D. Land
Answer: (SHOW ANSWER)

NEW QUESTION: 177
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. International Mobile Equipment Identifier (IMEI)
B. International mobile subscriber identity (IMSI)
C. Integrated circuit card identifier (ICCID)
D. Equipment Identity Register (EIR)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
You are a security analyst performing a penetration tests for a company in the Midwest.
After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router.
What have you discovered?
A. URL Obfuscation Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability

D. HTML Configuration Arbitrary Administrative Access Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Why is it a good idea to perform a penetration test from the inside?
A. To attack a network from a hacker's perspective
B. It is easier to hack from the inside
C. It is never a good idea to perform a penetration test from the inside
D. Because 70% of attacks are from inside the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 180
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?
A. hdd
B. hdc
C. hdb
D. hda
Answer: (SHOW ANSWER)

NEW QUESTION: 181
The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.
A. Kelly Policy
B. Silver-Platter Doctrine
C. Locard Exchange Principle
D. Clark Standard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
What is the following command trying to accomplish?
A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that UDP port 445 is closed for the 192.168.0.0 network

C. Verify that TCP port 445 is open for the 192.168.0.0 network
D. Verify that UDP port 445 is open for the 192.168.0.0 network
Answer: (SHOW ANSWER)

NEW QUESTION: 183
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. 31401
B. 31399
C. The zombie will not send a response
D. 31402
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Where are files temporarily written in Unix when printing?
A. /var/spool
B. /var/print
C. /spool
D. /usr/spool
Answer: A (LEAVE A REPLY)

NEW QUESTION: 185
This organization maintains a database of hash signatures for known software
A. American National standards Institute
B. Institute of Electrical and Electronics Engineers
C. International Standards Organization
D. National Software Reference Library
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?
A. Status of the network carrier
B. Network connections
C. Contents of the NetBIOS name cache
D. Contents of the network routing table
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187
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. Hidden running processes

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

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 188

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

A. A reserved file

B. A compressed file

C. A Data stream file

D. An encrypted file

Answer: C (LEAVE A REPLY)

NEW QUESTION: 189

Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.

The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

A. An environment set up before a user logs in

B. A Honeypot that traps hackers

C. A system Using Trojaned commands

D. An environment set up after the user logs in

Answer: B (LEAVE A REPLY)

NEW QUESTION: 190

When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as _____.

A. Empty clusters

B. Lost clusters

C. Bad clusters

D. Unused clusters

Answer: (SHOW ANSWER)

NEW QUESTION: 191

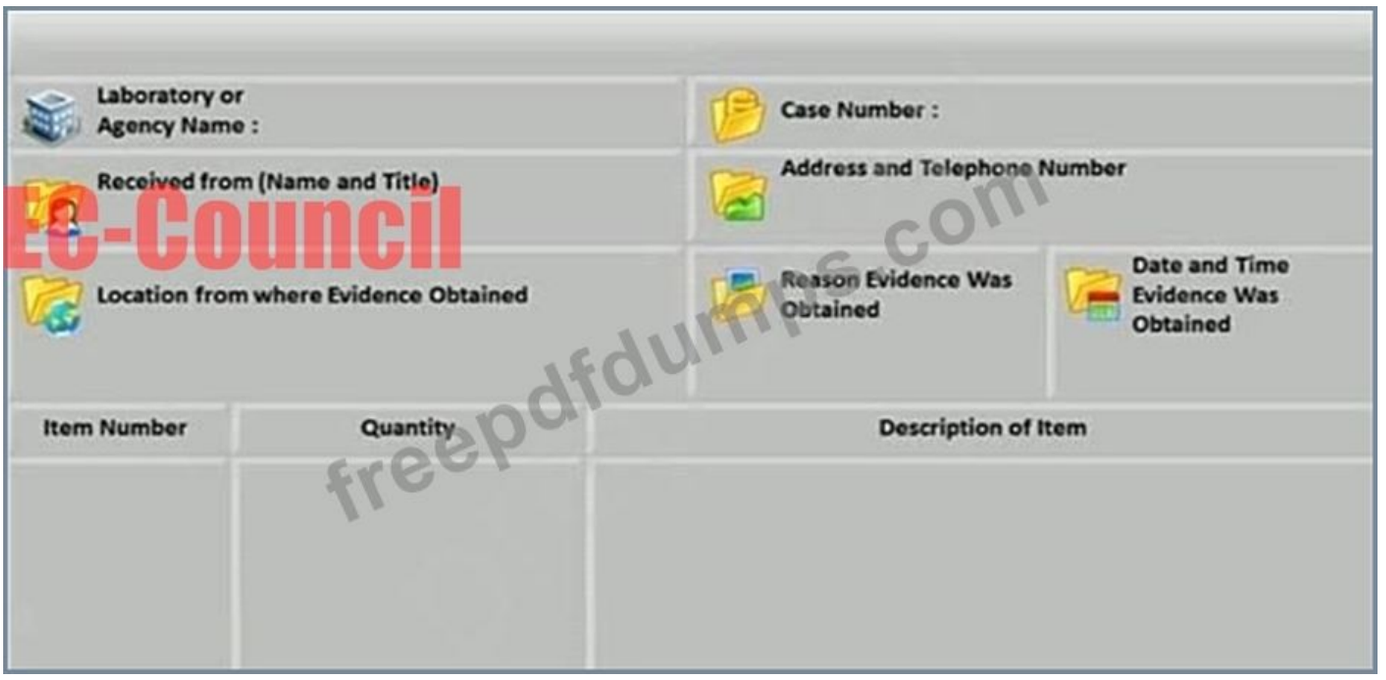
Software firewalls work at which layer of the OSI model?

A. Network
B. Application
C. Transport
D. Data Link
Answer: D (LEAVE A REPLY)

NEW QUESTION: 192
John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?
A. Cross-cut shredder
B. Strip-cut shredder
C. Cris-cross shredder
D. Cross-hatch shredder
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?
A. The sequence number for the parts of the same exhibit
B. The initials of the forensics analyst
C. The sequential number of the exhibits seized
D. The year the evidence was taken
Answer: C (LEAVE A REPLY)

NEW QUESTION: 194
What document does the screenshot represent?



A. Chain of custody form
B. Expert witness form
C. Search warrant form
D. Evidence collection form
Answer: D (LEAVE A REPLY)

NEW QUESTION: 195
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?
A. Two
B. One
C. Three
D. Four
Answer: A (LEAVE A REPLY)

NEW QUESTION: 196
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 109
B. Port 123
C. Port 110
D. Port 115
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
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. Deleted space
C. Cluster space
D. Sector space
Answer: A (LEAVE A REPLY)

NEW QUESTION: 198
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?
A. Simple Network Management Protocol
B. Border Gateway Protocol
C. Broadcast System Protocol
D. Cisco Discovery Protocol
Answer: D (LEAVE A REPLY)

NEW QUESTION: 199
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United
States?
A. Internet Fraud Complaint Center
B. Local or national office of the U.S. Secret Service
C. CERT Coordination Center

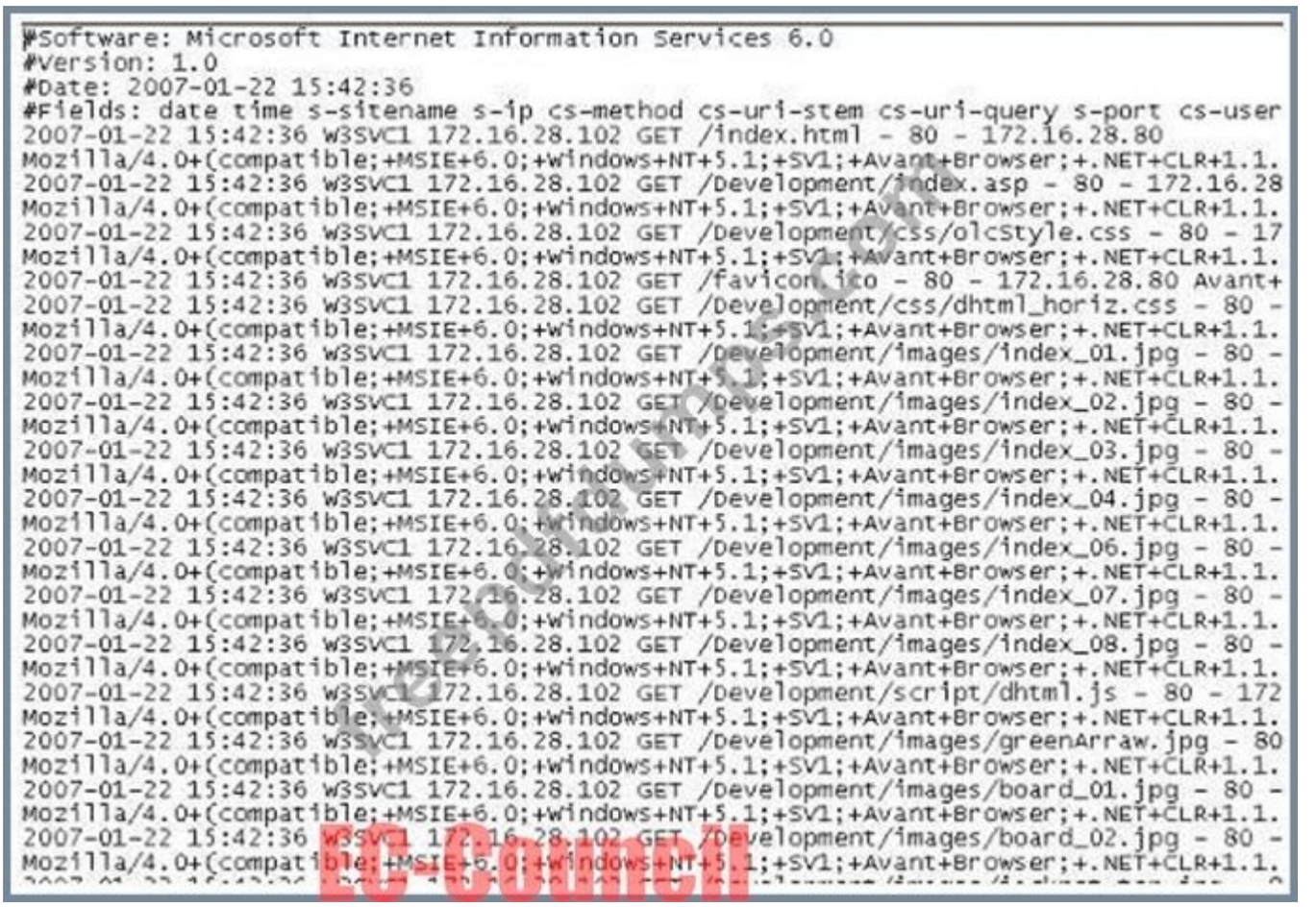
D. National Infrastructure Protection Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 200
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?
A. Distribute processing over 16 or fewer computers
B. Support for MD5 hash verification
C. Cracks every password in 10 minutes
D. Support for Encrypted File System
Answer: A (LEAVE A REPLY)

NEW QUESTION: 201
Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?
A. Identifying File Dependencies
B. Strings search
C. Dynamic analysis
D. File obfuscation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 202
What advantage does the tool Evidor have over the built-in Windows search?
A. It can find deleted files even after they have been physically removed
B. It can find files hidden within ADS
C. It can search slack space
D. It can find bad sectors on the hard drive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 203
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. UT

B. UTC

C. GMT

D. TAI

Answer: (SHOW ANSWER)

NEW QUESTION: 204

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. True

B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 205

Where is the startup configuration located on a router?

A. BootROM

B. Dynamic RAM

C. NVRAM

D. Static RAM

Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
Which of the following passwords are sent over the wire (and wireless) network, or stored on some media as it is typed without any alteration?
A. Hex passwords
B. Clear text passwords
C. Hashed passwords
D. Obfuscated passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 207
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets
A. Cached password hashes for the past 20 users
B. Service account passwords in plain text
C. IAS account names and passwords
D. Local store PKI Kerberos certificates
Answer: (SHOW ANSWER)

NEW QUESTION: 208
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. The total has not been reviewed and accepted by your peers
B. The tool hasn't been tested by the International Standards Organization (ISO)
C. You are not certified for using the tool
D. Only the local law enforcement should use the tool
Answer: (SHOW ANSWER)

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 §1029
C. 18 USC §1371
D. 18 USC §1030
Answer: D (LEAVE A REPLY)

NEW QUESTION: 210
A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.
A. distributed attack

B. blackout attack
C. automated attack
D. central processing attack
Answer: (SHOW ANSWER)

NEW QUESTION: 211
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?
A. HTTP Configuration Arbitrary Administrative Access Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 212
In the following email header, where did the email first originate from?

A. David1.state.ok.gov.us
B. Smtp1.somedomain.com

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

NEW QUESTION: 213
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. 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. Reciprocation
C. Social Validation
D. Friendship/Liking
Answer: B (LEAVE A REPLY)

NEW QUESTION: 214
How many possible sequence number combinations are there in TCP/IP protocol?
A. 4 billion
B. 1 billion
C. 32 million
D. 320 billion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 215
Volatile Memory is one of the leading problems for forensics.
Worms such as code Red are memory resident and do not write themselves to the hard drive, if you turn the system off they disappear.
In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?
A. Give the Operating System a minimal amount of memory, forcing it to use a swap file
B. Use Vmware to be able to capture the data in memory and examine it
C. Use intrusion forensic techniques to study memory resident infections
D. Create a Separate partition of several hundred megabytes and place the swap file there
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 216

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

NEW QUESTION: 217
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. Universal Time Set
B. Network Time Protocol
C. Time-Sync Protocol
D. SyncTime Service
Answer: B (LEAVE A REPLY)

NEW QUESTION: 218
When obtaining a warrant, it is important to:
A. generallydescribe the place to be searched and generally describe the items to be seized
B. generallydescribe the place to be searched and particularly describe the items to be seized
C. particularlydescribe the place to be searched and particularly describe the items to be seized
D. particularlydescribe the place to be searched and generally describe the items to be seized
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Which is a standard procedure to perform during all computer forensics investigations?
A. with the hard drive removed from the suspect PC, check the date and time in the system's RAM
B. with the hard drive in the suspect PC, check the date and time in the system's CMOS
C. with the hard drive in the suspect PC, check the date and time in the File Allocation Table
D. with the hard drive removed from the suspect PC, check the date and time in the system's CMOS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 220
Dumpster Diving refers to:
A. Convincing people to reveal the confidential information

B. Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes
C. Looking at either the user's keyboard or screen while he/she is logging in
D. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 221
Which of these Windows utility help you to repair logical file system errors?
A. Resource Monitor
B. Disk defragmenter
C. CHKDSK
D. Disk cleanup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
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 opening angle bracket, its hex or double-encoded hex equivalent
C. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
D. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 223
You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?
A. Make a bit-stream disk-to-image file
B. Create a compressed copy of the file with DoubleSpace
C. Make a bit-stream disk-to-disk file
D. Create a sparse data copy of a folder or file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 224
In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?
A. one who has NTFS 4 or 5 partitions
B. one who uses hard disk writes on IRQ 13 and 21
C. one who has lots of allocation units per block or cluster
D. one who uses dynamic swap file capability

Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to _____
A. Prevent contamination to the evidence drive
B. Automate collection from image files
C. Acquire data from the host-protected area on a disk
D. Avoiding copying data from the boot partition
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?
A. Net share
B. Net config
C. Net sessions
D. Net stat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 227
What malware analysis operation can the investigator perform using the jv16 tool?
A. Files and Folder Monitor
B. Network Traffic Monitoring/Analysis
C. Registry Analysis/Monitoring
D. Installation Monitor
Answer: (SHOW ANSWER)

NEW QUESTION: 228
Which of the following processes is part of the dynamic malware analysis?
A. File fingerprinting

B. Searching for the strings
C. Process Monitoring
D. Malware disassembly
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
The newer Macintosh Operating System (MacOS X) is based on:
A. BSD Unix
B. OS/2
C. Linux
D. Microsoft Windows
Answer: (SHOW ANSWER)

NEW QUESTION: 230
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?
A. Cracks every password in 10 minutes
B. Support for Encrypted File System
C. Distribute processing over 16 or fewer computers
D. Support for MD5 hash verification
Answer: (SHOW ANSWER)

NEW QUESTION: 231
Which of the following setups should a tester choose to analyze malware behavior?
A. A normal system with internet connection
B. A virtual system with network simulation for internet connection
C. A virtual system with internet connection
D. A normal system without internet connect
Answer: (SHOW ANSWER)

NEW QUESTION: 232
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. Web OS
C. Android
D. Symbian OS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 233
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?
A. Multiple access points can be set up on the same channel without any issues
B. So that the access points will work on different frequencies
C. Avoid over-saturation of wireless signals
D. Avoid cross talk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 234
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. SOX
C. GLBA
D. HIPAA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 235
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. 10 GB
C. 57.19 GB
D. 11.17 GB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 236
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 called in the FBI without correlating with the fingerprint data
B. They examined the actual evidence on an unrelated system
C. They attempted to implicate personnel without proof

D. They tampered with evidence by using it
Answer: D (LEAVE A REPLY)

NEW QUESTION: 237
Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?
A. The data is moved to the Restore directory and is kept there indefinitely
B. The data will reside in the L2 cache on a Windows computer until it is manually deleted
C. The data is still present until the original location of the file is used
D. It is not possible to recover data that has been emptied from the Recycle Bin
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
What will the following command accomplish in Linux?
fdisk /dev/hda
A. Fill the disk with zeros
B. Delete all files under the /dev/hda folder
C. Format the hard drive
D. Partition the hard drive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
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 he can use to recover the IMEI number?
A. #*06*#
B. *1MEI#
C. *#06#
D. #06r
Answer: C (LEAVE A REPLY)

NEW QUESTION: 240
An Expert witness give an opinion if:
A. To define the issues of the case for determination by the finder of fact
B. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
C. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case
D. To stimulate discussion between the consulting expert and the expert witness

Answer: B (LEAVE A REPLY)

NEW QUESTION: 241
Before you are called to testify as an expert, what must an attorney do first?
A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness
Answer: D (LEAVE A REPLY)

NEW QUESTION: 242
If a file (readme.txt) on a hard disk has a size of 2600 bytes, how many sectors are normally allocated to this file?
A. 6 Sectors
B. 4 Sectors
C. 5 Sectors
D. 7 Sectors
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Sectors in hard disks typically contain how many bytes?
A. 2048
B. 512
C. 256
D. 1024
Answer: (SHOW ANSWER)

NEW QUESTION: 244
Which of the following Event Correlation Approaches is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?
A. Vulnerability-Based Approach

B. Route Correlation
C. Rule-Based Approach
D. Bayesian Correlation
Answer: (SHOW ANSWER)

NEW QUESTION: 245
What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24
A. Verify that TCP port 445 is open for the 192.168.0.0 network
B. Verify that UDP port 445 is open for the 192.168.0.0 network
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network
Answer: (SHOW ANSWER)

NEW QUESTION: 246
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?
A. Netcraft
B. Dig
C. Nmap
D. Ping sweep
Answer: A (LEAVE A REPLY)

NEW QUESTION: 247
Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the_____.
A. IDS logs
B. Audit logs
C. Router cache
D. Application logs
Answer: (SHOW ANSWER)

NEW QUESTION: 248
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. review of SIDs in the Registry
B. forensic duplication of hard drive

C. analysis of volatile data
D. comparison of MD5 checksums
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
What does the superblock in Linux define?
A. available space
B. disk geometr
C. location of the first inode
D. file synames
Answer: C (LEAVE A REPLY)

NEW QUESTION: 250
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 sessions
C. Net use
D. Net config
Answer: C (LEAVE A REPLY)

NEW QUESTION: 251
Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?
A. Cookies
B. Temporary Files
C. Web Browser Cache
D. Open files
Answer: A (LEAVE A REPLY)

NEW QUESTION: 252
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. SOX
B. FISMA
C. GLBA
D. HIPAA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 253

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. TypedURLs key
B. UserAssist Key
C. RunMRU key
D. MountedDevices key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
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 for evidence themselves would not have any ill effects
B. Searching creates cache Files that would hinder the investigation
C. Searching could possibly crash the machine or device
D. Searching can change date/time stamps
Answer: (SHOW ANSWER)

NEW QUESTION: 255
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. SOX
B. HIPAA
C. GLBA
D. CAN-SPAM Act
Answer: (SHOW ANSWER)

NEW QUESTION: 256
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 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326
B. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"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../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\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: 257
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_CLASSES_SYSTEM
B. HKEY_LOCAL_ADMIN
C. HKEY_USERS
D. HKEY_CLASSES_ADMIN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 258
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 2016/11/10 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. Phishing
B. Email Spamming
C. Email Spoofing
D. Mail Bombing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?
A. at least two
B. only one

C. by law, three
D. quite a few
Answer: B (LEAVE A REPLY)

NEW QUESTION: 260
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 copied from C drive to D drive in fifth sequential order
B. A text file deleted from C drive in sixth sequential order
C. A text file copied from D drive to C drive in fifth sequential order
D. A text file deleted from C drive in fifth sequential order
Answer: D (LEAVE A REPLY)

NEW QUESTION: 261
Which Is a Linux journaling file system?
A. FAT
B. BFS
C. Ext3
D. HFS
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Which of the following is not a part of data acquisition forensics Investigation?
A. Permit only authorized personnel to access
B. Work on the original storage medium not on the duplicated copy
C. Disable all remote access to the system
D. Protect the evidence from extremes in temperature
Answer: B (LEAVE A REPLY)

NEW QUESTION: 263
Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?
A. Syllable attack
B. Brute force attack

C. Hybrid attack
D. Dictionary attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 264
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz?format, what does the nnn?denote?When marking evidence that has been collected with the ?aa/ddmmyy/nnnn/zz?format, what does the ?nnn?denote?
A. The initials of the forensics analyst
B. The sequential number of the exhibits seized
C. The sequence number for the parts of the same exhibit
D. The year the evidence was taken
Answer: B (LEAVE A REPLY)

NEW QUESTION: 265
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. Portable Document Format
B. Raw Format
C. Advanced Forensics Format (AFF)
D. Proprietary Format
Answer: C (LEAVE A REPLY)

NEW QUESTION: 266
Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?
A. d0 0f 11 e0
B. 25 50 44 46
C. 50 41 03 04
D. ff d8 ff
Answer: (SHOW ANSWER)

NEW QUESTION: 267
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 "3" for complete security
B. RestrictAnonymous must be set to "10" for complete security

C. There is no way to always prevent an anonymous null session from establishing
D. RestrictAnonymous must be set to "2" for complete security
Answer: (SHOW ANSWER)

NEW QUESTION: 268
Under which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?
A. 18 U.S.C. 1029 Possession of Access Devices
B. 18 U.S.C. 1831 Economic Espionage Act
C. 18 U.S.C. 1030 Fraud and related activity in connection with computers
D. 18 U.S.C. 1832 Trade Secrets Act
E. 18 U.S. 1343 Fraud by wire, radio or television
F. 18 U.S.C. 1362 Government communication systems
G. 18 U.S.C. 1361 Injury to Government Property
Answer: (SHOW ANSWER)

NEW QUESTION: 269
When a user deletes a file or folder, the system stores complete path including the original filename is a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.
A. Undo the last action performed on the system
B. Reboot Windows
C. Download the file from Microsoft website
D. Use a recovery tool to undelete the file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 270
Select the tool appropriate for finding the dynamically linked lists of an application or malware.
A. PEiD
B. Dependency Walker
C. ResourcesExtract
D. SysAnalyzer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 271
What does the 63.78.199.4(161) denotes 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. Login IP address
B. Destination IP address
C. None of the above

D. Source IP address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 272
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

A. Malicious URL detected
B. Security event was monitored but not stopped
C. Connection rejected
D. An email marked as potential spam
Answer: D (LEAVE A REPLY)

NEW QUESTION: 273
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. Add up the total size of all known partitions and compare it to the total size of the hard drive
B. 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
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: 274
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. Frye

B. Daubert
C. SWGDE & SWGIT
D. IOCE
Answer: B (LEAVE A REPLY)

NEW QUESTION: 275
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. Ettercap
B. RaidSniff
C. Snort
D. Airsnort
Answer: A (LEAVE A REPLY)

NEW QUESTION: 276
In Linux, what is the smallest possible shellcode?
A. 8 bytes
B. 80 bytes
C. 800 bytes
D. 24 bytes
Answer: (SHOW ANSWER)

NEW QUESTION: 277
How many sectors will a 125 KB file use in a FAT32 file system?
A. 256
B. 32
C. 25
D. 16
Answer: (SHOW ANSWER)

NEW QUESTION: 278
If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?
A. Remove the battery immediately
B. Remove any memory cards immediately
C. Keep the device powered on

D. Turn off the device immediately
Answer: (SHOW ANSWER)

NEW QUESTION: 279
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?
A. Kernel Stage
B. BootROM Stage
C. BIOS Stage
D. Bootloader Stage
Answer: (SHOW ANSWER)

NEW QUESTION: 280
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. IP Spoofing
B. DNS Poisoning
C. HTTP redirect attack
D. ARP Poisoning
Answer: (SHOW ANSWER)

NEW QUESTION: 281
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: A (LEAVE A REPLY)

NEW QUESTION: 282
Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?
A. Installing malware analysis tools
B. Using network simulation tools
C. Isolating the host device
D. Enabling shared folders

Answer: D (LEAVE A REPLY)

NEW QUESTION: 283
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: 284
Which of the following statements is not a part of securing and evaluating electronic crime scene checklist?
A. Blog about the incident on the internet
B. Transmit additional flash messages to other responding units
C. Request additional help at the scene if needed
D. Locate and help the victim
Answer: (SHOW ANSWER)

NEW QUESTION: 285
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. International Mobile Equipment Identifier (IMEI)
B. International mobile subscriber identity (IMSI)
C. Equipment Identity Register (EIR)
D. Integrated circuit card identifier (ICCID)
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?
A. Hackspionage
B. Spycrack
C. Netspionage
D. Spynet
Answer: C (LEAVE A REPLY)

NEW QUESTION: 287
Data acquisition system is a combination of tools or processes used to gather, analyze and record Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?
A. RS422
B. RS423
C. RS232
D. RS231
Answer: C (LEAVE A REPLY)

NEW QUESTION: 288
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. Crash the switch with a DoS attack since switches cannot send ACK bits
C. Enable tunneling feature on the switch
D. Trick the switch into thinking it already has a session with Terri's computer
Answer: (SHOW ANSWER)

NEW QUESTION: 289
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 -b
B. Netstat -ano
C. Netstat -r
D. Netstat -s
Answer: (SHOW ANSWER)

NEW QUESTION: 290
What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?
A. Every byte of the file(s) is verified using 32-bit CRC
B. Every byte of the file(s) is given an MD5 hash to match against a master file
C. Every byte of the file(s) is copied to three different hard drives
D. Every byte of the file(s) is encrypted using three different methods
Answer: (SHOW ANSWER)

NEW QUESTION: 291
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. The longer a disk is in use, the less likely it is that deleted files will be overwritten
C. When files are deleted, the data is overwritten and the cluster marked as available
D. While booting, the machine may create temporary files that can delete evidence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 292
Which among the following files provides email header information in the Microsoft Exchange server?
A. PRIV.STM
B. PRIV.EDB
C. gwcheck.db
D. PUB.EDB
Answer: B (LEAVE A REPLY)

NEW QUESTION: 293
This is the 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 Boot Record (MBR)
B. Master File Table (MFT)
C. File Allocation Table (FAT)
D. Disk Operating System (DOS)
Answer: C (LEAVE A REPLY)
A MBR is usually found on fixed disks, not floppy.
A MFT is part of NTFS, and NTFS is not used on floppy
DOS is an operating system, not a file structure database

NEW QUESTION: 294

What operating system would respond to the following command?
A. Mac OS X
B. FreeBSD
C. Windows 95
D. Windows XP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
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. Directory traversal
B. Security misconfiguration
C. Parameter/form tampering
D. Unvalidated input
Answer: A (LEAVE A REPLY)

NEW QUESTION: 296
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. Cylinder
B. Interface
C. Heads
D. Sectors
Answer: (SHOW ANSWER)

NEW QUESTION: 297
What method of copying should always be performed first before carrying out an investigation?
A. Parity-bit copy
B. Bit-stream copy
C. MS-DOS disc copy
D. System level copy
Answer: (SHOW ANSWER)

NEW QUESTION: 298
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. 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:\wintt\system32\Logfiles\W3SVC1
C. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test
D. 127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0' 200 2326
Answer: C (LEAVE A REPLY)

NEW QUESTION: 299
File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?
A. The computer looks at the clusters occupied by that file and does not avails space to store a new file
B. The last letter of a file name is replaced by a hex byte code E5h
C. Corresponding clusters in FAT are marked as used
D. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
Answer: D (LEAVE A REPLY)

NEW QUESTION: 300
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?
A. NTOSKRNL.EXE
B. LSASS.EXE
C. NTDETECT.COM
D. NTLDR
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?
A. WarDhving
B. WarFlying
C. WarChalking
D. WarWalking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 302
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024
A. Copy the master boot record to a 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 memory dump file to an image file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 303
What binary coding is used most often for e-mail purposes?
A. MIME
B. Uuencode
C. SMTP
D. IMAP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 304
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 attacker computer
B. The gateway will be the IP of the proxy server used by the attacker to launch the attack
C. The gateway will be the IP used to manage the access point
D. The gateway will be the IP used to manage the RADIUS server
Answer: (SHOW ANSWER)

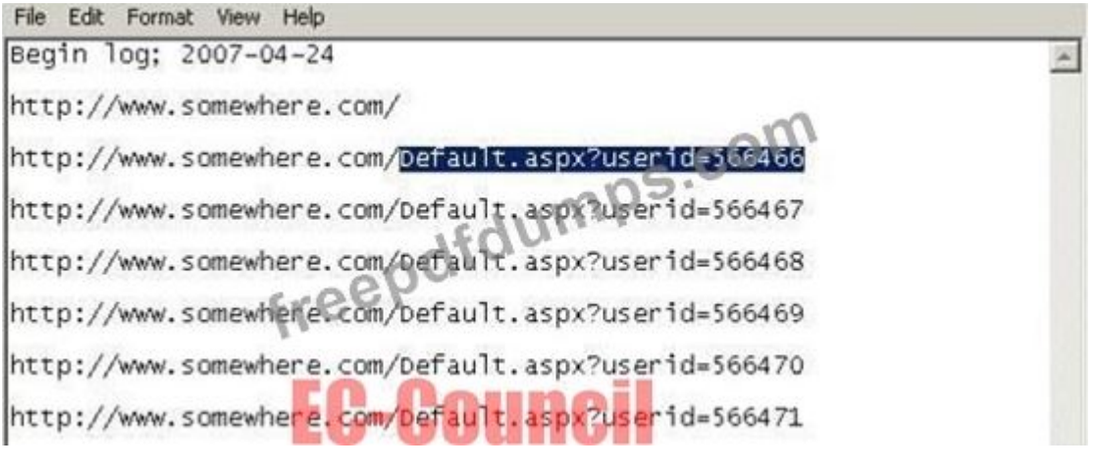
NEW QUESTION: 305
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?
A. Firewalk sets all packets with a TTL of one
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot pass through Cisco firewalls
D. Firewalk cannot be detected by network sniffers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 306
While analyzing a hard disk, the investigator finds that the file system does not use UEFIbased interface.
Which of the following operating systems is present on the hard disk?
A. Windows 7
B. Windows 8.1
C. Windows 10
D. Windows 8
Answer: A (LEAVE A REPLY)

NEW QUESTION: 307
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?
A. Text semagram
B. Grill cipher
C. Visual semagram
D. Visual cipher
Answer: C (LEAVE A REPLY)

NEW QUESTION: 308
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?
A. Direct Examination
B. Cross Examination
C. Witness Examination
D. Indirect Examination
Answer: B (LEAVE A REPLY)

NEW QUESTION: 309
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. Cross site scripting

B. Cookie Poisoning

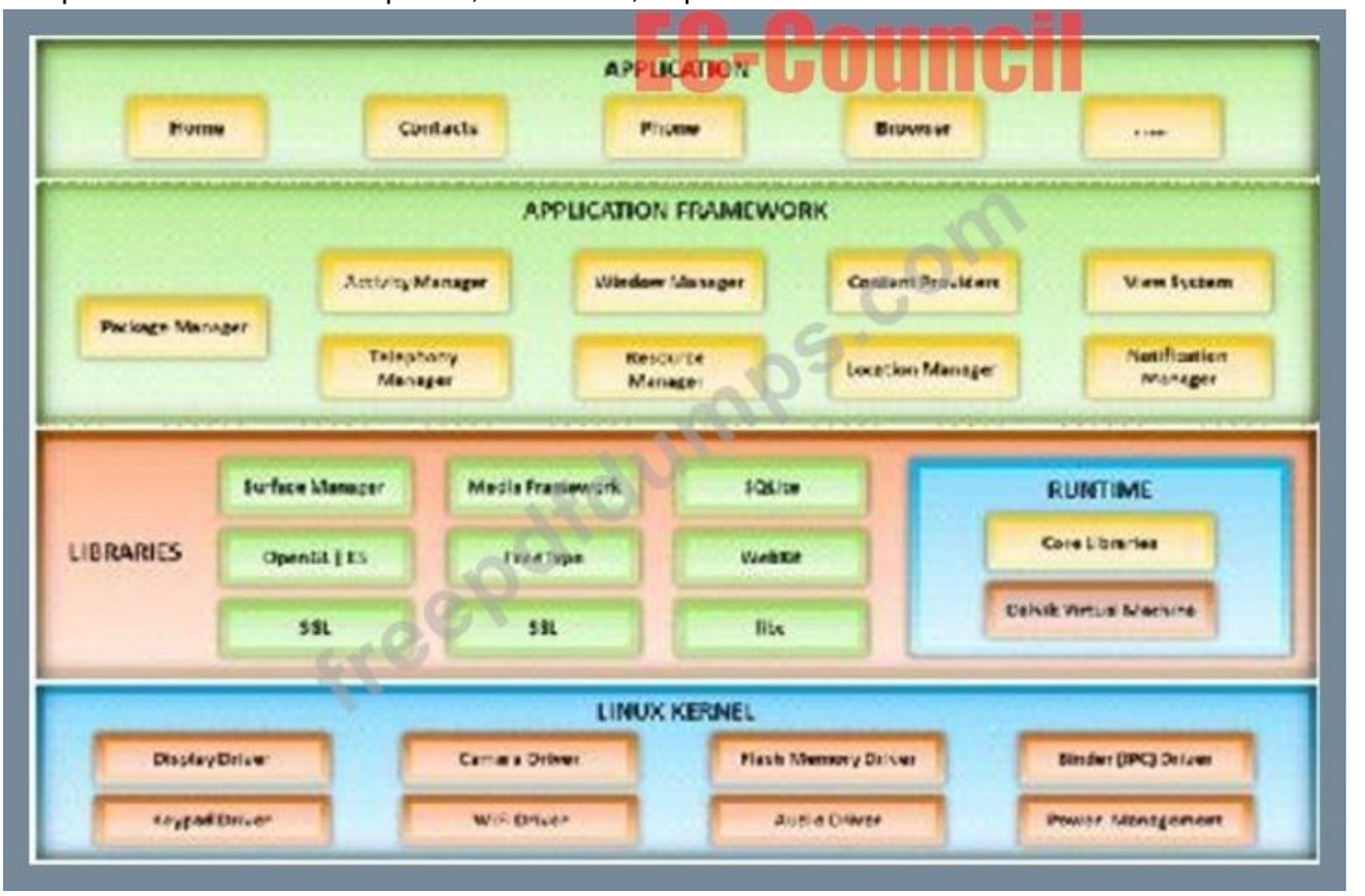
C. Parameter tampering

D. SQL injection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 310

A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.



Which mobile operating system architecture is represented here?

A. Windows Phone 7 Architecture

B. Symbian OS Architecture

C. webOS System Architecture

D. Android OS Architecture

Answer: (SHOW ANSWER)

NEW QUESTION: 311

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

A. Cross site scripting

B. SQL injection is possible

C. Web bugs

D. Hidden fields

Answer: B (LEAVE A REPLY)

NEW QUESTION: 312

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 network shares that Hillary has permissions

B. The SID of Hillary network account

C. The SAM file from Hillary computer

D. Hillary network username and password hash

Answer: D (LEAVE A REPLY)

NEW QUESTION: 313

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. Friendship/Liking
C. Reciprocation
D. Social Validation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 314
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?
A. All search engines that link to .net domains
B. All sites that link to ghttech.net
C. Sites that contain the code: link:www.ghttech.net
D. All sites that ghttech.net links to
Answer: B (LEAVE A REPLY)

NEW QUESTION: 315
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. Kernal injection
B. SQL injection
C. Format string bug
D. Buffer overflow
Answer: D (LEAVE A REPLY)

NEW QUESTION: 316
Which command line tool is used to determine active network connections?
A. nslookup
B. netsh
C. netstat
D. nbstat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 317
What must be obtained before an investigation is carried out at a location?
A. Habeas corpus
B. Search warrant
C. Modus operandi
D. Subpoena
Answer: (SHOW ANSWER)

NEW QUESTION: 318
The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.
A. Locard Exchange Principle
B. Clark Standard
C. Kelly Policy
D. Silver-Platter Doctrine
Answer: D (LEAVE A REPLY)
Answer "Silver-Platter Doctrine" is probably the most correct. However, the Silver-Platter Doctrine allowed the Federal court to introduce illegally or improperly "State" seized evidence as long as Federal officers had no role in obtaining it. Also wanted to note that this Doctrine was declared unconstitional in 1960, Elkins vs United States

NEW QUESTION: 319
A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

What can the investigator infer from the screenshot seen below?

A. A denial of service has been attempted

B. Network intrusion has occurred

C. Buffer overflow attempt on the firewall.

D. A smurf attack has been attempted

Answer: (SHOW ANSWER)

NEW QUESTION: 320

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 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. Information header

B. The RGBQUAD array

C. Image data

D. Header

Answer: B (LEAVE A REPLY)

NEW QUESTION: 321

What is the investigator trying to analyze if the system gives the following image as output?

A. Currently active logon sessions
B. Inactive logon sessions
C. All the logon sessions
D. Details of users who can logon
Answer: (SHOW ANSWER)

NEW QUESTION: 322
During forensics investigations, investigators tend to first collect the system time and then compare it with UTC. What does the abbreviation UTC stand for?
A. Universal Time for Computers
B. Coordinated Universal Time
C. Universal Computer Time
D. Correlated Universal Time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 324
During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
In the following email header, where did the email first originate from?

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

NEW QUESTION: 326
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-CURRENT_CONFIG
D. HKEY_LOCAL_MACHINE
Answer: D (LEAVE A REPLY)

NEW QUESTION: 327
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. Enticement

B. Intruding into ahoneypot is not illegal
C. Intruding into a DMZ is not illegal
D. Entrapment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 328
When examining the log files from a Windows IIS Web Server, how often is a new log file created?
A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started
Answer: B (LEAVE A REPLY)
Wecannot tell if the question is referring to the httperr.log file (IIS 6.0) or is it referring to the logfiles for the website.
If IIS is the case, "a new log file is created every day" should be the correct answer.
Microsoft creates the log files in the following format: exYYMMdd.log format and rotates them daily.

NEW QUESTION: 329
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. Kernal injection
B. SQL injection
C. Format string bug
D. Buffer overflow
Answer: D (LEAVE A REPLY)

NEW QUESTION: 330
Why should you never power on a computer that you need to acquire digital evidence from?
A. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
B. When the computer boots up, the system cache is cleared which could destroy evidence
C. Powering on a computer has no affect when needing to acquire digital evidence from it
D. When the computer boots up, files are written to the computer rendering the data nclean
Answer: D (LEAVE A REPLY)

NEW QUESTION: 331
In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?
A. one who uses dynamic swap file capability
B. one who uses hard disk writes on IRQ 13 and 21
C. one who has lots of allocation units per block or cluster
D. one who has NTFS 4 or 5 partitions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 332
The use of warning banners helps a company avoid litigation by overcoming an employee assumed
_____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.
A. Right of Privacy
B. Right of free speech
C. Right to work
D. Right to Internet Access
Answer: (SHOW ANSWER)

NEW QUESTION: 333
When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?
A. Firewall
B. Write-blocker
C. Disk editor
D. Protocol analyzer
Answer: (SHOW ANSWER)

NEW QUESTION: 334
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. 203.218.39.20
B. 137.189.96.52
C. 8.12.1.0
D. 203.218.39.50
Answer: (SHOW ANSWER)

NEW QUESTION: 335
Which of the following is not a part of the technical specification of the laboratory-based imaging system?
A. very low image capture rate
B. Remote preview and imaging pod
C. Anti-repudiation techniques
D. High performance workstation PC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 336
You are working as an independent computer forensics investigator and received 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 "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a "simple 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 proceeding?
A. Bit-stream Copy

B. Full backup Copy
C. Incremental Backup Copy
D. Robust Copy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 337
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 anyone using their service and can provide you with assistance
B. 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
C. ISP's never maintain log files so they would be of no use to your investigation
D. The ISP can't conduct any type of investigations on anyone and therefore can't assist you
Answer: B (LEAVE A REPLY)

NEW QUESTION: 338
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?
A. BIOS-MBR
B. Master Boot Record (MBR)
C. GUID Partition Table (GPT)
D. BIOS Parameter Block
Answer: C (LEAVE A REPLY)