EC-COUNCIL.312-49v11.v2025-07-29.q428

Exam Code:	312-49v11
Exam Name:	Computer Hacking Forensic Investigator (CHFI-v11)
Certification Provider:	EC-COUNCIL
Free Question Number:	428
Version:	v2025-07-29
# of views:	119
# of Questions views:	4280
https://www.freepdfdumps.com/EC-COUNCIL.312-49v11.v2025-07-29.q428.html	

NEW QUESTION: 1
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: 2
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?
A. RIM Messaging center
B. Blackberry Enterprise server
C. Blackberry desktop redirector
D. Microsoft Exchange server
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?
A. Directory traversal
B. Unvalidated input

C. Security misconfiguration
D. Parameter/form tampering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Data is striped at a byte level across multiple drives and parity information is distributed among all member drives.

What RAID level is represented here?
A. RAID Level 1
B. RAID Level0
C. RAID Level 5
D. RAID Level 3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
A major financial institution recently observed an unusually high number of failed login attempts on a critical server. The security analyst uses Splunk Enterprise Security (ES) to investigate the logs and suspect a possible brute-force attack. After examining the Windows Event Viewer logs, the analyst detects a series of event ID 4625 (failed logins) and event ID 4624 (successful logins). Which of the following SIEM features would be MOST beneficial for the analyst to accurately pinpoint the source of the potential attack and investigate it further?
A. Real-time threat detection capability of IBM QRadar SIEM
B. Advanced analytics capabilities of Splunk ES for detection and investigation
C. Risk-based alerting functionality of Splunk ES
D. Centralized insight provided by IBM QRadar SIEM across on-premises, SaaS, and IaaS environments
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.
A. False
B. True

Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
What is a chain of custody?
A. It Is a document that lists chain of windows process events
B. Chain of custody refers to obtaining preemptive court order to restrict further damage of evidence in electronic seizures
C. It is a search warrant that is required for seizing evidence at a crime scene
D. A legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory
Answer: (SHOW ANSWER)

NEW QUESTION: 8
During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?
A. Coordinated Universal Time
B. Universal Time for Computers
C. Universal Computer Time
D. Correlated Universal Time
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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 8.1
B. Windows 8
C. Windows 7
D. Windows 10
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
During an international cybercrime investigation, your team discovers an intercepted email with a sequence of special characters. Believing that the Unicode standard might have been used in encoding the message, which of the following elements could serve as the strongest indicator of this suspicion?
A. The presence of a unique number for each character, irrespective of the platform, program, and language
B. The presence of over 128.000 different characters in the intercepted email
C. The presence of characters from multiple modern and historic scripts
D. The presence of characters from a single non-English script
Answer: (SHOW ANSWER)

NEW QUESTION: 11
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?
A. src port 23 and dst port 23
B. src port 22 and dst port 22
C. udp port 22 and host 172.16.28.1/24
D. net port 22
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
In Steganalysis, which of the following describes a Known-stego attack?
A. During the communication process, active attackers can change cover
B. Original and stego-object are available and the steganography algorithm is known
C. Only the steganography medium is available for analysis
D. The hidden message and the corresponding stego-image are known
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:
A. FAT is an older and inefficient file system
B. FAT does not index files
C. NTFS is a journaling file system
D. NTFS has lower cluster size space
Answer: (SHOW ANSWER)

NEW QUESTION: 14
What are the security risks of running a "repair" installation for Windows XP?
A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Ctrl+F10 gives the user administrative rights
C. Pressing Shift+F1 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15

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. XSS attack
B. Directory traversal
C. File injection
D. SQL Injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
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. Digital attack
B. ARP redirect
C. Denial of service
D. Physical attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
How will you categorize a cybercrime that took place within a CSP's cloud environment?
A. Cloud as an Object
B. Cloud as an Audit
C. Cloud as a Tool
D. Cloud as a Subject
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Why should you never power on a computer that you need to acquire digital evidence from?
A. When the computer boots up, the system cache is cleared which could destroy evidence
B. When the computer boots up, files are written to the computer rendering the data nclean

C. Powering on a computer has no affect when needing to acquire digital evidence from it
D. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
John, a Forensic Lab Director, is planning to strengthen the security measures of his lab to maintain the trustworthiness and integrity of their investigations. He also wants to ensure that the forensics team members are assigned specific roles to streamline the investigation process. Given the following list of security measures and team roles, which combination should he NOT consider?
A. Installation of a TEMPEST system to shield workstations from electromagnetic signals and appointment of an Incident Responder to secure the crime scene and collect evidence
B. Instituting a physical lab surveillance system with guards around the premises and designating a single individual to fulfill the roles of Incident Analyzer, Evidence Documenter, and Evidence Manager
C. Providing an electronic sign-in log for visitors and assigning the role of Evidence Examiner to sort and prioritize the collected evidence based on usefulness and relevance
D. Establishing a fire safety protocol with trained personnel and assigning the role of Photographer to record the crime scene
Answer: (SHOW ANSWER)

NEW QUESTION: 20
SIM is a removable component that contains essential information about the subscriber. It has both volatile and non-volatile memory. The file system of a SIM resides in _____ memory.
A. Volatile
B. Non-volatile
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following tool creates a bit-by-bit image of an evidence media?
A. AccessData FTK Imager
B. Recuva
C. FileMerlin
D. Xplico
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
What will the following command accomplish in Linux?
fdisk /dev/hda

A. Delete all files under the /dev/hda folder
B. Fill the disk with zeros
C. Format the hard drive
D. Partition the hard drive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
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. A virus was detected in an email
B. The firewall rejected a connection
C. An email was marked as potential spam
D. The firewall dropped a connection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
What method of copying should always be performed first before carrying out an investigation?
A. Bit-stream copy
B. System level copy
C. MS-DOS disc copy
D. Parity-bit copy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Task list command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following task list commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?
A. tasklist/s
B. tasklist/u
C. tasklist/V
D. tasklist/p
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from client that has undergone a cyberattack. Brian

ran the executable file In the virtual environment to see what it would do. What type of analysis did Brian perform?

A. Static malware analysis

B. Static OS analysis

C. Status malware analysis

D. Dynamic malware analysis

Answer: D (LEAVE A REPLY)

NEW QUESTION: 27

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

A. Lawyers

B. System administrators

C. Local managers or other non-forensic staff

D. Forensic laboratory staff

Answer: D (LEAVE A REPLY)

NEW QUESTION: 28

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. D:\Exchsrvr\Message Tracking\servername.log

B. C:\Exchsrvr\Message Tracking\servername.log

C. C:\Program Files\Exchsrvr\servername.log

D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

What is a bit-stream copy?

A. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition

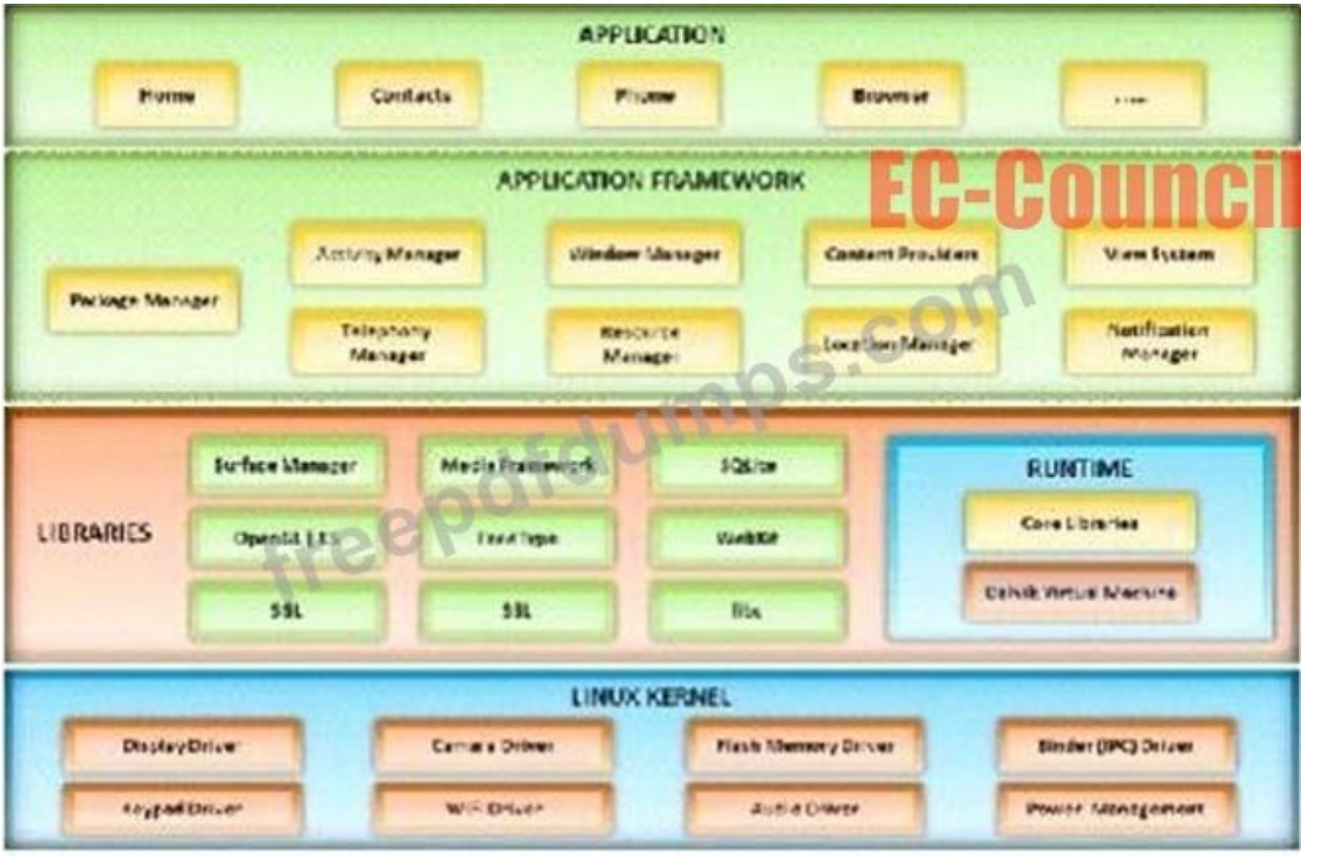
C. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk

D. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition

Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
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. Brute force attack
B. Hybrid attack
C. Dictionary attack
D. Syllable attack
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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. Android OS Architecture

D. webOS System Architecture
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?
A. config.db
B. Sync_config.db
C. filecache.db
D. sigstore.db
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or Illegal Information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?
A. Ransomware attack
B. Malware attack
C. Phishing
D. Denial-of-Service (DoS) attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
An experienced computer forensics investigator, Vince, was tasked with examining digital evidence associated with a serious corporate cybercrime. He successfully seized and bagged the evidence but faced logistical difficulties and workforce concerns for its onsite examination. He decided to transport the evidence to the lab for further analysis. In light of his decision, which of the following precautions is the least relevant to ensure the integrity of the evidence during its transportation?
A. Keeping the collected electronic evidence away from magnetic sources like speaker magnets

B. Ensuring the evidence bag's panel contains the name of the officer who prepared the crime scene sketch
C. Storing wireless or portable devices in signal-blocking containers to prevent them from connecting to the networks
D. Storing the electronic evidence in a cool, moisture-free environment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?
A. Autopsy
B. Stream Detector
C. TimeStomp
D. analyzeMFT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
Which of the following tool enables data acquisition and duplication?
A. Xplico
B. Wireshark
C. Colasoft's Capsa
D. DriveSpy
Answer: (SHOW ANSWER)

NEW QUESTION: 37
How do you define Technical Steganography?
A. Steganography that uses physical or chemical means to hide the existence of a message
B. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways
C. Steganography that utilizes visual symbols or signs to hide secret messages
D. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?
A. Master file tables
B. Rainbow tables
C. Database tables
D. Hash tables

Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?
A. Syllable attack
B. Hybrid attack
C. Rule-based attack
D. Brute forcing attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
The newer Macintosh Operating System (MacOS X) is based on:
A. BSD Unix
B. Microsoft Windows
C. OS/2
D. Linux
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which one of the following is not a first response procedure?
A. Crack passwords
B. Preserve volatile data
C. Take photos
D. Fill forms
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?
A. 110
B. 135
C. 25
D. 10
Answer: (SHOW ANSWER)

NEW QUESTION: 43

The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.
The ARP table can be accessed using the _____command in Windows 7.
A. C:\arp -b
B. C:\arp -d
C. C:\arp -s
D. C:\arp -a
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Place the following In order of volatility from most volatile to the least volatile.
A. Registers and cache, routing tables, temporary file systems, archival media, disk storage
B. Registers and cache, routing tables, temporary file systems, disk storage, archival media
C. Register and cache, temporary file systems, routing tables, disk storage, archival media
D. Archival media, temporary file systems, disk storage, archival media, register and cache
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?
A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern Europe
B. Data is being exfiltrated by an advanced persistent threat (APT)
C. Internal systems are downloading automatic Windows updates
D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?
A. Collect the evidence
B. Evaluate and secure the scene
C. Obtain search warrant
D. Acquire the data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
The working of the Tor browser is based on which of the following concepts?
A. Static routing
B. Both static and default routing
C. Default routing
D. Onion routing
Answer: D (LEAVE A REPLY)

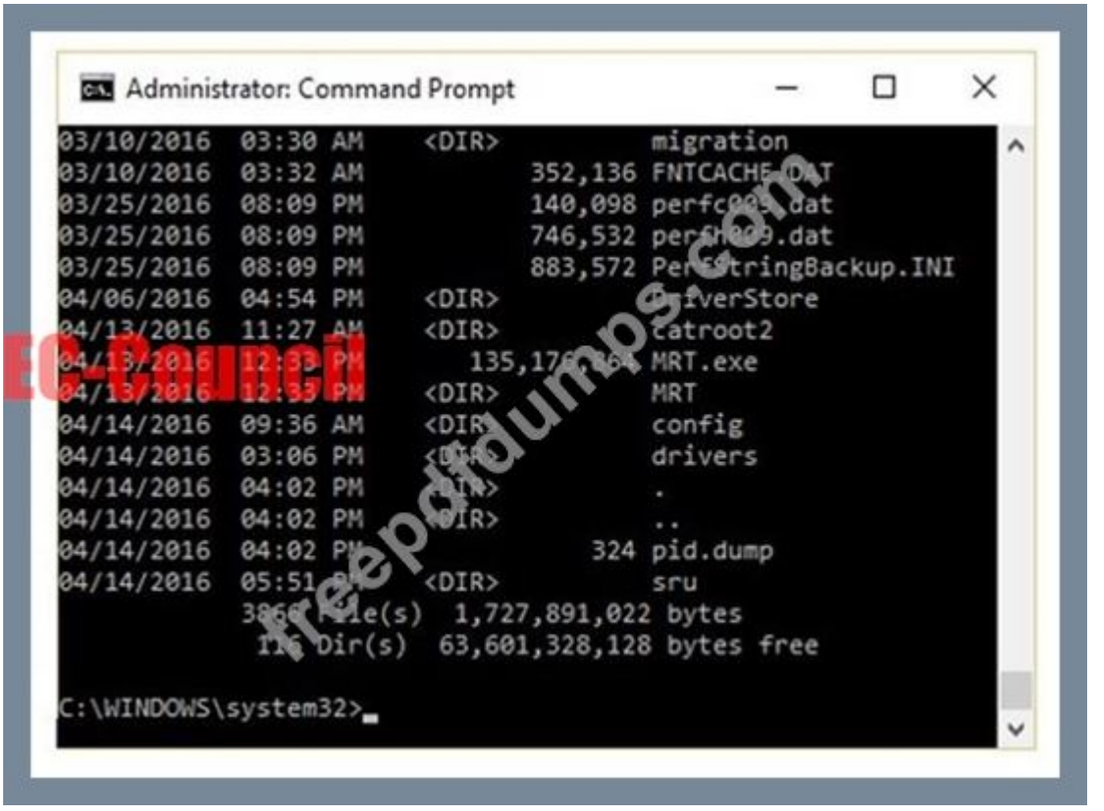
NEW QUESTION: 48
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software ?
A. National Institute of Standards and Technology (NIST)
B. Computer Forensics Tools and Validation Committee (CFTVC)
C. Association of Computer Forensics Software Manufactures (ACFSM)
D. Society for Valid Forensics Tools and Testing (SVFTT)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?
A. Rainbow attack
B. Distributed network attack
C. Replay attack
D. Man-in-the-middle (MITM) attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
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. Create a Separate partition of several hundred megabytes and place the swap file there

B. Use intrusion forensic techniques to study memory resident infections
C. Use Vmware to be able to capture the data in memory and examine it
D. Give the Operating System a minimal amount of memory, forcing it to use a swap file
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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:s
B. dir /o:n
C. dir /o:e
D. dir /o:d
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.
A. Physical block
B. Logical block
C. Hard disk block
D. Operating system block
Answer: (SHOW ANSWER)

NEW QUESTION: 53
A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.
A. Phone number receiving the call
B. A unique sequence number identifying the record
C. The call duration
D. The language of the call
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
Consider the scenario where a large multinational corporation suspects an internal security breach, with significant data possibly compromised. The corporate forensic team initiates the process of conducting a comprehensive forensic investigation following the search and seizure protocols. During this process, they want to ensure they capture all the required information and minimize disruption to the company's ongoing business operations. Which among the following activities should NOT be a part of their plan for this search and seizure operation?
A. Obtaining formal written consent from the company's owner before beginning the investigation process
B. Requesting a warrant for search and seizure detailing the exact locations and types of evidence expected to be found
C. Generating a comprehensive list of all potentially involved devices along with their specifications, status, and locations
D. Carrying out all search and seizure activities without seeking witness signatures for the activities performed
Answer: (SHOW ANSWER)

NEW QUESTION: 56
What is static executable file analysis?
A. It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment
B. It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances
C. It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances

D. It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
How many possible sequence number combinations are there in TCP/IP protocol?
A. 4 billion
B. 32 million
C. 1 billion
D. 320 billion
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?
A. netcat
B. ApexSQL Audit
C. Notepad++
D. Event Log Explorer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 59
A cybersecurity investigator is conducting a search and seizure operation involving a large data breach. She needs a witness's signature for the agreement to proceed. She is considering one of her team members as a witness but is unsure whether this would comply with standard procedures. According to best practices in obtaining witness signatures during such operations, what actions should she take?
A. She should choose a member from her team as a witness as it saves time and resources
B. If one witness is needed, she may consider her team member, given that they understand the relevance and can testify voluntarily
C. She should not involve any of her team members as a witness to avoid potential bias in court
D. She should choose anyone present during the seizure as a witness regardless of their understanding of the case
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
You should make at least how many bit-stream copies of a suspect drive?
A. 2
B. 4
C. 1
D. 3

Answer: (SHOW ANSWER)

NEW QUESTION: 61
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 D drive to C drive in fifth sequential order
B. A text file deleted from C drive in sixth sequential order
C. A text file deleted from C drive in fifth sequential order
D. A text file copied from C drive to D drive in fifth sequential order
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?
A. Create another VM by using the snapshot
B. Delete the OS disk of the affected VM altogether
C. Delete the snapshot from the source resource group
D. Recommend changing the access policies followed by the company
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
How many times can data be written to a DVD+R disk?
A. Once
B. Zero
C. Infinite
D. Twice
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.
Why were these passwords cracked so Quickly?
A. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
B. The passwords that were cracked are local accounts on the Domain Controller
C. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
D. Passwords of 14 characters or less are broken up into two 7-character hashes
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?
A. Civil Investigation
B. Both Civil and Criminal Investigations
C. Criminal Investigation
D. Administrative Investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?
A. ESE Database
B. Sparse files
C. Slack Space
D. Virtual Memory
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?
A. WIN-DTRAI83202X-bin.nnnnnn
B. WIN-DTRAI83202Xslow.log

C. WIN-DTRAI83202Xrelay-bin.index
D. relay-log.info
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following tools will help the investigator to analyze web server logs?
A. LanWhois
B. Deep Log Monitor
C. XRY LOGICAL
D. Deep Log Analyzer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
When cataloging digital evidence, the primary goal is to
A. Preserve evidence integrity
B. Not remove the evidence from the scene
C. Not allow the computer to be turned off
D. Make bit-stream images of all hard drives
Answer: (SHOW ANSWER)

NEW QUESTION: 70
What will the following URL produce in an unpatched IIS Web Server?
http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\
A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of C: drive on the web server
D. Directory listing of the C:\windows\system32 folder on the web server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
During a computer hacking forensic investigation, an investigator is tasked with acquiring volatile data from a live Linux system with limited physical access. Which methodology would be the most suitable for this scenario?
A. Performing remote acquisition of volatile data from a Linux machine using dd and netcat
B. Using the fmem module and dd command locally to access the RAM and acquire its content directly
C. Performing local acquisition of RAM using the LiME tool
D. Using Belkasoft Live RAM Capturer to extract the entire contents of the computer's volatile memory
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure.
What forensics privacy issue was not addressed prior to collecting the evidence?
A. Compliance with the Third Amendment of the U.S. Constitution
B. None of these
C. Compliance with the Fourth Amendment of the U.S. Constitution
D. Compliance with the Second Amendment of the U.S. Constitution
Answer: (SHOW ANSWER)

NEW QUESTION: 73
As a Computer Hacking Forensics Investigator, you are tasked with tracing a series of illegal transactions believed to originate from the dark web. You know the transactions were made using Tor, a browser providing anonymity. However, in an authoritarian country where the usage of the Tor network is restricted, the suspect is believed to be using an undisclosed Tor network feature to bypass these restrictions. What feature is likely being used in this scenario?
A. Exit Relay
B. Tor Bridge Node
C. Middle Relay
D. Entry/Guard Relay
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74
Study the log given below and answer the following question:
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from
194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 ->
172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 ->
172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:
194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from
24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 ->
172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 ->
172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:
198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 ->
172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for
user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user
simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 ->
172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23
-> 213.28.22.189:4558
Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?
A. Disallow UDP 53 in from outside to DNS server
B. Block all UDP traffic
C. Disallow TCP 53 in from secondaries or ISP server to DNS server
D. Allow UDP 53 in from DNS server to outside
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
An experienced forensic investigator, Chris, is tasked with preparing a testbed for malware analysis. Given the complexity of the malware samples, which are mostly compatible with Windows binary executables, Chris must take meticulous precautions to ensure the integrity of the lab environment. Which of the following procedures would Chris NOT be likely to follow in preparing the testbed for malware analysis?
A. Enabling shared folders and guest isolation allows easy data transfer between host and guest operating systems
B. Using tools such as INetSim to simulate internet services while ensuring that the NIC card is in "host only" mode
C. Installing a guest OS such as Ubuntu in virtual machines will serve as forensic workstations
D. Creating a snapshot of the virtual machine state prior to malware analysis for easy reversion in case of accidental system corruption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
Which MySQL log file contains information on server start and stop?

A. Slow query log file
B. General query log file
C. Error log file
D. Binary log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 77
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. Backup a disk to an image file
C. Search for disk errors within an image file
D. Copy a partition to an image file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
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. 32-bit address
D. 16-bit address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?
A. Verbal Informal Report
B. Written Formal Report
C. Verbal Formal Report
D. Written Informal Report

Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document It Is. whether It Is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?
A. pdfid.py
B. oleid.py
C. oleform.py
D. oledir.py
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
In a forensic investigation on an Android device, a Computer Hacking Forensics Investigator is required to extract information from the SQLite database. They aim to recover the user's web browsing history. Which is the correct SQLite database path that the investigator should focus on?
A. \data\com.android.providers.calendar\databases\calendar.db
B. \data\data\com.android.browser\databases\browser2.db
C. \data\data\com.android.providers.telephony\databases\mmssms.db
D. \data\data\com.android.providers.contacts\databases\contacts2.db
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?
A. PEiD
B. Dependency Walker
C. SysAnalyzer
D. Comodo Programs Manager
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A. Security Layer
B. Access Layer
C. Presentation Layer
D. Discovery Layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
Why is it a good idea to perform a penetration test from the inside?
A. It is never a good idea to perform a penetration test from the inside
B. To attack a network from a hacker's perspective
C. Because 70% of attacks are from inside the organization
D. It is easier to hack from the inside
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
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. Parameter Tampering
B. Cross Site Request Forgery
C. Session Fixation Attack
D. Cookie Tampering
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
An investigator seized a notebook device installed with a Microsoft Windows OS.
Which type of files would support an investigation of the data size and structure in the device?
A. HFS and GNUC
B. NTFSandFAT
C. APFSandHFS
D. Ext2 and Ext4
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Rule-based approach
B. Graph-based approach

C. Automated field correlation approach
D. Neural network-based approach
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling It. the dates and times when it Is being handled, and the place of storage of the evidence. What do you call this document?
A. Chain of custody
B. Consent form
C. Log book
D. Authorization form
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:
A. Terrible evidence
B. exculpatory evidence
C. mandatory evidence
D. Inculpatory evidence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
A Computer Hacking Forensics Investigator (CHFI) is working on a case involving an encrypted file from a user profile that was deleted. The investigator knows that the file was encrypted using the Encrypted File System (EFS) on a Windows operating system. The system is still bootable, but the original user profile is gone, and the system administrator has reset the account password. What would be the most suitable tool to recover this EFS-encrypted file?
A. VeraCrypt, a widely used tool in anti-forensics encryption
B. Advanced EFS Data Recovery, a tool for decrypting protected files
C. Shredlt, a disk wiping utility tool
D. AnalyzeMFT, a tool for examining MACE times in NTFS file systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
What is cold boot (hard boot)?
A. It is the process of restarting a computer that is already in sleep mode
B. It is the process of shutting down a computer from a powered-on or on state

C. It is the process of starting a computer from a powered-down or off state
D. It is the process of restarting a computer that is already turned on through the operating system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
An investigator is conducting a forensic analysis on a Windows machine suspected of accessing the Dark Web. The investigator has found Tor browser artifacts, but the Tor browser has been uninstalled. Which of the following steps should the investigator take next to obtain more information on the user's activities?
A. Examine the registry key: HKEY_USERS\\SOFTWARE\Mozilla\Firefox\Launcher for path information
B. Check the prefetch files using a tool such as WinPrefetchView
C. Look for the 'State' file in the \Tor Browser\Browser\TorBrowser\Data\Tor\ directory
D. Use the netstat -ano command to check the active network connections
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?
A. ISO/IEC 17025
B. ISO/IEC 16025
C. ISO/IEC 18025
D. ISO/IEC 19025
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Cyber-crime is defined as any Illegal act involving a gun, ammunition, or its applications.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?
A. MS-office Word OneNote
B. Portable Document Format
C. MS-office Word PowerPoint
D. MS-office Word Document
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
During the process of a forensic investigation after a cyber incident, a team of forensic analysts conducts the initial response on-site. One member of the team is packaging the collected electronic evidence. What is the most appropriate step the team member should take during this phase according to the standard forensic investigation process?
A. The team member should connect the collected electronic devices to a safe computer system to create backup data
B. The team member should turn off all devices before packaging to prevent any potential damage to the data
C. The team member should strictly follow exhibit numbering and provide accurate information on the front panel of the evidence bags
D. The team member should conduct a preliminary analysis of the collected evidence before packaging
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Raw data acquisition format creates _____of a data set or suspect drive.
A. Simple sequential flat files
B. Segmented image files
C. Compressed image files
D. Segmented files
Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
International Mobile Equipment Identifier (IMEI) is a 15-dlgit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:
A. Integrated Circuit Code (ICC)
B. Type Allocation Code (TAC)
C. Device Origin Code (DOC)
D. Manufacturer identification Code (MIC)

Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
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. Connection rejected
C. An email marked as potential spam
D. Security event was monitored but not stopped
Answer: (SHOW ANSWER)

NEW QUESTION: 100
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: 101
Graphics Interchange Format (GIF) is a ____ RGB bitmap image format for images with up to 256 distinct colors per frame.
A. 32-bit
B. 8-bit
C. 24-bit
D. 16-bit
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.
A. Devcon
B. fsutil
C. Reg.exe

D. DevScan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
Physical security recommendations: There should be only one entrance to a forensics lab
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
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. 7 Sectors
B. 6 Sectors
C. 5 Sectors
D. 4 Sectors
Answer: (SHOW ANSWER)

NEW QUESTION: 105
The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used. Which command displays the network configuration of the NICs on the system?
A. tasklist
B. ipconfig /all
C. net session
D. netstat
Answer: (SHOW ANSWER)

NEW QUESTION: 106
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 the 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. Incremental backup copy
B. Full backup copy
C. Robust copy

D. Bit-stream copy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry key Smith will check to find the above information?
A. MountedDevices key
B. RunMRU key
C. TypedURLs key
D. UserAssist Key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
A computer forensic report is a report which provides detailed information on the complete forensics investigation process.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?
A. Only an HTTPS session can be hijacked
B. Only DNS traffic can be hijacked
C. HTTP protocol does not maintain session
D. Only FTP traffic can be hijacked
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion

B. Cross Site Request Forgery

C. Insecure Direct Object References

D. Cross Site Scripting

Answer: C (LEAVE A REPLY)

NEW QUESTION: 111

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

A. Timeout Exploitation

B. Password Exploitation

C. I/O exploitation

D. Session ID in URLs

Answer: (SHOW ANSWER)

NEW QUESTION: 112

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

A. Kernel ring buffer information

B. Debugging log messages

C. Global system messages

D. All mail server message logs

Answer: A (LEAVE A REPLY)

NEW QUESTION: 113

Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

A. TRIPWIRE

B. Capsa

C. RAM Computer

D. Regshot

Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
What is the smallest physical storage unit on a hard drive?
A. Track
B. Platter
C. Cluster
D. Sector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.
A. Drive:\$Recycle.Bin
B. DriveARECYCLER
C. C:\RECYCLED
D. DriveARECYCLED
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.

A. 44
B. 001451548
C. 245252
D. 89
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
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: 118
Which of the following is a part of a Solid-State Drive (SSD)?
A. NAND-based flash memory
B. Cylinder
C. Spindle
D. Head
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
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: (SHOW ANSWER)

NEW QUESTION: 120
Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?
A. Dynamic analysis
B. File fingerprinting
C. Static analysis
D. Identifying file obfuscation
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format.
SAM file in Windows is located at:
A. C:\windows\system32\Boot\SAM
B. C:\windows\system32\drivers\SAM
C. C:\windows\system32\con\SAM
D. C:\windows\system32\config\SAM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
Which of these Windows utility help you to repair logical file system errors?
A. CHKDSK
B. Resource Monitor
C. Disk cleanup
D. Disk defragmenter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?
A. RestrictAnonymous must be set to "2" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. RestrictAnonymous must be set to "10" for complete security
D. There is no way to always prevent an anonymous null session from establishing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

A. Those connections are in listening mode

B. Those connections are in closed/waiting mode

C. Those connections are in timed out/waiting mode

D. Those connections are established

Answer: (SHOW ANSWER)

NEW QUESTION: 125

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

NEW QUESTION: 126
Where are files temporarily written in Unix when printing?
A. /usr/spool
B. /spool
C. /var/print
D. /var/spool
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
Injection flaws are web application vulnerabilities that allow untrusted data to be Interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?
A. SQL Injection
B. Password brute force
C. Nmap Scanning
D. Footprinting
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?
A. Status of network hardware
B. Information about network connections
C. Net status of computer usage
D. Status of users connected to the internet
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network.

Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic

B. Metamorphic

C. Transmorphic

D. Oligomorhic

Answer: (SHOW ANSWER)

NEW QUESTION: 130

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

A. 512 Bytes

B. 4092 Bytes

C. 1048 Bytes

D. Depends on the capacity of the storage device

Answer: (SHOW ANSWER)

NEW QUESTION: 131

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port == 21

B. tcp.port == 21 || tcp.port == 22

C. tcp.port != 21

D. tcp.port = 23

Answer: A (LEAVE A REPLY)

NEW QUESTION: 132

In an email crime investigation, the forensic investigator analyses a computer using the Microsoft Outlook application. The investigator knows that Outlook stores email data in both .pst and .ost file formats. They want to focus on the files that hold the email data even when there is no internet connection. Which files should the investigator target for a deeper analysis?

A. Personal Storage Table (.pst) files located at C:\Users\%USERNAME%\Documents\Outlook Files

B. Offline Storage Table (.ost) files located at C:\Users\%USERNAME%\AppData\Local\Microsoft \Outlook

C. Email data located within Mozilla Thunderbird and Apple Mail email clients
D. Archived email files in .pst format located via File -> Options -> Advanced -> AutoArchive Settings
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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's PBX system be called?
A. Crunching
B. Pretexting
C. Phreaking
D. Squatting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
When investigating a Windows System, it is important to view the contents of the page or swap file because:
A. A Large volume of data can exist within the swap file of which the computer user has no knowledge
B. Windows stores all of the systems configuration information in this file
C. This is file that windows use to communicate directly with Registry
D. This is the file that windows use to store the history of the last 100 commands that were run from the command line
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?
A. Justification
B. Authentication
C. Certification
D. Reiteration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136

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

NEW QUESTION: 137
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?
A. Use a system that has a dynamic addressing on the network
B. Use a system that is not directly interacing with the router
C. It doesn't matter as all replies are faked
D. Use it on a system in an external DMZ in front of the firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 138
What layer of the OSI model do TCP and UDP utilize?
A. Session
B. Transport
C. Network
D. Data Link
Answer: B (LEAVE A REPLY)

NEW QUESTION: 139
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?
A. Malvertising
B. Compromising a legitimate site
C. Click-jacking
D. Spearphishing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
A. PUB.EDB
B. gwcheck.db
C. PRIV.EDB
D. PRIV.STM
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Why would you need to find out the gateway of a device when investigating a wireless attack?
A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP used to manage the access point
C. The gateway will be the IP of the attacker computer
D. The gateway will be the IP used to manage the RADIUS server
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Before performing a logical or physical search of a drive in Encase, what must be added to the program?
A. File signatures
B. Bookmarks
C. Keywords
D. Hash sets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
You should always work with original evidence
A. False

B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 145
Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?
A. Botnets
B. Emulators
C. Packers
D. Password crackers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 146
A digital forensic investigator examines a Windows system to identify suspicious activity related to a recent cyber incident. She has collected volatile and non-volatile registry hives for analysis. The investigator has noticed modifications in a user's profile settings, including changes in desktop wallpaper and screen colors. Which hive and component cells in the registry should she examine more closely for further evidence of user-specific activity?
A. Examine HKEY_CLASSES_ROOT; focus on security descriptor cells and value cells
B. Examine HKEY_LOCAI MACHINE; focus on value cells and subkey list cells
C. Examine HKEY_CURRENT_USER; focus on key cells and value list cells
D. Examine HKEY_CURRENT_CONFIG: focus on subkey list cells and value cells
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
During an investigation, a forensics analyst discovers an unusual increase in outbound network traffic, network traffic traversing on non-standard ports, and multiple failed login attempts on a host system. The analyst also found that certain programs were using these unusual ports, appearing to be legitimate. If these are the primary Indicators of Compromise, what should be the next immediate step in the investigation to contain the intrusion effectively?
A. Examining the logs for repeated requests for the same file, indicating a possible exploit attempt
B. Analyzing Uniform Resource Locators for any signs of phishing or spamming activities
C. Conducting a deep dive into user-agent strings to determine if there is any spoofing of device OS and browser information
D. Enforcing stringent password policies and re-authenticating all users to prevent further login anomalies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
An investigator is examining a compromised system and comes across some files that have been compressed with a packer. The investigator knows that these files contain malicious content, but

cannot access them due to a password protection mechanism. The investigator does not have the password. Which approach is the most suitable for accessing the contents of the packed files?

A. The investigator should attempt static analysis on the packed file

B. The investigator should attempt to reverse engineer the packed file in an attempt to bypass password protection

C. The investigator should attempt to crack the password using a brute force attack

D. The investigator should run the packed executable in a controlled environment for dynamic analysis

Answer: D (LEAVE A REPLY)

NEW QUESTION: 149

This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?

A. Testimony by the accused

B. Limited admissibility

C. Hearsay rule

D. Rule 1001

Answer: C (LEAVE A REPLY)

NEW QUESTION: 150

Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every_____.

A. 10.000 packets

B. 15,000 packets

C. 5,000 packets

D. 20.000 packets

Answer: (SHOW ANSWER)

NEW QUESTION: 151

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.

(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772
=+=
+=
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+=
+=
03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104
Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c............
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....
3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost
=+=
+=+=+
03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168
TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF
AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23679878 2880015
63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;
69 64 3B id;

A. The attacker has scanned and exploited the system using Buffer Overflow
B. The attacker has installed a backdoor
C. The attacker has conducted a network sweep on port 111
D. The attacker has used a Trojan on port 32773

Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
When using an iPod and the host computer is running Windows, what file system will be used?
A. FAT16
B. iPod+
C. FAT32
D. HFS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 153
Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:
A. Drive:\REYCLED
B. Drive:\$ Recycle. Bin
C. Drive:\RECYCLER
D. DriveARECYCIE.BIN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
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. Trace files record, user-defined events, and specific system events
D. Forensic investigator uses SQL Server Profiler to view error log files
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?
A. fsck
B. dmesg
C. grep
D. pgrep
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?
A. Cloud as an object
B. Cloud as a service
C. Cloud as a tool
D. Cloud as a subject
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?
A. Obfuscator
B. Dropper
C. Injector
D. Packer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 158
Shortcuts are the files with the extension .lnk that are created and are accessed by the users. These files provide you with information about:
A. Running application
B. Application logs
C. System logs
D. Files or network shares
Answer: (SHOW ANSWER)

NEW QUESTION: 159
If you come across a sheepdip machine at your client site, what would you infer?
A. A sheepdip coordinates several honeypots
B. A sheepdip computer defers a denial of service attack
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer is another name for a honeypot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?
A. BMP
B. ASCII
C. JPEG
D. GIF
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Which of the following techniques can be used to beat steganography?
A. Cryptanalysis
B. Decryption

C. Encryption
D. Steganalysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
A forensic investigator is analyzing a Windows 10 machine that has unexpectedly crashed several times in the past week. The investigator needs to determine whether these crashes are due to an internal error or caused by a remote attacker who exploited a bug in the operating system. The investigator has crash dump files and access to various tools. What should be the investigator's most immediate action?
A. Analyze the crash dump files using DumpChk to examine the system crash's cause and identify any errors in the applications or the operating system
B. Use the Process Dumper tool to dump the entire process space and analyze the contents in the RAM dump file
C. Utilize Redline to perform Indicators of Compromise (IOC) analysis and construct a timeline of potential cyber incidents
D. Apply Handle.exe to see the object types and names of all the handles of the crashed programs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 163
The investigative team at a private security firm is conducting a forensic examination of a complex cyberattack case. They need to follow the ACPO Principles of Digital Evidence during the investigation. However, one of the investigators is unsure of some of these principles. Which of the following statements correctly represents the ACPO principles?
A. Any original data accessed for the investigation can be changed by any team member if deemed necessary
B. The audit trail of all processes applied to the digital evidence must be created and preserved, but a third-party examination is not necessary
C. Any individual, regardless of their competence level, can access original data held on a computer if they can explain the relevance of their actions
D. The person leading the investigation is responsible for ensuring the adherence to the law and these principles, regardless of the actions of their subordinates
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which list contains the most recent actions performed by a Windows User?
A. Recents
B. Activity
C. Windows Error Log
D. MRU

Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
A clothing company has recently deployed a website on Its latest product line to Increase Its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from Intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?
A. Kon-Boot
B. ModSecurity
C. CryptaPix
D. Recuva
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
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. RaidSniff
B. Airsnort
C. Ettercap
D. Snort
Answer: (SHOW ANSWER)

NEW QUESTION: 167
During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9\%]+" in analyzed evidence details. What is the expression used for?
A. Checks for closing angle bracket, hex or double-encoded hex equivalent
B. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

C. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
D. Checks for opening angle bracket, its hex or double-encoded hex equivalent
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?
A. Service level management
B. Service level agreement
C. National and local regulation
D. Key performance indicator
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
A. Heads
B. Interface
C. Cylinder
D. Sectors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 170
Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____in order to control the process execution, crash the process and modify internal variables.
A. Target rainbow table
B. Target process's address space
C. Target remote access
D. Target SAM file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 171
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?
A. Microsoft Outlook
B. Eudora
C. Microsoft Outlook Express
D. Mozilla Thunderbird

Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
Area density refers to:
A. the amount of data per platter
B. the amount of data per partition
C. the amount of data per disk
D. the amount of data per square inch
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 173
During an investigation of a suspected email crime, the forensics team noted that the criminal used emails to sell illegal narcotics and execute numerous frauds. The team identified that the criminal had also used an advanced phishing technique to target a specific executive in the victim's organization. Which phishing technique was likely used in this scenario?
A. Spear Phishing
B. Pharming
C. Spimming
D. Whaling
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
When NTFS Is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code
A. First 16
B. First 22
C. First 24
D. First 12
Answer: (SHOW ANSWER)

NEW QUESTION: 175
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. ff d8 ff
B. d0 0f 11 e0
C. 25 50 44 46
D. 50 41 03 04
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176

Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?
A. Click-jacking
B. Compromising a legitimate site
C. Malvertising
D. Spearphishing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
Digital evidence is not fragile in nature.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178
An "idle" system is also referred to as what?
A. Bot
B. Zombie
C. PC not being used
D. PC not connected to the Internet
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Printing under a Windows Computer normally requires which one of the following files types to be created?
A. EME
B. MEM
C. EMF
D. CME
Answer: C (LEAVE A REPLY)

NEW QUESTION: 180
There's a digital forensics investigator delving into a case right now. The situation involves an SQL Server database that's been tampered with by an intruder. Some data from the database has vanished, and the real kicker is that there aren't any backup files to be found. The investigator's task is to recover as much data as possible. The investigator needs to understand which SQL Server data file will most likely assist in the data recovery. What should be the investigator's primary focus?
A. LDF because it holds the log information associated with the database
B. MDF because it stores all data in the database objects
C. Page Header because it contains metadata about the page like page ID, page type

D. NDF because it can store additional data separate from the primary data file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 181
Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:
A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management
Answer: (SHOW ANSWER)

NEW QUESTION: 182
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. UDP
B. OSPF
C. BPG
D. ATM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 183
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

A. *#06#
B. #*06*#
C. *IMEI#
D. #06#*
Answer: (SHOW ANSWER)

NEW QUESTION: 184
What system details can an investigator obtain from the NetBIOS name table cache?
A. List of connections made to other systems
B. List of the system present on a router
C. List of files shared between the connected systems
D. List of files opened on other systems
Answer: (SHOW ANSWER)

NEW QUESTION: 185
William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000) "GET / HTTP/1.1" 200 1861.
Which of the following logs does the log entry belong to?
A. The combined log format of Apache access log
B. IIS log
C. Apache error log
D. The common log format of Apache access log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 186
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 zero
B. Firewalk sets all packets with a TTL of one
C. Firewalk cannot be detected by network sniffers
D. Firewalk cannot pass through Cisco firewalls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
An international corporation is targeted by a severe data breach, resulting in massive corruption in its MySQL database. The forensic investigator is responsible for recovering the corrupted data and tracing the perpetrators. During the investigation, the team detected a high number of unauthorized access attempts from several hostnames and usernames that coincided with the attack. Which MySQL utility program would most suitably validate these access attempts in this scenario?

A. Mysqldump, for its capacity to dump a database or a collection of databases for backup and restore purposes
B. Myisamlog, for its functionality to process the contents of the MyISAM log file and perform recovery operations
C. Mysqlbinlog, due to its ability to read and display binary log files in text format
D. Mysqlaccess, due to its ability to check and validate the access privileges defined for a hostname or username
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?
A. .txt
B. .ibl
C. .log
D. .cbl
Answer: (SHOW ANSWER)

NEW QUESTION: 189
To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?
A. Post-investigation phase
B. Investigation phase
C. Reporting phase
D. Pre-investigation phase
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following is not an example of a cyber-crime?
A. Deliberate circumvention of the computer security systems
B. Fraud achieved by the manipulation of the computer records
C. Intellectual property theft, including software piracy
D. Firing an employee for misconduct
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
Which of the following statements is incorrect when preserving digital evidence?
A. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
B. Verify if the monitor is in on, off, or in sleep mode
C. Remove the plug from the power router or modem

D. Turn on the computer and extract Windows event viewer log files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 192
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 criminal case must be secured more tightly than in a civil case
B. evidence in a civil case must be secured more tightly than in a criminal case
C. evidence procedures are not important unless you work for a law enforcement agency
D. evidence must be handled in the same way regardless of the type of case
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
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. Samspade.org
C. Proxify.net
D. Archive.org
Answer: D (LEAVE A REPLY)

NEW QUESTION: 194
While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h.
What does this indicate on the computer?
A. The files are corrupt and cannot be recovered
B. The files have been marked for deletion
C. The files have been marked as read-only
D. The files have been marked as hidden
Answer: (SHOW ANSWER)

NEW QUESTION: 195
What will the following command accomplish?
dd if=/dev/xxx of=mbr.backup bs=512 count=1
A. Restore the master boot record
B. Mount the master boot record on the first partition of the hard drive
C. Restore the first 512 bytes of the first partition of the hard drive
D. Back up the master boot record
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196

A considerable data breach has struck a global company, leading to the unfortunate loss of confidential data. The corporation's Cybersecurity unit now faces the task of conducting a deep-dive investigation into this incident. Their findings suggest that advanced hacking tools were utilized in the breach, with the attack seemingly initiated from inside the organization itself. Based on this information which statement best describes the type of cybercrime and the potential challenge in this forensic investigation?

A. Cybercrime can be categorized as an external attack, and the primary challenge will be tracing the IP addresses of the attacker

B. Cybercrime can be categorized as an external attack, and the primary challenge will be identifying the source of the sophisticated hacking tools

C. Cybercrime can be categorized as an internal attack, and the major challenge will be the probable damage to the physical infrastructure

D. Cybercrime can be categorized as an internal attack, and a potential challenge will be proving the insider's intent since the attack tools were advanced

Answer: D (LEAVE A REPLY)

NEW QUESTION: 197

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

A. True

B. False

Answer: A (LEAVE A REPLY)

NEW QUESTION: 198

Investigator Janet comes across a suspicious Windows registry key during a computer hacking forensic investigation. She believes modifying this key is associated with the recent cyberattack on the company's servers. In order to confirm this, Janet needs to reference a timestamp embedded inside the registry key. What is the correct name of this timestamp?

A. User Activity Time

B. Last Write Time

C. System Modification Time

D. Current System Time

Answer: B (LEAVE A REPLY)

NEW QUESTION: 199
According to RFC 3227, which of the following is considered as the most volatile item on a typical system?
A. Temporary system files
B. Kernel statistics and memory
C. Archival media
D. Registers and cache
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
Windows identifies which application to open a file with by examining which of the following?
A. The file attributes
B. The file signature at the beginning of the file
C. The File extension
D. The file Signature at the end of the file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
A Computer Hacking Forensic Investigator (CHFI) arrives at the crime scene in an incident involving cybercrime. While performing the initial search of the scene, the investigator spots a GPS device, a keyboard, and a telephone line connected to a caller ID box. Considering the steps involved in searching for evidence, which of the following actions should the investigator perform first?
A. Record observations about the current situation at the scene
B. Initiate the search and seizure evidence log to document details of the identified devices
C. Survey the GPS device to explore potential sources of digital information
D. Secure the keyboard to protect any potential fingerprints
Answer: B (LEAVE A REPLY)

NEW QUESTION: 202
When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?
A. The initials of the forensics analyst
B. The sequential number of the exhibits seized by the analyst
C. The sequence number for the parts of the same exhibit
D. The year he evidence was taken
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203

Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?
A. Data Rows point to the location of actual data
B. Data Rows store the actual data
C. Data Rows spreads data across multiple databases
D. Data Rows present Page type. Page ID, and so on
Answer: D (LEAVE A REPLY)

NEW QUESTION: 204
A forensic investigator is examining an attack on a MySQL database. The investigator has been given access to a server, but the physical MySQL data files are encrypted, and the database is currently inaccessible. The attacker seems to have tampered with the data. Which MySQL utility program would most likely assist the investigator in determining the changes that occurred during the attack?
A. Myisamchk, because it views the status of the MyISAM table or checks, repairs, and optimizes them
B. Mysqlbinlog, because it reads the binary log files directly and displays them in text format
C. Mysqlaccess, because it checks the access privileges defined for a hostname or username
D. Mysqldump, because it allows dumping a database for backup purposes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:
A. Type Allocation Code (TAC)
B. Integrated Circuit Code (ICC)
C. Device Origin Code (DOC)
D. Manufacturer Identification Code (MIC)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?
A. Blind bug
B. CGI code
C. Web bug

D. Trojan.downloader
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
Your organization is implementing a new database system and has chosen MySQL due to its pluggable storage engine capability and ability to handle parallel write operations securely. You are responsible for selecting the best-suited storage engine for your company's needs, which predominantly involves transactional processing, crash recovery, and high data consistency requirements. What would be the most appropriate choice?
A. MyISAM storage engine, because it offers unlimited data storage and high-speed data loads
B. InnoDB storage engine, because it supports traditional ACID and crash recovery, and is used in online transaction processing systems
C. BDB storage engine, because it provides an alternative to InnoDB and supports additional transaction methods such as COMMIT and ROLLBACK
D. Memory storage engine, because it offers in-memory tables and implements a hashing mechanism for faster data retrieval
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?
A. Messaging Application Programming Interface (MAPI)
B. Simple Mail Transfer Protocol (SMTP)
C. Internet Message Access Protocol (IMAP)
D. Post Office Protocol version 3 (POP3)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 209
During an intense cybercrime investigation, an inexperienced first responder mistakenly mishandled a piece of digital evidence. It was later discovered that the chain of custody was also incomplete. If not properly documented, which of the following details would make the chain of custody deficient?
A. The exact number of photos taken at the crime scene
B. The reason and process for obtaining the evidence
C. The manufacturing company of the device from which evidence was extracted
D. The color of the digital device from which the evidence was extracted
Answer: B (LEAVE A REPLY)

NEW QUESTION: 210
You are a Computer Hacking Forensic Investigator (CHFI) employed by an international tech firm.

One of your tasks involves overseeing and providing guidance on legal considerations during digital forensic investigations across different jurisdictions. One day, you find yourself dealing with unauthorized system access and data alteration incidents across multiple branches in Germany, Italy, Canada, Singapore, Belgium, Brazil, the Philippines, and Hong Kong. Recognizing that different countries have different laws that can impact the investigation, which of the following legal provisions should you apply when the main offence is the unauthorized modification of computer data?

A. Italy's Penal Code Article 615 ter (Unauthorized access to a computer or telecommunication systems)

B. Germany's Penal Code Section 303a (Alteration of Data)

C. Canada's Criminal Code Section 342.1 (Obtain any computer service and interception of a computer system)

D. Belgium's Article 550(b) of the Criminal Code (Exceeding power of access to a computer system)

Answer: (SHOW ANSWER)

NEW QUESTION: 211

What is a first sector ("sector zero") of a hard disk?

A. Secondary boot record

B. Hard disk boot record

C. Master boot record

D. System boot record

Answer: C (LEAVE A REPLY)

NEW QUESTION: 212

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies?

What type of Penetration Testing is Larry planning to carry out?

A. Internal Penetration Testing

B. Firewall Penetration Testing

C. Router Penetration Testing

D. DoS Penetration Testing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 213
A mid-sized enterprise recently suffered a security breach in their AWS-hosted application. The responsibility for identifying the source and cause of this breach falls under the purview of the internal security team. Based on the AWS shared responsibility model, which of the following would be the appropriate action for the team?
A. Investigate AWS's underlying infrastructure including hardware and databases for security flaws
B. Conduct a full review of AWS's global infrastructure including regions, availability zones, and edge locations
C. Audit the application security and IAM configurations within the enterprise's AWS services
D. Check for security vulnerabilities in AWS container services' OS and application platform
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
An Investigator Is checking a Cisco firewall log that reads as follows:
Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside
What does %ASA-1-106021 denote?
A. Type of traffic
B. Firewall action
C. Mnemonic message
D. Type of request
Answer: B (LEAVE A REPLY)

NEW QUESTION: 215
In a digital forensics investigation involving a data breach at a large corporation, the lead investigator is preparing to obtain a search warrant for seizing potential evidence. She needs to decide which type of warrant is appropriate given that the main suspect s activities seem to have involved significant online communication and data transfer. Which of the following actions should she take?
A. Obtain an electronic storage device search warrant to seize the suspect's personal computer
B. Obtain a service provider search warrant to access the suspect's online communication records
C. Obtain a search warrant for the suspect's company property only, as this is where the crime occurred
D. Obtain a search warrant for the suspect's car, as it's possible that physical evidence may be found there
Answer: B (LEAVE A REPLY)

NEW QUESTION: 216
Where is the startup configuration located on a router?
A. NVRAM
B. Dynamic RAM
C. BootROM
D. Static RAM
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
A cybersecurity forensics investigator is tasked with acquiring data from a suspect's drive for a civil litigation case. The suspect drive is 1TB, and due to time constraints, the investigator decides to prioritize and acquire only data of evidentiary value. The original drive cannot be retained. In this context, which of the following steps should the investigator prioritize?
A. Utilize DriveSpace or DoubleSpace to reduce the data size
B. Use a reliable data acquisition tool to make a copy of the original drive
C. Execute logical acquisition considering the one-time opportunity to capture data
D. Opt for disk-to-image copying for the large suspect drive
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Which of the following commands shows you all of the network services running on Windows-based servers?
A. Net share
B. Net Session
C. Net start
D. Net use
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?
A. Cocoa Touch
B. Media services
C. Core OS
D. Core Services
Answer: C (LEAVE A REPLY)

NEW QUESTION: 220
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

A. HD-DVD
B. Blu-Ray single-layer
C. Blu-Ray dual-layer
D. DVD-18
Answer: C (LEAVE A REPLY)

NEW QUESTION: 221
This organization maintains a database of hash signatures for known software
A. National Software Reference Library
B. International Standards Organization
C. American National standards Institute
D. Institute of Electrical and Electronics Engineers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?
A. APK Analyzer
B. SDK Manager
C. Android Debug Bridge
D. Xcode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 223
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. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
C. It is not possible to have hidden partitions on a hard drive
D. Add up the total size of all known partitions and compare it to the total size of the hard drive
Answer: (SHOW ANSWER)

NEW QUESTION: 224
What is the default IIS log location?
A. %SystemDrive%\inetpub\logs\LogFiles
B. %SystemDrive\logs\LogFiles
C. SystemDrive\logs\LogFiles
D. SystemDrive\inetpub\LogFiles
Answer: (SHOW ANSWER)

NEW QUESTION: 225

Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

A. He should again attempt PIN guesses after a time of 24 hours

B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN

C. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 226

What technique is used by JPEGs for compression?

A. TCD

B. ZIP

C. DCT

D. TIFF-8

Answer: C (LEAVE A REPLY)

NEW QUESTION: 227

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. 11.17 GB

D. 57.19 GB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 228
Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera.
Why did she not collect the digital camera?
A. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
B. The digital camera was not listed as one of the digital devices in the warrant
C. Debbie overlooked the digital camera because it is not a computer system
D. The digital camera was old. had a cracked screen, and did not have batteries.Therefore, it could not have been used in a crime.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 229
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
A. Encrypt the backup tapes and use a courier to transport them.
B. Hash the backup tapes and transport them in a lock box.
C. Encrypt the backup tapes and transport them in a lock box
D. Degauss the backup tapes and transport them in a lock box.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 230
A forensics investigator is studying the Event ID logs on a domain controller for a corporation, following a suspected security breach. He notices that a domain user account was created, then modified, and then added to a group in a very short span of time. The investigator realizes that he must cross-verify the audit policies on the local system to understand if any changes were made to it. Assuming that the investigator has the correct audit policy settings, which of the following Event IDs should he focus on?
A. Event ID 624
B. Event ID 642
C. Event ID 612
D. Event ID 644
Answer: (SHOW ANSWER)

NEW QUESTION: 231
What TCP/UDP port does the toolkit program netstat use?
A. Port 69
B. Port 15
C. Port 7
D. Port 23
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
During an ongoing cybercrime investigation involving a significant amount of encrypted communication, a Computer Hacking Forensic Investigator (CHFI) believes the suspect's computer holds crucial evidence. However, there's a high chance that the suspect could destroy the evidence before obtaining a warrant. Which action is legally permissible in this circumstance according to the US courts?
A. The investigator should wait for a warrant regardless of potential evidence destruction
B. The investigator can seize the evidence without a warrant but must immediately seek a retroactive warrant
C. The investigator can seize the evidence without a warrant if there's probable cause to believe that the computer holds evidence of the crime
D. The investigator cannot seize the evidence without the suspect's consent, even if there's an imminent risk of evidence destruction
Answer: (SHOW ANSWER)

NEW QUESTION: 233
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?
A. Four
B. One
C. Two
D. Three
Answer: (SHOW ANSWER)

NEW QUESTION: 234
During a complex malware investigation, a forensic investigator found a binary executable suspected to contain malicious code. The investigator decides to perform static malware analysis to identify and analyze the threat. Which of the following actions should be performed next by the investigator to reveal essential information about the executable's functionalities and features?
A. Calculating the cryptographic hash of the binary file for file fingerprinting
B. Disassembling the binary executable to study its structure and functionality

C. Performing a string search in the binary using ResourcesExtract tool
D. Submitting the executable to VirusTotal for online scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 235
A forensic investigator prepares to present digital evidence related to a high-profile cybercrime case in court. He needs to ensure that the evidence complies with the five basic rules of evidence. Which of the following actions does NOT align with these rules?
A. He ensures that the evidence is complete, providing sufficient information to either prove or disprove the consensual fact in the litigation
B. He works directly on the original digital evidence to maintain its reliability
C. He gets an expert opinion to confirm the investigation process and make the evidence understandable
D. He gathers supporting documents regarding the authenticity of the evidence, including the source and its relevance to the case
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?
A. Scientific Working Group on Digital Evidence
B. Daubert Standard
C. Fyre Standard
D. Enterprise Theory of Investigation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 237
A forensic investigator is analyzing a Windows system for possible malicious activity. The investigator is specifically interested in the recent actions of a suspect on the system, including any deleted directories or files, mounted drives, and actions taken. Which of the following approaches and tools would be the most effective for obtaining this information?
A. Examining the MRUListEx key and NodeSlot value in Windows Explorer
B. Parsing the BagMRU and Bags registry keys using SBag
C. Analyzing LNK files using ShellBags Explorer
D. Investigating Jump Usts using ShellBagsView
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
What is the first step taken in an investigation for laboratory forensic staff members?
A. Securing and evaluating the electronic crime scene
B. Conducting preliminary interviews

C. Transporting the electronic evidence
D. Packaging the electronic evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 239
In the context of file deletion process, which of the following statement holds true?
A. While booting, the machine may create temporary files that can delete evidence
B. Secure delete programs work by completely overwriting the file in one go
C. The longer a disk is in use, the less likely it is that deleted files will be overwritten
D. When files are deleted, the data is overwritten and the cluster marked as available
Answer: A (LEAVE A REPLY)

NEW QUESTION: 240
An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:
A. Dynamic analysis
B. Threat analysis
C. Threat hunting
D. Static analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 241
What stage of the incident handling process involves reporting events?
A. Containment
B. Identification
C. Follow-up
D. Recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 242

The Recycle Bin exists as a metaphor for throwing files away, but it also allows 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. LOGINFO1 file
B. LOGINFO2 file
C. INFO1 file
D. INFO2 file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 243
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?
A. Only Windows systems will reply to this scan
B. Only IBM AS/400 will reply to this scan
C. Only Unix and Unix-like systems will reply to this scan
D. A switched network will not respond to packets sent to the broadcast address
Answer: C (LEAVE A REPLY)

NEW QUESTION: 244
When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 245
The MD5 program is used to:
A. verify that a disk is not altered when you examine it
B. make directories on a evidence disk
C. view graphics files on an evidence drive
D. wipe magnetic media before recycling it
Answer: (SHOW ANSWER)

NEW QUESTION: 246
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Event Reaction
B. Incident Response
C. Network Forensics
D. Computer Forensics
Answer: D (LEAVE A REPLY)

NEW QUESTION: 247
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 config
B. Net sessions
C. Net stat
D. Net share
Answer: (SHOW ANSWER)

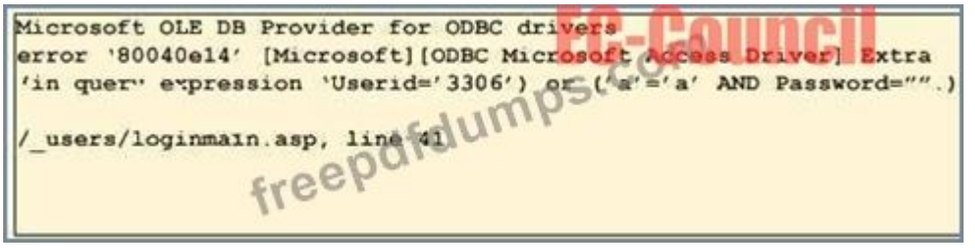
NEW QUESTION: 248
An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.
A. Expert law graduate appointed by attorney
B. Witness present at the crime scene
C. Subject matter specialist
D. Expert in criminal investigation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 249
Corporate investigations are typically easier than public investigations because:
A. the investigator does not have to get a warrant
B. the users can load whatever they want on their machines
C. the users have standard corporate equipment and software
D. the investigator has to get a warrant
Answer: A (LEAVE A REPLY)

NEW QUESTION: 250
Rule 1002 of Federal Rules of Evidence (US) talks about_____
A. Admissibility of other evidence of contents
B. Admissibility of duplicates
C. Requirement of original
D. Admissibility of original
Answer: C (LEAVE A REPLY)

NEW QUESTION: 251
Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data.
Which type of Azure blob storage can he use for this purpose?
A. Page blob
B. Append blob
C. Block blob
D. Medium blob
Answer: (SHOW ANSWER)

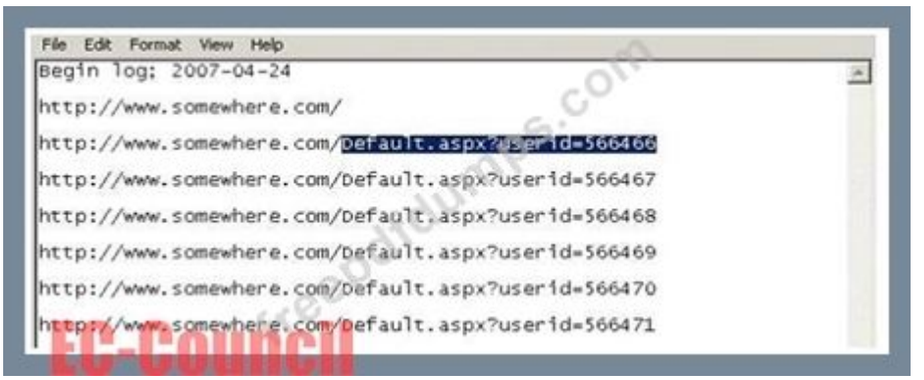
NEW QUESTION: 252
Click on the Exhibit Button. To test your website for vulnerabilities, you type in a Quotation mark (? for the username field. After you click Ok, you receive the following error message window:
What can you infer from this error window?



A. SQL injection is possible
B. The user for line 3306 in the SQL database has a weak password
C. SQL injection is not possible
D. The Quotation mark (? is a valid username
Answer: A (LEAVE A REPLY)

NEW QUESTION: 253
Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?
A. Volume Boot Record
B. GUID Partition Table
C. Master File Table
D. Master Boot Record
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
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. Cookie Poisoning
B. Cross site scripting
C. Parameter tampering
D. SQL injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 255
Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.
What type of malware analysis is Edgar performing?
A. Static analysis
B. Dynamic malware analysis/behavioral analysis
C. VirusTotal analysis
D. Malware disassembly
Answer: B (LEAVE A REPLY)

NEW QUESTION: 256
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?
A. The year the evidence was taken
B. The sequential number of the exhibits seized
C. The sequence number for the parts of the same exhibit
D. The initials of the forensics analyst
Answer: (SHOW ANSWER)

NEW QUESTION: 257
Diskcopy is:
A. a utility by AccessData
B. a standard MS-DOS command
C. Digital Intelligence utility
D. dd copying tool
Answer: B (LEAVE A REPLY)
diskcopy is a STANDARD DOS utility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

NEW QUESTION: 258
What is the "Best Evidence Rule"?
A. It states that the court only allows the original evidence of a document, photograph, or recording at the trial rather than a copy
B. It contains system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, and command history
C. It contains information such as open network connection, user logout, programs that reside in memory, and cache data
D. It contains hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
Which of the following statement is not correct when dealing with a powered-on computer at the crime scene?
A. If a computer is switched on and the screen is viewable, record the programs running on screen and photograph the screen
B. If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph
C. If a computer is on and the monitor shows some picture or screen saver, move the mouse slowly without depressing any mouse button and take a photograph of the screen and record the information displayed

D. If the computer is switched off. power on the computer to take screenshot of the desktop
Answer: (SHOW ANSWER)

NEW QUESTION: 260
A CHFI has been tasked to analyze Windows Security Logs in a highly complex and multi-layered security breach investigation. The breach involved an account creation, privilege escalation, and the installation of a service, all happening sequentially within a short duration. The investigator is required to retrieve a combination of Event IDs that would chronologically corroborate these events. Which combination of Event IDs should the investigator focus on?
A. Event ID 624, Event ID 500, and Event ID 7045
B. Event ID 624, Event ID 4670, and Event ID 6011
C. Event ID 4720, Event ID 4672, and Event ID 7045
D. Event ID 4720, Event ID 500, and Event ID 6011
Answer: C (LEAVE A REPLY)

NEW QUESTION: 261
Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.
A. Malvertising
B. Drive-by downloads
C. Phishing
D. Internet relay chats
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, "X" represents the _____.
A. Sequential number
B. Original file name
C. Drive name
D. Original file name's extension
Answer: C (LEAVE A REPLY)

NEW QUESTION: 263
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers?hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?
A. Unplug all connected devices

B. Power off all devices if currently on
C. Photograph and document the peripheral devices
D. Place PDA, including all devices, in an antistatic bag
Answer: C (LEAVE A REPLY)

NEW QUESTION: 264
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?
A. The SID of Hillary network account
B. The SAM file from Hillary computer
C. The network shares that Hillary has permissions
D. Hillary network username and password hash
Answer: (SHOW ANSWER)
Note: From the question, we would have to assume that John is not the Administrator, since he needs to run L0phtcrack in sniffing mode. But what if the company is using switches instead of Hubs? John would either try to degarde the switch or perform a man in the middle attack.

NEW QUESTION: 265
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?
A. Integrity-Based Detection
B. Heuristic/Behavior-Based Detection
C. Cross View-Based Detection
D. Signature-Based Detection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 266
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. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test
B. 127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200
C. http://victim.com/scripts/..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0% af./..%c0%af./../winnt/system32/cmd.exe?/c+dir+c:\wintt\system32\Logfiles\W3SVC1
D. 127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0' 200
Answer: (SHOW ANSWER)

NEW QUESTION: 267

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

A. Prior statement by witness

B. Statement of personal or family history

C. Statement against interest

D. Statement under belief of impending death

Answer: D (LEAVE A REPLY)

NEW QUESTION: 268

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: 269

Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

A. Logs of high temperatures the drive has reached

B. Power Off time

C. All the states (running and discontinued) associated with the OS

D. List of running processes

Answer: (SHOW ANSWER)

NEW QUESTION: 270

When dealing with the powered-off computers at the crime scene, if the computer is switched off, turn it on

A. False

B. True

Answer: A (LEAVE A REPLY)

NEW QUESTION: 271

What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35 (8084) -> 56.58.152.114(445), 1 packet

A. None of the above

B. Source IP address

C. Login IP address

D. Destination IP address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 272
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.) Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from
194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 ->
172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 ->
172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:
194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from
24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 ->
172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:
198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 ->
172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for
user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user
simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 ->
172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23
-> 213.28.22.189:4558
From the options given below choose the one which best interprets the following entry:
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 ->
172.16.1.107:53
A. A buffer overflow attempt
B. A DNS zone transfer
C. Data being retrieved from 63.226.81.13
D. An IDS evasion technique
Answer: (SHOW ANSWER)

NEW QUESTION: 273
Which of the following filesystem is used by Mac OS X?
A. EFS
B. HFS+
C. EXT2
D. NFS
Answer: B (LEAVE A REPLY)
EFS (Encrypting File System) is part of NTFS and used on Windows EXT2 is used on Linux NFS (Network File System) is for access to a network file system over TCP/IP

NEW QUESTION: 274
Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?
A. Sparse or Logical Acquisition
B. Bit-by-bit Acquisition
C. Bit-stream disk-to-disk Acquisition
D. Static Acquisition
Answer: A (LEAVE A REPLY)

NEW QUESTION: 275
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: 276
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. #06r
C. *1MEI#
D. #*06*#
Answer: (SHOW ANSWER)

NEW QUESTION: 277
Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?
A. Manual acquisition
B. Physical acquisition
C. Logical acquisition
D. Direct acquisition
Answer: B (LEAVE A REPLY)

NEW QUESTION: 278
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. Unauthorized expenses
B. Scope Creep
C. Hard Drive Failure
D. Overzealous marketing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 279
A forensic investigator is examining a potential intrusion involving an Amazon Echo. The investigator has acquired an affected Echo and the smartphone synced to it. For further data analysis, he needs to retrieve relevant database files from the smartphone. Which files will the investigator primarily focus on to retrieve essential information?

A. /data/data/com.amazon.dee.app/databases/map_data_storage_v2.db and /data/data/com.amazon.dee.app/databases/DeviceInfo.db
B. /data/data/com.amazon.dee.app/databases/map_data_storage_v1.db and /data/data/com.amazon.dee.app/databases/DataStore.db
C. /data/data/com.amazon.dee.app/databases/DataStore.db and /data/data/com.amazon.dee.app/databases/map_data_storage_v3.db
D. /data/data/com.amazon.dee.app/databases/map_data_storage_v2.db and /data/data/com.amazon.dee.app/databases/DataStore.db
Answer: (SHOW ANSWER)

NEW QUESTION: 280
Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?
A. Datagrab
B. Helix
C. Coreography
D. Ethereal
Answer: (SHOW ANSWER)

NEW QUESTION: 281
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?
A. Run the command fsutil behavior set enablelastaccess 0
B. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
C. Run the command fsutil behavior set disablelastaccess 0
D. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 282
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. Contents of the NetBIOS name cache
B. Status of the network carrier
C. Network connections
D. Contents of the network routing table
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
Quality of a raster Image is determined by the _____and the amount of information in each pixel.
A. Compression method
B. Image file format
C. Image file size
D. Total number of pixels
Answer: (SHOW ANSWER)

NEW QUESTION: 284
The offset in a hexadecimal code is:
A. The 0x at the end of the code
B. The 0x at the beginning of the code
C. The first byte after the colon
D. The last byte after the colon
Answer: (SHOW ANSWER)

NEW QUESTION: 285
During a high-stakes corporate espionage case, an investigator seeks digital evidence to reveal unauthorized data access and leakage. The investigator possesses the skills to recover deleted files, decrypt encrypted files, and inspect hidden files. Given the availability of multiple potential evidence sources, which category of files is most likely to yield the most valuable information in this scenario?
A. Files stored on peripheral devices
B. User-Protected Files
C. Computer-Created Files
D. User-Created Files
Answer: B (LEAVE A REPLY)

NEW QUESTION: 286
System software password cracking is defined as cracking the operating system and all other utilities that enable a computer to function
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 287
What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?
A. Username and password
B. Firewall log
C. E-mail header
D. Internet service provider information
Answer: (SHOW ANSWER)

NEW QUESTION: 288
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?
A. Time and date of deletion
B. File Name
C. File origin and modification
D. File Size
Answer: (SHOW ANSWER)

NEW QUESTION: 289
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 cipher
B. Text semagram
C. Grill cipher
D. Visual semagram
Answer: D (LEAVE A REPLY)

NEW QUESTION: 290
SO/IEC 17025 is an accreditation for which of the following:
A. Encryption
B. Chain of custody

C. CHFI issuing agency
D. Forensics lab licensing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 291
An investigator is analyzing EXIF metadata in a case involving cybercrime. She finds that the timestamp data has been modified, potentially misleading the investigation. What is the best next step she should take in her forensic examination?
A. Discard the EXIF metadata as it has been tampered with and is no longer useful
B. Change the focus of the investigation, as tampered EXIF metadata indicates a false lead
C. Accept the tampered EXIF metadata as it's the only information available
D. Validate the EXIF metadata with other sources of information to corroborate its accuracy
Answer: (SHOW ANSWER)

NEW QUESTION: 292
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?
A. Principle 3
B. Principle 1
C. Principle 4
D. Principle 2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 293
When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.
A. A Capital X
B. A Blank Space
C. The Underscore Symbol
D. The lowercase Greek Letter Sigma (s)
Answer: D (LEAVE A REPLY)
When a file is deleted, the first byte is replaced with 0xE5 to marked the file as deleted or erased, and is the same for FAT12/16/32. An 0xE5 translates also to a ASCII 229, a "O" with a tilde. However, using the greek alphabet (see: http://www.ascii.ca/iso8859.7.htm) the ASCII code 229 is "the lowercase Greek Letter Epsilon, and Ascii code 243 is Lower case Greek Letter Sigma. http://chexed.com/ComputerTips/asciicodes.php says that Ascii 229 is Lowercase Greek Letter Sigma So, although D looks like the correct answer here, it may require more understanding of the underlying intent of the question.

NEW QUESTION: 294
Which of the following is not a part of disk imaging tool requirements?
A. The tool should log I/O errors in an accessible and readable form, including the type and location of the error
B. The tool should not compute a hash value for the complete bit stream copy generated from an image file of the source
C. The tool should not change the original content
D. The tool must have the ability to be held up to scientific and peer review
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
In Windows, prefetching is done to improve system performance. There are two types of prefetching:
boot prefetching and application prefetching.
During boot prefetching, what does the Cache Manager do?
A. Determines the data associated with value EnablePrefetcher
B. Checks hard page faults and soft page faults
C. Monitors the first 10 seconds after the process is started
D. Checks whether the data is processed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 296
Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?
A. Administrative Investigation
B. Civil Investigation
C. Criminal Investigation
D. Both Criminal and Administrative Investigation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
In the middle of a high-pressure cybercrime investigation, you stumble upon a cryptic message. It appears to be encoded with the ASCII standard. The encrypted message contains a combination of lower ASCII and higher ASCII codes. Which statement is the most accurate concerning the interpretation of this message?
A. The lower ASCII codes refer to non-printable system codes, while the higher ASCII codes represent alphanumeric characters and punctuation
B. ASCII codes at the lower end represent alphanumeric characters and punctuation. On the other hand, those at the higher end are typically used to denote non-printable system codes

C. Both lower and higher ASCII codes primarily contain alphanumeric characters and punctuation
D. The lower ASCII codes represent basic alphanumeric characters and punctuation, while the higher ASCII codes are generally used for graphics and non-ASCII characters in documents
Answer: (SHOW ANSWER)

NEW QUESTION: 298
BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?
A. Header
B. Image data
C. The RGBQUAD array
D. Information header
Answer: (SHOW ANSWER)

NEW QUESTION: 299
Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 300
This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.
A. European Anti-Spam act
B. Federal Spam act
C. Telemarketing act
D. The CAN-SPAM act
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?
A. Cross Examination
B. Direct Examination
C. Witness Examination
D. Indirect Examination

Answer: (SHOW ANSWER)

NEW QUESTION: 302
In a cyber-forensic investigation, a CHFI expert found a Linux system unexpectedly booting into a different OS kernel. The system was configured with the Grand Unified Bootloader (GRUB). The expert suspects that an attacker may have tampered with the bootloader stage of the Linux boot process. Which one of the following is NOT a step performed during the bootloader stage in a normal Linux boot process?
A. Loading the Linux kernel and optional initial RAM disk
B. Execution of the Linuxrc program to generate the real file system for the kernel
C. Loading the kernel into memory
D. Detecting the device that contains the file system and loading the necessary modules
Answer: (SHOW ANSWER)

NEW QUESTION: 303
Someone in the field of forensic investigation is looking at an Apache access log. They're searching for any evidence of a command injection attack. During this process, they find a log entry where the IP address "10.0.0.8" placed a GET request using the command ip=127.0.0.1;ls +/var/www/html. Judging by this data, what might be the individual's objective behind this attack?
A. The individual behind the attack is working towards replacing the target file on the host server
B. The individual behind the attack is attempting a brute-force attack on the host server
C. The individual behind the attack aims to see what's inside the /var/www/html directory of the host server
D. The individual behind the attack is working to put an XML external entity into the web application
Answer: C (LEAVE A REPLY)

NEW QUESTION: 304
In an ongoing cybercrime investigation, Laura, a certified Computer Hacking Forensics Investigator (CHFI), has identified a system involved in illegal activities. The system is connected to a network with many other users. Laura needs to gather evidence related to the identified system's internet usage. Which legal and privacy considerations should be her utmost priority?

A. Maintaining the anonymity of non-target users connected to the system
B. Obtaining explicit consent from the system owner before starting the investigation
C. Acquiring a search warrant specifically mentioning the identified system
D. Informing the authorities about the identified illegal activities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 305
In the event of a fileless malware attack, a Computer Hacking Forensics Investigator (CHFI) notes that the fileless malware has managed to persist even after the system reboots. What built- in Windows tool/utility might the attacker most likely have leveraged for this persistent behavior?
A. Windows Process Explorer
B. Windows Task Scheduler
C. Windows AutoStart registry keys
D. Windows Operation system components
Answer: B (LEAVE A REPLY)

NEW QUESTION: 306
Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form in not the same as that of her bank's. Identify the type of external attack performed by the attacker In the above scenario?
A. Brute-force
B. Espionage
C. Taiigating
D. Aphishing
Answer: D (LEAVE A REPLY)

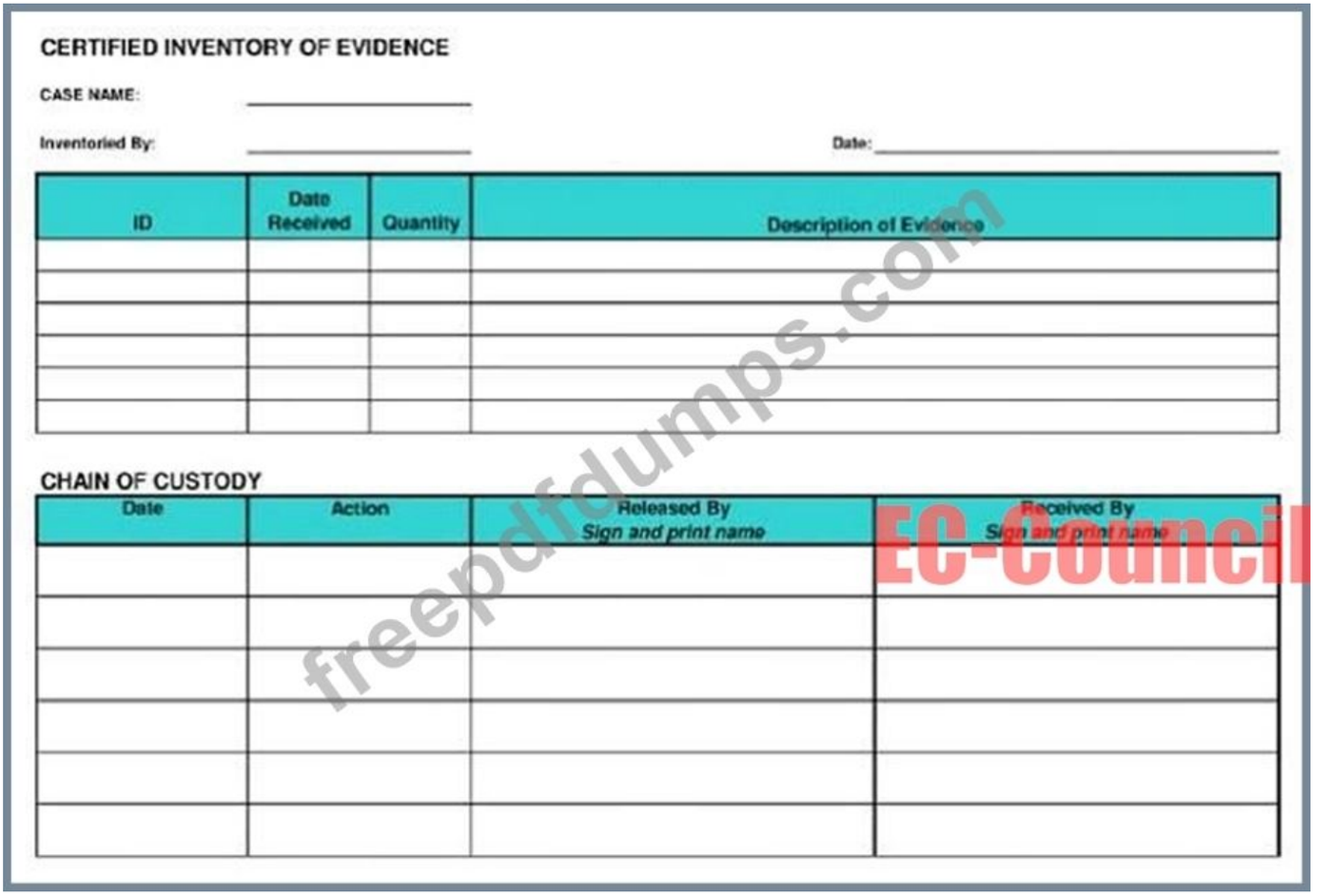
NEW QUESTION: 307
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation.
Which of the following should he use in this scenario?
A. Azure Portal
B. Azure CLI
C. Azure Monitor
D. Azure Active Directory
Answer: (SHOW ANSWER)

NEW QUESTION: 308
When is it appropriate to use computer forensics?

A. If a financial institution is burglarized by robbers
B. If copyright and intellectual property theft/misuse has occurred
C. If sales drop off for no apparent reason for an extended period of time
D. If employees do not care for their boss?management techniques
Answer: B (LEAVE A REPLY)

NEW QUESTION: 309
In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?
A. Zygote
B. Media server
C. Daemon
D. init
Answer: A (LEAVE A REPLY)

NEW QUESTION: 310
What document does the screenshot represent?


CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____ Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By Sign and print name	Received By Sign and print name

A. Search warrant form
B. Evidence collection form
C. Expert witness form

D. Chain of custody form
Answer: (SHOW ANSWER)

NEW QUESTION: 311
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. Offset
C. Steganography
D. Rootkit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 312
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?
A. Physical
B. Network
C. Data Link
D. Transport
Answer: (SHOW ANSWER)

NEW QUESTION: 313
Which file is a sequence of bytes organized into blocks understandable by the system's linker?
A. Object file
B. None of these
C. source file
D. executable file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 314
As a forensic investigator, you are investigating a suspected cyberattack that led to the system crash of a Windows 10 computer. You obtained a memory dump file and intend to utilize Microsoft's DumpChk tool for a quick analysis. However, you are interested in isolating a particular process that you suspect is responsible for the crash, rather than inspecting the whole memory dump file. Based on the given details and your knowledge of Windows memory analysis, which of the following would be the most efficient approach?
A. Use the Process Dumper tool to dump the entire process space of the suspected process to a file, then analyze the dump file using DumpChk
B. Use ListDLLs.exe to list all DLLs loaded into the suspected process, then analyze these DLLs using DumpChk
C. Directly analyze the entire memory dump file using DumpChk, then isolate the details of the suspected process

D. Run DumpChk with the -y SymbolPath parameter, specifying the path to the symbols of the suspected process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 315
During a recent network intrusion investigation, a CHFI received logs from Juniper IDS, Check Point IPS, and a Kippo Honeypot. Which log provides information about the network traffic and bandwidth adjustment, aiding in business risk valuation?
A. Kippo Honeypot
B. None of the above
C. Juniper IDS
D. Check Point IPS
Answer: (SHOW ANSWER)

NEW QUESTION: 316
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. RS231
B. RS422
C. RS423
D. RS232
Answer: (SHOW ANSWER)

NEW QUESTION: 317
A digital forensics investigator is examining a suspect's hard disk drive. The hard disk is known to have 16,384 cylinders, 16 heads, and 63 sectors per track, with a sector size of 512 bytes. During the investigation, the forensic analyst identifies a particular file that resides in two sectors.

Considering that each sector contains data plus overhead information such as ID, synchronization fields. ECC, and gaps, what is the maximum potential size of this particular file stored on the disk?

A. Less than 512 bytes

B. Equal to 512 bytes

C. Equal to or more than 1024 bytes

D. More than 512 bytes but less than 1024 bytes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 318

Consider that you are investigating a machine running an Windows OS released prior to Windows VistA. 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 restored, a .exe file

B. D drive, fourth file deleted, a .exe file

C. D drive, sixth file deleted, a .exe file

D. D drive. fifth file deleted, a .exe file

Answer: (SHOW ANSWER)

NEW QUESTION: 319

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

A. central processing attack

B. automated attack

C. blackout attack

D. distributed attack

Answer: B (LEAVE A REPLY)

NEW QUESTION: 320

In a suspected cyberattack scenario, a seasoned Computer Hacking Forensics Investigator (CHFI) comes across evidence that the attacker used cloud infrastructure to host attack toolkits and launch the attack. What should be the investigator's primary approach to unravel the tracks covered by the attacker and retrieve evidence?

A. Review the access logs for all cloud infrastructure services used during the attack period

B. Contact the cloud service provider and request the deletion of data for the suspected period

C. Recover and analyze the residual data left on the cloud servers after the attacker destroyed the infrastructure

D. Launch a counterattack on the suspected IP addresses linked with the cloud infrastructure

Answer: A (LEAVE A REPLY)

NEW QUESTION: 321
Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?
A. Volatility
B. RAM Mapper
C. Memcheck
D. Autopsy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 322
You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?
A. All forms should be placed in an approved secure container because they are now primary evidence in the case
B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container
C. All forms should be placed in the report file because they are now primary evidence in the case
D. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
Which of the following Perl scripts will help an investigator to access the executable image of a process?
A. Lpsi.pl
B. Lspm.pl
C. Lspi.pl
D. Lspd.pl
Answer: (SHOW ANSWER)

NEW QUESTION: 324
An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion.
A. False

B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?
A. Kismet
B. Snort
C. Accunetix
D. Nikto
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?
A. Cookie Poisoning Attack
B. Session poisoning
C. DNS Redirection
D. DNS Poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 327
Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment.
Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?
A. The 1st Amendment
B. The 10th Amendment
C. The 5th Amendment
D. The 4th Amendment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 328
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: 329
Microsoft Outlook maintains email messages in a proprietary format in what type of file?
A. .doc
B. .email
C. .pst
D. .mail
Answer: (SHOW ANSWER)

NEW QUESTION: 330
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?
A. Hearsay
B. Locard's Principle
C. Rule 1003: Admissibility of Duplicates
D. Limited admissibility
Answer: D (LEAVE A REPLY)

NEW QUESTION: 331
A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?
A. Helix
B. NetCat
C. Wireshark
D. R-Studio
Answer: D (LEAVE A REPLY)

NEW QUESTION: 332
What is the extension used by Windows OS for shortcut files present on the machine?
A. .log
B. .dat
C. .lnk
D. .pf
Answer: (SHOW ANSWER)

NEW QUESTION: 333
An organization just experienced a serious cybersecurity incident involving data theft. The first responder on the scene is anon-forensics staff member. Based on the guidelines provided, which of the following actions should they take as the first response to this incident?
A. They should isolate the affected systems and document every detail relevant to the incident without tampering with them
B. They should launch a preliminary investigation into the breach before the forensics team arrives
C. They should power down the compromised systems to prevent further attacks
D. They should start retrieving the stolen data from the compromised systems immediately to minimize further damage
Answer: (SHOW ANSWER)

NEW QUESTION: 334
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?
A. Phishing
B. Email spoofing
C. Email spamming
D. Mail bombing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 335
If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
A. The system has been compromised using a t0rnrootkit
B. The system administrator has created an incremental backup
C. Nothing in particular as these can be operational files
D. The system files have been copied by a remote attacker

Answer: C (LEAVE A REPLY)

NEW QUESTION: 336
The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 337
You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different.
What area of the law is the employee violating?
A. Brandmark law
B. Trademark law
C. Printright law
D. Copyright law
Answer: B (LEAVE A REPLY)

NEW QUESTION: 338
What is the smallest allocation unit of a hard disk?
A. Disk platters
B. Slack space
C. Spinning tracks
D. Cluster
Answer: D (LEAVE A REPLY)

NEW QUESTION: 339
In an echo data hiding technique, the secret message is embedded into a _____as an echo.
A. Phase spectrum of a digital signal
B. Pseudo-random signal
C. Pseudo- spectrum signal
D. Cover audio signal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 340
A security firm investigating an IoT-based cybercrime involving an Android smartwatch found on the crime scene. The smartwatch is suspected of capturing sensitive information such as PINs and passwords through motion sensors and GPS tracking. The paired smartphone is not available. Which of the following steps should the investigator undertake first to proceed with the forensics process effectively?
A. Extract data from the smartwatch's memory before it gets volatile
B. Look for cloud data and mobile data linked to the smartwatch
C. Identify APIs like Data API, Message API, and Node API on the smartwatch
D. Generate forensic images of the evidence found on the crime scene
Answer: A (LEAVE A REPLY)

NEW QUESTION: 341
What file structure database would you expect to find on floppy disks?
A. NTFS
B. FAT32
C. FAT16
D. FAT12
Answer: D (LEAVE A REPLY)
Explanation: NTFS is not designed for removable media, although used on some removable media that is very large, never for floppy disks. FAT32 has a minimum space requirement which is larger than floppy disks FAT16 would seem like a logical choice, but is not usually used on floppies FAT12 would be on floppy disks, and probably not seen on anything else. Since floppy disk media is small in size (less than 2 MB), a FAT12 file system has lower overhead and is more efficient.

NEW QUESTION: 342
An investigator is studying a suspicious Windows service discovered on a corporate system that seems to be associated with malware. The service has a name similar to a genuine Windows service, runs as a SYSTEM account, and exhibits potentially harmful behavior. Which tool and method should the investigator use to study the service's behavior without allowing it to inflict more damage?
A. Utilize the Windows Service Manager to create an identical service and study its behavior
B. Deploy Autoruns for Windows to check if the suspicious service is configured to run at system bootup
C. Inspect the startup folder for the presence of the suspicious service using command prompt commands
D. Use SrvMan to stop the suspicious service and analyze its impact on the system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 343
Which of the following Windows event logs record events related to device drives and hardware changes?
A. Application log
B. Security log
C. Forwarded events log
D. System log
Answer: (SHOW ANSWER)

NEW QUESTION: 344
When discussing the chain of custody in an investigation, what does a link refer to?
A. Evidence that links one piece of evidence to another, like a usb cable
B. The most critical piece of evidence in an investigation
C. Someone that takes possession of a piece of evidence
D. The transportation used when moving evidence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 345
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?
A. Blackberry Message Center
B. Microsoft Exchange
C. Blackberry WEP gateway
D. Blackberry WAP gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 346
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: B (LEAVE A REPLY)

NEW QUESTION: 347
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. Email Spamming
B. Phishing
C. Email Spoofing
D. Mail Bombing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 348
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 can change date/time stamps
B. Searching creates cache files, which would hinder the investigation
C. Searching could possibly crash the machine or device
D. Searching for evidence themselves would not have any ill effects
Answer: A (LEAVE A REPLY)

NEW QUESTION: 349
An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).
Which property of the image shows you the number of colors available for each pixel in an image?
A. File Formats
B. Pixel
C. Bit Depth
D. Image File Size
Answer: (SHOW ANSWER)

NEW QUESTION: 350
In Linux, what is the smallest possible shellcode?
A. 80 bytes

B. 800 bytes
C. 24 bytes
D. 8 bytes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 351
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 a DMZ is not illegal
C. Entrapment
D. Intruding into ahoneypot is not illegal
Answer: (SHOW ANSWER)

NEW QUESTION: 352
Paraben Lockdown device uses which operating system to write hard drive data?
A. Windows
B. Mac OS
C. Red Hat
D. Unix
Answer: A (LEAVE A REPLY)

NEW QUESTION: 353
During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
What does the first four digits (89 and 44) In the ICCID represent?
A. TAC and industry identifier
B. Issuer identifier number and TAC
C. Industry identifier and country code
D. Country code and industry identifier
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
As part of an ongoing cyber investigation in a rapidly expanding organization, the Computer Hacking Forensic Investigator (CHFI) has to choose the most effective Security Information and Event Management (SIEM) tool for the company's ever-growing IT infrastructure. This SIEM tool

must efficiently collect, index, and alert real-time machine data and offer functionalities for rapid detection and response to both internal and external threats. Additionally, the tool should be capable of leveraging AI-powered machine learning for actionable insights. Based on these requirements, the investigator should consider the following:

A. Splunk Enterprise Security (ES) only

B. Both Splunk ES and IBM QRadar, but IBM QRadar has an edge due to prebuilt reports and templates

C. Both Splunk ES and IBM QRadar, but Splunk ES has an edge due to AI-powered machine learning capabilities

D. IBM QRadar only

Answer: C (LEAVE A REPLY)

NEW QUESTION: 355

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to web bugs

B. Your website is vulnerable to SQL injection

C. Your website is not vulnerable

D. Your website is vulnerable to CSS

Answer: D (LEAVE A REPLY)

NEW QUESTION: 356

Which of the following tool is used to locate IP addresses?

A. Deep Log Analyzer

B. SmartWhois

C. XRY LOGICAL

D. Towelroot

Answer: (SHOW ANSWER)

NEW QUESTION: 357

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

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

NEW QUESTION: 358
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. Integrated circuit card identifier (ICCID)
B. International Mobile Equipment Identifier (IMEI)
C. Equipment Identity Register (EIR)
D. International mobile subscriber identity (IMSI)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 359
In a situation where an investigator needs to acquire volatile data from a live Linux system, the physical access to the suspect machine is either restricted or unavailable. Which of the following steps will be the most suitable approach to perform this task?
A. The investigator should leverage OSXPMem to remotely parse the physical memory in the Linux machine and create AFF4 format images for analysis
B. The investigator should employ the LiME tool and 'netcat', starting a listening session using tcp:port on the suspect machine and then establishing a connection from the forensic workstation using 'netcat'
C. The investigator should initiate a listening session on the forensic workstation using 'netcat', then execute a 'dd' command on the suspect machine and pipe the output using 'netcat'
D. The investigator should use the Belkasoft Live RAM Capturer on the forensic workstation, then remotely execute the tool on the suspect machine to acquire the RAM image
Answer: B (LEAVE A REPLY)

NEW QUESTION: 360
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?
A. mysql-bin
B. iblog
C. mysql-log
D. ibdata1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 361
A cybercrime investigator is evaluating a data breach in a company's AWS infrastructure. The breached service was categorized as an AWS container service. What primary security aspects were likely managed by the company and not by AWS, which the investigator should first focus on?
A. Network configuration of the container services
B. Application platform and Operating System (OS) security
C. Data management and firewall configuration
D. Physical infrastructure and foundational services
Answer: B (LEAVE A REPLY)

NEW QUESTION: 362
George was recently fired from his job as an IT analyst at Pitts and Company in Dallas Texas. His main duties as an analyst were to support the company Active Directory structure and to create network polices. George now wants to break into the company's network by cracking some of the service accounts he knows about.
Which password cracking technique should George use in this situation?
A. Rule-based attack
B. Syllable attack
C. Dictionary attack
D. Brute force attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 363
Which of the following Ii considered as the starting point of a database and stores user data and database objects in an MS SQL server?
A. Transaction log data files (LDF)
B. Primary data files (MDF)
C. Ibdata1
D. Application data files (ADF)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 364
Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?
A. WIN-ABCDE12345F.log
B. WIN-ABCDE12345F.pid
C. WIN-ABCDE12345F-bin.n
D. WIN-ABCDE12345F.err
Answer: (SHOW ANSWER)

NEW QUESTION: 365
As a forensic investigator, you are asked to identify whether the Dropbox application was installed on a suspect's computer running Windows 10. The request is made by an attorney. You are considering different tools and approaches for your investigation. What would be the most appropriate next step in the forensic investigation process?
A. Rely on your past experience and intuition to confirm or disprove the installation of Dropbox without formulating any hypothesis
B. Formulate a hypothesis and design an experiment to test the hypothesis on a similar system before examining the suspect's machine
C. Immediately start examining the suspect's computer with any readily available digital forensic tool
D. Use the most expensive commercial tool to guarantee a thorough investigation and reliable findings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 366
Software firewalls work at which layer of the OSI model?
A. Network
B. Application
C. Transport
D. Data Link
Answer: B (LEAVE A REPLY)

NEW QUESTION: 367
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold needs?
A. Application-level proxy firewall
B. Data link layer firewall
C. Packet filtering firewall
D. Circuit-level proxy firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 368
After an SQL Injection attack, an investigator is examining a log entry in an IIS log from a Windows-based server. The investigator notices a suspicious GET request: Id=ORD-001%27%20or%201=1;--. What can the investigator infer from this decoded query in the investigation?
A. The attack was made from a Linux machine
B. The attack is trying to retrieve the number of columns that are vulnerable to attack
C. The attack has attempted to extract database and table names

D. The attack has bypassed authentication to access sensitive data from the database
Answer: D (LEAVE A REPLY)

NEW QUESTION: 369
What is a SCSI (Small Computer System Interface)?
A. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps
B. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer
C. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
D. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives. CD-ROM drives, printers, and scanners
Answer: D (LEAVE A REPLY)

NEW QUESTION: 370
What should you do when approached by a reporter about a case that you are working on or have worked on?
A. Answer only the questions that help your case
B. Answer all the reporter's questions as completely as possible
C. Say, "no comment"
D. Refer the reporter to the attorney that retained you
Answer: (SHOW ANSWER)

NEW QUESTION: 371
What binary coding is used most often for e-mail purposes?
A. Uuencode
B. SMTP
C. MIME
D. IMAP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 372
In the midst of a cybercrime investigation, a key witness has suddenly become unavailable due to a serious illness. According to Federal Rule 804, which exception to the rule against hearsay allows for introducing this witness's previous testimony at a different trial in a current proceeding?
A. Former Testimony
B. Statement of Personal or Family History
C. Statement Against Interest
D. Statement Under the Belief of Imminent Death
Answer: A (LEAVE A REPLY)

NEW QUESTION: 373
During an ongoing cybercrime investigation, a non-expert witness, who is an employee of the organization, testifies to observing unusual computer activity. Simultaneously, an expert witness introduces a record of the regularly conducted activity of the organization. The record was kept near the incident's time adept as part of the regular activity. It reveals a similar observation as the non-expert witness. How would the Federal Rules of Evidence classify and treat these testimonies in this scenario?
A. Both testimonies are admissible; the lay witness testimony is under Rule 701, and the record is under Rule 803(6)
B. The lay witness testimony is admissible under Rule 701, but the record is inadmissible hearsay under Rule 803(6)
C. The lay witness testimony is inadmissible hearsay under Rule 801. but the record is admissible under Rule 803(6)
D. Both testimonies are inadmissible; the lay witness testimony is hearsay under Rule 801, and the record is hearsay under Rule 803(6)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 374
What does the Rule 101 of Federal Rules of Evidence states?
A. Purpose of the Rules
B. Limited Admissibility of the Evidence
C. Rulings on Evidence
D. Scope of the Rules, where they can be applied
Answer: D (LEAVE A REPLY)

NEW QUESTION: 375
Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?
A. R-Studio
B. Passware Kit Forensic
C. TestDisk for Windows
D. Windows Password Recovery Bootdisk
Answer: B (LEAVE A REPLY)

NEW QUESTION: 376
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 16
B. 48
C. 64
D. 32

Answer: D (LEAVE A REPLY)

NEW QUESTION: 377
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. GUID Partition Table (GPT)
B. BIOS-MBR
C. BIOS Parameter Block
D. Master Boot Record (MBR)
Answer: (SHOW ANSWER)

NEW QUESTION: 378
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?
A. PDF passwords are converted to clear text when sent through E-mail
B. When sent through E-mail, PDF passwords are stripped from the document completely
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. PDF passwords can easily be cracked by software brute force tools
Answer: (SHOW ANSWER)

NEW QUESTION: 379
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: (SHOW ANSWER)

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: 380
Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used In an Incident that occurred earlier. He started Inspecting and gathering the contents of RAM, cache, and DLLs to Identify Incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.
A. Live data acquisition
B. Static data acquisition
C. Non-volatile data acquisition
D. Dead data acquisition
Answer: C (LEAVE A REPLY)

NEW QUESTION: 381
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?
A. Statefull firewall

B. Application-level proxy firewall
C. Circuit-level proxy firewall
D. Packet filtering firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 382
A Computer Hacking Forensics Investigator (CHFI) has been called in to handle a complex data breach at a large corporation. The investigator plans to follow the rules of thumb for data acquisition during the investigation. Which of the following actions is NOT in line with these best practices?
A. Verifying the integrity of the duplicates by comparing them to the original using hash values
B. Producing two copies of the original media before starting the investigation process
C. Creating a duplicate bit-stream image of the suspicious drive for analysis
D. Performing the forensic investigation directly on the original evidence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 383
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
A. Connect the target media; Delete the system for acquisition; Secure the evidence; Copy the media
B. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
C. Prepare the system for acquisition; Connect the target media; Copy the media; Secure the evidence
D. Secure the evidence; Prepare the system for acquisition; Connect the target media; Copy the media
Answer: C (LEAVE A REPLY)

NEW QUESTION: 384
When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____.
A. 4902
B. 3904
C. 4904
D. 3902
Answer: A (LEAVE A REPLY)

NEW QUESTION: 385
Which of the following is an iOS Jailbreaking tool?
A. One Click Root
B. Redsn0w
C. Kingo Android ROOT
D. Towelroot
Answer: B (LEAVE A REPLY)

NEW QUESTION: 386
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. FF D8 FF E0 00 10
B. FF 00 FF 00 FF 00
C. FF FF FF FF FF FF
D. EF 00 EF 00 EF 00
Answer: (SHOW ANSWER)

NEW QUESTION: 387
What type of analysis helps to identify the time and sequence of events in an investigation?
A. Time-based
B. Relational
C. Functional
D. Temporal
Answer: (SHOW ANSWER)

NEW QUESTION: 388
You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?
A. The Host Domain Name
B. The E-mail Header
C. The SMTP reply Address
D. The X509 Address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 389
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?
A. Nmap scan
B. Fraggle

C. Ping of death
D. Smurf
Answer: C (LEAVE A REPLY)

NEW QUESTION: 390
What type of equipment would a forensics investigator store in a StrongHold bag?
A. Hard drives
B. PDAPDA?
C. Backup tapes
D. Wireless cards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 391
In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?
A. Blueborne attack
B. Sybil attack
C. Jamming attack
D. Replay attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 392
When obtaining a warrant it is important to:
A. particularly describe the place to be searched and particularly describe the items to be seized
B. generally describe the place to be searched and generally describe the items to be seized
C. particularly describe the place to be searched and generally describe the items to be seized
D. generally describe the place to be searched and particularly describe the items to be seized
Answer: A (LEAVE A REPLY)

NEW QUESTION: 393
Which of the following file in Novel GroupWise stores information about user accounts?
A. gwcheck.db

B. PRIV.STM
C. PRIV.EDB
D. ngwguard.db
Answer: (SHOW ANSWER)

NEW QUESTION: 394
During a forensic investigation, an attorney requested a forensic investigator to check if Dropbox was installed on the suspect's hard drive. The investigator finds traces of Dropbox artifacts in C:\Users\Admin\AppData\Roaming\, C:\Program Files (x86) and C:\Program Files directories. If the hypothesis is that the operating system installed is Windows 10, and Dropbox installation is confirmed by its artifacts in the mentioned directories, which assertion is the investigator most likely to make?
A. The Dropbox artifacts were manually moved to the mentioned directories on the suspect's hard drive
B. The Dropbox application was most likely installed on the system running Windows 10
C. The Dropbox installation occurred using Windows 10's built-in installation manager
D. The Dropbox was installed on the suspect's machine using the open-source version of the installation package
Answer: B (LEAVE A REPLY)

NEW QUESTION: 395
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question wheather evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?
A. There is no reason to worry about this possible claim because state labs are certified
B. Make MD5 hashes of the evidence and compare it to the standard database developed by NIST
C. Sign a statement attesting that the evidence is the same as it was when it entered the lab
D. Make MD5 hashes of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
Answer: (SHOW ANSWER)

NEW QUESTION: 396
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. Unused clusters
C. Bad clusters
D. Lost clusters

Answer: (SHOW ANSWER)

NEW QUESTION: 397
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. Inspecting WLAN and surrounding networks
B. Scanning the network
C. Sniffing the packets from the airwave
D. Broadcasting a probe request frame
Answer: D (LEAVE A REPLY)

NEW QUESTION: 398
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?
A. BIOS Parameter Block (BPB) and the OEM ID
B. Jump instruction and the OEM ID
C. Bootstrap code and the end of the sector marker
D. BIOS Parameter Block (BPB) and the extended BPB
Answer: D (LEAVE A REPLY)

NEW QUESTION: 399
What happens lo the header of the file once It Is deleted from the Windows OS file systems?
A. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5
B. The hex byte coding of the file remains the same, but the file location differs
C. The OS replaces the first letter of a deleted file name with a hex byte code: E5h
D. The OS replaces the entire hex byte coding of the file.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 400
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. Data items and vulnerability scanning
B. Interviewing employees and network engineers
C. Source code review
D. Reviewing the firewalls configuration
Answer: C (LEAVE A REPLY)

NEW QUESTION: 401
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_CONFIG
D. HKEY_USERS
Answer: (SHOW ANSWER)

NEW QUESTION: 402
A security breach has occurred at a multinational company. The forensic investigator was asked to identify whether a specific application, say "SecureBox", was installed on a Windows 10 system under suspicion. Which approach should the investigator follow to validate this?
A. Choosing commercial tools for investigation because they have a market value and provide a diverse and in-depth investigation
B. Experimenting and testing various plans in an environment similar to the suspect machine
C. Formulating an opinion based on the review of several artifacts and determining exactly when SecureBox was installed
D. Making observations, hypothesizing about the incident, and then checking for SecureBox artifacts in specific operating system directories
Answer: (SHOW ANSWER)

NEW QUESTION: 403
On NTFS file system, which of the following tools can a forensic Investigator use In order to identify timestomping of evidence files?
A. Timestomp
B. Exiv2
C. analyzeMFT
D. wbStego
Answer: (SHOW ANSWER)

NEW QUESTION: 404
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 bit blocks
B. Adjacent memory locations
C. Adjacent buffer locations
D. Adjacent string locations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 405
The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance,

server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.
192.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524, 100, 0, GET, /dollerlogo.gif,
A. 3524
B. W3SVC2
C. 100
D. 4210
Answer: C (LEAVE A REPLY)

NEW QUESTION: 406
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. HTTP Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. HTML Configuration Arbitrary Administrative Access Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 407
Which of the following technique creates a replica of an evidence media?
A. Bit Stream Imaging
B. Backup
C. Data Extraction
D. Data Deduplication
Answer: (SHOW ANSWER)

NEW QUESTION: 408

A large corporation has recently undergone a cyberattack. The forensic analyst finds suspicious activities in the Windows Event logs during the investigation. The analyst notes that a specific service on the machine has been frequently starting and stopping during the time of the attack. What event IDs should the analyst look for in the System log to confirm this suspicious behavior?

A. Event ID 7031 and Event ID 7032

B. Event ID 1 and Event ID 7035

C. Event ID 7035 and Event ID 7036

D. Event ID 7036 and Event ID 7037

Answer: C (LEAVE A REPLY)

NEW QUESTION: 409

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. 70 years

B. The life of the author plus 70 years

C. The life of the author

D. Copyrights last forever

Answer: B (LEAVE A REPLY)

NEW QUESTION: 410

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

A. Poison the DNS records with false records

B. Establish a remote connection to the Domain Controller

C. Enumerate domain user accounts and built-in groups

D. Enumerate MX and A records from DNS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 411

Which Is a Linux journaling file system?

A. FAT

B. Ext3

C. BFS

D. HFS

Answer: (SHOW ANSWER)

NEW QUESTION: 412

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

A. It is useful for reading and handling of the configuration files

B. It handles allocation of resource pools
C. It handles server start-ups and timeouts
D. It takes care of all the data exchange and socket connections between the client and the server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 413
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: 414
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: (SHOW ANSWER)

NEW QUESTION: 415
Email spoofing refers to:
A. A sudden spike of "Reply All" messages on an email distribution list, caused by one misdirected message
B. 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
C. The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source
D. The criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user's personal or account information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 416
In the context of cybercrime investigations, when the crime perpetrator uses an anonymity tool like Tor Browser to perform illicit activities, the investigator encounters a significant challenge. Considering the scenario, which of the following would best describe the difficulty faced by the investigator?
A. The investigator cannot legally access the data without proper authorization and warrants

B. The investigator is limited by the jurisdiction in which they can carry out their investigation
C. The investigator cannot reliably trace the source of the criminal activity
D. The investigator struggles with the speed of accessing and interpreting data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 417
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?
A. HIPAA 1996
B. GLBA
C. PCI DSS
D. SOX
Answer: (SHOW ANSWER)

NEW QUESTION: 418
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
Answer: B (LEAVE A REPLY)

NEW QUESTION: 419
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: C (LEAVE A REPLY)

NEW QUESTION: 420
An investigator has been tasked to analyze a suspicious executable file potentially containing malware. She uses a static analysis method to examine the file. Which step below should she NOT include as part of her static malware analysis process?
A. Running the executable in a sandboxed environment to observe its behavior

B. Conducting a file fingerprinting on the binary code to determine its function
C. Searching for embedded strings in the binary code to infer the functionality
D. Comparing the hash value of the file with online malware databases for recognition
Answer: (SHOW ANSWER)

NEW QUESTION: 421
Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?
A. FATKit
B. CacheInf
C. Belkasoft Live RAM Capturer
D. Coreography
Answer: C (LEAVE A REPLY)

NEW QUESTION: 422
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 7361
B. 18 USC 1030
C. 18 USC 7029
D. 18 USC 7371
Answer: B (LEAVE A REPLY)

NEW QUESTION: 423
Sectors in hard disks typically contain how many bytes?
A. 1024
B. 2048
C. 256
D. 512
Answer: D (LEAVE A REPLY)

NEW QUESTION: 424

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 25

B. 993

C. 110

D. 143

Answer: C (LEAVE A REPLY)

NEW QUESTION: 425

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A. Technical testimony

B. Civil litigation testimony

C. Expert testimony

D. Victim advocate testimony

Answer: A (LEAVE A REPLY)

NEW QUESTION: 426

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

A. Domain Controller

B. Firewall

C. SIEM

D. IDS

Answer: (SHOW ANSWER)

NEW QUESTION: 427

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

A. A normal system without internet connect

B. A normal system with internet connection

C. A virtual system with network simulation for internet connection

D. A virtual system with internet connection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 428

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

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

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

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

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

Answer: D (LEAVE A REPLY)

Although D in this question is probably the closest, the answer may have been transcribed incorrectly. CHS stands for Cylinder Head Sector, and S is not sides. Each side of a platter of a disk has its own head. A cylinder is an alignment of all tracks under one head position. So the answer is number of cylinders x number of heads x number of sectors (per track) x 512 bytes per sector (assuming that is the sector size as some disks may have larger sector sizes). The number of tracks per side of disk, or the number of tracks that a single head can access is equal to the number of cylinders.