EC-COUNCIL.312-49v11.v2026-05-19.q364

Exam Code:	312-49v11
Exam Name:	Computer Hacking Forensic Investigator (CHFI-v11)
Certification Provider:	EC-COUNCIL
Free Question Number:	364
Version:	v2026-05-19
# of views:	162
# of Questions views:	3640
https://www.freeqas.com/qa/EC-COUNCIL/312-49v11/EC-COUNCIL.312-49v11.v2026-05-19.q364.html	

NEW QUESTION: 1
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. Packer
D. Injector
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
In a high-tech firm located in Austin, Texas, cybersecurity analyst Dr. Liam Hartley was investigating a recent breach where attackers overwhelmed the company ' s online services with a barrage of bogus requests, rendering the platform unavailable to legitimate users and causing significant downtime during peak business hours. The incident disrupted normal operations and led to financial losses as customers could not access services. Based on the attack method described, what type of cybercrime is Dr. Hartley most likely dealing with in this case?
A. Privilege Escalation Attack
B. Brute-force Attack
C. Denial-of-Service DOS Attack
D. Phishing or Spoofing
Answer: (SHOW ANSWER)
The correct answer is C because the defining feature of the incident is that the attackers flooded the organization's online services with illegitimate requests until legitimate users could no longer access them.

That is the classic operational effect of a Denial-of-Service attack. CHFI v11 covers network and web application threats and attacks, including service disruption scenarios that affect organizational operations.
The question does not describe unauthorized privilege gain, repeated password guessing, or deceptive messaging aimed at tricking users, so privilege escalation, brute force, and phishing do not fit as well. What matters here is the deliberate exhaustion of service availability. From a forensic viewpoint, this kind of event is usually recognized through abnormal traffic volume, connection floods, incomplete sessions, or repeated application requests designed to consume bandwidth, server threads, or processing resources.
Because availability is the primary security property being attacked and the platform becomes unreachable to legitimate customers, the most accurate classification is a Denial-of-Service attack. That aligns directly with CHFI's focus on identifying attack categories from their observable effect on systems and services.

NEW QUESTION: 3
Mia, a network administrator, is reviewing the logs of a Cisco router after noticing some performance degradation in her network. While examining the logs, she encounters a particular message that states: "The system was not able to process the packet because there was not enough room for all of the desired IP header options." Mia needs to identify which mnemonic in the Cisco IOS logs corresponds to this specific issue.
Which of the following log mnemonics should Mia look for to find this message?
A. %SEC-4-TOOMANY
B. %IPV6-6-ACCESSLOGP
C. %SEC-6-IPACCESSLOGP
D. %SEC-6-IPACCESSLOGRL
Answer: A (LEAVE A REPLY)
According to the CHFI v11 Network Forensics and Log Analysis objectives, Cisco IOS log messages use standardized mnemonics to describe specific security and packet-processing conditions. The message indicating that "there was not enough room for all of the desired IP header options" is associated with abnormal or excessive IP header options , which can be indicative of malformed packets, reconnaissance activity, or denial-of-service (DoS) attempts .
The mnemonic %SEC-4-TOOMANY is generated when a router receives packets containing too many IP options for the available buffer space. Cisco devices impose limits on IP header options to protect system resources, and when these limits are exceeded, the packet is dropped and logged with this mnemonic. CHFI v11 highlights such logs as important artifacts when investigating network performance degradation, packet manipulation, and potential attack traffic .
The other options are unrelated to this condition. %IPV6-6-ACCESSLOGP applies to IPv6 access control logging. %SEC-6-IPACCESSLOGP and %SEC-6-IPACCESSLOGRL relate

to access-list permit/deny logging and rate-limited ACL messages, not IP header option exhaustion.
From a forensic perspective, identifying %SEC-4-TOOMANY helps investigators correlate performance issues with malformed or malicious traffic patterns and supports attribution during network attack investigations.
Therefore, the correct Cisco IOS log mnemonic corresponding to this issue-fully aligned with CHFI v11-is
%SEC-4-TOOMANY (Option A) .

NEW QUESTION: 4
Olivia, a forensic investigator, is analyzing the behavior of malware that was executed on a compromised Windows system. During her investigation, she discovers that the malware made several changes to the system registry to ensure its persistence. Olivia wants to focus on the areas of the registry most likely to have been targeted by the malware to automatically execute upon system startup. Which registry keys should Olivia focus on to track malware persistence through auto-start functionality? analyzing the behavior of malware that was executed on a compromised Windows system. During her investigation, she discovers that the malware made several changes to the system registry to ensure its persistence. Olivia wants to focus on the areas of the registry most likely to have been targeted by the malware to automatically execute upon system startup. Which registry keys should Olivia focus on to track malware persistence through auto start functionality?
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \Explorer\ShellN
B. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer \Advanced
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Answer: D (LEAVE A REPLY)
Option D is the correct answer because CHFI v11 explicitly includes registry-based malware persistence mechanisms , identifying malware persistence , and system behavior analysis involving registry artifacts, startup programs, processes, services, and Windows event logs .
The Run key under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Run is one of the most common Windows registry locations used by malware to achieve automatic execution at startup . When a value is placed there, the referenced program can be launched when the system starts or when a user logs in, depending on the context. Because the question specifically asks about auto-start functionality , this key is the most relevant place to examine.
The other paths are less suitable. Explorer\Advanced generally stores user interface preferences, Uninstall relates to installed program information, and Policies\Explorer \ShellNoRoam is not the primary classic auto- start persistence location being tested here.

Under CHFI malware forensics and Windows registry analysis objectives, the examiner should focus first on the CurrentVersion\Run key to track persistence behavior tied to startup execution.

NEW QUESTION: 5
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 must be handled in the same way regardless of the type of case
C. evidence in a civil case must be secured more tightly than in a criminal case
D. evidence procedures are not important unless you work for a law enforcement agency
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which of the following technique creates a replica of an evidence media?
A. Data Deduplication
B. Bit Stream Imaging
C. Data Extraction
D. Backup
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following is not a part of the technical specification of the laboratory-based imaging system?
A. Remote preview and imaging pod
B. very low image capture rate
C. High performance workstation PC
D. Anti-repudiation techniques
Answer: (SHOW ANSWER)

NEW QUESTION: 8
On the heels of a massive coordinated cyberattack, a multinational corporation called upon the services of veteran forensic investigator, Lisa. The attack infiltrated their MSSQL servers, and Lisa suspected the breach was a result of a sophisticated SQL Injection method that was executed from multiple sources and locations simultaneously. To determine the attack ' s origin, Lisa needs to not only collect but also examine the evidence files on the MSSQL server. To cope with the breach ' s scale and sophistication, which tool should Lisa rely on?
A. Sqlmap
B. Nessus
C. EnCase

D. SQLsus
Answer: (SHOW ANSWER)
Option C. EnCase is the best answer because the question is about a forensic investigation of an MSSQL server where Lisa needs to collect and examine evidence files in a defensible manner. CHFI v11 explicitly includes SQL Server Logs , Investigating SQL Injection , and broad use of forensic tools for acquisition and examination of digital evidence.
Among the choices, EnCase is the forensic suite most appropriate for evidence collection, preservation, and detailed analysis . It supports imaging, examination, and evidentiary workflow, which are central to determining attack origin in a legally sound way. Sqlmap and SQLsus are offensive or testing-oriented tools associated with SQL injection activity, not primary forensic evidence examination platforms. Nessus is a vulnerability scanner, useful for assessment but not the best answer for collecting and analyzing MSSQL evidence after a breach.
Because the scenario centers on forensic examination of compromised database-server evidence, the strongest CHFI-aligned answer is EnCase , not exploit or scanning tools. It best supports evidence preservation, analysis, and reporting in a large-scale SQL-injection investigation.

NEW QUESTION: 9
A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?
A. Image the disk and try to recover deleted files
B. Check the Windows registry for connection data (you may or may not recover)
C. Seek the help of co-workers who are eye-witnesses
D. Approach the website's administrator for evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?
A. PRIV.EDB
B. PUB.EDB
C. PRIV.STM
D. PUB.STM
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
As a Computer Hacking Forensic Investigator, you are analyzing an intrusion incident in a corporate network. You discovered the traces of a fileless malware attack that utilized a memory exploit. The indicators suggest that the initial payload was delivered via a malicious Word document received through a phishing email. As part of the response and prevention plan, which among the following steps would be the most effective to disrupt the Infection Chain of the detected fileless malware?
A. Disabling the use of all scripting languages, such as JavaScript, in the corporate environment
B. Replacing the currently used traditional antivirus solution with the latest signature-based IDS
C. Implementing a strict policy on macros embedded in Office documents across the organization
D. Patching the vulnerabilities in Flash and Java plugins in all browsers within the corporate network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
During a file-carving operation at a digital-marketing agency in Atlanta, Georgia, forensic examiners use a utility to inspect binary data in both hexadecimal and ASCII views, enabling them to locate file signatures at specific byte positions such as 0x0000 and recover fragmented image files from unallocated space. Which feature best characterizes this tool used for low-level evidence examination?
A. Character Area
B. Hexadecimal Notation
C. Hex Editor
D. Hexadecimal area
Answer: C (LEAVE A REPLY)
A hex editor allows investigators to examine raw binary data in hexadecimal and ASCII views, locate file signatures at exact offsets, and analyze or carve fragments from unallocated disk space.

NEW QUESTION: 13
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?
A. ReFS
B. FAT File System
C. NTFS File System
D. exFAT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
Imagine you, as a forensic investigator, are assigned to investigate a cybercrime involving a Windows-based system. The system has experienced significant file loss due to the attack, and retrieving the missing files is essential for the investigation. To facilitate this, you choose an automated tool capable of restoring critical files that were lost during the incident, ensuring the integrity of the evidence.
Which tool would be the most suitable for this task?
A. Adopting Cain & Abel to recover passwords and sniff network traffic for restoring the lost files.
B. Using R-Studio to scan the file system and recover corrupted, deleted, or damaged files from the Windows system.
C. Leveraging Ophcrack to recover passwords from the target system to back up the critical files.
D. Employing Pwdump7 to extract password hashes from the system for reconstructing the missing files in their original state.
Answer: (SHOW ANSWER)
Under the CHFI v11 Operating System Forensics domain, investigators are required to analyze Windows file systems and recover evidence that may have been deleted, corrupted, or intentionally destroyed during a cybercrime. File loss incidents commonly occur due to malware infections, insider activity, ransomware attacks, or deliberate anti-forensic actions. Recovering such files is often critical to reconstructing events and identifying attacker intent.
R-Studio is a specialized forensic data recovery tool designed to analyze Windows file systems such as NTFS, FAT, and exFAT. It can scan allocated and unallocated disk space, identify lost partitions, and recover deleted or damaged files while preserving original metadata such as timestamps and file structure. CHFI v11 recognizes file recovery tools like R-Studio as essential for post-incident Windows forensics, especially when investigators must restore evidence without modifying the source media.

NEW QUESTION: 15
As part of an ongoing investigation, a CHFI is tasked with identifying and analyzing stealthy malware that has caused severe damage to a major corporation's systems. The malware has left minimal traces, demonstrating its sophisticated nature. It's also believed that the malware originated from the dark web. Based on the available information, what should be the investigator's priority in the malware forensic process?
A. Creating a list of IoCs from other machines in the network to check for malware presence
B. Immediately searching the dark web for similar malware signatures
C. Sending a copy of the malware to anti-virus companies for urgent signature development

D. Setting up a controlled malware analysis lab to study the behavior of the malware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
During a forensic investigation involving an Android device, the investigator needs to establish communication between the device and a computer running the Android Software Developer Kit (SDK). This communication will allow the investigator to access system files, logs, and other relevant data for analysis. To facilitate this, the investigator enables a specific Android developer feature on the device.
Which feature must be enabled to allow the device to communicate with the workstation running the Android SDK?
A. The forensic investigator can enable USB restriction mode on the Android device connected to the external workstation.
B. The investigator can turn on upgrade mode on the target device to be examined in the lab setup.
C. The forensic investigator can trigger recovery mode on the device before connecting to the workstation.
D. The investigator can activate USB debugging mode on the suspected device being analyzed.
Answer: D (LEAVE A REPLY)
This question maps directly to CHFI v11 objectives underMobile and IoT Forensics, specifically Android device acquisition and analysis procedures. In Android forensics, communication between the device and a forensic workstation running the Android SDK is primarily achieved using theAndroid Debug Bridge (ADB)
. ADB enables investigators to interact with the device's file system, retrieve logs, execute commands, and collect forensic artifacts in a controlled manner.
To use ADB,USB Debugging mode must be enabledon the Android device. CHFI v11 explicitly highlights USB debugging as a critical prerequisite for logical acquisition, live data collection, and application-level analysis on Android devices. When enabled, it allows authenticated communication between the device and the forensic workstation without requiring intrusive methods that could alter evidence unnecessarily.
USB restriction mode limits data communication, recovery mode is used mainly for system repairs or flashing firmware, and "upgrade mode" is not a standard Android forensic feature. None of these allow normal SDK- based interaction for forensic analysis.
Therefore, consistent with CHFI v11 Android forensic methodology, enablingUSB debugging modeis the correct and essential step to establish communication with the Android SDK workstation.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17
What stage of the EDRM cycle is being applied when, in an intellectual property theft case in Boston, Massachusetts, custodians are formally instructed to retain all electronically stored information and prevent any deletion or modification of potentially relevant data?
A. Production
B. Processing
C. Information governance
D. Preservation
Answer: (SHOW ANSWER)
The correct answer is D because preservation is the EDRM stage focused on ensuring that potentially relevant electronically stored information remains intact and is not altered or destroyed once a legal duty to retain it arises. The scenario describes custodians being formally instructed to keep data and prevent deletion or modification, which is the classic preservation step in eDiscovery practice. Information governance is broader and deals with general data management policies before a specific matter arises. Processing and production occur later, after data has already been preserved and collected. CHFI v11 includes the eDiscovery process flow and the Electronic Discovery Reference Model cycle, so candidates are expected to connect legal hold style activities with the correct EDRM phase. In practical forensic and litigation support work, preservation is the stage that protects the evidence population from spoliation and ensures that later collection and review remain defensible. Because the question centers on retaining relevant ESI and freezing changes to it, preservation is the exact stage being applied.

NEW QUESTION: 18
During a security audit of a web application, suspicious activity indicative of a directory traversal attack is detected in the server logs. The attack appears to exploit vulnerabilities to gain unauthorized access to sensitive files and directories.
In digital forensics, what is the primary objective of investigating a directory traversal attack?
A. To identify potential loopholes in server hardware configurations
B. To optimize network bandwidth and reduce latency
C. To determine the extent of unauthorized access and data compromise
D. To enhance user experience on the web application

Answer: C (LEAVE A REPLY)
According to the CHFI v11 Network and Web Attacks domain, a directory traversal attack (also known as path traversal) is a web-based attack in which an attacker manipulates input parameters (such as ../ sequences) to access files and directories outside the intended web root.
This can expose sensitive resources such as configuration files, credentials, source code, system files, and application logs.
The primary forensic objective when investigating a directory traversal attack is to determine the scope and impact of unauthorized access. CHFI v11 emphasizes that investigators must analyze web server logs, application logs, and access records to identify:
Which files or directories were accessed
Whether sensitive or confidential data was exposed
The time frame of the attack
The attacker's source IP and request patterns
Whether data was viewed, downloaded, or potentially modified
Understanding the extent of data compromise is critical for incident response, regulatory notification, damage assessment, and legal proceedings. It also helps determine whether further attacks (such as privilege escalation or lateral movement) may have occurred following the traversal exploit.

NEW QUESTION: 19
A rising tech startup suffered a severe blow when its RAID 5 array crashed, rendering crucial project data inaccessible. Nick, a digital forensic expert, has been appointed to salvage as much data as possible from the damaged RAID. Upon examination, he found that two out of the four hard drives in the array were severely damaged. Given the importance and the sheer volume of lost data, it is imperative that Nick retrieves the lost information. The RAID controller was not salvageable, and no documentation was available on the configuration of the disks in the RAID array. What should be Nick's course of action in this scenario?
A. Nick should reconstruct the RAID array manually by determining the order of the disks and parity distribution.
B. Nick should use a RAID-rebuilding software to automatically detect and restore the RAID configuration.
C. Nick should send the damaged hard drives for hardware recovery.
D. Nick should perform a file carving operation on each of the remaining drives separately.
Answer: C (LEAVE A REPLY)
RAID 5 can tolerate only a single disk failure. With two severely damaged drives, logical reconstruction is not feasible until the failed disks are physically recovered. Sending the drives for hardware recovery is necessary to restore enough data for any further reconstruction attempts.

NEW QUESTION: 20
Under which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?
A. 18 U.S.C. 1343 Fraud by wire, radio or television
B. 18 U.S.C. 1030 Fraud and related activity in connection with computers
C. 18 U.S.C. 1832 Trade Secrets Act
D. 18 U.S.C. 1831 Economic Espionage Act
E. 18 U.S.C. 1029 Possession of Access Devices
F. 18 U.S.C. 1362 Government communication systems
G. 18 U.S.C. 1361 Injury to Government Property
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Which list contains the most recent actions performed by a Windows User?
A. Windows Error Log
B. MRU
C. Activity
D. Recents
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
While examining a Windows workstation as part of a digital-fraud investigation in Seattle, Washington, forensic examiners study the disk-level effects of file deletion. Their analysis shows that the reference to a file is removed, yet the underlying data remains recoverable until the same storage space is reused. What statement best reflects this file-system behavior on Windows systems?
A. The deleted file can be recovered if the space is not allocated to any other file.
B. The clusters allocated to the deleted file are marked as free in the $BitMap, and the computer uses that space for a new file.
C. The OS replaces the first letter of a deleted file name with the hex byte code E5h.
D. The OS marks the file entry as unallocated in the Master File Table (MFT) but does not delete the actual file contents.
Answer: D (LEAVE A REPLY)
On Windows NTFS systems, deleting a file marks its MFT record as unallocated while the file's actual data remains on disk until the clusters are overwritten by new data. This is why deleted files may be recoverable during forensic analysis.

NEW QUESTION: 23
In a large multinational organization, an advanced persistent threat (APT) has been detected.

One of the Linux servers of the company seems to be communicating with a known malicious IP address. Alice, a cybersecurity analyst, has been given the task to analyze the situation. She collects volatile information from the server to examine active network connections and running processes. Alice is confused between three options: Redline, Volatility, and Rekall. Which tool should Alice use to perform the analysis most effectively?

A. Redline

B. Volatility

C. Rekall

D. OSForensics

Answer: B (LEAVE A REPLY)

Volatility is widely used for analyzing volatile memory, allowing investigators to examine active processes, network connections, and other in-memory artifacts on compromised systems, making it the most effective choice for this scenario.

NEW QUESTION: 24

During a high-profile fraud case in New York City, examiners receive an iPhone that repeatedly fails to complete a restore in its standard recovery workflow. To proceed with a lower-level restore state that allows reloading firmware even when the normal recovery process is unsuccessful, which option should the team use?

A. SecureROM

B. Recovery mode

C. iBoot

D. Device Firmware Update (DFU) mode

Answer: (SHOW ANSWER)

Device Firmware Update mode is a low-level restore state used when standard recovery mode cannot complete successfully. It allows the device firmware to be reloaded before the normal bootloader or operating system fully starts, making it suitable for deeper recovery or restore operations.

NEW QUESTION: 25

A suspected cyber-criminal was captured, and his computer was seized while he was online. The investigators found that the Tor Browser was open, and some dark websites were visited. They want to obtain as much information as possible from this active session. The investigator needs to decide between collecting a memory dump or powering down the machine for hard drive analysis. Which option would provide the most information in this situation?

A. Shutting down the computer and analyzing the hard drive.

B. Restarting the machine in safe mode and conduct a system scan.

C. Unplugging the machine immediately to preserve the hardware integrity.

D. Leaving the computer running and collecting a memory dump.

Answer: D (LEAVE A REPLY)

Option D is the best answer because the computer was seized while the Tor Browser was actively open , meaning the most valuable evidence may still exist in volatile memory . In CHFI methodology, when a live system contains potentially crucial active-session evidence, investigators should follow the order of volatility and collect the most easily lost evidence first. A memory dump may preserve active browser session data, in- memory artifacts, decrypted content, process information, network connections, and traces of recently accessed dark web activity that might never be written clearly to disk.
Shutting down or unplugging the machine would destroy this volatile evidence immediately. Restarting into safe mode would also alter or erase the active session context. Hard drive analysis remains important later, but it would not capture the full live state of the Tor session as effectively as RAM collection.
Because the goal is to obtain as much information as possible from the active session , the strongest CHFI- aligned answer is to leave the system running and collect a memory dump first before taking further acquisition steps.

NEW QUESTION: 26
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. Degauss the backup tapes and transport them in a lock box.
B. Encrypt the backup tapes and transport them in a lock box
C. Hash the backup tapes and transport them in a lock box.
D. Encrypt the backup tapes and use a courier to transport them.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?
A. Cloud as an Object
B. Cloud as a Subject
C. Cloud as an Application
D. Cloud as a Tool
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
The newer Macintosh Operating System (MacOS X) is based on:
A. OS/2

B. Linux
C. Microsoft Windows
D. BSD Unix
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
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. 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
C. 127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0' 200
D. 127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200
Answer: (SHOW ANSWER)

NEW QUESTION: 30
During a healthcare IoT breach in Houston, Texas, examiners find multiple wearables still using out-of-box credentials. Attackers leveraged these settings to bypass basic access controls and intercept data. Which security issue in the IoT stack most directly enabled this exposure?
A. Insecure API
B. Default passwords
C. No encryption for storage and communications
D. Improper communications encryption
Answer: B (LEAVE A REPLY)
Default passwords are out-of-box credentials that attackers can easily guess or look up from vendor documentation. When IoT devices are left with these credentials unchanged, attackers can bypass basic access controls and gain unauthorized access to device data or management functions.

NEW QUESTION: 31
Sarah, a forensic investigator, is conducting an investigation on a macOS device that is suspected to have been compromised. She is tasked with gathering evidence of unauthorized access to the system. As part of her investigation, she needs to locate information related to when and who accessed the system. In addition to reviewing general system logs, Sarah knows she must focus on certain types of system files that might

provide detailed data on unauthorized activities. Which area of the macOs file system would provide the most relevant information regarding logon attempts and other authentication events?

A. The User Account data

B. The Safari history

C. The Home folder

D. The LaunchDaemons directory

Answer: (SHOW ANSWER)

User account data on macOS contains records related to logins, authentication attempts, and user activity, making it the most relevant source for identifying unauthorized access events.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32

In Microsoft file structures, sectors are grouped together to form:

A. Partitions

B. Clusters

C. Drives

D. Bitstreams

Answer: (SHOW ANSWER)

NEW QUESTION: 33

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

B. RestrictAnonymous must be set to "2" 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: (SHOW ANSWER)

NEW QUESTION: 34
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?
A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field
Answer: A (LEAVE A REPLY)
The Ping of Death occurs when the ICMP Header field contains a packet size lager than 65507 bytes.

NEW QUESTION: 35
In a product liability lawsuit at a manufacturing plant in Detroit, Michigan, a compliance officer determines that potentially responsive records are scattered across multiple departmental repositories. This fragmentation complicates retrieval and increases the risk of omissions that could trigger sanctions. During early case preparation to support defensible collection, what step should be addressed first?
A. Reduce data volume using review or data-reduction techniques
B. Select approbate technology for data collection
C. Map data to identify custodians and data locations
D. Limit and de-duplicate custodians
Answer: C (LEAVE A REPLY)
Data mapping identifies where potentially responsive information resides, which custodians control it, and which repositories must be preserved or collected from. This is the first step when records are scattered across departments because it supports complete, defensible collection and reduces the risk of missing relevant evidence.

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

D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Answer: (SHOW ANSWER)

NEW QUESTION: 37

A system administrator is configuring a new storage array for a critical application and selects a RAID level that uses data stripping and dedicated parity. The RAID setup requires a minimum of three disks, and it ensures data is striped at the byte level across multiple drives, with one drive set aside to store the parity information for fault tolerance. After configuring the RAID system, the administrator tests its ability to tolerate a single drive failure and confirms the system can still function without data loss. Which RAID level is the system administrator using in this scenario?

A. RAID 10

B. RAID 1

C. RAID 3

D. RAID 0

Answer: (SHOW ANSWER)

RAID 3 uses byte-level striping across multiple disks with a dedicated parity disk. It requires at least three drives and can tolerate a single disk failure while maintaining data integrity through parity reconstruction.

NEW QUESTION: 38

An investigator has been assigned to analyze network activity and user interactions on a corporate IIS web server after a suspected security breach. The task requires the investigator to process large volumes of IIS log data, focusing on identifying suspicious traffic trends, user access, and potential exploitation attempts. The tool used must allow for efficient log parsing, anomaly detection, and the generation of detailed reports to help reconstruct the event timeline.

Given these requirements, which tool should the investigator choose to analyze the IIS logs effectively?

A. Sawmill

B. DSInternals PowerShell

C. Jatheon

D. Hunchly

Answer: A (LEAVE A REPLY)

Sawmill is designed for high-volume log analysis, including IIS logs. It provides efficient parsing, trend analysis, anomaly detection, and detailed reporting capabilities, which are essential for reconstructing timelines and identifying suspicious activity in web server logs.

NEW QUESTION: 39

During a financial crime investigation at a credit union in Dallas, Texas, a forensic examiner is tasked with collecting evidence from a suspect's workstation. To ensure the evidence remains admissible in court and follows best practices, which rule of thumb must the examiner apply during data acquisition?

A. Preserve original evidence

B. Reduce data exposure

C. Document every process

D. Quality assurance

Answer: A (LEAVE A REPLY)

Preserving original evidence is the primary rule of thumb in forensic acquisition. Examiners should avoid altering the source media and should work from verified forensic copies whenever possible, maintaining evidence integrity and admissibility.

NEW QUESTION: 40

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.

Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. 2.4Ghz Cordless phones

B. Satellite television

C. CB radio

D. Computers on his wired network

Answer: A (LEAVE A REPLY)

NEW QUESTION: 41

During a consent-based search at a software company in Austin, Texas, investigators are granted permission to examine specific electronic systems. To avoid exceeding the limits of authorization and to ensure the legality of any evidence collected, the consent documentation must be sufficiently detailed. Which requirement best addresses this need?

A. The consent must be acknowledged by relevant internal authorities

B. The consent must be granted by the owner of the organization or the device

C. The consent must clearly outline the scope of permitted search and seizure activities

D. The consent must be formally documented before initiating the search

Answer: C (LEAVE A REPLY)

The correct answer is C because the main legal risk in a consent-based search is exceeding the permission that was actually granted. For that reason, the consent documentation must clearly define the scope of what systems may be searched, what actions are permitted, and what evidence may be seized or examined. CHFI v11 includes

seeking consent, search and seizure, and best practices for handling digital evidence, so candidates are expected to recognize that detailed scope control is what keeps the search lawful and defensible. Formal documentation is important, and valid authority to consent also matters, but neither addresses the specific problem in the question as directly as a clearly defined scope. In digital investigations, devices and systems often contain far more data than is relevant, so ambiguity in consent can quickly create legal problems. Since the question asks what requirement best prevents investigators from going beyond the authorized boundaries, the strongest answer is that the consent must clearly outline the scope of permitted search and seizure activities.

NEW QUESTION: 42
Microsoft Outlook maintains email messages in a proprietary format in what type of file?
A. .mail
B. .pst
C. .doc
D. .email
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
SMTP (Simple Mail Transfer protocol) receives outgoing mail from clients and validates source and destination addresses, and also sends and receives emails to and from other SMTP servers.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Dariel, a forensic investigator, has been assigned to investigate a recent security incident that occurred within the organization's network. As part of the investigation, Dariel installs a command-line interface packet sniffer on a Unix-based system to monitor and capture network traffic, looking for signs of unauthorized access or malicious activity. The captured data will help Dariel identify the sources of the security breach and trace the attacker's actions through the network. The tool used must be efficient for analyzing real-time network traffic and capable of running on a Unix-based operating system. Which of the following tools did Dariel employ in the above scenario?
A. tcpdump
B. Metashield Analyzer
C. Timestomp
D. Billboard
Answer: A (LEAVE A REPLY)

According to the CHFI v11 curriculum under Network Forensics, investigators must be proficient in using packet sniffing tools to capture and analyze live network traffic. tcpdump is a widely used command-line packet analyzer that runs natively on Unix, Linux, and BSD-based systems. It allows investigators to capture packets in real time, apply powerful filters, and save traffic in PCAP format for further offline analysis using tools such as Wireshark.
In forensic investigations, tcpdump is especially valuable because it provides low-level visibility into network communications, including source and destination IP addresses, ports, protocols, TCP flags, and payload data. This enables investigators to detect suspicious behaviors such as unauthorized connections, port scans, malware command-and-control traffic, data exfiltration attempts, and denial-of-service activities. CHFI v11 specifically highlights tcpdump as a core tool for network traffic investigation and evidence gathering in Unix-based environments.

NEW QUESTION: 45
You are the leading forensic analyst at a digital forensic firm. One of your significant clients, a government agency, has suffered a security breach resulting in an unauthorized leak of classified documents. Initial investigations have shown that the attacker, suspected to be an employee, used an anonymous, encrypted email service to send these documents to multiple unknown recipients. As part of your investigation, you have obtained disk images from the suspect ' s workstation. Your task is to extract and analyze the relevant evidence that could lead to identifying the unknown recipients. What should be your first step?
A. Review the disk image for any signs of a trojan or other malware that could have been used in the data breach.
B. Analyze internet history files for potential traces of the anonymous, encrypted email service.
C. Execute a full search of the disk image for file artifacts related to the anonymous, encrypted email service.
D. Inspect the email client on the disk image for any unencrypted data that could contain the recipient ' s information.
Answer: B (LEAVE A REPLY)
Option B is the best first step because the scenario already points to the use of an anonymous, encrypted email service , and the most direct source of evidence on the disk image is likely to be internet history and browser artifacts associated with access to that service. In forensic investigations, the first priority after acquiring the image is to identify the user's interaction with the suspected communication platform. Browser history, cached pages, cookies, form entries, session remnants, and related web artifacts can reveal service usage patterns, access times, account identifiers, or other traces that help identify unknown recipients or at least narrow the communication path.

Option C is broader and may be useful later, but a full search of all artifacts is less targeted as an initial move.
Option D is weaker because the question specifically refers to an anonymous encrypted email service, which is often web-based rather than tied to a traditional email client. Option A shifts attention to malware without evidence that malware was the primary method of exfiltration. Therefore, the most logical CHFI-style first step is to examine internet history files and related web-use artifacts for traces of the anonymous email activity.

NEW QUESTION: 46
Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?
A. It is file deleted from R drive
B. It is a doc file deleted in seventh sequential order
C. RIYG6VR.doc is the name of the doc file deleted from the system
D. It is a deleted doc file
Answer: D (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 47
As a forensic investigator specializing in cybersecurity, you've been assigned to analyze a suspicious PDF document named "infected.pdf." This document was discovered on a company server and is suspected to contain malicious scripts that could pose a threat to the organization's systems and network. As part of your investigation into the PDF document, what initial step would you take to identify potential malicious components within the file?
A. Run the command python pdfid.py infected.pdf in a Linux terminal to review the file's structure and identify any embedded scripts.
B. Open the PDF document in a virtual machine environment to observe potential malicious behavior.
C. Utilize a web-based tool to extract metadata from the PDF document and analyze any anomalies.

D. Use a hex editor to manually inspect the contents of the PDF document for suspicious patterns.

Answer: A (LEAVE A REPLY)

According to the CHFI v11 objectives under Malware Forensics and Static Malware Analysis, the correct initial step when analyzing a suspicious document--such as a potentially malicious PDF-- is to perform static analysis before any execution. Running the tool PDFiD using the command python pdfid.py infected.pdf is a standard and CHFI-aligned first action. PDFiD is designed to quickly scan a PDF file and identify suspicious elements such as /JavaScript, /OpenAction,
/Launch, /EmbeddedFile, and /AA, which are commonly abused by attackers to deliver malware through PDF documents.

This approach is non-intrusive and ensures the investigator does not accidentally trigger malicious code, thereby preserving evidence integrity and maintaining forensic soundness. Opening the file in a virtual machine (Option B) constitutes dynamic analysis, which should only be performed after initial static indicators suggest malicious intent and after proper containment controls are in place. Metadata extraction (Option C) is useful but limited, as metadata alone does not reliably expose embedded exploit code. Manual hex inspection (Option D) is advanced and time-consuming and is not recommended as the first step.

NEW QUESTION: 48

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 color of the digital device from which the evidence was extracted

C. The manufacturing company of the device from which evidence was extracted

D. The reason and process for obtaining the evidence

Answer: D (LEAVE A REPLY)

NEW QUESTION: 49

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor.

What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To avoid electromagnetic emanations

B. To make the lab sound proof

C. To strengthen the walls, ceilings, and floor

D. To control the room temperature

Answer: (SHOW ANSWER)

NEW QUESTION: 50

Sophia, a forensic analyst, is examining the event log files on a compromised server. During her investigation, she identifies an entry in the event log header that seems unusual. The entry's ELF_LOGFILE_HEADER value indicates that records have been written to the log, but the event log file has not been properly closed. Based on this information, which ELF_LOGFILE_HEADER value would Sophia identify?

A. ELF_LOGFILE_HEADER_DIRTY0x0001

B. ELF_LOGFILE_ARCHIVE_SET0x0008

C. ELF_LOGFILE_HEADER_WRAP0x0002

D. ELF_LOGFILE_LOGFULL_WRITTEN0x0004

Answer: A (LEAVE A REPLY)

The DIRTY flag indicates that the event log contains records but was not properly closed, meaning the log file may be in an inconsistent state due to improper shutdown or tampering.

NEW QUESTION: 51

In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Known-message attack

B. Known-stego attack

C. Known-cover attack

D. Chosen-message attack

Answer: (SHOW ANSWER)

NEW QUESTION: 52

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. Circuit-level proxy firewall

C. Data link layer firewall

D. Packet filtering firewall

Answer: A (LEAVE A REPLY)

NEW QUESTION: 53

During a document-recovery effort at a publishing house in New York City, forensic examiners carve fragmented text strings from a suspect's deleted email archive. The recovered characters represent only English letters, numbers, and basic punctuation encoded in a compact 7-bit format limited to 128 specified symbols. Which encoding standard best matches this constraint for reconstructing readable English content?

A. UNICODE
B. UTF-16
C. ASCII
D. UTF-8
Answer: (SHOW ANSWER)
ASCII is a 7-bit character encoding standard that represents 128 characters, including English letters, numbers, control characters, and basic punctuation. It matches the recovered compact text format used for readable English content.

NEW QUESTION: 54
David, a network security analyst, is tasked with investigating a possible breach involving an Apache web server. After reviewing the logs, he notices several failed login attempts, and HTTP error messages related to unavailable files. Which of the following Apache log entries will provide the most useful information to help David determine whether these failed attempts were part of a larger security issue?
A. [Mon Dec 11 14:35:36.878945 2023] [core:notice] [pid 12356:tid 8689896234] [client 10.0.0.8] Connection closed gracefully
B. [Mon Dec 11 14:35:38.878945 2023] [core:error] [pid 12356:tid 8689896234] [client 10.0.0.8] File not found: /images/folder/pic.jpg
C. [Mon Dec 11 14:35:38.878945 2023] [auth.debug] [pid 12356:tid 8689896234] [client 10.0.0.8] Invalid user attempt
D. [Mon Dec 11 14:35:38.878945 2023] [mod_security:info] [pid 12356:tid 8689896234] [client 10.0.0.8] Rule triggered: Possible SQL Injection attempt
Answer: D (LEAVE A REPLY)
Option D is the most useful answer because it provides the clearest indication that the activity may be part of a larger security issue rather than just routine login failures or missing-file requests. A mod_security entry showing that a rule was triggered for a possible SQL injection attempt directly suggests malicious web- application attack behavior and points to a broader intrusion pattern.
Option C is useful for confirming failed authentication activity, but by itself it may still reflect simple credential guessing or user error. Option B only shows a missing file request, which could be benign or accidental. Option A is the least suspicious of the choices. By contrast, an application firewall or security module explicitly flagging a possible SQL injection attempt strongly indicates that the server may be under targeted attack and that the failed logins could be part of a coordinated campaign.
From a CHFI perspective, log entries that directly indicate known attack techniques are especially valuable during web-server investigations. Therefore, the Apache log entry most likely to help David determine that the failed attempts were tied to a larger security problem is the mod_security alert for possible SQL injection .

NEW QUESTION: 55

David, a digital forensics examiner, is investigating a cybercrime incident for a multinational corporation. He wants to ensure that the organization's practices for managing digital evidence comply with internationally recognized standards. Which ISO/IEC standard provides guidelines for the establishment, maintenance, and improvement of a digital forensic capability within an organization?

A. ISO/IEC 27043
B. ISO/IEC 27042
C. ISO/IEC 27041
D. ISO/IEC 27037

Answer: C (LEAVE A REPLY)

ISO/IEC 27041 provides guidance on establishing, maintaining, and improving an organization's digital forensic capability. It focuses on ensuring that forensic methods, processes, and practices are suitable, reliable, and repeatable for handling digital evidence.

NEW QUESTION: 56

During a cybersecurity investigation, logs from a Cisco switch, VPN, and DNS server are collected.

These logs contain valuable information about network activities and potential security breaches.

In digital forensics, what role do Cisco switch, VPN, and DNS server logs play when analyzing network incidents?

A. Provides insights on network traffic, device connections, and security incidents.
B. Tracks website visits and browser history exclusively.
C. Not pertinent to digital forensics.
D. Details user activities within the local network.

Answer: A (LEAVE A REPLY)

This question aligns with CHFI v11 objectives under Network and Web Attacks and Network Log Analysis . In digital forensics, network infrastructure logs are critical sources of evidence for detecting, analyzing, and reconstructing network-based attacks. CHFI v11 specifically emphasizes the forensic value of logs generated by network devices such as Cisco switches, VPN gateways, and DNS servers .

Cisco switch logs provide information about device connections, port activity, MAC address mappings, VLAN assignments, and potential unauthorized access within the internal network. VPN logs reveal details about remote connections, including authentication attempts, user identities, IP addresses, session durations, and encrypted tunnel activity-crucial for identifying compromised credentials or unauthorized remote access. DNS server logs record domain name queries and responses, which help investigators detect command-and-control communication, data exfiltration attempts, malware beaconing, and access to malicious domains.

Together, these logs allow investigators to correlate events across the network, trace attacker movement, identify affected systems, and establish timelines of security incidents. The other options are incorrect because browser history is host-based evidence, and these logs are highly relevant to forensic investigations.
Therefore, consistent with CHFI v11 network forensics principles, these logs provide insights into network traffic, device connections, and security incidents.

NEW QUESTION: 57
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



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

NEW QUESTION: 58
When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?
A. Brute-force attack
B. Cookie poisoning attack
C. SQL injection attack
D. Cross-site scripting attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
In a large software development company, an investigation conducted into an incident of source code theft. The initial investigation hints at an insider being responsible. The inquiry should validate the breach, pinpoint the method of its execution and compile proof that can stand up in court. Considering the case details and the goal of the inquiry, what investigative approach should be taken that would serve best?
A. A civil investigation focusing on mutual understanding between involved parties
B. An administrative investigation limited to identifying policy or protocol violations
C. A mix of civil and criminal investigations, taking the strengths from both
D. A criminal investigation, with the onus on law enforcement to prove guilt
Answer: C (LEAVE A REPLY)

NEW QUESTION: 60
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: 61
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. Telemarketing act
B. Federal Spam act
C. European Anti-Spam act
D. The CAN-SPAM act
Answer: D (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 62
Olivia, a security analyst, is performing a penetration test on a banking website to identify potential vulnerabilities. While reviewing the input fields, she suspects that the site might be vulnerable to SQL injection attacks. During her testing, she observes a URL that seems to have unusual encoding techniques applied to it. One URL stands out, in which the input appears to have been double encoded, potentially to evade detection and bypass filters that prevent SQL injection. Which of the following URLs indicates double encoding to execute an SQL injection attack?
A. http://www.bank.com/accounts.php?id=1%252f%252a*/union%252f%252a*/select %252f%252a*/1,
2,3%252f%252a*/from%252f%252a*/users--
B. http://www.bank.com/accounts.php?id=1+UnIoN/**/SeLeCT/**/1,2,3--
C. http://www.bank.com/accounts.php?id=1+UNunionION+SEselectLECT+1,2,3--
D. http://www.bank.com/accounts.php?id=1+uni%0bon+se%0blect+1,2,3--
Answer: A (LEAVE A REPLY)

According to theCHFI v11 Web Application Forensics and Network & Web Attacks module, attackers commonly useencoding and obfuscation techniquesto bypass input validation mechanisms, web application firewalls (WAFs), and intrusion detection systems. One such advanced technique isdouble URL encoding, which involves encoding already URL-encoded characters a second time.
In URL encoding, the forward slash / is represented as %2F. When this value is encoded again, % becomes %
25, resulting in %252F. InOption A, multiple occurrences of %252f clearly indicate that characters such as / and comment markers (/* */) have beendouble encoded. When processed by the web server or application, the input may be decoded twice, ultimately reconstructing a valid SQL injection payload like UNION SELECT, thereby bypassing security filters.
Options B and C rely oncase manipulation and keyword splitting, which are evasion techniques butnot double encoding. Option D useshex-encoded control characters, which is a different obfuscation method and does not represent double URL encoding.
CHFI v11 explicitly highlightsdouble encodingas a common technique used in SQL injection attacks to evade detection and filtering mechanisms. Therefore, the URL that clearly demonstratesdouble-encoded SQL injection payloadsisOption A, making it the correct and CHFI-aligned answer.

NEW QUESTION: 63
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. Mysqlbinlog, due to its ability to read and display binary log files in text format
C. Myisamlog, for its functionality to process the contents of the MyISAM log file and perform recovery operations
D. Mysqlaccess, due to its ability to check and validate the access privileges defined for a hostname or username
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which Is a Linux journaling file system?
A. BFS
B. FAT
C. Ext3

D. HFS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
You should make at least how many bit-stream copies of a suspect drive?
A. 4
B. 2
C. 1
D. 3
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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. Application logs
B. Files or network shares
C. System logs
D. Running application
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
In a corporate espionage investigation at a pharmaceutical research facility in Raleigh, North Carolina, examiners obtain multiple Outlook mailbox archives stored on a seized external drive. Initial attempts to open the files in forensic viewers fail due to structural inconsistencies that prevent proper mounting or parsing.
Before any content extraction or verification can proceed, the team uses EaseUS Email Recovery Wizard to address these file issues. From the listed capabilities of this tool, which function directly enables the examiners to resolve the structural problems and make the archives accessible for analysis?
A. Recover deleted folders, contacts, attachments, calendars and meeting requests
B. Repair corrupted PST files
C. Recover lost or deleted emails from Microsoft Outlook
D. Preview deleted or lost emails before recovering them
Answer: (SHOW ANSWER)
The correct answer is B because the problem described is structural corruption of PST archives, not simple deletion or preview needs. EaseUS documents that its email recovery product includes the ability to repair damaged or corrupted PST files so they can be accessed again. That capability directly addresses the scenario, where the Outlook archives cannot be mounted or parsed because of structural inconsistencies. Recovering

deleted folders or messages would only matter after the PST structure is readable enough for examination.
Previewing lost emails is also a later-stage function, not the step that fixes the file itself. CHFI v11 includes email forensics and evidence acquisition from email sources, so tool-selection questions of this kind test whether the examiner can distinguish between repair functions and recovery functions. In forensic workflow terms, corrupted archive repair is the prerequisite step that restores accessibility and enables later parsing, verification, and content extraction. Because the archives are failing to open due to corruption, the function that directly resolves the issue is repair corrupted PST files.

NEW QUESTION: 68
An investigator is reviewing the Apache access logs for suspicious traffic. She notices a series of requests for /admin.php from an IP address that is not normally associated with administrative access. What should she do next to determine whether this is an unauthorized access attempt?
A. Analyze the user-agent strings associated with the requests to identify the browser being used.
B. Check the HTTP status codes in the log entries for these requests to identify whether they were successful.
C. Review the timestamps of the requests to determine if they occurred during business hours.
D. Cross-reference the IP address with the server's DNS logs to see if it is part of a known network.
Answer: B (LEAVE A REPLY)
Checking the HTTP status codes reveals whether the requests to /admin.php were successful or denied. This directly indicates if unauthorized access attempts resulted in actual access, which is critical for determining the severity of the activity.

NEW QUESTION: 69
Following a data breach at a global financial institution, the company ' s incident response team has been working tirelessly to identify the breach ' s origin. The database administrator noticed that some tables within the company ' s SQL Server database were altered. She found that there were changes made in the order history, financials, and customer details. The transaction log showed modifications with numerous queries which were quite uncommon. It seemed the attacker gained access via a remote connection, suggesting that the login details might have been compromised. As a forensic investigator, what would be your next step to identify the source of the breach?
A. You would need to evaluate the server logs for unusual login patterns.
B. You would need to perform a complete system scan.
C. You would need to assess the most recently accessed files.
D. You would need to identify the source IP from where the connection was initiated.

Answer: A (LEAVE A REPLY)
Option A is the best answer because the scenario already suggests that the attacker likely gained access through a remote connection using compromised credentials . The most logical next forensic step is to examine server logs for unusual login patterns , including failed logons, successful remote logins at abnormal times, privileged account use, and suspicious authentication sources. CHFI v11 explicitly includes event logs , types of logon events , evaluating account management events , and SQL Server logs as relevant evidence sources in operating system and application forensics.
Although identifying the source IP may later become important, investigators usually first validate the unauthorized access path through log review and then correlate it with IP data, account activity, and timeline evidence. A complete system scan is too broad as the next step, and reviewing recently accessed files does not directly answer how the attacker entered the database environment.
Because CHFI emphasizes log analysis , authentication event review , and timeline reconstruction when investigating intrusions, the strongest next step is to evaluate the server logs for unusual login patterns that explain how the attacker gained access.

NEW QUESTION: 70
A new corporation is setting up a Computer Forensics Lab (CFL) to handle potential cybercrimes.
They want to establish a CFL that covers all necessary considerations to ensure smooth and effective investigations. Which of the following sets of steps does NOT represent a proper way to set up a CFL?
A. Focus solely on internal corporate investigations, overstaff with inexperienced personnel, use demo versions of forensic software, underestimate lab size and budget, ignore physical security measures, and disregard licensing and accreditation processes
B. Choose types of investigations, estimate the number of investigators, determine equipment and software requirements, calculate lab size, ensure access to essential services, establish workstation requirements, and enhance physical security
C. Determine the number of expected cases, hire certified professionals, purchase forensic and non- forensic workstations, design the lab for easy access to emergency services, install a dedicated Integrated Services Digital Network (ISDN), maintain a log register, and ensure a comfortable lab ambience
D. Evaluate crime statistics of the previous year, ensure the use of licensed software versions, arrange for storage lockers, maintain lab cleanliness, ensure the lab has proper lighting systems, keep workstations under surveillance, and set up an intrusion alarm system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 71

You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?
A. The firewall failed-bypass
B. The firewall failed-closed
C. The firewall ACL has been purged
D. The firewall failed-open
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
During a malware intrusion investigation at an enterprise workstation, forensic analysts use Magnet AXIOM to reconstruct how suspicious executables were introduced and run over time. The investigation requires an artifact that records metadata about executed programs, including file paths and execution context, even when the original binaries are no longer present on disk. This artifact is used to support execution timeline analysis in conjunction with other system evidence. Which artifact should investigators prioritize for this purpose?
A. UserAssist entries
B. ShimCache AppCompatCache
C. Amcache
D. Prefetch files
Answer: (SHOW ANSWER)
The best answer is D because Prefetch files are one of the strongest Windows artifacts for reconstructing program execution history and building execution timelines. Magnet notes that Prefetch files are valuable because Windows creates them when an application runs from a particular location, and they preserve useful metadata about that application history. They can remain available even if the original executable is no longer present, which makes them especially helpful in malware cases where binaries are deleted after use. In CHFI v11, Windows artifact analysis includes executed-program evidence and timeline reconstruction, so candidates are expected to identify the artifact that most directly supports execution analysis. UserAssist is useful but is more limited to certain user-driven GUI activity. ShimCache and Amcache are important artifacts, yet they are often better treated as evidence of presence or compatibility tracking rather than definitive proof of execution by themselves. Since the question emphasizes executed programs, file paths, and timeline support in AXIOM, Prefetch files are the most precise and defensible answer. They are commonly correlated with other artifacts to strengthen the narrative of malware launch and persistence.

NEW QUESTION: 73
During a preliminary scan at a financial services firm in New York City, a suspicious binary exhibits unusually high entropy and yields almost no readable strings, suggesting concealment tactics that evade basic signatures without execution. To uncover these evasion layers in the file ' s structure prior to any runtime testing, which static analysis technique should the team prioritize to reveal the transformation methods applied to the sample?
A. Local and online malware scanning
B. File fingerprinting
C. Performing strings search
D. Identifying packing or obfuscation methods
Answer: (SHOW ANSWER)
The correct answer is D because high entropy and the absence of readable strings are classic indicators that a sample may be packed, encrypted, or otherwise obfuscated. In static malware analysis, one of the first priorities in such a case is to identify the packing or obfuscation method so the analyst can understand how the file has been transformed and what additional unpacking or decoding steps may be needed. CHFI v11 includes static and dynamic malware analysis, analysis of suspicious files, and techniques for understanding malware structure before execution. Local or online malware scanning can provide reputation information, but it does not directly explain the structural concealment method. File fingerprinting identifies known samples, and strings analysis is useful, but the question already tells us that strings are scarce and entropy is high, making raw string extraction less informative. In forensic malware work, those clues point directly to packing or obfuscation. Therefore, the most appropriate static technique is to identify the packing or obfuscation methods used by the sample before any runtime testing begins.

NEW QUESTION: 74
Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?
A. Middleware layer
B. Application layer
C. Access gateway layer
D. Edge technology layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?
A. Nuix
B. HashKey
C. PWdump7

D. FileMerlin
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
Sarah, a CHFI investigator, is assigned to a case involving potential child exploitation material distributed through a private network. A concerned citizen discovered the network and reported it to the authorities. Sarah's job is to investigate and gather evidence from this network without violating any laws or regulations. Given the sensitivity of the case and the potential for severe penalties for those involved, Sarah must ensure that the evidence she collects will hold up in court. What should be Sarah's first step in this investigation?
A. Obtain a search warrant based on the initial report to legally collect evidence from the network
B. Access the network covertly to gather evidence without alerting suspects
C. Monitor network traffic to identify potential suspects
D. Leverage social engineering tactics to infiltrate the network and identify the users involved
Answer: A (LEAVE A REPLY)
Obtaining a search warrant ensures that evidence collection is conducted legally and in compliance with regulations, preserving admissibility in court and protecting the integrity of the investigation.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77
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\drivers\SAM
B. C:\windows\system32\Boot\SAM
C. C:\windows\system32\con\SAM
D. C:\windows\system32\config\SAM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?
A. bmp
B. jpeg
C. gif
D. png
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
Debbie has obtained a warrant to search a known pedophile's 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 digital camera was old. had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.
B. The digital camera was not listed as one of the digital devices in the warrant
C. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
D. Debbie overlooked the digital camera because it is not a computer system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
During a cybercrime investigation, investigators obtain a warrant to search a suspect's computer system for evidence of hacking activities. As they collect data from the suspect's electronic devices, they inadvertently access information revealing the identities of other users connected to the system.
Which step in the cybercrime investigation process raises concerns related to privacy issues?
A. Implementing network security measures
B. Conducting forensic analysis
C. Preserving the anonymity of other users
D. Obtaining search warrants
Answer: B (LEAVE A REPLY)
According to theCHFI v11 Regulations, Policies, and Ethicsdomain,privacy issues most commonly arise during the forensic analysis phaseof a cybercrime investigation. While search warrants legally authorize investigators to collect and examine specific digital evidence, they are typicallyscope-limitedto the suspect, systems, data types, and timeframes defined in the warrant.
Duringforensic analysis, investigators may inadvertently encounterpersonal or sensitive information belonging to third parties, such as usernames, email addresses, chat records, credentials, or identifiers of other users connected to the system. CHFI v11 explicitly

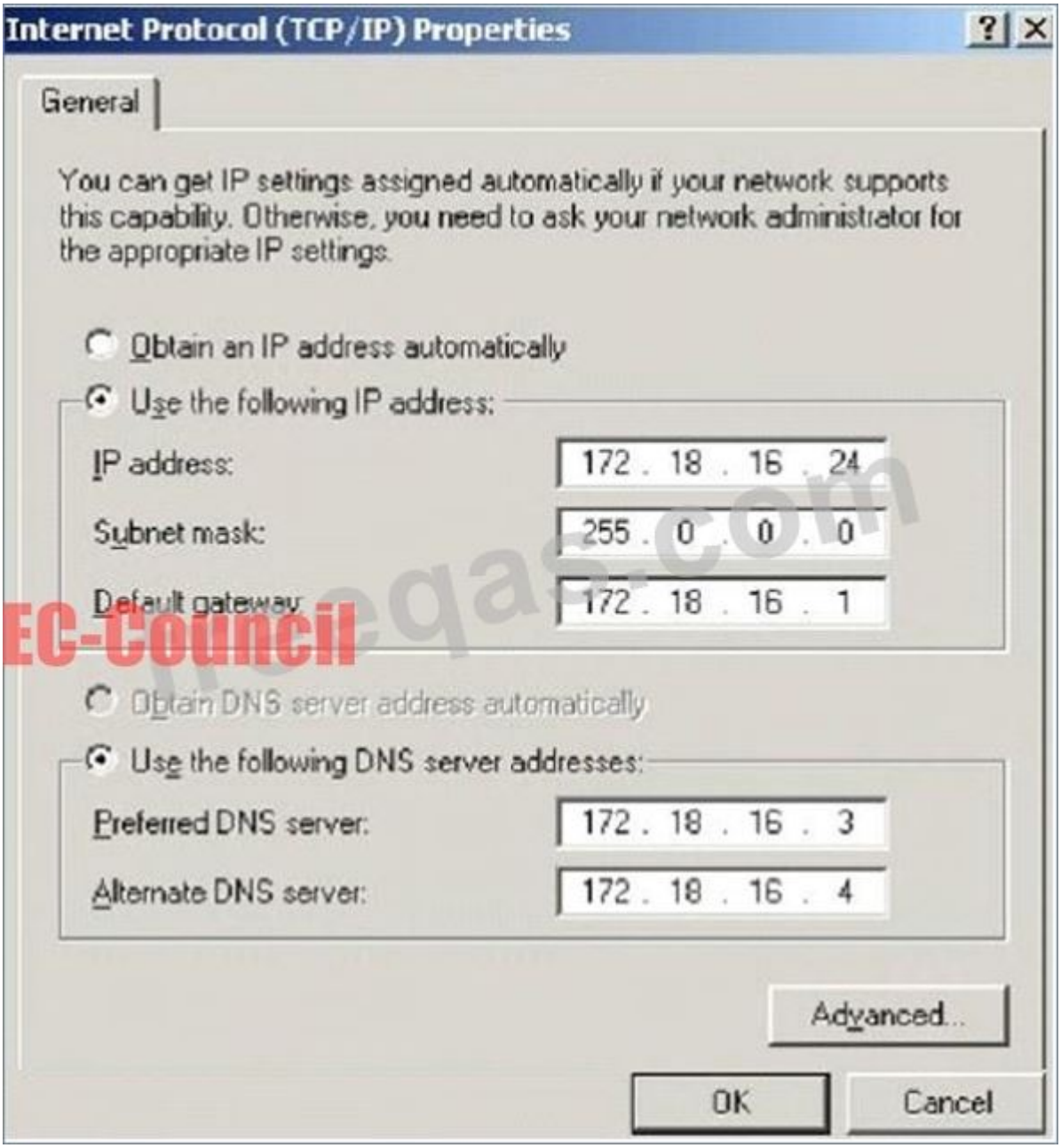
highlights this phase as legally and ethically sensitive because analysts must ensure thatnon-relevant data and third-party information are handled carefullyto avoid violations of privacy laws and data protection regulations.
Implementing network security measures is a preventive activity, not an investigative one. Obtaining search warrants is a legal safeguard designed to protect privacy, not create privacy concerns. Preserving anonymity is a mitigation action, not the step that introduces the risk.
CHFI v11 stresses the importance ofminimization, access control, proper documentation, and legal oversightduring forensic analysis to prevent misuse or overexposure of unrelated personal data. Failure to manage privacy during this phase can result in legal challenges, evidence exclusion, or regulatory violations.
Therefore, the step that raisesprivacy-related concernsin this scenario isconducting forensic analysis, makingOption Bthe correct and CHFI v11-verified answer.

NEW QUESTION: 81
A renowned global retail corporation recently underwent a sophisticated attack cyber-attack leading to a significant loss of data. The company had invested heavily in its Security Operations Center (SOC) which was expected to act as the first line of defense against such cyber threats.
However, the SOC was unable to detect the attack until it was too late. In retrospect what aspect of the SOC's role in computer forensics might have been overlooked in this scenario?
A. SOC's role in conducting a forensic investigation.
B. SOC's role in preserving evidence for forensic investigations.
C. SOC's role in maintaining and securing log data.
D. SOC's role in continuously monitoring and analyzing network traffic.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
In the course of a detailed investigation into a potential breach, forensic analysts scrutinize the logs of an organization's security devices and uncover an unexpected pattern of activity originating from an internal IP address. These activities involve frequent communication with an external server located in a foreign country, previously not associated with any authorized business functions. The volume of interactions is significantly higher than what is typically seen in standard operations for this particular system. Some of the requests reveal an unusual type of data-large binary files-that are atypical for the kind of processes the internal systems typically perform. Upon further analysis, the data exchanges appear to be irregular, as they do not align with any known workflows, and the destination server is outside the organization ' s usual trusted zones.
Which indicator of compromise (IoC) does this behavior most likely signify?
A. Multiple failed attempts to connect to unauthorized external IPs.

B. Unusual login behavior from internal systems during non business hours.
C. Abnormal outbound traffic suggesting data exfiltration.
D. Unusual internal system reboots causing a disruption in normal operations.
Answer: C (LEAVE A REPLY)
Option C is the strongest answer because the scenario describes frequent, high-volume outbound communications from an internal system to an untrusted external server , including large binary files that do not fit normal business workflows. CHFI v11 explicitly includes Indicators of Compromise (IoC) , Analyze Traffic to Detect Malware Activity , and Examine Data Exfiltration Attempts made through FTP under its network-forensics objectives.
These are classic signs of data exfiltration . The foreign destination, unusual data type, abnormal transfer volume, and deviation from standard operations all point toward unauthorized outbound movement of sensitive information. That is a more precise fit than failed connection attempts, off-hours logins, or reboot anomalies.
In CHFI terms, investigators use traffic analysis, log review, and event correlation to identify whether an internal host is behaving like a staging or exfiltration node. Since the question focuses on unexpected external communications and atypical outbound file transfers, the most accurate indicator of compromise is abnormal outbound traffic suggesting data exfiltration .

NEW QUESTION: 83
What is the CIDR from the following screenshot?



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

B. /24A./24A./24

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 84

In a complex cybercrime investigation, forensic experts encounter a severely fragmented hard drive that lacks usable file system metadata. By employing advanced file carving techniques, they successfully recover crucial evidence hidden by a suspect who deliberately manipulated file extensions to obfuscate data.

What advanced method do forensic investigators employ to recover hidden files from a fragmented hard drive lacking file system metadata?

A. Reconstructing the file system architecture from scratch.

B. Decrypting files encrypted using sophisticated algorithms.
C. Extracting files from inaccessible sectors using firmware-level access.
D. Analyzing file signatures and patterns in unallocated space.
Answer: D (LEAVE A REPLY)
According to the CHFI v11 Anti-Forensics Techniques and Digital Evidence Analysis objectives, attackers often attempt to evade detection by deleting files, corrupting file system metadata, fragmenting data, or manipulating file extensions . When file system structures such as the MFT, FAT, or directory entries are missing or damaged, traditional file recovery methods fail. In such scenarios, investigators rely on file carving
.
File carving is an advanced forensic technique that recovers files based on file signatures (headers and footers) and content patterns , rather than file system metadata. CHFI v11 explains that file carving scans unallocated space, slack space, and raw disk sectors to identify known byte patterns associated with specific file types (for example, JPEG headers FFD8FFE0 or PDF headers %PDF). This allows investigators to recover files even when filenames, extensions, and directory information have been intentionally altered or destroyed.
This technique is particularly effective against anti-forensic tactics such as file extension mismatch and metadata wiping. While file carving may not always restore original filenames or timestamps, it is highly valuable for recovering the actual content of hidden or deleted files. The other options are not aligned with CHFI methodology: rebuilding file systems from scratch is impractical, decryption addresses a different problem, and firmware-level access is not a standard forensic recovery method.
CHFI v11 explicitly highlights signature-based and pattern-based carving as the correct approach for recovering evidence from fragmented drives with missing metadata.
Therefore, the correct answer is analyzing file signatures and patterns in unallocated space , making Option D the correct choice.

NEW QUESTION: 85
During a botnet takedown case in Los Angeles, California, an ISP ' s abuse desk keeps receiving legal complaints about malicious traffic traced to an IP that belongs to Tor infrastructure. Investigators explain that, although the traffic did not originate there, this Tor component is the one seen by destination servers as the source and therefore attracts most abuse complaints and shutdown demands. Which Tor component are they referring to?
A. Middle Relay
B. Entry Guard Relay
C. Exit Relay
D. Bridge Node
Answer: (SHOW ANSWER)

The correct answer is C because the exit relay is the final Tor relay that sends traffic out to the destination service. Tor's own documentation states that the website, chat service, email provider, or other destination will see the IP address of the exit relay instead of the actual Tor user. That is exactly why abuse complaints and takedown pressure usually focus on exit relays. Entry guards see the user first, middle relays pass traffic inside the circuit, and bridge nodes help users connect to Tor when normal entry points are blocked, but those components are not normally the publicly visible source IP presented to outside services. CHFI v11 includes dark web concepts, TOR relays, TOR bridge nodes, and the forensic risks of investigating anonymized environments, so understanding relay roles is directly relevant to the exam. In attribution or infrastructure investigations, analysts must know which relay type will appear in third-party logs or external complaints.
Since destination systems see the exit node as the apparent source of outbound traffic, the best answer is exit relay.

NEW QUESTION: 86
Which password cracking technique uses every possible combination of character sets?
A. Rainbow table attack
B. Rule-based attack
C. Brute force attack
D. Dictionary attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
Henry, a forensic investigator, is analysing a system suspected of being compromised by a stealthy rootkit. The rootkit appears to be sophisticated, hiding its files and processes to avoid detection. Henry decides to conduct a memory and registry analysis to uncover the hidden rootkit.
Which of the following tools would be the best choice for Henry's task?
A. RegRipper
B. Volatility
C. DumpIt
D. Autopsy
Answer: B (LEAVE A REPLY)
Volatility is specifically designed for analyzing memory dumps and can uncover hidden processes, injected code, and rootkit activity that evade disk-based tools, making it the most effective choice for detecting stealthy rootkits.

NEW QUESTION: 88
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
=+=+=+

NEW QUESTION: 89
In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?
A. Law of probability
B. Chain of custody
C. Policy of separation
D. Rules of evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 90
"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court" - this principle Is advocated by which of the following?
A. FBI Cyber Division
B. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence
C. Locard's exchange principle
D. Scientific Working Group on Imaging Technology (SWGIT)
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Data density of a disk drive is calculated by using _____.
A. Track density, areal density, and bit density.
B. Track space, bit area, and slack space.
C. Slack space, bit density, and slack density.
D. Track density, areal density, and slack density.
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 92
Following a data breach at a global financial institution, the company's incident response team has been working tirelessly to identify the breach's origin. The database administrator noticed that some tables within the company's SQL Server database were altered. She found that there were changes made in the order history, financials, and customer details.

The transaction log showed modifications with numerous queries which were quite uncommon. It seemed the attacker gained access via a remote connection, suggesting that the login details might have been compromised.
As a forensic investigator, what would be your next step to identify the source of the breach?
A. You would need to identify the source IP from where the connection was initiated.
B. You would need to assess the most recently accessed files.
C. You would need to evaluate the server logs for unusual login patterns.
D. You would need to perform a complete system scan.
Answer: A (LEAVE A REPLY)
Identifying the source IP of the remote connection directly helps trace where the unauthorized access originated, providing a key lead to the attacker's location or entry point.

NEW QUESTION: 93
Arnold, a forensic investigator, was tasked with analyzing a corporate network that was suspected of having unauthorized access points. He was particularly concerned about the possibility of rogue access points that might have been introduced by an attacker. To gain full visibility into the network and its components, Arnold employed a forensic tool that allowed him to analyze network traffic, monitor various access points for anomalies, and detect suspicious behaviors indicative of rogue devices. Arnold examined the log data provided by the tool, which gave him insights into the network ' s activities and helped him confirm whether any unauthorized devices were operating on the network. Which tool did Arnold employ in the above scenario?
A. Time Machine
B. Promqry
C. Freta
D. Security Onion
Answer: (SHOW ANSWER)
According to the CHFI v11 Network Forensics, Incident Detection, and SIEM objectives , Security Onion is a widely used open-source platform designed specifically for network security monitoring, intrusion detection, and forensic analysis . It integrates multiple tools such as Snort/Suricata (IDS/IPS) , Zeek (Bro) for network traffic analysis, Elastic Stack , and SIEM capabilities , providing deep visibility into network activities.
In the given scenario, Arnold required a solution capable of analyzing live and stored network traffic , monitoring access points , detecting anomalies , and identifying rogue or unauthorized devices . Security Onion fulfills all these requirements by collecting and correlating logs, monitoring network behavior, and generating alerts for suspicious patterns such as unknown MAC addresses, abnormal traffic flows, and unauthorized access point activity.

The other options do not align with the scenario. Time Machine is a macOS backup utility, not a network forensic tool. Promqry is used for querying Prometheus metrics and is not designed for forensic traffic analysis. Freta is a cloud-based memory forensics tool focused on Linux runtime analysis, not network-wide access point monitoring.
CHFI v11 emphasizes the use of SIEM and network monitoring platforms like Security Onion for detecting rogue devices, investigating unauthorized access, and performing evidence correlation using network logs and alerts. Therefore, the correct and CHFI-verified answer is Security Onion (Option D) .

NEW QUESTION: 94
During a malware investigation on a Linux server in Phoenix, investigators suspect that the malicious process is making frequent system calls to access protected resources. To analyze this behavior, they decide to trace and log the system calls made by the process. Which strace command provides a summary count of time, calls, and errors for each system call?
A. strace -p
B. strace -c ls > /dev/null
C. strace -P ls /var/empty
D. strace -o out.txt ./
Answer: B (LEAVE A REPLY)
The correct answer is B because the strace -c option produces a statistical summary showing, for each system call, the time spent, number of calls, and error counts. Linux tracing references describe this summary mode as the way to obtain aggregate syscall statistics instead of a full line-by-line trace. That matches the question exactly. The command shown in option B runs a sample command under strace with summary mode enabled and redirects normal command output away, leaving the syscall summary visible for analysis. Option A attaches to a process but does not request the summary table. Option C is malformed for the stated purpose, and option D writes a detailed trace to a file rather than generating the summarized count-time-error view.
CHFI v11 includes Linux forensics, malware behavior analysis, and system-level examination, so recognizing the correct tool usage for syscall analysis fits directly within scope. When investigators want a compact overview of syscall frequency, time consumption, and errors to identify suspicious behavior patterns, the correct strace usage is the command with the -c summary option.

NEW QUESTION: 95
Following a cyber incident in an organization where most employees use MacBooks, a forensic investigator named Alex is tasked with analyzing one of the affected Mac systems. Alex needs a comprehensive Mac forensic tool capable of analyzing system logs, artifacts, file systems, and user activities. What should be Alex
' s tool of choice?

A. Wireshark
B. Magnet AXIOM
C. Metasploit
D. IDA Pro
Answer: B (LEAVE A REPLY)
Option B. Magnet AXIOM is the best answer because CHFI v11 explicitly includes MAC Forensic Tools , Collecting and Analyzing macOS Artifacts , Analyzing macOS User Activities , Viewing Log Messages in Mac , and APFS file system analysis as important objectives for operating system forensics.
The question asks for a comprehensive Mac forensic tool that can handle system logs, artifacts, file systems, and user activity. Among the options, Magnet AXIOM is the one that best fits that broad forensic role.
Wireshark is a network traffic analysis tool, not a full Mac forensic suite. Metasploit is a penetration testing and exploitation framework, not an evidence-analysis platform. IDA Pro is used for reverse engineering binaries, which is far narrower than the full-system forensic requirement described here.
Because Alex needs a single tool capable of broad macOS evidence examination, the most suitable CHFI- aligned answer is Magnet AXIOM . It best matches the blueprint's focus on Mac artifact analysis, user activity reconstruction, and forensic tool use across operating systems.

NEW QUESTION: 96
Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads It to VirusTotal in order to confirm whether the file Is malicious, provide information about Its functionality, and provide Information that will allow to produce simple network signatures. What type of malware analysis was performed here?
A. Hybrid
B. Static
C. Volatile
D. Dynamic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
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. Last Write Time
B. User Activity Time

C. System Modification Time
D. Current System Time
Answer: A (LEAVE A REPLY)
Windows registry keys store a timestamp known as Last Write Time, indicating the last time the key (or its values) was modified. This is the standard forensic timestamp used to correlate registry changes with incident timelines.

NEW QUESTION: 98
During an insider-theft investigation at a software company in Austin, Texas, analysts need to verify whether a user changed Windows Explorer folder views (e.g., icons vs. details, sort order, window position) across multiple folders and drives. They have captured the user's NTUSER.DAT hive and want the primary registry location that organizes these view-preference artifacts system- wide so they can pivot into per-folder entries. Which registry location should be examined first for folder view-preference analysis?
A. HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
B. HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Shell\Bags
C. Shell key (under each Bags subkey)
D. HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Shell\BagMRU
Answer: A (LEAVE A REPLY)
BagMRU is the primary registry location used to organize folder view artifacts in a hierarchy of accessed folders. It allows investigators to pivot into the corresponding Bags entries, where Windows stores view preferences such as layout, sort order, icon mode, and window settings.

NEW QUESTION: 99
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 Task Scheduler
B. Windows AutoStart registry keys
C. Windows Process Explorer
D. Windows Operation system components
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
What does Locard's Exchange Principle state?
A. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
B. Digital evidence must have some characteristics to be disclosed in the court of law

C. Any information of probative value that is either stored or transmitted in a digital form
D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
During an ongoing ransomware incident at a hospital in Seattle, Washington, investigators must analyze streaming logs under severe time pressure, with decisions made as outputs are produced. Which category of forensic examination of logs aligns with this requirement?
A. An investigator can examine the log files several times
B. A real-time analysis is performed during an ongoing attack, and its results are also generated simultaneously
C. Investigators perform a postmortem analysis to detect and study the incidents that have already taken place in a network
D. An artifact is created that contains details about the exact cause of the incident and a set of actions necessary to ensure that something similar does not take place in the future
Answer: B (LEAVE A REPLY)
Real-time log analysis is performed while an attack is still in progress, allowing investigators to examine streaming log data and generate findings immediately as events occur. This supports rapid decision-making during an active ransomware incident.

NEW QUESTION: 102
Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?
A. Database tables
B. Rainbow tables
C. Hash tables
D. Master file tables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
John, a system administrator at a growing e-commerce company, is tasked with configuring a RAID 5 array to support the company's increasing data storage needs. He needs to set up the array using three hard drives, ensuring that the data is both protected and accessible in the event of a drive failure. While configuring the array, John needs to understand how the RAID 5 system handles data redundancy and how parity data is distributed across the drives. How is the parity data stored and distributed in RAID 5?
A. Parity data is stored on one drive, with no redundancy.
B. Parity data is distributed across all drives in the array.
C. Parity data is mirrored across two drives.
D. Parity data is stored on a dedicated parity drive.

Answer: (SHOW ANSWER)

According to the CHFI v11 Digital Evidence and Storage Fundamentals, RAID (Redundant Array of Independent Disks) configurations are critical for investigators to understand because they directly impact data availability, fault tolerance, and evidence reconstruction during forensic analysis. RAID 5 is one of the most commonly deployed RAID levels in enterprise environments due to its balance between performance, storage efficiency, and redundancy.

In a RAID 5 configuration, data and parity information are striped across all disks in the array.

This means that parity blocks are not stored on a single dedicated drive; instead, parity is rotated among all participating drives. This design eliminates the bottleneck associated with a single parity disk and improves read performance while still providing fault tolerance.

If one drive fails, RAID 5 uses the distributed parity information along with the remaining data blocks to reconstruct the missing data on-the-fly, ensuring continued access to information. From a forensic perspective, this distributed parity mechanism is significant because investigators must correctly identify the RAID structure to rebuild the array and recover digital evidence accurately.

NEW QUESTION: 104

Allison, a CHFI investigator, was brought into a case by a law firm, handling a breach of client data. Allison needs to investigate the firm ' s digital assets for evidence of the breach and the potential culprit. Before starting her investigation, Allison seeks consent from the firm ' s partners. However, they are reluctant to grant consent due to concerns about client confidentiality. In line with the principles of seeking consent in a CHFI investigation, what should Allison ' s approach be?

A. Proceed with the investigation covertly to identify the culprit quickly

B. Use her authority as a CHFI investigator to access the required data without consent

C. Withdraw from the case due to the lack of consent

D. Respect the firm ' s concerns and seek other means of gathering evidence without breaching client confidentiality

Answer: D (LEAVE A REPLY)

Option D is the best answer because CHFI v11 explicitly includes Seeking Consent , Best Practices for Handling Digital Evidence , Legal Issues, Privacy Issues and Legal Compliance , and Managing Clients or Employers during Investigations .

When consent is not granted, the investigator cannot simply access sensitive client data on their own authority. At the same time, immediately withdrawing may not be the only appropriate response if there are lawful and ethical alternative ways to obtain relevant evidence without violating confidentiality. The CHFI- aligned approach is to respect the client's concerns , remain within legal and ethical boundaries, and explore other permissible evidence-gathering options, such as narrower collection scopes, anonymized review procedures, or additional legal authorization where appropriate.

Options A and B clearly violate consent and confidentiality principles. Option C is too absolute and does not reflect the possibility of lawful alternative approaches. Therefore, the strongest answer under CHFI's consent and legal-compliance principles is to respect the firm's concerns and seek other means of gathering evidence without breaching client confidentiality .

NEW QUESTION: 105
Sophia, a forensic investigator, has been working on a significant corporate data theft case. The suspect, an IT employee, allegedly downloaded hundreds of confidential files onto his laptop before resigning abruptly.
Sophia obtained a search and seizure warrant, and during the execution, she found the suspect ' s laptop, a desktop computer, and several storage devices. To ensure she maintains the chain of custody and abides by the ACPO principles of digital evidence, what should be her next step?
A. She should ask the suspect for the passwords to the devices to expedite the investigation.
B. She should immediately begin analyzing the digital devices on-site.
C. She should only seize the personal laptop as per the information on the warrant.
D. She should seize all the devices and send them to a forensic lab for analysis.
Answer: D (LEAVE A REPLY)
Option D is the best answer because CHFI v11 places strong emphasis on search and seizure , preserving evidence , chain of custody , and best practices for handling digital evidence . Once lawful authority exists and multiple potentially relevant devices are found, the proper next step is to seize the devices in a controlled manner , document them carefully, and move them to a forensic environment for structured analysis.
Analyzing devices on-site can increase the risk of contamination, incomplete documentation, or unintended alteration. Asking for passwords may be considered in some cases, but it is not the primary next step being tested here. Seizing only the laptop would be too narrow if the warrant and circumstances support collection of other relevant storage devices tied to the offense.
This approach aligns with CHFI's legal and procedural objectives because it preserves evidence integrity, supports a proper chain of custody, and ensures later analysis occurs in a controlled forensic lab environment.
Therefore, the correct action is to seize all relevant devices and send them to the forensic lab for examination .

NEW QUESTION: 106
Sophia, a forensic investigator, is analyzing a file suspected to be an image. She is examining the file's hexadecimal signature to identify its format. Upon inspection, she notices that the first three bytes of the file are 47 49 46 in hexadecimal. Based on this information, which of the following image formats is the file most likely to be?

A. PNG
B. BMP
C. GIF
D. JPEG
Answer: C (LEAVE A REPLY)
According to the CHFI v11 Computer Forensics Fundamentals and File Analysis modules, identifying file types using file signatures (magic numbers) is a core forensic technique. File extensions can be easily manipulated by attackers as an anti-forensics tactic, so investigators rely on hexadecimal headers to determine the true file format.
The hexadecimal sequence 47 49 46 corresponds to the ASCII characters "GIF". This signature appears at the beginning of all Graphics Interchange Format (GIF) files and is typically followed by version identifiers such as GIF87a or GIF89a. CHFI v11 explicitly lists GIF file headers as a common example when teaching file signature verification using hex editors.
For comparison:
PNG files start with the signature 89 50 4E 47
BMP files start with 42 4D (ASCII "BM")
JPEG files typically start with FF D8 FF
Because the investigator observes 47 49 46 at the beginning of the file, this conclusively identifies the file as a GIF image, regardless of its filename or extension.
CHFI v11 emphasizes that hexadecimal signature analysis is essential when investigating disguised files, malware hidden as images, or data exfiltration attempts using file extension mismatch techniques.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 107
A cybersecurity analyst is tasked with investigating a series of network anomalies. They employ various event correlation approaches, including graph-based analysis to map system dependencies and neural network-based anomaly detection. Through rule-based correlation and vulnerability-based mapping, they pinpoint potential threats and prioritize response actions effectively.
Which event correlation approach involves constructing a graph with system components as nodes and their dependencies as edges?

A. Rule-Based Approach
B. Codebook-Based Approach
C. Neural Network-Based Approach
D. Graph-Based Approach
Answer: D (LEAVE A REPLY)
This question aligns with CHFI v11 objectives under Procedures and Methodology , specifically event correlation and analysis techniques used to investigate complex incidents. Event correlation is essential for transforming large volumes of logs and alerts into meaningful incident narratives. CHFI v11 describes multiple correlation approaches, each suited to different investigative needs.
The graph-based approach models systems, applications, users, and network components as nodes , while relationships such as dependencies, communications, or trust relationships are represented as edges . By constructing such graphs, investigators can visualize how events propagate across interconnected systems, identify attack paths, and determine how a compromise in one component impacts others. This approach is particularly effective in analyzing lateral movement, dependency-based failures, and multi-stage attacks in enterprise environments.
Rule-based approaches rely on predefined conditions, codebook-based approaches match patterns against known attack templates, and neural network-based approaches focus on anomaly detection using machine learning. While these are valuable, only the graph-based approach explicitly represents system dependencies and relationships in a node-edge structure. Therefore, consistent with CHFI v11 event correlation methodologies, the correct answer is Graph-Based Approach .

NEW QUESTION: 108
What is the following command trying to accomplish?
C:\> nmap -sU -p445 192.168.0.0/24
A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that UDP port 445 is closed for the 192.168.0.0 network
C. Verify that UDP port 445 is open for the 192.168.0.0 network
D. Verify that TCP port 445 is open for the 192.168.0.0 network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
During a routine digital investigation, forensic analysts suspect that sensitive information may be hidden within seemingly innocuous files. Despite extensive scanning and analysis, they are unable to detect any abnormalities using conventional surveillance techniques. What technique might attackers use to hide sensitive information within seemingly normal files, making it difficult for forensic investigators to detect?
A. Trial obfuscation
B. Hiding data in file system structures

C. File extension mismatch
D. Steganography
Answer: D (LEAVE A REPLY)
According to the CHFI v11 Anti-Forensics Techniques domain, steganography is a sophisticated method used by attackers to conceal sensitive or malicious information within seemingly normal files such as images, audio files, video files, or documents. Unlike encryption, which makes data unreadable but visibly suspicious, steganography hides the existence of the data itself , making detection significantly more challenging during forensic analysis.
In steganography, data is embedded into unused or less noticeable parts of a file-such as the least significant bits (LSB) of image pixels or audio samples-without noticeably altering the file's appearance or functionality. As a result, standard antivirus tools, intrusion detection systems, and basic forensic scans may not flag these files as suspicious. CHFI v11 highlights steganography as a common anti-forensic tactic used for covert data exfiltration, command-and-control communication, and storage of illegal or confidential information.
The other options are less effective in this scenario. File extension mismatch can often be detected through file signature analysis. Hiding data in file system structures leaves traces in metadata or unallocated space.
Trial obfuscation is not a formally recognized anti-forensics technique in CHFI v11.
CHFI v11 emphasizes that detecting steganography often requires specialized steganalysis tools , statistical analysis, and anomaly detection techniques beyond conventional scanning.
Therefore, the technique used to hide sensitive information within normal-looking files-fully aligned with CHFI v11-is Steganography , making Option D the correct answer.

NEW QUESTION: 110
Megan, a CHFI investigator, is examining a complicated breach at a cutting-edge IoT technology company that designs systems for smart homes. The company ' s IoT devices have experienced a massive scale breach, with numerous devices sending unauthorized data to an external server. The company uses a public cloudbased model to manage IoT devices. The unique problem Megan faces is that the breach did not occur via the traditional IoT vulnerabilities as the devices have been designed with state-of-the-art security features and yet the attacker has managed to bypass all security measures.
Which of the following is the most plausible method the attacker could have used to compromise the IoT devices?
A. Used a botnet to flood the network with traffic
B. Exploited weak encryption protocols in the company ' s IoT devices
C. Hacked into the TOR Bridge Node used by the company
D. Manipulated the Cloud API to gain unauthorized access
Answer: (SHOW ANSWER)

Option D is the most plausible answer because the scenario specifically states that the organization uses a public cloud-based model to manage IoT devices and that the compromise did not occur through traditional IoT weaknesses. CHFI v11 explicitly includes Cloud Computing Threats and Attacks , Cloud Forensics , Google Cloud Forensics , and IoT Forensics as major study areas, showing that investigators must understand how cloud environments can become the control point for attacks against connected devices.
If an attacker successfully manipulates the cloud API , they may be able to issue unauthorized commands, alter configurations, retrieve device telemetry, or direct IoT devices to communicate with an attacker- controlled server. That fits the fact pattern much better than the other choices. A botnet flood mainly causes denial of service, not controlled unauthorized outbound communications. Weak encryption protocols are ruled out by the statement that the devices were built with strong security features. TOR Bridge Node involvement is unrelated to the company's IoT management model. Therefore, under CHFI's cloud and IoT objectives, a compromised cloud API is the strongest answer.

NEW QUESTION: 111
Jane, who holds the title of Computer Hacking Forensic Investigator, is knee-deep in a case of a system security breach in a vast global corporation. The breach may have started its trouble- making journey in another country. Jane is focusing on preserving and investigating digital evidence. Keeping in mind the fragile and volatile nature of digital evidence, what is the first step Jane should take in the process of investigation?
A. Begin documenting all the traces and records of the attack in the system
B. Gather system data before an intruder can alter it
C. Notify all jurisdictions involved about the breach
D. Contact local law enforcement in the country where the attack originated
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
To check for POP3 traffic using Ethereal, what port should an investigator search by?
A. 143
B. 110
C. 125
D. 25
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
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. Compliance with the Fourth Amendment of the U.S. Constitution
C. None of these
D. Compliance with the Second Amendment of the U.S. Constitution
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
After a cybercrime investigation involving a compromised Windows system, an investigator is tasked with recovering private browsing artifacts. The investigator decides to retrieve data from the pagefile.
sys and other live memory captures to identify traces of activity from private browsing modes.
Which tool should the investigator use to analyze the live system and recover these private browsing artifacts?
A. PsLoggedOn
B. Exeinfo
C. FTK Imager
D. zsteg
Answer: C (LEAVE A REPLY)
This question aligns with CHFI v11 objectives underOperating System ForensicsandVolatile and Non- Volatile Data Analysis, particularly the recovery of artifacts from live memory and system files such as pagefile.sys. Private browsing modes (e.g., InPrivate, Incognito) are designed to minimize persistent artifacts on disk; however, CHFI v11 emphasizes thatmemory, page files, and swap files often retain remnants of browsing activity, including URLs, session data, cached content, and credentials.
FTK Imageris a forensically sound tool widely used forlive data acquisition, memory capture, and analysis of volatile artifacts. It allows investigators to acquire RAM, pagefile.sys, hiberfil.sys, and other critical system files without altering evidence integrity. CHFI v11 specifically highlights FTK Imager as a preferred tool for collecting and examining live system data and recovering artifacts that are not available through traditional disk-only analysis.
PsLoggedOn is used to identify logged-in users, Exeinfo analyzes executable file formats, and zsteg is a steganography detection tool. None of these are suitable for live memory or pagefile analysis. Therefore, consistent with CHFI v11 forensic best practices,FTK Imageris the correct tool to recover private browsing artifacts from live Windows systems.

NEW QUESTION: 115
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. What will happen to the data?

A. The data will become corrupted, making it unrecoverable
B. The data will be moved to new clusters in unallocated space
C. The data will be overwritten with zeroes
D. The data will remain in its original clusters until it is overwritten
Answer: D (LEAVE A REPLY)

NEW QUESTION: 116
What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?
A. Restore point interval
B. System CheckPoints required for restoring
C. Automatically created restore points
D. Restore point functions
Answer: (SHOW ANSWER)

NEW QUESTION: 117
During an investigation at a hosting provider in Denver, Colorado, analysts must bulk-scan web server logs for path/directory traversal attempts that may appear in encoded as well as literal form. To reliably match these dot-dot-slash patterns across encodings in one pass, which expression should they apply?
A. %5C
B. %2e%2e%2f
C. ((\.|%2E)(\.|%2E)(\/|%2F|\\|%5C))
D. ((\.\.\\)(\.\.\/))
Answer: C (LEAVE A REPLY)
This expression matches directory traversal patterns by detecting literal or URL-encoded dot characters followed by a slash or backslash in literal or encoded form. It allows investigators to identify dot-dot-slash traversal attempts such as ../, .., %2e%2e%2f, and related encoded variants in web server logs.

NEW QUESTION: 118
In a corporate espionage investigation at a pharmaceutical research facility in Raleigh, North Carolina, examiners obtain multiple Outlook mailbox archives stored on a seized external drive.
Initial attempts to open the files in forensic viewers fail due to structural inconsistencies that prevent proper mounting or parsing. Before any content extraction or verification can proceed, the team uses EaseUS Email Recovery Wizard to address these file issues.
From the listed capabilities of this tool, which function directly enables the examiners to resolve the structural problems and make the archives accessible for analysis?
A. Recover lost or deleted emails from Microsoft Outlook
B. Repair corrupted PST files

C. Preview deleted or lost emails before recovering them
D. Recover deleted folders, contacts, attachments, calendars, and meeting requests
Answer: B (LEAVE A REPLY)
Repairing corrupted PST files directly addresses structural inconsistencies in Outlook mailbox archives. This makes the PST files accessible for mounting, parsing, and later forensic content extraction or verification.

NEW QUESTION: 119
During Dynamic Malware Analysis in a sandbox at a healthcare provider in Nashville, the sample shows no immediate network activity. After a controlled restart, the executable launches automatically at logon without user interaction. To capture the system changes responsible for this behavior across a reboot cycle, what area of system activity should investigators focus on monitoring?
A. Monitoring processes
B. Monitoring registry artifacts
C. Monitoring services and startup programs
D. Monitoring event logs
Answer: (SHOW ANSWER)
The correct answer is C because the behavior described is reboot-persistent auto-start execution, which most directly points to services and startup programs. CHFI v11 explicitly includes malware persistence mechanisms and system behavior analysis through monitoring services, startup programs, registry artifacts, and related operating system changes. When malware launches automatically after restart and logon, investigators should focus first on the execution mechanisms that survive reboot and trigger program start without manual action. Services and startup entries are classic persistence locations for this kind of behavior.
Registry artifacts can also be involved, especially through Run keys, but the question asks what area of system activity should be monitored to capture the reboot-linked execution behavior itself. That makes services and startup programs the best fit because they directly govern automatic launch at system boot or user logon. In dynamic malware analysis, tracing these persistence points across a restart cycle helps investigators understand how the malware reappears, whether it is service-based, startup-folder based, or tied to another auto-launch mechanism.

NEW QUESTION: 120
Following a post-breach investigation at a manufacturing company in Denver, Colorado, forensic analysts begin capturing and examining live network traffic between internal and external hosts.
The objective is to uncover communication patterns, detect unauthorized access, and determine the attacker's methods. What activity falls outside the primary objectives of network traffic investigation?

A. To detect and examine an ongoing attack by monitoring network traffic communication patterns
B. To identify hosts or networks involved in a network security incident
C. To trace information or packets related to a security intrusion and collect them as evidence
D. To erase the traces of intrusion by clearing captured packets from network devices
Answer: D (LEAVE A REPLY)
Network traffic investigation focuses on monitoring communication patterns, identifying involved hosts, tracing packets related to intrusions, and collecting evidence. Erasing intrusion traces or clearing captured packets would destroy evidence and is not a forensic investigation objective.

NEW QUESTION: 121
Theodore, a forensic expert, was tasked with investigating a cybercrime involving a Windows operating system running on NTFS. In the course of the investigation, he accessed and analyzed several metadata files stored in the root directory of the file system. These metadata files maintain records for every file stored on the system, including information such as file names, sizes, timestamps, and location on disk. While examining these files, Theodore was able to discover crucial data that helped track malicious events linked to the cybercrime.
Which of the following system files did Theodore access to retrieve these records?
A. $volume
B. $logfile
C. $mftmirr
D. $mft
Answer: D (LEAVE A REPLY)
This question directly maps to CHFI v11 objectives under Operating System Forensics, specifically NTFS file system analysis and metadata examination. In NTFS, the Master File Table (MFT) is the core metadata file that contains a record for every file and directory on the volume.
CHFI v11 emphasizes that the $MFT is one of the most critical artifacts in Windows forensics because it stores essential attributes such as file names, file sizes, creation/modification/access timestamps, permissions, and the physical location of file data on disk.
Each file on an NTFS volume has at least one corresponding MFT entry, making $MFT invaluable for reconstructing user activity, detecting deleted files, and correlating timelines during cybercrime investigations. Investigators often analyze the $MFT to uncover evidence of malicious file creation, modification, execution, or deletion--even when files have been removed from the file system view.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122
A multinational corporation utilizes Google Cloud Storage (GCS) to store critical business data including financial records and customer information. Recently, the corporation discovered unauthorized access to sensitive documents within their GCS environment, raising concerns about potential data breaches. Which type of information can be found in access logs and metadata within Google Cloud Storage?
A. Timestamps of file access and modification.
B. Employee login credentials.
C. Encryption keys for stored files.
D. Details of network infrastructure configuration.
Answer: (SHOW ANSWER)
Access logs and metadata in Google Cloud Storage record events such as when objects are accessed, created, or modified, providing timestamps and activity details essential for auditing and forensic analysis.

NEW QUESTION: 123
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?
A. Supervisors
B. Administrative assistant in charge of writing policies
C. Employees themselves
D. IT personnel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
Alex, a system administrator, is tasked with converting an existing EXT2 file system to an EXT3 file system on a Linux machine. The EXT2 file system is currently in use, and Alex

needs to enable journaling to convert it to EXT3. Which of the following commands should Alex use to achieve this conversion?

A. C: > ECHO text_message > myfile.txt:stream1

B. C: > MORE < myfile.txt:stream1

C. dd if=mbr.backup of=/dev/xxx bs=512 count=1

D. # /sbin/tune2fs -j

Answer: D (LEAVE A REPLY)

According to the CHFI v11 syllabus under Operating System Forensics and Linux File System Analysis , understanding Linux file systems and their conversion methods is essential for both system administration and forensic investigations. The EXT2 file system is a non-journaling file system, whereas EXT3 extends EXT2 by adding journaling capabilities , which significantly improve system recovery and forensic traceability after crashes or improper shutdowns.

The correct command to convert an existing EXT2 file system into EXT3 is:

/sbin/tune2fs -j

This command enables journaling on the EXT2 file system without reformatting or destroying existing data , making it a safe and efficient conversion method. CHFI v11 explicitly highlights this command as the standard approach for adding a journal to an EXT2 partition. Once journaling is enabled, the file system is recognized as EXT3.

The other options are incorrect and unrelated to Linux file system conversion. Options A and B involve NTFS Alternate Data Streams , which are Windows-specific. Option C is a disk-level command used for copying raw sectors, such as backing up or restoring an MBR, and does not modify file system journaling features.

The CHFI Exam Blueprint v4 emphasizes knowledge of Linux file systems (EXT2, EXT3, EXT4) and administrative commands like tune2fs , as they are frequently referenced in forensic analysis and recovery scenarios, making Option D the correct and exam-aligned answer

NEW QUESTION: 125

You are contracted to work as a computer forensics investigator for a regional bank that has four

30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?

A. Create a sparse data copy of a folder or file

B. Make a bit-stream disk-to-image file

C. Create a compressed copy of the file with DoubleSpace

D. Make a bit-stream disk-to-disk file

Answer: A (LEAVE A REPLY)

NEW QUESTION: 126

A company has been receiving unsolicited commercial emails from an unknown source promoting a third-party product. The email contains false header information and is not identified as an advertisement. The emails are being sent to addresses that are generated through a dictionary attack. As a Computer Hacking Forensics Investigator, which violations of the CAN-SPAM Act are present in this scenario?

A. Violating the prohibition against dictionary attacks and not identifying the commercial email as an ad only

B. Using false or misleading header information and not identifying the commercial email as an ad only

C. Using false or misleading header information, not identifying the commercial email as an ad. and violating the prohibition against dictionary attacks

D. Using false or misleading header information and violating the prohibition against dictionary attacks only

Answer: C (LEAVE A REPLY)

NEW QUESTION: 127

Sarah, a forensic investigator, is conducting an investigation on a macOS device that is suspected to have been compromised. She is tasked with gathering evidence of unauthorized access to the system. As part of her investigation, she needs to locate information related to when and who accessed the system. In addition to reviewing general system logs. Sarah knows she must focus on certain types of system files that might provide detailed data on unauthorized activities. Which area of the macOS file system would provide the most relevant information regarding logon attempts and other authentication events?

A. The User Account data

B. The LaunchDaemons directory

C. The Home folder

D. The Safari history

Answer: A (LEAVE A REPLY)

Option A. The User Account data is the most appropriate answer because the question is specifically about identifying when and who accessed the system , which points to authentication, account usage, and user activity evidence. CHFI v11 includes MAC Forensics Data, Log Files, and Directories , collecting and analyzing macOS artifacts , and analyzing macOS user activities as core examination areas.

In a macOS forensic investigation, artifacts associated with user accounts are the most relevant place to correlate logon activity, authentication-related behavior, and traces of user access. These can help examiners establish which account was involved, what user context was active, and when suspicious access may have occurred. This is far more aligned with the question than other directories centered on startup services, personal files, or browser activity.

The LaunchDaemons directory may reveal persistence or background services, but it is not the primary source for identifying user logon attempts. The Home folder contains user files and activity artifacts, while Safari history is limited to web browsing evidence. Since the objective is to determine access and authentication-related activity, User Account data is the strongest CHFI-aligned answer.

NEW QUESTION: 128
Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?
A. Replay attack
B. Man-in-the-middle (MITM) attack
C. Rainbow attack
D. Distributed network attack
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Following a wireless security audit at a retail corporation in New York City, New York, the forensics team identifies an authorized access point broadcasting its factory SSID and accepting connections with unchanged vendor credentials, creating an unintended entry point for unauthorized users despite being part of the inventory. This oversight stems from post-upgrade settings not aligned with organizational policies, exposing the network to potential exploitation.
What indicator should the team flag as evidence of misconfiguration in this access point?
A. The configuration of the access point is not on par with the current WLAN security policy
B. It uses the default SSID
C. The access point is set to default configurations, such as using default usernames and passwords
D. The access point has weak security settings
Answer: (SHOW ANSWER)
An access point left with default configurations, especially unchanged vendor usernames and passwords, is a clear misconfiguration because it allows unauthorized users to exploit known factory settings. This creates an avoidable entry point even when the device itself is authorized and inventoried.

NEW QUESTION: 130
A forensic investigator has been assigned to extract data from several IoT devices involved in a complex investigation. The devices include drones, smart TVs, and wearables that are crucial to the case. These devices may contain valuable evidence, including video footage, sensor data, and user interactions. The investigator needs a tool that can handle a variety of IoT devices and supports both physical and logical extraction methods to ensure that no

evidence is missed. Given the complexity of IoT forensics, which of the following tools should the investigator use to collect evidence from these devices effectively?

A. Freta

B. Promqry

C. Gephi

D. MD-NEXT

Answer: D (LEAVE A REPLY)

Option D. MD-NEXT is the best answer because the question is specifically about a forensic tool suitable for collecting evidence from multiple IoT device types while supporting broad extraction needs. CHFI v11 includes IoT forensics , evidence extraction from embedded and smart devices , and understanding the methods used to acquire and analyze data from nontraditional digital systems. In that context, the correct choice is the tool that is actually designed for device-level forensic extraction rather than one intended for unrelated analytical or cloud-focused purposes.

The other options are less appropriate. Freta is associated with cloud-scale memory analysis concepts rather than hands-on IoT extraction. Gephi is a graph visualization and network-analysis tool, not a forensic acquisition platform. Promqry is not the established choice for this type of physical and logical evidence extraction scenario. MD-NEXT , by contrast, fits the role of a specialized forensic solution for handling diverse devices and collecting evidence in a structured manner.

Because the scenario emphasizes variety of IoT devices , forensic extraction , and the need not to miss evidence, the most suitable CHFI-aligned answer is MD-NEXT .

NEW QUESTION: 131

After a credential theft at a logistics company in Memphis, Tennessee, investigators review packet captures and event logs to understand how the adversary moved from the VPN gateway to an internal database through several intermediate hosts. Their immediate goal is to reconstruct the sequence of network hops the attacker used across segments. Which outcome of network forensics best fits this objective?

A. Intrusion techniques an attacker used

B. Path of intrusion

C. Source of security incidents

D. Traces and evidence

Answer: B (LEAVE A REPLY)

The path of intrusion identifies the route an attacker followed through the network, including intermediate hosts, hops, and segments used to move from the initial access point to the target system. This directly supports reconstruction of attacker movement from the VPN gateway to the internal database.

NEW QUESTION: 132

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

NEW QUESTION: 133
Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?
A. Event ID 4657
B. Event ID 4688
C. Event ID 7040
D. Event ID 4624
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
Greg, a seasoned CHFI professional, has been contracted to investigate a case of intellectual property theft at a major software company. While working on the case, he discovered that the company ' s email server might hold crucial evidence. However, the server is shared with a different company, and accessing it might risk violating that company ' s privacy rights. To respect the rules and regulations about the search and seizure of evidence, what should Greg ' s initial approach be in this scenario?
A. Consult with legal experts and the company ' s management to explore the best way forward
B. Avoid the email server and focus on other potential sources of evidence
C. Ignore potential privacy violations and seize the server
D. Immediately obtain a warrant to search and seize the server
Answer: A (LEAVE A REPLY)
Option A is the best answer because CHFI v11 explicitly includes Rules of Evidence , Best Practices for Handling Digital Evidence , Seeking Consent , Obtaining a Warrant for

Search and Seizure , Legal Issues, Privacy Issues and Legal Compliance , and the Role of Local/International Agencies during Cybercrime Investigation . When a server is shared with another company , privacy and ownership concerns become especially important, and the initial step should be to consult the appropriate legal and organizational stakeholders before taking action.
Immediately seizing the server or ignoring privacy implications could violate legal boundaries and compromise admissibility. Avoiding the server entirely may also be inappropriate if it contains critical evidence. Likewise, jumping straight to a warrant may not be the most suitable first move until counsel and management clarify ownership, scope, privacy exposure, and the least intrusive legally defensible path.
Therefore, the strongest CHFI-aligned initial approach is to consult legal experts and company management to determine the correct lawful path forward before attempting access or seizure. That protects privacy rights, preserves admissibility, and aligns the investigation with proper search-and-seizure procedure.

NEW QUESTION: 135
After a significant malware attack on a corporation, Bob, a forensic analyst, was asked to investigate. The malware had made numerous modifications in files and folders across the system to cover its tracks. Bob decides to monitor these changes closely to understand the malware's operation. What tool can Bob use to monitor and log all the changes happening in the system's files and folders?
A. IDA Pro
B. EnCase
C. Sysmon
D. FTK Imager
Answer: C (LEAVE A REPLY)
Sysmon logs detailed system activity, including file creation and modification events, enabling investigators to track changes made by malware across files and folders.

NEW QUESTION: 136
An online banking system fell victim to a significant security breach. The attacker managed to access confidential customer data and the bank's internal communication. During the investigation, the forensic team noticed a pattern of unusual queries containing "& # x 0 0;" in the system logs. This led them to believe that an exploitation technique may have been used to bypass security filters and firewalls. Based on this information, which type of attack was most likely used?
A. Directory Traversal attack.
B. Command Injection attack.
C. XML External Entity (XXE) attack.
D. SQL Injection attack.
Answer: C (LEAVE A REPLY)

The sequence represents a null-byte style encoding often associated with XML parsing and XXE exploitation attempts. XXE attacks abuse XML processors to access sensitive files, internal resources, or bypass input filters through crafted XML entities.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 137
After reviewing a suspicious Excel spreadsheet circulated internally via email at a financial services firm in Philadelphia, Pennsylvania, examiners observe recent modifications, but the identity of the user responsible for the latest save is disputed. Which embedded metadata property should be examined to determine who last saved the document?
A. Author
B. Revision Number
C. Last Saved By
D. Total Editing Time
Answer: (SHOW ANSWER)
The correct answer is C because the metadata field specifically intended to record the identity associated with the most recent save operation is Last Saved By. Microsoft's support documentation for inspecting Office file properties lists standard document properties such as Author and other descriptive fields, and in forensic practice Office metadata commonly distinguishes the original creator from the user who most recently saved the file. The Author field may identify the original creator or default profile owner, but that is not necessarily the person responsible for the latest modification. Revision Number tracks version increments, and Total Editing Time reflects duration rather than identity. CHFI v11 includes analysis of Word, PowerPoint, and Excel files and their metadata, so candidates are expected to know which property best answers a specific attribution question. When the dispute concerns who performed the most recent save rather than who created the spreadsheet, the most relevant embedded metadata property is Last Saved By. That field directly supports attribution of the latest document-save action.
(support.microsoft.com)

NEW QUESTION: 138
Which of the following statements is true regarding SMTP Server?

A. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server
B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server
C. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server
D. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server
Answer: (SHOW ANSWER)

NEW QUESTION: 139
In an echo data hiding technique, the secret message is embedded into a _____as an echo.
A. Pseudo-random signal
B. Phase spectrum of a digital signal
C. Pseudo- spectrum signal
D. Cover audio signal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
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. Blackberry desktop redirector
B. Blackberry Enterprise server
C. RIM Messaging center
D. Microsoft Exchange server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 141
During a malware analysis investigation, a suspicious Microsoft Office document is identified as a potential threat. The document contains embedded macros and triggers unusual behavior when opened. In digital forensics, what is the primary purpose of analyzing suspicious Microsoft Office documents?
A. To determine the author's identity
B. To optimize the formatting and layout of the document
C. To identify potential malware or malicious code embedded within the document
D. To improve the performance of Microsoft Office applications
Answer: (SHOW ANSWER)
According to the CHFI v11 objectives underMalware ForensicsandStatic and Dynamic Malware Analysis, Microsoft Office documents are one of the most common delivery

mechanisms for malware, especially throughmalicious macros, embedded scripts, and exploit-laden objects. Attackers frequently weaponize Word, Excel, and PowerPoint files to execute malicious code when a user opens the document or enables macros.
Theprimary forensic purposeof analyzing suspicious Microsoft Office documents is toidentify embedded malware or malicious codeand understand how it executes. Investigators examine macro code (VBA), embedded objects, OLE streams, and document metadata to detect indicators such as obfuscated scripts, PowerShell execution commands, shellcode loaders, or downloader functionality. CHFI v11 emphasizes that this analysis helps determine theinfection chain, execution triggers, and potential impact on the compromised system.
Options A, B, and D are not valid forensic goals in this context. Identifying the document author (Option A) may be supplementary but does not address the core threat. Formatting optimization (Option B) and performance improvement (Option D) are unrelated to forensic or security investigations.
The CHFI Exam Blueprint v4 explicitly includesanalyzing suspicious Word, Excel, and PDF documentsas part of malware investigations, highlighting the need to detect hidden malicious logic and prevent further compromise. Therefore, identifying embedded malware or malicious code is the correct and exam-aligned objective

NEW QUESTION: 142
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.
A. Windows 98
B. Linux
C. Windows 8.1
D. Windows XP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 143
Camila, a forensic investigator, is working on a Linux machine that has been suspected of running malicious software. She wants to analyze the interactions between the running processes and the kernel, as these interactions could provide important clues about the behavior of the malware. To track the system calls made by the processes, she decides to use a tool that can intercept and record these system calls in real-time. Which tool should Camila use to monitor the system calls generated by processes on the system?
A. strace
B. Wireshark
C. tcpdump
D. Process Explorer
Answer: A (LEAVE A REPLY)

Option A. strace is the best answer because the question asks for a tool that can intercept and record system calls in real time on a Linux system. That is exactly what strace is designed to do. CHFI v11 includes Linux forensics , Linux memory forensics , and also references system behavior analysis and system calls monitoring when examining malware behavior on systems.
Monitoring system calls is important because it shows how a suspicious process interacts with the operating system kernel, including file access, network activity, process creation, permissions use, and other low-level behavior. That makes strace especially useful when investigating malware on Linux.
The other options do not fit the requirement. Wireshark and tcpdump are network traffic analysis tools, so they observe packets rather than kernel system calls. Process Explorer is associated with Windows process investigation, not Linux syscall tracing. Since the question is specifically about real-time observation of process-to-kernel interactions on Linux, strace is the most accurate and CHFI-aligned tool choice.

NEW QUESTION: 144
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. EF 00 EF 00 EF 00
B. FF 00 FF 00 FF 00
C. FF D8 FF E0 00 10
D. FF FF FF FF FF FF
Answer: (SHOW ANSWER)

NEW QUESTION: 145
During an investigation, an examiner opens an Excel file with a .xism extension, indicating that the document is capable of containing malicious code. Upon closer inspection, the investigator must determine if the file poses a threat. What should the investigator focus on to identify potential risks?
A. Inspect the file to see if any external resources, such as links or network calls, are embedded in the document.
B. Check if any streams in the file are labeled as containing macros.
C. Check the file size to determine if it is unusually large or small, as this might indicate hidden data.
D. Inspect the metadata of the file for details about its author, creation date, and last modification.
Answer: B (LEAVE A REPLY)
The .xlsm format supports macros, which can contain malicious code. Checking for macro-containing streams directly identifies whether executable code is embedded and potentially harmful.

NEW QUESTION: 146
During a forensic investigation into a suspected cyberattack, the investigator checks network logs that were collected during the period of the incident. The investigator's objective is to examine these logs to determine the exact sequence of events that took place, identify the source of the attack, and understand the nature of the incident. This analysis helps in uncovering what occurred, how it happened, and who was responsible for it.
Which of the following techniques is the investigator using in this case?
A. The investigator performs eavesdropping on communications to intercept sensitive information.
B. The investigator performs a postmortem analysis of system records to evaluate previous security breaches.
C. The investigator conducts a real-time analysis of network traffic logs to detect the nature of the incident.
D. The investigator carries out IP address spoofing to identify the source of the attack.
Answer: (SHOW ANSWER)
This scenario aligns closely with CHFI v11 objectives underProcedures and Methodology, specifically postmortem analysis and log-based forensic investigation. Postmortem analysis refers to the examination of collected system, application, and network logsafter an incident has occurred, with the goal of reconstructing events and determining the root cause of a security breach.
In this case, the investigator is reviewinghistorical network logs collected during the incident window, not monitoring live traffic. CHFI v11 emphasizes that postmortem analysis is essential for answering the core forensic questions:what happened, how it happened, when it happened, and who was responsible. By correlating timestamps, IP addresses, protocols, and event sequences across logs, investigators can identify attack vectors, trace the origin of the attack, and understand attacker behavior.
Option C is incorrect because real-time analysis applies to live monitoring during an active incident. Option A describes an illegal activity unrelated to forensics, and option D refers to an attack technique rather than an investigative method. Therefore, consistent with CHFI v11 forensic methodologies, the investigator is performing apostmortem analysis of system records, making optionBthe correct answer.

NEW QUESTION: 147
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 Unix and Unix-like systems will reply to this scan

B. Only IBM AS/400 will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Windows systems will reply to this scan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
Frank, a Computer Hacking Forensics Investigator (CHFI), is investigating a multi-jurisdictional cybercrime. His team successfully collected digital evidence and ascertained that the attacker had breached the security of the system from a different country. Given the international nature of the case, which of the following would be the most complex issue he might encounter during his investigation?
A. The different legal systems and their rules for acquiring, preserving, investigating, and presenting digital evidence
B. The volatility of the collected digital evidence
C. The rapid changes in the technology used by the attacker
D. The circumstantial nature of digital evidence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
Emily, a seasoned digital forensics investigator, has been tasked with conducting an investigation on a Linux system running the ext2 file system. The system was involved in a suspected data exfiltration incident, and Emily needs to gather detailed information about the metadata of a specific file that may have been accessed or modified during the attack. After reviewing the system ' s file system structure, Emily aims to focus on the source that contains the file's metadata, such as timestamps, permissions, and file size. Which of the following would be the best source for this critical information?
A. The file ' s data blocks
B. The dentry cache
C. The superblock
D. The inode table
Answer: D (LEAVE A REPLY)
Option D. The inode table is the correct answer because, in Linux file systems such as ext2, file metadata including timestamps, permissions, ownership, and file size is stored in the file's inode , not in the file's content blocks. CHFI v11 explicitly includes Windows, Linux, and macOS File Systems , Linux File System Analysis Tools , and File System Analysis using The Sleuth Kit (TSK) , showing that exam candidates are expected to understand file-system structures and where key forensic metadata resides.
The data blocks contain file content, while the superblock stores overall file-system-level information such as layout and status. The dentry cache is a kernel memory structure related to name lookups and is not the primary persistent source for file metadata in this

context. For detailed per-file forensic metadata, the examiner must look at the inode information.
Therefore, when Emily wants the most critical metadata about a specific ext2 file, the best source is the inode table , because that is where the file's core descriptive attributes are maintained.

NEW QUESTION: 150
During a mobile fraud investigation in Atlanta, Georgia, analysts review a compromised Android handset's startup artifact. The timeline shows that, after the kernel initializes, a component preloads core libraries and then rapidly creates new application processes on demand to handle user activity. To pinpoint the element responsible for spawning those app processes during the boot sequence, which Android component should investigators focus on?
A. Android Runtime (ART)
B. System Server
C. Hardware Abstraction Layer (HAL)
D. Zygote
Answer: D (LEAVE A REPLY)
Zygote is the Android process that preloads core libraries and framework classes during startup, then forks new application processes as needed. This makes it the key component responsible for rapidly spawning app processes after the kernel and runtime initialization stages.

NEW QUESTION: 151
In a smart city surveillance breach at a municipal agency in Chicago, Illinois, investigators identify anomalous data flows from field sensors to cloud services, where intermediate processing for data aggregation, data filtering, access control, and device information discovery would reveal policy violations. Which IoT architecture layer, acting as an interface between hardware and applications, should be the focus?
A. Middleware Layer
B. Application Layer
C. Access Gateway Layer
D. Edge Technology Layer
Answer: (SHOW ANSWER)
The middleware layer acts as the interface between IoT hardware and application services. It supports functions such as data aggregation, filtering, access control, device discovery, and service management, making it the appropriate layer to examine for policy violations in sensor-to- cloud data flows.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 152
David, a digital forensics examiner, is investigating a cybercrime incident involving the theft of sensitive data from his company's servers. As part of the investigation, he needs to ensure that the procedures followed for handling digital evidence comply with internationally recognized standards. Which ISO standard provides guidelines for the establishment, maintenance, and improvement of a digital forensic capability within an organization?
A. ISO 27043: Incident Investigation Guidelines
B. ISO 27001: Information Security Management System
C. ISO 27037: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence
D. ISO 27041: Guidelines for Digital Forensics Readiness
Answer: (SHOW ANSWER)
The correct answer isISO 27041, which provides formal guidance for establishing, maintaining, and continuously improving adigital forensic capabilitywithin an organization. According to the CHFI v11 syllabus and Exam Blueprint v4, ISO standards play a critical role in ensuring that forensic processes are repeatable, reliable, legally defensible, and aligned with global best practices.
ISO 27041 specifically focuses onforensic readiness, which involves preparing an organization in advance to efficiently respond to digital incidents. This includes defining forensic policies, identifying evidence sources, ensuring tool and process validation, assigning roles and responsibilities, and integrating forensic procedures into incident response and business continuity plans. CHFI v11 emphasizes forensic readiness as a proactive approach that reduces investigation time, lowers costs, and improves evidence quality during cybercrime investigations.
By contrast, ISO 27037 (Option C) addresses only theidentification, collection, acquisition, and preservationof digital evidence, not the broader capability-building aspect. ISO 27043 (Option A) focuses on incident investigation principles and processes, while ISO 27001 (Option B) defines aninformation security management system (ISMS)and is not specific to digital forensics operations.
Therefore, for ensuring organizational-level forensic capability aligned with internationally recognized standards,ISO 27041is the most appropriate and CHFI v11-aligned answer

NEW QUESTION: 153
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 7035 and Event ID 7036
B. Event ID 7031 and Event ID 7032
C. Event ID 7036 and Event ID 7037
D. Event ID 1 and Event ID 7035
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
Which one of the following is not a consideration in a forensic readiness planning checklist?
A. Define the business states that need digital evidence
B. Take permission from all employees of the organization
C. Identify the potential evidence available
D. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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 the computer is switched off. power on the computer to take screenshot of the desktop
C. If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph
D. 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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
A forensic investigator has been assigned to extract data from several IoT devices involved in a complex investigation. The devices include drones, smart TVs, and wearables that are crucial to the case. These devices may contain valuable evidence, including video footage,

sensor data, and user interactions. The investigator needs a tool that can handle a variety of IoT devices and supports both physical and logical extraction methods to ensure that no evidence is missed.
Given the complexity of IoT forensics, which of the following tools should the investigator use to collect evidence from these devices effectively?
A. MD-NEXT
B. Gephi
C. Promqry
D. Freta
Answer: A (LEAVE A REPLY)
MD-NEXT is a specialized forensic tool designed to handle a wide range of devices, including IoT, and supports both physical and logical data extraction, making it suitable for comprehensive evidence collection in complex investigations.

NEW QUESTION: 157
Edward, an experienced CHFI professional, was conducting an investigation into potential intellectual property theft at a major corporation. The company had identified the suspected system, and Edward was tasked with collecting data. Given the high-stakes nature of the investigation, Edward needed to ensure that the collected data was forensically sound, maintained its integrity, and could withstand scrutiny in a court of law. To accomplish this, which rule of thumb for data acquisition should Edward adhere to?
A. Edward should opt for live data acquisition, irrespective of the system state.
B. Edward should rely on network-based acquisition as it is less intrusive.
C. Edward should focus on non-volatile data as it remains consistent.
D. Edward should avoid making changes to the original data.
Answer: (SHOW ANSWER)
The fundamental principle in forensic data acquisition is to preserve the original evidence in its exact state. Avoiding any modification ensures integrity, maintains evidentiary value, and guarantees that the data remains admissible in court.

NEW QUESTION: 158
You're a digital forensics investigator tasked with analyzing a bitmap image file (BMP) to gather information about its structure and contents. Understanding the file structure and data components is essential for conducting a thorough analysis. Which component of a bitmap image file contains data about the type, size, and layout of the file?
A. File header
B. Image data
C. Information header
D. RGBQUAD array
Answer: A (LEAVE A REPLY)

The BMP file begins with a file header (BITMAPFILEHEADER), which contains the signature identifying the file type, the overall file size, and the offset to the image data.

NEW QUESTION: 159
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. LOGINFO2 file
B. INFO1 file
C. LOGINFO1 file
D. INFO2 file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
A digital forensic investigator is tasked with analyzing an NTFS image file extracted from a pen drive. They leverage The Sleuth Kit (TSK) for this task, specifically utilizing the fsstat command- line tool. By employing fsstat, they delve into the file system's intricate details, such as metadata, inode numbers, and block or cluster information, thereby facilitating a comprehensive examination.
How can an investigator use TSK to analyze disk images?
A. By performing network scans
B. By conducting manual inspections
C. By using the plug-in framework
D. By writing custom code
Answer: (SHOW ANSWER)
According to the CHFI v11 Operating System Forensics and Digital Evidence Analysis objectives, The Sleuth Kit (TSK) is a core open-source forensic framework used to analyze disk images and file systems, including NTFS, FAT, EXT, and others. TSK is designed as a modular toolkit, offering both command-line utilities (such as fsstat, fls, and istat) and a plug-in framework that enables structured, extensible analysis.
The fsstat tool is part of this framework and is used to extract file system metadata, including cluster size, inode structure, allocation status, and volume layout--key artifacts required for timeline reconstruction and anomaly detection. CHFI v11 emphasizes that investigators typically analyze disk images using TSK's plug-in-based architecture, which allows multiple forensic modules to operate consistently on the same evidence source without altering it. This architecture is also what enables higher-level forensic platforms (such as Autopsy) to integrate TSK seamlessly.

NEW QUESTION: 161

During a late-evening review at a financial services firm, analysts suspect that sensitive files are being transferred off the network using a built-in file transfer client on a compromised workstation.
The team needs a centralized, non-intrusive way to surface this activity for initial triage without interacting directly with the endpoint. What monitoring action best supports detection of this activity?
A. Capturing live packet data directly from the suspect host
B. Monitoring aggregate FTP data transfer volumes through a SIEM platform
C. Blocking outbound FTP connections at the firewall
D. Reviewing endpoint file access logs on the affected workstation
Answer: (SHOW ANSWER)
Monitoring aggregate FTP data transfer volumes through a SIEM provides centralized visibility into suspicious file-transfer activity without directly interacting with the compromised endpoint.
This supports non-intrusive triage by highlighting unusual outbound FTP patterns, transfer spikes, or unauthorized destinations.

NEW QUESTION: 162
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?
A. Surface Manager
B. Application Framework
C. Media Framework
D. Resource Manager
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
During a robbery investigation in Phoenix, Arizona, detectives obtain carrier records to associate a seized handset with account-level activity observed around multiple towers near the crime scene. The team needs the field that identifies the subscriber in the provider ' s records rather than the handset hardware or the dialable number to correlate movements with the account. Which field should they prioritize?
A. MSISDN
B. Cell ID
C. IMEI
D. IMSI
Answer: D (LEAVE A REPLY)
The correct answer is D because IMSI is the identifier tied to the subscriber identity in the mobile network.
GSMA explains that the IMSI uniquely identifies the subscription associated with a SIM and is used by the mobile network to recognize the subscriber. That makes it the best field

when investigators want to correlate tower activity and account-level records to the subscriber rather than to the handset hardware. By contrast, IMEI identifies the physical device, MSISDN is the dialable phone number, and Cell ID identifies the serving cell tower sector rather than the user account. CHFI v11 includes cellular network components, subscriber identity modules, and cell site analysis, so candidates are expected to distinguish subscriber identity from device identity and location identifiers. In a forensic context, if the goal is to associate movements across towers with the actual subscription record held by the carrier, the most relevant field is IMSI. That is the core subscriber identifier used by the provider's network systems. (gsma.com)

NEW QUESTION: 164
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. GIF
B. BMP
C. ASCII
D. JPEG
Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
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. oledir.py
C. oleid.py
D. oleform.py
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
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. RS423
B. RS232

C. RS231
D. RS422
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 167
A company experiences a major data breach within its cloud infrastructure after a critical failure on the part of its cloud service provider (CSP). The breach occurs because the CSP's infrastructure fails to adequately segregate and safeguard the data of different customers in a multi-tenant environment. The attacker exploits this weakness, gaining unauthorized access to sensitive data from multiple clients sharing the same cloud systems. As a result, customer data is revealed across several accounts, with the attacker using this access to move laterally through the system, escalating privileges, and accessing additional confidential information. The breach remained undetected for an extended period, allowing the attacker to cover their tracks and exfiltrate large volumes of data. What threat is most likely to be the cause of this issue?
A. Loss of client control over cloud infrastructure and data.
B. Failure in due diligence during the cloud service selection.
C. Insufficient resource isolation causing cross-tenant data exposure.
D. Lack of monitoring leading to unnoticed data breaches.
Answer: C (LEAVE A REPLY)
The breach stems from inadequate separation of customer data in a multi-tenant cloud environment. Poor resource isolation allows one tenant to access another's data, leading to cross-tenant exposure and unauthorized access.

NEW QUESTION: 168
Windows identifies which application to open a file with by examining which of the following?
A. The file attributes
B. The File extension
C. The file signature at the beginning of the file
D. The file Signature at the end of the file
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Michael, a forensic examiner, is conducting a forensic analysis of an image file obtained from a suspect's machine. While examining the file using a hex editor, he discovers that the hex value of the file starts with the sequence "89 50 4e." The file appears to be suspicious, so Michael needs to identify the type of the file to understand its structure and determine whether it contains any malicious content. Given this information, what type of file is Michael looking at?
A. PDF
B. JPEG
C. BMP
D. PNG
Answer: (SHOW ANSWER)
The hexadecimal signature "89 50 4E" corresponds to the beginning of a PNG file header (commonly "89 50 4E 47"), identifying the file as a PNG image.

NEW QUESTION: 170
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. DevScan
B. Devcon
C. Reg.exe
D. fsutil
Answer: (SHOW ANSWER)

NEW QUESTION: 171
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. Trademark law
B. Brandmark law
C. Printright law
D. Copyright law
Answer: A (LEAVE A REPLY)

NEW QUESTION: 172
Why is it a good idea to perform a penetration test from the inside?
A. To attack a network from a hacker's perspective
B. It is never a good idea to perform a penetration test from the inside
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: 173
Henry, a forensic investigator, has been assigned to analyze a cyber-attack that occurred on a web application hosted on an Apache server running on an Ubuntu system. The attacker is suspected of exploiting vulnerabilities within the application, and Henry needs to examine the server's logs to identify any suspicious activities.
As part of the investigation, Henry begins by navigating to the log file storage locations to analyze the Apache access logs and error logs. These logs are crucial for understanding the nature of the attack, identifying the source IPs, the exact times of the attack, and the type of attack executed.
Henry needs to locate the configuration file for Apache on Ubuntu to find where the log files are stored. In which of the following storage locations on an Ubuntu machine can Henry find useful information regarding the log files for Apache?
A. /var/log/httpd/access_log
B. /usr/local/etc/apache22/httpd.conf
C. /etc/httpd/conf/httpd.conf
D. /etc/apache2/apache2.conf
Answer: D (LEAVE A REPLY)
According to the CHFI v11 Web Application and Linux Forensics objectives, understanding default web server configurations and log locations is essential for investigating web-based attacks. On Ubuntu systems, the Apache web server package is typically installed as apache2, and its primary configuration file is located at /etc/apache2/apache2.conf.
This configuration file plays a central role in Apache forensics because it defines or references critical settings, including log file locations, logging formats, enabled modules, virtual host configurations, and included configuration directories (such as sites-enabled and conf-enabled).
The actual access and error logs are usually stored in /var/log/apache2/access.log and /var/log/apache2/error.log, but the paths to these logs are defined or confirmed through the apache2.conf file and its included configuration files.

NEW QUESTION: 174

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

A. Container Name

B. Encrypted FEK

C. EFS Certificate Hash

D. Checksum

Answer: D (LEAVE A REPLY)

NEW QUESTION: 175

A multinational company has recently fallen victim to a severe cyberattack. As part of the incident response team, you are analyzing the Apache web server logs to track the attacker s activities.

You notice that modifications are made to the HTTP.REQUEST component of the Apache core, suggesting changes in request handling. To discern the type of modifications made, which of the following elements of the Apache web server architecture would you focus on examining?

A. Apache modules: To uncover extended functionalities that may have been tampered with

B. http_protocol module: To identify the client and server data exchange details

C. http_config module: To check alterations in configuration files and modules management

D. http_main module: To identify server startups and timeouts

Answer: A (LEAVE A REPLY)

Apache request processing behavior is commonly extended or altered through dynamically loaded modules (e.g., mod_security, mod_rewrite, custom modules). If HTTP.REQUEST handling appears changed, examining loaded/added/modified modules is the most direct way to find injected functionality or tampering that affects request flow.

NEW QUESTION: 176

Investigators may encounter issues with image file compatibility after acquiring data from suspect media.

This section outlines scenarios like converting E01 format for Linux, creating a bootable VM, dealing with Windows file systems on Linux, and handling APFS file systems. Solutions for each scenario are discussed, concluding with image viewing methods for Windows, Linux, and Mac. What challenges might investigators face when preparing image files for examination?

A. Converting E01 format for Windows

B. Handling APFS file systems on a Windows workstation

C. Creating a bootable VM from acquired evidence

D. Viewing image files on a Mac workstation

Answer: B (LEAVE A REPLY)
According to the CHFI v11 objectives underImage/Evidence ExaminationandOperating System Forensics, one of the most significant challenges investigators face when preparing image files for examination isfile system compatibility across operating systems.APFS (Apple File System)is the default file system used by modern macOS devices, and it isnot natively supported on Windows workstations. This creates a clear challenge when investigators attempt to analyze APFS-based forensic images on Windows platforms.
CHFI v11 highlights that special tools, drivers, or forensic platforms are required to mount, parse, and analyze APFS volumes on non-macOS systems. Without proper support, investigators may be unable to access directories, metadata, snapshots, or encrypted APFS containers, potentially delaying investigations or risking incomplete analysis.
The other options describe scenarios that are typically manageable with standard forensic workflows.
Converting E01 images (Option A) is well-supported using tools like ewfmount. Creating bootable VMs (Option C) is an advanced but solvable task using virtualization tools. Viewing images on macOS (Option D) is generally straightforward with native or commercial forensic software.
The CHFI Exam Blueprint v4 explicitly mentionsAPFS file system analysis challengesand cross-platform compatibility issues as key considerations during forensic image preparation. Therefore, handling APFS file systems on a Windows workstation represents a genuine and commonly encountered challenge, making Option B the correct and exam-aligned answer

NEW QUESTION: 177
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
A. AA00
B. AA55
C. 00AA
D. A100
Answer: (SHOW ANSWER)

NEW QUESTION: 178
What must be obtained before an investigation is carried out at a location?
A. Modus operandi
B. Habeas corpus
C. Subpoena
D. Search warrant
Answer: D (LEAVE A REPLY)

NEW QUESTION: 179

During a retail email audit in Dallas, a recipient clicked unsubscribe but continued receiving messages from the sender for two weeks. Under the CAN-SPAM Act, which requirement was violated?

A. Do not use deceptive subject lines

B. Do not use false or misleading header information

C. The commercial email must be identified as an ad

D. Honor the opt-out request

Answer: D (LEAVE A REPLY)

The correct answer is D because the CAN-SPAM Act requires senders to honor a recipient's opt-out request.

The scenario specifically says the recipient unsubscribed but continued to receive messages for two weeks, which directly points to a failure to comply with that requirement. CHFI v11 includes legal issues that affect forensic investigations, including U.S. laws against email crime such as the CAN-SPAM Act. In that context, candidates are expected to match a sender's behavior to the violated statutory requirement. The other choices describe separate obligations under CAN-SPAM, such as avoiding deceptive subject lines, avoiding false header information, or properly identifying advertising content. None of those addresses the factual problem described here. In practical legal and forensic review, unsubscribe handling is a distinct compliance point because it creates a clear audit issue when the sender continues messaging after the opt-out request. Since the triggering fact is the failure to stop sending after the unsubscribe action, the requirement violated is the obligation to honor the opt-out request.

NEW QUESTION: 180

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

A. Safari

B. Microsoft Edge

C. Google Chrome

D. Mozilla Firefox

Answer: B (LEAVE A REPLY)

NEW QUESTION: 181

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. Router Penetration Testing

B. DoS Penetration Testing

C. Firewall Penetration Testing

D. Internal Penetration Testing

Answer: B (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 182
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. 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
B. All forms should be placed in the report file because they are now primary evidence in the case
C. All forms should be placed in an approved secure container 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: A (LEAVE A REPLY)

NEW QUESTION: 183
During an internal audit at a financial services firm in Chicago, forensic analysts investigate a suspicious administrator login followed by several account management events. Within a short timeframe, the logs record group creation, member additions, and member deletions. To reconstruct the sequence of activity and identify the action that enabled subsequent privilege escalation, which event should analysts prioritize as the initial step?
A. 4729: A member was removed from a security-enabled global group
B. 4727: A security-enabled global group was created
C. 4728: A member was added to a security-enabled global group
D. 4730: A security-enabled global group was deleted
Answer: B (LEAVE A REPLY)

Event ID 4727 records the creation of a security-enabled global group. In a sequence involving group creation followed by member additions and deletions, this is the initial account- management action that establishes the group later used for privilege-related changes.

NEW QUESTION: 184
During an investigation of a high-profile cybercrime case, a law enforcement agency realized the need for specialized computer forensic investigators. Their general forensic investigators were struggling with the specific demands of computer forensics. Although they considered hiring external forensic investigators, they decided against it due to budget constraints. What could be a potential solution to this predicament?
A. Training their current investigators in computer forensics.
B. Outsourcing the investigations to a private firm.
C. Investing in advanced forensic tools to assist their current investigators.
D. Collaborating with international law enforcement agencies for assistance.
Answer: A (LEAVE A REPLY)
Training existing investigators in computer forensics builds in-house expertise, enabling them to handle specialized digital investigations effectively without incurring the higher costs of outsourcing.

NEW QUESTION: 185
A digital forensics investigator performs a browser history analysis after a suspected breach. The investigator deals with three web browsers: Mozilla Firefox, Coogle Chrome, and Microsoft Edge.
The suspect was using Windows. The investigator must locate the cache, cookies, and history for all three browsers. What are the correct locations?
A. Firefox: History - C:\Users\\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default \cookies.sqlite; Chrome: Cache - C:\Users\{user}\AppData\Local\Coogle\Chrome\User Data\Default\Cache; Edge: Cookies - C:\Users\Admin\AppData\Local\Packages \Microsoft.MicrosoftEdge_xxxxxxxxxx\AC\MicrosoftEdg e\Cookies
B. Firefox: Cache - C:\UsersWAppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default \cache2; Chrome: History - C:\Users\{user)\AppData\Local\Google\Crrome\User Data \Default; Edge: Cookies - C:\Users\Admin\AppData\Local\Packages \Microsoft.MicrosoftEdge_xxxxxxxxxx\AC\MicrosoftEdg e\Cookies
C. Firefox: Cookies - C:\Users\\AppData\Roaming\Mozilla\Firefox\Profiles \XXXXXXXX.default\cookies.sqlite; Chrome: Cache - C:\Users\{user}\AppData\Local \Coogle\Chrome\User Data\Default\Cache; Edge: History - C:\Users\Admin\AppData\Local \Microsoft\Windows\History
D. Firefox: Cache - C:\UsersWAppData\Roaming\Mozilla\Firefox\Profiles \XXXXXXXX.default\places.sqlite; Chrome: Cookies - C:\Users\{user}\AppData\Local

\Google\Chrome\User Data\Default; Edge: History - C:\Users\Admin\AppData\Local \Microsoft\Windows\WebCache
Answer: (SHOW ANSWER)

NEW QUESTION: 186
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?
A. ACK flag scanning
B. Inverse TCP flag scanning
C. TCP Scanning
D. IP Fragment Scanning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 187
Detective Sarah, a skilled digital forensics investigator, begins probing a compromised computer system linked to a cybercrime ring. Prioritizing volatile data, she meticulously plans her evidence- collection strategy. Amidst the investigation, various data sources emerge, each holding potential clues to unraveling the illicit scheme.
Which data source should you prioritize for collection, considering the order of volatility outlined in the RFC 3227 guidelines?
A. Disk or other storage media containing potentially critical files
B. Temporary file systems where recent activity might be stored
C. Archival media such as a DVD-ROM or a CD-ROM
D. The physical configuration and network topology of the system
Answer: D (LEAVE A REPLY)
This question directly relates to CHFI v11 objectives under Data Acquisition and Duplication and the concept of order of volatility, which is formally defined in RFC 3227 (Guidelines for Evidence Collection and Archiving). CHFI v11 stresses that forensic investigators must collect the most volatile data first, as it is the most likely to be lost or altered during system shutdowns or continued operation.
According to RFC 3227, the order of volatility starts with data that changes most rapidly, such as system state and network-related information. This includes the physical configuration of the system, network topology, routing tables, ARP cache, active network connections, and running processes. These elements can disappear immediately if the system is powered off or network connectivity changes, making them the highest priority during live response.

NEW QUESTION: 188

During a data-exfiltration case at a Seattle design firm, investigators need the macOS encrypted container that securely stores user account names and passwords for Mac, apps, servers, and websites and can also hold confidential information such as credit card numbers or bank PIN numbers. What Mac forensics data source should they examine?
A. Apple Mail
B. Time Machine
C. Property list or plist files
D. Keychain
Answer: (SHOW ANSWER)
The correct answer is D because Keychain is the macOS secure storage mechanism used to hold sensitive credentials and other protected secrets. Apple states that Keychain stores website usernames and passwords, and related secure information such as credit card details, while Keychain Access on Mac allows viewing keys, certificates, and other stored items. That matches the scenario exactly. CHFI v11 includes macOS forensic data, log files, and directories, so candidates are expected to know where valuable user authentication material and confidential account data are stored. Apple Mail contains email artifacts, Time Machine contains backup history, and plist files store many configuration details, but none of those is the primary encrypted credential container described in the question. From a forensic perspective, Keychain can be highly significant in data-theft, access-abuse, and credential-misuse investigations because it may reveal stored account relationships and secrets relevant to attacker activity or user actions. When the exam asks for the macOS source that securely holds account names, passwords, and other confidential values, the answer is Keychain.

NEW QUESTION: 189
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 internal attack, and the major challenge will be the probable damage to the physical infrastructure
B. 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
C. Cybercrime can be categorized as an external attack, and the primary challenge will be identifying the source of the sophisticated hacking tools
D. Cybercrime can be categorized as an external attack, and the primary challenge will be tracing the IP addresses of the attacker
Answer: (SHOW ANSWER)

NEW QUESTION: 190
During a digital-forensic investigation at a financial company in San Jose, California, analysts discover that the first 512-byte sector of a suspect ' s hard disk has been overwritten by a malicious installer. After hardware checks complete, the system cannot locate the operating system or transfer control to the startup program on the active partition. Based on the structures found in this sector, which component ' s corruption most likely caused the failure?
A. Partition Table
B. Boot signature 0x55AA
C. Bootloader
D. Master Boot Code
Answer: D (LEAVE A REPLY)
The correct answer is D because the Master Boot Code in the first sector of an MBR disk is the executable code that runs after BIOS hands off control. Its job is to examine the partition table, identify the active partition, and transfer execution to that partition's boot sector. If that code is corrupted, the system can no longer locate and hand off to the startup program on the active partition, which matches the failure described in the question. The partition table is also present in the same sector and is important, but the wording specifically focuses on failure to transfer control after hardware checks, which is the role of the executable boot code. The boot signature 0x55AA only indicates that the sector is bootable in format terms; it does not perform the control transfer. CHFI v11 includes Windows boot process and logical disk structures, so candidates are expected to understand what each MBR component does. Since the startup failure is tied to the executable handoff function within the first sector, the most likely corrupted component is the Master Boot Code.

NEW QUESTION: 191
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. Both Criminal and Administrative Investigation
B. Criminal Investigation
C. Administrative Investigation
D. Civil Investigation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
Cynthia, a CHFI specialist, is working on a high-stakes case involving a multinational corporation's data leak. She has narrowed down her investigation to a particular server believed to hold the compromised data. However, the server is integral to the company's operations and cannot be taken down for a standard dead acquisition. Cynthia considers

the order of volatility and realizes that some critical data may soon be lost if not properly captured. What should be Cynthia's next step to effectively collect the evidence needed for her investigation?

A. Conduct a live acquisition immediately.

B. Conduct a dead acquisition during non-working hours

C. Use network sniffing to gather data passively.

D. Ask the IT department to create a server backup for analysis.

Answer: A (LEAVE A REPLY)

Since the server is active and cannot be taken offline, live acquisition is necessary to capture volatile data before it is lost. This approach aligns with the order of volatility and ensures critical in-memory and active system information is preserved while the system remains operational.

NEW QUESTION: 193

In a suspected malware outbreak at a financial services company in Chicago, investigators observe that the organization ' s mail server is relaying suspicious traffic and generating unusual message errors across multiple systems. The behavior suggests that the system may be compromised and distributing unsolicited messages. What indicator of malware should investigators prioritize to validate this suspicion?

A. Unexplained bounced emails

B. Alerts of spam messages from the system or email

C. Numerous unwanted emails and social posts

D. System slowdown and longer reboot times

Answer: B (LEAVE A REPLY)

Option B is the strongest answer because it directly points to a host or mail system being used to send spam, which is a common operational sign of malware compromise. The CHFI v11 blueprint includes malware behavior, malware artifacts and indicators, and system and network level analysis. In a case where a mail server is relaying suspicious traffic and message errors are appearing, investigators should focus first on alerts showing that spam is being sent from the affected system or associated email environment. That is more specific and more probative than general performance symptoms such as slowdown. Unexplained bounced emails can occur as a side effect, but they are less direct than confirmed alerts of outbound spam activity.

Numerous unwanted emails and social posts is too broad and less tied to forensic validation of the suspect host. From an examiner's perspective, the key is to identify evidence that the compromised machine is actively participating in spam distribution or botnet-style messaging behavior. That aligns with CHFI's expectation that analysts recognize malware indicators not just by file artifacts, but also by suspicious communications and abnormal message-sending patterns across the environment.

NEW QUESTION: 194

You are a forensic investigator working for a cybersecurity firm tasked with analyzing a suspicious Microsoft Office document named "infected_doc." The document was discovered in an email attachment sent to multiple employees at a large corporation. Concerns have been raised about potential malware embedded within the document, particularly involving VBA macros.
As a forensic investigator examining the "infected_doc" Microsoft Office document, what initial step would you take to identify suspicious or malicious components within the file?
A. Execute the command oleid "" on a Linux workstation to review all components for suspicious elements.
B. Open the document in a sandbox environment to observe any unusual behavior.
C. Run the command analyze_doc "" to scan the document for potential threats.
D. Utilize a browser-based tool to inspect the document's metadata for any anomalies.
Answer: (SHOW ANSWER)
This question aligns with CHFI v11 objectives under Malware Forensics and Static Malware Analysis of Suspicious Documents. When analyzing potentially malicious Microsoft Office documents, CHFI v11 emphasizes that investigators should always begin with static analysis before attempting any form of execution. This approach minimizes risk and helps identify embedded threats such as VBA macros, OLE objects, exploits, and obfuscation techniques without activating the payload.
The oleid tool (part of the oletools suite) is specifically designed for the initial inspection of OLE- based Microsoft Office documents. It quickly identifies indicators of compromise such as the presence of macros, embedded objects, suspicious file formats, encryption, and known exploit characteristics. CHFI v11 highlights oleid as a safe, non-intrusive first step to triage Office documents and determine whether deeper analysis (e.g., macro extraction or sandbox execution) is warranted.

NEW QUESTION: 195
A cybersecurity firm has recently discovered a new strain of ransomware circulating on the internet, posing a significant threat to organizations worldwide. This ransomware is highly sophisticated and capable of evading traditional antivirus software. To effectively combat this threat, the cybersecurity firm decides to utilize a malware sandbox for detailed analysis. Given the scenario described, what would be the primary objective of using a malware sandbox in this situation?
A. To permanently remove the ransomware from infected systems.
B. To encrypt sensitive data on the host systems to prevent ransomware infection.
C. To distribute the ransomware to other systems for further analysis.
D. To execute and observe the behavior of the ransomware in a controlled environment.
Answer: (SHOW ANSWER)
A malware sandbox provides an isolated, controlled environment where the ransomware can be safely executed and monitored. This allows analysts to observe its behavior,

understand its functionality, and identify indicators of compromise without risking infection of production systems.

NEW QUESTION: 196
During triage of a suspicious Android application, an examiner sets up a local static-analysis environment using MobSF on a forensic workstation. Before any application artifacts can be submitted or results reviewed, the examiner must initialize the analysis environment so that MobSF ' s interface becomes available for use.
Which action enables this environment to become operational?
A. Open
a web browser and go to http://localhost:8000 for accessing the homepage
B. Run python manage.py runserver
C. Upload the suspicious APK file that is required to analyze
D. Examine the information such as application hash sum, component types and numbers on the dashboard
Answer: B (LEAVE A REPLY)
The correct answer is B because MobSF must first be started as a local web application before the interface can be reached in a browser. The installation and startup workflow for MobSF includes launching the server process so that the web interface becomes available. Opening a browser to localhost is the next step only after the application is already running. Uploading an APK and reviewing dashboard data are later actions that depend on the service being operational first. CHFI v11 includes malware analysis and mobile application forensics, and this kind of question tests whether the examiner can distinguish initialization steps from later analytical use. In practical forensic triage, the analysis environment must be brought online before any application submission or review can take place. That makes the server-start action the correct operational enabler. The exact command can vary slightly by installation method or version, but among the listed options, the one that actually initializes the local analysis environment is running the server process. Therefore, the best answer is running python manage.py runserver.
(github.com)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 197

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

A. AMS

B. Shadow file

C. SAM

D. Password.conf

Answer: C (LEAVE A REPLY)

NEW QUESTION: 198

During an after-hours incident at a news portal in Raleigh, North Carolina, analysts observe many hits to the login page from the same IP over a short period. Minutes later, they see a single entry that differs from the prior pattern. To distinguish ongoing brute-force attempts from post-auth navigation to the admin area, which element in the log most strongly indicates the latter?

A. " login attempts within a very short timeframe "

B. " HTTP 302 status indicates URL redirection "

C. " from the same IP "

D. " the URL has been changed to /wordpress/wp-admin/ "

Answer: D (LEAVE A REPLY)

The correct answer is D because the clearest sign of post-auth navigation is the change in requested resource from the login endpoint to the WordPress admin area. A burst of repeated login attempts from the same IP suggests brute-force activity, but it does not prove successful entry. A 302 redirect can happen in several contexts and is less definitive by itself. The strongest indicator that the attacker moved beyond guessing credentials and into an authenticated area is a subsequent request for /wordpress/wp-admin/, which is the administrative interface path. CHFI v11 includes investigation of brute-force attacks and web application forensic analysis through web server logs, so candidates are expected to distinguish unsuccessful login pressure from navigation that occurs after access is obtained. In forensic interpretation, the requested URL often provides stronger context than timing or source IP alone. Since the question asks what most strongly indicates post-auth activity rather than continued brute-force behavior, the change to the admin URL is the best answer.

NEW QUESTION: 199

During a financial investigation in Boston, Massachusetts, a forensic analyst duplicates a suspect's hard drive. To confirm that the duplicate image is an exact copy of the original, which validation method should the analyst apply?

A. Perform RAID reconstruction of the acquired drive

B. Compute cryptographic hash values such as MD5 or SHA-256

C. Apply compression to reduce the image file size

D. Use data sanitization on the target media

Answer: (SHOW ANSWER)
Cryptographic hash values are used to verify forensic image integrity by comparing the hash of the original drive with the hash of the duplicate image. Matching hashes confirm that the duplicate is an exact bit-for-bit copy of the original evidence.

NEW QUESTION: 200
Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions.
What tool should Mark use to restore the data?
A. iskvlew
B. EFSDump
C. R-Studio
D. Diskmon D
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?
A. Virtual Files
B. Image Files
C. Prefetch Files
D. Shortcut Files
Answer: (SHOW ANSWER)

NEW QUESTION: 202
During a targeted intrusion at a financial firm in Seattle, Washington, a forensic analyst must determine which log source can best help identify the initial inbound connection used by the attacker. The analyst has access to multiple network device logs - some showing packet rejections, others displaying decoy interactions, DHCP lease history, and intrusion alerts. Which log type should the analyst prioritize to trace the first connection attempt to the organization's internal host?
A. Honeypot logs
B. DHCP logs
C. IDS logs
D. Firewall logs
Answer: D (LEAVE A REPLY)
Firewall logs should be prioritized because they record inbound and outbound connection attempts, including source IP addresses, destination IP addresses, ports, protocols, timestamps, and allowed or blocked traffic. This makes them the best source for tracing the attacker's initial connection attempt to an internal host.

NEW QUESTION: 203
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. Firewall
B. Domain Controller
C. IDS
D. SIEM
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Liam, a digital forensic investigator, is examining evidence from a cyber-attack that targeted a Linux-based system. While analyzing the system, he discovers that several files are missing. Upon further inspection, he notices that a particular executable file, which had been running at the time of the attack, erased its own content, making recovery more challenging. To recover the lost file, Liam needs to identify the correct command in Linux that would help him retrieve the file. Which of the following commands should Liam use to recover the lost file on the Linux system?
A. cp /proc/$PID/exe /tmp/file
B. cd C:\RECYCLER\S-..User SID
C. D < # > .
D. $R < # > .
Answer: (SHOW ANSWER)
Option A is the correct answer because the question describes a Linux executable that was running at the time of the attack and then deleted or erased from normal file-system visibility. In Linux forensics, if a process is still running, the executable image may still be accessible through the /proc/$PID/exe link for that process. Copying that path to another location is a recognized way to preserve the executable content for analysis before the process terminates.
This aligns with CHFI v11's coverage of Linux file system analysis tools , Linux memory forensics , tools to collect volatile and non-volatile information on Windows and Linux , and Windows and Linux forensics using Python , all of which reflect the importance of understanding live Linux evidence sources and recovery opportunities.
The other options are unrelated to Linux executable recovery. The RECYCLER path is Windows-specific, and $R < # > style entries are associated with Windows Recycle Bin artifacts, not Linux process recovery.
Therefore, for a deleted-but-still-running Linux executable, the correct CHFI-aligned recovery command is cp
/proc/$PID/exe /tmp/file .

NEW QUESTION: 205
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. Session poisoning
B. Cookie Poisoning Attack
C. DNS Poisoning
D. DNS Redirection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin.
What is the size limit for Recycle Bin in Vista and later versions of the Windows?
A. No size limit
B. Maximum of 4.99 GB
C. Maximum of 5.99 GB
D. Maximum of 3.99 GB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
During a forensic investigation, Robert discovers that the attacker modified the file extensions of certain malicious files to make them appear benign. These files were originally executable but had their extensions changed to disguise their true nature. Robert needs to identify and extract these files despite their misleading extensions. Which of the following tools can help Robert detect file extension mismatches and recover the actual file types during the investigation?
A. OSForensics
B. Timestomp
C. Autopsy
D. StegoHunt
Answer: (SHOW ANSWER)
According to the CHFI v11 objectives under Digital Forensics Review and Anti-Forensics Techniques , attackers frequently use file extension manipulation as an anti-forensic technique to conceal malicious executables by renaming them with harmless-looking extensions such as .txt, .jpg, or .pdf. This tactic relies on the assumption that investigators or users will trust the file extension rather than verifying the file's true structure.

Autopsy , which is built on The Sleuth Kit (TSK) , provides a dedicated capability to detect file extension mismatches by analyzing file headers (magic numbers) and comparing them against the file's extension. If a file's internal signature does not match its extension, Autopsy flags it as suspicious, allowing investigators to identify hidden executables and recover their true file types. CHFI v11 explicitly highlights "Detecting File Extension Mismatch using Autopsy" as a key forensic technique for defeating anti-forensics.
OSForensics is primarily used for detecting data hiding techniques such as alternate data streams and overwritten metadata, while Timestomp is itself an anti-forensic tool used to manipulate timestamps.
StegoHunt focuses on steganography detection rather than file type validation.
The CHFI Exam Blueprint v4 emphasizes the importance of file type analysis and extension mismatch detection when investigating disguised malware, making Autopsy the most appropriate and exam-aligned tool in this scenario

NEW QUESTION: 208
At a financial services provider ' s online trading platform in Boston, Massachusetts, forensic analysts are examining centralized logs using Sumo Logic IIS Log Analyzer as part of an investigation into suspected resource-exhaustion activity. Overall request volume and average latency appear within normal ranges, yet certain user sessions exhibit intermittent delays that do not correlate with specific endpoints or servers. To reveal whether completion durations are concentrated within particular intervals or display skewed frequency patterns across the full dataset, which analytic view should the team select?
A. Response throughputs
B. Requests by server
C. Slowest pages
D. Response times in histogram form
Answer: (SHOW ANSWER)
The correct answer is D because a histogram is the view designed to show how response times are distributed across ranges, making it ideal for spotting clusters, skew, long tails, or intermittent delay bands that averages can hide. Sumo Logic's IIS Log Analyzer documentation explicitly lists "Response times in histogram form" as one of the available views in the app. That makes it the most appropriate choice when analysts need to determine whether delays are concentrated in specific intervals rather than simply looking at aggregate throughput or server counts. Requests by server would help compare load across hosts, slowest pages would identify particular endpoints with high latency, and response throughputs would focus on volume over time.
None of those directly answers the distribution question posed in the scenario. CHFI v11 includes IIS log analysis and web-application attack investigation, so candidates should be able to select the visualization that best supports a given forensic question. When the goal

is to reveal response-time frequency patterns across the whole dataset, the correct analytic view is response times in histogram form.

NEW QUESTION: 209
Liam, a digital forensic investigator, is examining evidence from a cyber-attack that targeted a Linux-based system. While analyzing the system, he discovers that several files are missing.
Upon further inspection, he notices that a particular executable file, which had been running at the time of the attack, erased its own content, making recovery more challenging. To recover the lost file, Liam needs to identify the correct command in Linux that would help him retrieve the file.
Which of the following commands should Liam use to recover the lost file on the Linux system?
A. cd C:\RECYCLER\S-<User SID>
B. D<#>.
C. cp /proc/$PID/exe /tmp/file
D. $R<#>.
Answer: C (LEAVE A REPLY)
According to the CHFI v11 objectives under Operating System Forensics, Linux Memory and Process Analysis, and Anti-Forensics Techniques, attackers sometimes use a technique where a malicious executable deletes or overwrites itself after execution to evade detection. Although the file may be erased from disk, if the process is still running, Linux maintains a reference to the executable in memory through the /proc filesystem. Each running process in Linux has a directory under /proc/<PID>/, and the symbolic link /proc/<PID>/exe points to the executable image currently loaded into memory. By copying this link using the command:
cp /proc/$PID/exe /tmp/file
an investigator can successfully recover the in-memory version of the executable, even if it has been deleted from disk. This is a well-documented forensic technique in CHFI v11 for recovering malware binaries and analyzing fileless or self-deleting malware.

NEW QUESTION: 210
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 should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
C. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM
D. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
Answer: (SHOW ANSWER)

NEW QUESTION: 211
During dynamic malware analysis, a suspicious executable file is executed in a controlled, sandboxed environment. The malware exhibits behavior indicative of network communication and file encryption.
In dynamic malware analysis, what is the primary objective of executing a suspicious file in a sandboxed environment?
A. To observe the behavior and interactions of the malware without risking damage to the host system
B. To enhance the performance of the operating system
C. To determine the author's identity
D. To optimize the storage utilization of the system
Answer: (SHOW ANSWER)
This question aligns with CHFI v11 objectives underMalware Forensics, specificallystatic vs. dynamic malware analysisand the use ofsandboxed environments. Dynamic malware analysis involves executing a suspicious file in a controlled and isolated environment to safely observe its real-time behavior. CHFI v11 emphasizes that many modern malware samples use obfuscation, packing, or fileless techniques that conceal their functionality unless they are actually executed.
The primary objective of running malware in a sandbox is tomonitor its behavior without endangering production systems. Investigators can observe network communications (such as command-and-control traffic), file system changes, registry modifications, process injection, persistence mechanisms, and encryption activity. These behaviors provide critical indicators of compromise (IoCs) and help investigators understand the malware's capabilities, intent, and impact.
Sandboxing ensures forensic safety by isolating the malware from the host operating system and broader network, preventing unintended damage or data loss. The other options are not valid forensic objectives- performance optimization, author attribution, or storage efficiency are unrelated to dynamic malware execution. Therefore, consistent with CHFI v11 malware analysis methodology, the correct objective is to safely observe malware behavior and interactions in a controlled environment.

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 212
During a digital forensics investigation, a mobile device running Android OS is seized from a suspect. Upon examination, files are discovered indicating interactions with both Windows and Linux systems. In Android and iOS forensic analysis, which of the following is a crucial step when examining files associated with Windows and Linux systems?
A. Analyzing files to identify interactions and potential evidence across different operating systems
B. Focusing only on files native to the mobile device
C. Extracting data solely from Android and iOS files
D. Ignoring files associated with Windows and Linux
Answer: A (LEAVE A REPLY)
According to the CHFI v11 objectives underMobile and IoT ForensicsandOperating System Forensics, mobile devices often act ascross-platform interaction points, storing artifacts related to communications, file transfers, backups, or synchronization withWindows and Linux systems. These artifacts may include shared documents, SSH keys, SMB access traces, USB connection records, cloud sync remnants, or application logs indicating interaction with external operating systems.
A crucial forensic step in such cases isanalyzing files to identify interactions and potential evidence across different operating systems. This enables investigators to reconstruct user activity beyond the mobile device itself and establish links between the mobile device and other systems involved in the incident. CHFI v11 emphasizes the importance ofcorrelating evidence across heterogeneous platformsto build a complete and accurate timeline of events.
Focusing only on native mobile files (Options B and C) risks overlooking critical evidence that may demonstrate lateral movement, data exfiltration, or coordination between devices. Ignoring Windows- or Linux-related artifacts (Option D) directly contradicts forensic best practices and may lead to incomplete or flawed conclusions.
The CHFI Exam Blueprint v4 explicitly highlightsAndroid and iOS forensic analysis,cross-platform evidence correlation, andfile system analysisas key competencies. Therefore, analyzing cross-OS artifacts is essential for uncovering hidden relationships, validating investigative hypotheses, and ensuring legally defensible findings, making Option A the correct and exam-aligned answer

NEW QUESTION: 213
Why should you never power on a computer that you need to acquire digital evidence from?
A. Powering on a computer has no affect when needing to acquire digital evidence from it
B. When the computer boots up, files are written to the computer rendering the data nclean
C. When the computer boots up, the system cache is cleared which could destroy evidence
D. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 214
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. Conducting a file fingerprinting on the binary code to determine its function
B. Searching for embedded strings in the binary code to infer the functionality
C. Running the executable in a sandboxed environment to observe its behavior
D. Comparing the hash value of the file with online malware databases for recognition
Answer: C (LEAVE A REPLY)

NEW QUESTION: 215
During a malware forensic investigation, a newly added entry was identified in the Windows AutoStart registry keys after a malware execution on a compromised system. The entry indicates a VB script file named "CaoCIboog.vbs" installed in the 'Run' key to achieve persistence and run automatically upon user login. As a Computer Hacking Forensic Investigator (CHFI), where would you expect to find this suspicious entry in the registry hive?
A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
B. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Answer: B (LEAVE A REPLY)

NEW QUESTION: 216
Lucas, a forensic investigator, has been tasked with analyzing the behavior of a malware sample that has infected a Linux-based system. After executing the malware, Lucas suspects that the malware is performing suspicious activities such as modifying system files, accessing restricted resources, and interacting with the kernel. In order to track the

malware's interaction with the operating system, Lucas decides to monitor the system calls made by the malware during its execution. To gather this data, which of the following tools should Lucas use to effectively track and analyze the system calls initiated by the malware, providing insights into how the malware communicates with the OS and performs its malicious activities?

A. Process Explorer

B. strace

C. Autoruns

D. Regshot

Answer: B (LEAVE A REPLY)

According to the CHFI v11 objectives under Malware Forensics and Linux Memory and System Behavior Analysis, monitoring system calls is a core technique for understanding how malware interacts with the operating system at a low level. On Linux systems, strace is the primary and most effective tool for this purpose.

Strace intercepts and records system calls made by a process, along with the signals received and return values. Since all interactions between user-space programs and the Linux kernel occur via system calls, tracing them provides deep visibility into malware behavior. Using strace, investigators can observe actions such as file creation or modification (open, write), privilege escalation attempts (setuid), network communications (connect, sendto), process creation (fork, execve), and access to protected system resources. This makes strace indispensable for dynamic malware analysis on Linux, as emphasized in CHFI v11.

NEW QUESTION: 217

Which of the following commands shows you the NetBIOS name table each?

A. nbtstat -n

B. nbtstat -r

C. nbtstat -c

D. nbtstat -s

Answer: A (LEAVE A REPLY)

NEW QUESTION: 218

An investigator is working on a complex financial fraud case involving multiple government agencies. As part of the investigation, the investigator seeks to acquire certain government records to help uncover potentially fraudulent activities and determine the full scope of the crime. However, one of the government agencies involved denies access to some of the requested records, citing national security concerns and invoking a statutory exemption. Which law governs the investigator's right to request these records, and which exemption might prevent disclosure?

A. The Federal Records Act of 1950

B. The Freedom of Information Act (FOIA)

C. The National Information Infrastructure Protection Act of 1996
D. The Protect America Act of 2007
Answer: B (LEAVE A REPLY)
According to theCHFI v11 Regulations, Policies, and Ethicsmodule, theFreedom of Information Act (FOIA)is the primary U.S. federal law that governs an investigator's right to request access to records held by government agencies. FOIA establishes a legal framework that promotestransparency and accountabilityby allowing investigators, journalists, and the public to obtain government records, subject to specific statutory exemptions.
CHFI v11 clearly explains that while FOIA provides broad access rights, it also includesnine exemptionsthat allow agencies to lawfully withhold information. One of the most significant and commonly invoked exemptions isExemption 1, which protects information related tonational security, including classified defense, intelligence, and foreign policy information. If disclosure of records could reasonably be expected to harm national security, agencies are legally permitted to deny access.
The other laws listed do not govern public or investigative access to government records in this manner. The Federal Records Act of 1950focuses on records management and preservation, not disclosure rights. The National Information Infrastructure Protection Act of 1996addresses cybercrime offenses, and theProtect America Act of 2007relates to foreign intelligence surveillance authorities.
CHFI v11 emphasizes that forensic investigators must understandFOIA limitations and exemptionsto set realistic expectations during multi-agency investigations and to remain compliant with legal and ethical boundaries. Therefore, the correct and CHFI v11-verified answer isThe Freedom of Information Act (FOIA), makingOption Bcorrect.

NEW QUESTION: 219
A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM.
Where is the hidden swap file in Windows located?
A. C:\hiberfil.sys
B. C:\ALCSetup.log
C. C:\pagefile.sys
D. C:\config.sys
Answer: C (LEAVE A REPLY)

NEW QUESTION: 220
Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?
A. grep
B. fsck
C. pgrep

D. dmesg
Answer: D (LEAVE A REPLY)

NEW QUESTION: 221
During a large-scale financial investigation in Chicago, Illinois, forensic analysts encounter a corporate RAID array used for archiving transaction records. When examining the array, they find that data and parity information are distributed across multiple disks, allowing the system to continue functioning if two drives fail simultaneously. Which RAID configuration best matches this forensic observation of dual-drive fault tolerance?
A. RAID 5
B. RAID 0
C. RAID 6
D. RAID 1
Answer: C (LEAVE A REPLY)
The correct answer is C because RAID 6 uses distributed parity and is designed to tolerate the failure of any two drives in the array. Storage references and vendor documentation describe RAID 6 as similar to RAID 5 but with an additional parity block arrangement that allows continued operation after two simultaneous disk failures. That matches the scenario exactly. RAID 5 also distributes parity, but it only tolerates a single drive failure. RAID 0 offers striping with no redundancy at all, and RAID 1 relies on mirroring rather than the distributed data-plus-parity design described in the question. CHFI v11 includes RAID storage systems and the logical structure of disks, so candidates are expected to know how fault tolerance differs across RAID levels. In forensic analysis of enterprise storage, recognizing the correct RAID configuration matters because it affects data availability, reconstruction strategy, and interpretation of how evidence survives hardware faults. Since the array continues functioning after two drive failures with distributed parity, the correct answer is RAID 6. (ibm.com)

NEW QUESTION: 222
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?
A. Steganalysis
B. Typography
C. Picture encoding
D. Steganography
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
During a service-manipulation investigation at a logistics company in Columbus, Ohio, an examiner reviews the Windows System log from a compromised workstation. The timeline

shows an entry indicating that a request was issued to stop a critical service, but the service did not immediately transition to a stopped state.
To correctly interpret this log entry and distinguish intent from outcome, the examiner must understand what the recorded event represents. What does Event ID 7035 indicate in this context?
A. A custom application event written by logevent.exe
B. A Windows service successfully transitioned to a started or stopped state
C. A control request was sent to a service to start or stop
D. A remote-access connection recorded in the Application log
Answer: C (LEAVE A REPLY)
The correct choice is C because Event ID 7035 from the Service Control Manager records that a control command was sent to a service, such as a start or stop request. It documents the issuance of the command, not the final service state. That distinction is important in forensic analysis because a stop request may appear in the timeline even if the service fails to stop, delays stopping, or transitions later. Option B more closely describes a successful state change, which is typically associated with a different event pattern such as 7036.
In a CHFI v11 context, this fits the objective on Windows event logs, organization of event records, and the use of log files as evidence. Examiners are expected not only to read logs, but to interpret what an event actually means in operational terms. Here, the event shows administrative or malicious intent to manipulate the service, which can be highly relevant in persistence or sabotage investigations. For that reason, the most accurate interpretation is that a start or stop control request was sent to the service.

NEW QUESTION: 224
What hashing method is used to password protect Blackberry devices?
A. RC5
B. SHA-1
C. MD5
D. AES
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
During a complex investigation, an investigator is tasked with extracting email data from a corrupt file format generated by the organization ' s email client. The investigator requires a tool capable of converting this file into the widely compatible EML format, ensuring that the data is easily accessible for analysis. The tool must also support migration to various email servers and web-based platforms, with advanced filtering options to selectively migrate only relevant data. Which tool would be most suitable for this task?
A. Kernel for OST to PST
B. Email Checker

C. ZeroBounce
D. EmailSherlock
Answer: A (LEAVE A REPLY)
According to the CHFI v11 objectives under Email Forensics and Digital Evidence Examination , investigators must be capable of extracting, converting, and analyzing email data stored in proprietary or corrupt formats. Microsoft Outlook commonly stores mailbox data in OST (Offline Storage Table) files, which can become inaccessible or corrupt during incidents such as system crashes, insider attacks, or malware infections.
Kernel for OST to PST is a specialized forensic and eDiscovery tool designed to recover and convert OST files into accessible formats such as PST, EML, MSG, and MBOX . Its ability to export emails into EML format is particularly important in forensic investigations, as EML is widely supported by multiple forensic tools and email analysis platforms. CHFI v11 highlights the importance of using reliable tools that support selective extraction, filtering, and migration , allowing investigators to isolate relevant emails, attachments, headers, and metadata while maintaining evidence integrity.
Additionally, Kernel for OST to PST supports migration to various email servers and web-based platforms
, aligning with CHFI requirements for handling enterprise email evidence across heterogeneous environments.
The other options are unsuitable: Email Checker and ZeroBounce are email validation tools, and EmailSherlock focuses on email address investigation rather than mailbox data extraction.
Therefore, consistent with CHFI v11 best practices for email evidence acquisition and conversion , Kernel for OST to PST is the correct and exam-aligned answer

NEW QUESTION: 226
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. Opt for disk-to-image copying for the large suspect drive
B. Execute logical acquisition considering the one-time opportunity to capture data
C. Use a reliable data acquisition tool to make a copy of the original drive
D. Utilize DriveSpace or DoubleSpace to reduce the data size
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com

312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 227
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?
A. HKEY_USERS
B. HKEY_LOCAL_MACHINE
C. HKEY_CLASSES_ROOT
D. HKEY_CURRENT_CONFIG
Answer: C (LEAVE A REPLY)

NEW QUESTION: 228
Thomas, a cybersecurity analyst, is investigating a potential intrusion into a web server after receiving an alert for suspicious activity. Upon reviewing the IIS logs, he notices an unusually high number of requests coming from the same IP address within a short time period. These requests are spread across various times during the day and seem to target multiple resources on the server. Thomas suspects that the requests may be part of a larger attempt to scan for vulnerabilities or exploit a specific weakness. Which of the following log fields should Thomas focus on to better understand the nature of these requests?
A. sc-status (Status code)
B. cs-uri-stem (Requested URI)
C. cs-ip (Client IP address)
D. cs-user-agent (User-Agent string)
Answer: B (LEAVE A REPLY)
Option B. cs-uri-stem (Requested URI) is the best answer because the question is about understanding what resources were being targeted and whether the pattern suggests scanning, probing, or exploitation. CHFI v11 explicitly includes IIS Web Server Architecture and Logs , Analyzing IIS Logs , and investigating web attacks by examining server logs. The requested URI tells the investigator exactly which pages, scripts, directories, or endpoints the client attempted to access. That is crucial when determining whether a single IP is walking through administrative paths, probing known vulnerable resources, or repeatedly targeting a specific application component. It provides more insight into the nature of the activity than simply knowing the client IP, which is already known from the scenario.
sc-status is useful for checking whether requests succeeded, and cs-user-agent can help identify tools or automation, but neither is as central as the requested resource path when

the goal is to understand the intent and pattern of the requests. Therefore, under CHFI web-log analysis objectives, the most informative field here is cs-uri-stem .

NEW QUESTION: 229
Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads it to VirusTotal in order to confirm whether the file is malicious, provide information about its functionality, and provide information that will allow to produce simple network signatures. What type of malware analysis was performed here?
A. Static
B. Hybrid
C. Dynamic
D. Volatile
Answer: A (LEAVE A REPLY)

NEW QUESTION: 230
During a forensic investigation of a corporate workstation in Chicago, analysts notice that malicious executables continue to launch automatically every time the system is rebooted. Further inspection reveals that the malware inserted instructions into the Windows registry to ensure persistence. Which Windows AutoStart registry location enables a program to execute at each user logon, supporting recurring persistence after reboot?
A. Run
B. RunOnce
C. RunServicesOnce
D. RunServices
Answer: A (LEAVE A REPLY)
The right answer is A because the Windows Run key is intended to launch a program every time a user logs on, which makes it a classic registry-based persistence mechanism for malware. In contrast, RunOnce is designed for one-time execution and is removed after processing, so it does not best match the wording about recurring execution after reboot. The CHFI v11 blueprint specifically covers registry-based malware persistence mechanisms and identifying how malicious software survives restarts. That objective expects candidates to distinguish one-time startup artifacts from repeat-execution startup artifacts. From a forensic angle, the Run key is highly valuable because it can show how a threat repeatedly re-establishes itself, launches payloads, or triggers follow-on scripts whenever a user session begins. This kind of persistence is commonly examined alongside other startup evidence such as services, scheduled tasks, and startup folders. Microsoft's own documentation states that the Run key makes a program run every time the user logs on, while RunOnce executes only one time. That makes Run the only answer that fully matches the persistence behavior described in the question.

NEW QUESTION: 231
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. Audit the application security and IAM configurations within the enterprise's AWS services
B. Conduct a full review of AWS's global infrastructure including regions, availability zones, and edge locations
C. Check for security vulnerabilities in AWS container services' OS and application platform
D. Investigate AWS's underlying infrastructure including hardware and databases for security flaws
Answer: A (LEAVE A REPLY)

NEW QUESTION: 232
During an insider data theft investigation at a software company in San Jose, California, a forensic examiner must select the most appropriate data acquisition format to ensure broad compatibility with analysis tools while avoiding compression and metadata overhead. What format should be chosen by the examiner?
A. Proprietary format
B. Raw format
C. AFF format
D. AFF4 format
Answer: B (LEAVE A REPLY)
Raw format creates a simple bit-for-bit image of the source media without compression or added metadata overhead. It is widely supported by forensic and general analysis tools, making it appropriate when broad compatibility is the priority.

NEW QUESTION: 233
During a forensic recovery operation at a defense contractor's research facility in Denver, Colorado, analysts are restoring corrupted evidence drives from a rack-mounted workstation. The drives require simultaneous bidirectional data transfer and redundancy between multiple controllers to maintain availability, even if one path fails. Based on these operational requirements, which disk interface would provide the most reliable connection for this environment?
A. Serial ATA (SATA)
B. Small Computer System Interface (SCSI)
C. Peripheral Component Interconnect Express (PCIe)
D. Serial Attached SCSI (SAS)
Answer: (SHOW ANSWER)

Serial Attached SCSI provides full-duplex communication, supports multiple controllers through dual-porting, and offers enterprise-grade reliability and redundancy. These features make it suitable for high-availability rack-mounted systems where drives must remain accessible even if one data path fails.

NEW QUESTION: 234
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, "X" represents the _____.
A. Original file name
B. Drive name
C. Sequential number
D. Original file name's extension
Answer: (SHOW ANSWER)

NEW QUESTION: 235
A forensic investigator has collected a compromised Amazon Echo Dot and a smartphone from a crime scene. The Alexa app on the smartphone is synced with the Echo Dot. To begin investigating these devices, the investigator needs to obtain certain artifacts. In this scenario, which of the following sequence of steps should the investigator follow to acquire the necessary artifacts for a client-based analysis?
A. Generate an image of the firmware -> Retrieve database files using the adb pull command -> Parse database files -> Conduct data analysis
B. Retrieve database files using the adb pull command -> Generate an image of the firmware -> Parse database files -> Conduct data analysis
C. Parse database files -> Retrieve database files using the adb pull command -> Generate an image of the firmware -> Conduct data analysis
D. Retrieve database files using the adb pull command -> Parse database files -> Generate an image of the firmware -> Conduct data analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
A seasoned forensic investigator is assigned a case involving an international drug trafficking operation. The main suspect in the case allegedly uses the dark web to communicate with his network. While analyzing the suspect's computer, the investigator found a string
"LC_CTYPE=en_US.UTF-8". In what artifact is the investigator most likely to encounter this string?
A. TOR Command Prompt history
B. TOR Windows Registry key
C. TOR Prefetch file
D. Malware binary

Answer: A (LEAVE A REPLY)
The string "LC_CTYPE=en_US.UTF-8" is an environment variable typically set in command-line environments. It is commonly found in command prompt or shell history associated with running TOR, rather than in registry keys, prefetch files, or binaries.

NEW QUESTION: 237
What is one method of bypassing a system BIOS password?
A. Removing the CMOS battery
B. Login to Windows and disable the BIOS password
C. Remove all the system memory
D. Removing the processor
Answer: A (LEAVE A REPLY)

NEW QUESTION: 238
Jessica is conducting a forensic analysis on a Windows machine suspected of being involved in data exfiltration. She wants to identify any suspicious login attempts and track the number of failed login attempts to see if a brute-force attack was attempted. Which of the following event IDs will provide this information?
A. 4732
B. 4727
C. 4758
D. 4625
Answer: (SHOW ANSWER)
Event ID 4625 in Windows Security logs records failed logon attempts, including details such as the account used, source IP, and failure reason, which helps identify patterns consistent with brute-force attacks.

NEW QUESTION: 239
In a corporate setting, a Security Operations Center (SOC) is responsible for monitoring and protecting the organization ' s digital assets. Consider a situation where an organization is experiencing a series of suspicious network activities. The SOC team needs to identify the appropriate technology to detect and mitigate these potential threats effectively. Which technology should the SOC team primarily utilize to monitor and analyze security events in real time?
A. Password Management Software
B. Security Information and Event Management (SIEM) System
C. Vulnerability Assessment Tool
D. Data Loss Prevention (DLP) Solution
Answer: B (LEAVE A REPLY)
According to the CHFI v11 objectives related to Network Forensics, Incident Detection, and SOC Operations , the primary technology used by a Security Operations Center (SOC) to

monitor, correlate, and analyze security events in real time is a Security Information and Event Management (SIEM) system .
A SIEM system centrally collects logs and events from multiple sources such as firewalls, IDS/IPS, servers, endpoints, applications, authentication systems, and network devices. It then performs real-time correlation, normalization, alerting, and analysis to identify suspicious patterns such as brute-force attacks, lateral movement, malware activity, data exfiltration attempts, and insider threats. CHFI v11 emphasizes SIEM solutions as a core component for incident detection, investigation, and evidence correlation within SOC environments.
The other options do not meet this requirement. Password Management Software focuses on credential storage and rotation, not threat monitoring. Vulnerability Assessment Tools are used for periodic scanning to identify weaknesses, not real-time event analysis. Data Loss Prevention (DLP) solutions are designed to prevent unauthorized data leakage but do not provide comprehensive, centralized security event correlation across the enterprise.
CHFI v11 explicitly highlights the use of SIEM solutions for centralized logging, real-time monitoring, and forensic investigation support , making them essential for SOC teams dealing with active threats.
Therefore, the correct and CHFI-verified answer is Security Information and Event Management (SIEM) System (Option B) .

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

NEW QUESTION: 241
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. Utilize Redline to perform Indicators of Compromise (IOC) analysis and construct a timeline of potential cyber incidents
B. 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
C. Apply Handle.exe to see the object types and names of all the handles of the crashed programs

D. Use the Process Dumper tool to dump the entire process space and analyze the contents in the RAM dump file
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 242
Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?
A. ISO 9660
B. IEC 3490
C. ISO/IEC 13940
D. ISO 9060
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
Sophia, a forensic expert, is analyzing a system for signs of malware. She observes that the malware has been modifying Windows services and running processes to ensure its operation in the background without detection. She needs to determine which services are automatically starting when the system boots. Which tool should Sophia use to examine the Windows services that are set to start automatically?
A. Autoruns
B. Task Manager
C. Process Explorer
D. Event Viewer
Answer: A (LEAVE A REPLY)
Autoruns displays all programs and services configured to run automatically at system startup, allowing investigators to identify persistence mechanisms used by malware.

NEW QUESTION: 244
Lucas, a forensic investigator, encounters a laptop during his investigation that is locked with a BIOS password. The laptop's owner does not remember the BIOS password, and Lucas needs to bypass it in order to continue the forensic analysis. He decides to use a

method that involves removing and reinserting the CMOS battery. What is the purpose of removing the CMOS battery in this scenario?
A. To remove encryption from the hard drive
B. To bypass user account passwords
C. To reset the system password in BIOS
D. To reset the BIOS password
Answer: D (LEAVE A REPLY)
Removing and reinserting the CMOS battery clears the stored BIOS settings, including the BIOS password, effectively resetting it and allowing access to the system firmware configuration.

NEW QUESTION: 245
In a suspected malware outbreak at a financial services company in Chicago, investigators observe that the organization's mail server is relaying suspicious traffic and generating unusual message errors across multiple user accounts. The behavior suggests that the system may be compromised and distributing unsolicited messages. What indicator of malware should investigators prioritize to validate this suspicion?
A. Alerts of spam messages from the system or email
B. Numerous unwanted emails and social posts
C. System slowdown and longer reboot times
D. Unexplained bounced emails
Answer: A (LEAVE A REPLY)
Spam alerts from the system or email infrastructure directly indicate that the mail server or user accounts may be compromised and sending unsolicited messages. This evidence best validates suspected malware-driven spam distribution from the organization's environment.

NEW QUESTION: 246
Following a cybersecurity incident at an organization, a forensic investigator is tasked with collecting Electronically Stored Information (ESI) as part of the investigation. To streamline the data collection process, the investigator restricts the range and size of ESI from custodians, limiting the collection to specific file types and directories on a computer. This approach ensures that only relevant information is collected while minimizing the impact on other devices. Which eDiscovery collection methodology is being used in this scenario?
A. Investigator leverages custodian self-collection to gather sensitive evidence data.
B. Investigator uses incremental collection, focusing on newly created or modified data.
C. Investigator uses remote acquisition of data from custodians ' systems via network connections.
D. Investigator employs a directed collection of definite data sets and system areas.
Answer: D (LEAVE A REPLY)

As defined in the CHFI v11 Procedures and Methodology domain, directed collection is an eDiscovery methodology in which investigators deliberately limit evidence collection to specific data sets, file types, directories, custodians, or system areas that are known or highly likely to contain relevant information. This approach is commonly used to reduce data volume, minimize business disruption, and lower legal and operational costs while maintaining forensic relevance.
In the given scenario, the investigator intentionally restricts the scope of ESI by targeting specific directories and file types , rather than collecting full disk images or all user data. CHFI v11 explicitly describes this as directed (or targeted) collection , which is aligned with the Electronic Discovery Reference Model (EDRM) best practices. Directed collection helps investigators remain compliant with legal proportionality requirements and reduces exposure to irrelevant or private third-party data.
The other options do not match the scenario. Custodian self-collection introduces risk and is generally discouraged due to evidence integrity concerns. Incremental collection focuses on changes since a prior collection, not selective scope reduction. Remote acquisition refers to the method of access, not the collection strategy itself.
CHFI v11 emphasizes directed collection as a preferred methodology when investigators already understand where relevant evidence resides and need to collect it efficiently and defensibly. Therefore, the correct and CHFI v11-verified answer is directed collection of definite data sets and system areas , making Option D correct.

NEW QUESTION: 247
In event correlation, two types are discussed: Same-Platform, where a single OS is used throughout (e.g., Microsoft Windows), and Cross-Platform, where different OS and hardware are employed (e.g., Windows clients with a Linux firewall). In Cross-Platform Correlation, which scenario best illustrates its application?
A. Implementing uniform software versions throughout the network
B. Utilizing Windows servers and Linux-based firewalls
C. Using Linux-based servers exclusively
D. Employing different antivirus software across devices
Answer: B (LEAVE A REPLY)
Event correlation in CHFI v11 is a critical investigative technique used to reconstruct attack timelines by analyzing and correlating events from multiple log sources. The CHFI blueprint clearly distinguishes between Same-Platform Correlation and Cross-Platform Correlation under the domain of Image/Evidence Examination and Event Correlation .
Cross-Platform Correlation applies when an investigation involves heterogeneous environments , meaning different operating systems, hardware platforms, or network devices are involved in the incident. A common real-world example-explicitly referenced in CHFI training-is an enterprise environment where Windows-based client systems or servers interact with Linux-based infrastructure components such as firewalls, IDS/IPS devices, or proxies . In such cases, investigators must correlate Windows Event Logs with

Linux syslogs, firewall logs, and network device records to build a unified timeline of attacker activity.
Option B correctly reflects this scenario by describing the use of Windows servers alongside Linux-based firewalls , which is a textbook example of Cross-Platform Correlation. Option A relates to standardization, not correlation. Option C represents a single-platform environment, and Option D refers to security tooling diversity rather than operating system or platform diversity.
CHFI v11 emphasizes Cross-Platform Correlation as essential for detecting multi-stage attacks , lateral movement, and perimeter breaches in modern hybrid infrastructures, making Option B the correct and exam- aligned answer

NEW QUESTION: 248
What is the first step that needs to be carried out to crack the password?
A. If it matches, that password has been cracked and the password cracker displays the unencrypted version of the password
B. The hashed wordlist is compared against the target hashed password, generally one word at a time
C. A word list is created using a dictionary generator program or dictionaries
D. The list of dictionary words is hashed or encrypted
Answer: C (LEAVE A REPLY)

NEW QUESTION: 249
What is the smallest physical storage unit on a hard drive?
A. Track
B. Platter
C. Sector
D. Cluster
Answer: C (LEAVE A REPLY)

NEW QUESTION: 250
Elena, a forensic investigator, is analyzing the behavior of a suspected malware infection. During her analysis, she notices several abnormal entries in the Windows Event Logs, specificallyEvent ID 5156. What key information can Elena expect from these logs that could help her trace the malicious activity?
A. The username and password used for unauthorized access
B. The location of the file that was deleted by the malware
C. The malicious process's registry key modification details
D. The name of the process and the IP address it communicated with
Answer: D (LEAVE A REPLY)
According to theCHFI v11 Operating System and Malware Forensics objectives,Windows Event ID 5156 is generated by theWindows Filtering Platform (WFP)and indicates that a

network connection has been permitted. This event is highly valuable in malware investigations because it records detailed information aboutprocess-level network activity, which is a common indicator of compromise.
Event ID 5156 logs typically include:
* Process name and Process ID (PID)that initiated the network connection
* Source and destination IP addresses
* Source and destination ports
* Protocol used (TCP/UDP)
* Direction of the connection (inbound or outbound)
CHFI v11 explicitly highlights the importance ofWindows Security Event Logsin tracing malware behavior, especially for identifyingcommand-and-control (C2) communications, data exfiltration attempts, and lateral movement. By analyzing Event ID 5156, investigators can directly correlate aspecific executable or malicious processwithexternal IP addresses, helping establish attacker infrastructure and timelines.
The other options are incorrect because Event ID 5156 does not record credentials, file deletion paths, or registry modification details. Those artifacts are found in other event IDs or forensic sources such as registry hives, file system metadata, or Sysmon logs.
Therefore, the key forensic value ofEvent ID 5156lies in revealingthe process responsible for the network communication and the IP address it connected to, makingOption Dthe correct and CHFI v11-verified answer.

NEW QUESTION: 251
How many bits is Source Port Number in TCP Header packet?
A. 64
B. 16
C. 32
D. 48
Answer: B (LEAVE A REPLY)

NEW QUESTION: 252
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 \Schedule
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
Answer: (SHOW ANSWER)

NEW QUESTION: 253
Your team has identified unusual traffic patterns from a server in the corporate network. Upon investigation, you find multiple established connections to unfamiliar foreign IP addresses. After capturing the network traffic for analysis, you notice that the traffic content seems random and does not correspond to any known protocol. What might this suggest?
A. The server is part of a botnet.
B. The server is communicating with a Command and Control server.
C. The server is infected with ransomware.
D. The server is under a DDoS attack.
Answer: (SHOW ANSWER)
Option B is the best answer because the scenario describes established outbound connections to unfamiliar foreign IP addresses with traffic that appears random or nonstandard , which strongly suggests encrypted or obfuscated communications with a command-and-control (C2) server . CHFI v11 explicitly includes Analyze Traffic to Detect Malware Activity , Indicators of Compromise (IoC) , and identifying suspicious network behavior associated with malware operations.
Command-and-control traffic often appears unusual because it may use custom protocols, encrypted payloads, or covert communications that do not match ordinary business applications. The fact that the connections are persistent and outbound to unknown external infrastructure is a classic indicator of a compromised host maintaining contact with an attacker-controlled system.
A botnet is possible at a broader level, but the most direct interpretation of the observed traffic is active communication with a C2 server . Ransomware is not the best answer from network evidence alone, and DDoS would typically show different traffic characteristics.
Therefore, under CHFI network-forensics objectives, this pattern most strongly indicates communication with a Command and Control server .

NEW QUESTION: 254
During a forensic investigation of a cyberattack, the team is tasked with reconstructing the timeline of events to trace the attacker ' s actions within the compromised network. However, as they delve into system logs and critical documents, the forensic team notices discrepancies-files that should have been altered during the attack show timestamps indicating they were modified after the attacker had already left the system. Backup and system logs further reveal unusual patterns, with some files appearing to have been modified during regular operational hours, suggesting tampering to conceal the true sequence of events.
These inconsistencies raise suspicions among the investigators that the attacker may have intentionally manipulated the timestamps of critical files to disrupt the forensic timeline. This tactic, aimed at confusing the team and hindering their ability to reconstruct the breach, points to a deliberate effort to mislead the investigation, making it appear as

though the malicious activities were part of normal operations. Which anti- forensics technique does this behavior most likely represent?
A. Artifact wiping to remove all traces of unauthorized activity from the system.
B. Alternate Data Streams (ADS) to store and hide malicious files in a way that avoids detection.
C. Trail obfuscation by corrupting the file metadata.
D. Program packers to compress and conceal executable files, making them harder to analyze.
Answer: (SHOW ANSWER)
Option C is the best answer because the scenario describes deliberate manipulation of timestamps and metadata to confuse investigators and distort the event timeline. CHFI v11 explicitly lists Trail Obfuscation and Overwriting Data/Metadata among the major anti-forensics techniques , and it also emphasizes timeline analysis , metadata investigation , and the need to detect actions intended to mislead forensic reconstruction.
This kind of behavior is a classic form of trail obfuscation . By altering file times and related metadata, the attacker attempts to make malicious actions appear normal or unrelated, thereby undermining the investigator' s ability to accurately reconstruct the incident. That is more specific than general artifact deletion and better matches the facts in the question. Artifact wiping would focus on removing evidence entirely, ADS hides data in alternate streams, and program packers conceal executable content. None of those directly explain manipulated timestamps intended to falsify chronology. Therefore, within CHFI's anti-forensics framework, the most accurate classification is trail obfuscation through tampering with file metadata .

NEW QUESTION: 255
Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?
A. WarFlying
B. WarDhving
C. WarChalking
D. WarWalking
Answer: (SHOW ANSWER)

NEW QUESTION: 256
What layer of the OSI model do TCP and UDP utilize?
A. Network
B. Data Link
C. Transport
D. Session
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 257
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: 258
During an intellectual property breach inquiry at a publishing house in New York, the director provides consent for examiners to inspect company laptops. Before any device handling begins, an additional individual is present to validate that the authorization was properly executed. Which responsibility best explains the purpose of that individual ' s presence?
A. Determines whether one or more witness signatures are required
B. Confirms the agreement was voluntarily signed by the parties
C. Provides testimony or attends court if required
D. Ensures seizure authority based on the investigator ' s role
Answer: B (LEAVE A REPLY)
The correct answer is B because, in a consent-based forensic examination, the role of the witness is to confirm that the consent was knowingly and voluntarily given by the person authorizing the search. Under the CHFI v11 blueprint, investigators are expected to understand seeking consent, obtaining witness signatures, search and seizure procedures, and best practices for handling digital evidence. A witness is not primarily present to decide legal authority, and the witness does not create seizure powers for the examiner. Instead, the witness helps support the validity of the consent process by confirming that the agreement was actually signed and that it was not coerced or improperly obtained. This can become especially important later if the defense challenges whether the examination was authorized. Option A refers to deciding procedural requirements, which is not the witness's core function. Option C may happen in some cases, but it is not the main reason the witness is present at the time of signing. CHFI emphasizes defensibility and proper evidence-handling foundations, so validating voluntary consent is the best answer.

NEW QUESTION: 259
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?
A. Thorough
B. Complete event analysis
C. Point-to-point
D. End-to-end
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
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. NDF because it can store additional data separate from the primary data file
B. MDF because it stores all data in the database objects
C. LDF because it holds the log information associated with the database
D. Page Header because it contains metadata about the page like page ID, page type
Answer: (SHOW ANSWER)

NEW QUESTION: 261
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?
A. Slack Space
B. MFT
C. Metadata
D. Sector
Answer: A (LEAVE A REPLY)

NEW QUESTION: 262
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. Bit-by-bit Acquisition
B. Bit-stream disk-to-disk Acquisition
C. Static Acquisition
D. Sparse or Logical Acquisition
Answer: D (LEAVE A REPLY)

NEW QUESTION: 263

During a forensic investigation of a compromised system, the investigator is analyzing various forensic artifacts to determine the nature and scope of the attack. The investigator is specifically looking for information related to failed sign-in attempts, security policy changes, alerts from intrusion detection systems, and unusual application malfunctions. Which type of forensic artifact is most likely to contain this critical information?

A. Cryptographic artifacts that store information about encryption and decryption operations.

B. Browser artifacts that track user browsing history and website interactions.

C. Process and memory artifacts that contain information about running processes and system memory.

D. Log file anomalies that provide detailed records of events and errors on the device.

Answer: D (LEAVE A REPLY)

This question aligns directly with CHFI v11 objectives under Computer Forensics Fundamentals and Log Analysis . Log files are among the most critical forensic artifacts because they provide a chronological and authoritative record of system, security, and application events . CHFI v11 emphasizes that logs are essential for reconstructing attack timelines, identifying unauthorized access attempts, and determining the scope of a compromise.

Artifacts such as failed sign-in attempts , security policy modifications , IDS alerts , and application errors are routinely recorded in log sources including Windows Security logs, system logs, application logs, firewall logs, and IDS/IPS logs. These logs allow investigators to correlate events across systems, identify brute-force attacks, detect privilege escalation, and recognize abnormal behavior caused by malware or misconfiguration.

Cryptographic artifacts focus on key usage and encryption operations, browser artifacts relate to user web activity, and process or memory artifacts provide insight into live execution states-but none provide the comprehensive, event-based historical visibility required to answer all aspects of the question. CHFI v11 highlights log analysis as the primary method for understanding what happened, when it happened, how it happened, and who was involved . Therefore, log file anomalies are the most relevant and reliable forensic artifacts in this scenario.

NEW QUESTION: 264

What will the following command accomplish?

dd if=/dev/xxx of=mbr.backup bs=512 count=1

A. Restore the master boot record

B. Back up the master boot record

C. Mount the master boot record on the first partition of the hard drive

D. Restore the first 512 bytes of the first partition of the hard drive

Answer: (SHOW ANSWER)

NEW QUESTION: 265
A company has been sending promotional emails to its customers as part of an ongoing marketing campaign.
However, the company begins to receive multiple complaints from recipients stating that they are unable to unsubscribe from future emails. Customers express frustration as they report that the unsubscribe link, which is legally required to be included in every commercial email, is either completely missing from the emails or not functioning as intended. This prevents recipients from easily opting out of receiving further communications, which directly violates the provisions of the CAN-SPAM Act. The absence or malfunctioning of the unsubscribe feature has caused significant dissatisfaction among the recipients and is now a point of concern for the company.
The company is now under investigation by the Federal Trade Commission (FTC) for potential violations of the CAN-SPAM Act, which sets rules for commercial email practices. The company is facing legal action, and the authorities are examining whether they failed to comply with key provisions of the CAN-SPAM Act, such as the requirement for clear and accessible unsubscribe options and truthful subject lines. What violation of the CAN-SPAM Act is the company most likely being investigated for?
A. The company did not include the necessary email signature with the sender's valid postal address, which led to a violation of the CAN-SPAM Act.
B. The company failed to honor opt-out requests, violating the law ' s requirement.
C. The company used false header information in the emails, which is a direct violation of the law's provisions.
D. The company allowed a hacker to access their email system and use it for unauthorized spam activity.
Answer: B (LEAVE A REPLY)
Option B is the best answer because the question centers on recipients being unable to unsubscribe from future commercial emails. Under the CAN-SPAM framework, one of the core compliance requirements is that recipients must be given a clear and functioning opt-out mechanism , and those opt-out requests must be honored properly. The scenario directly describes failure in that area.
The other options describe different types of possible CAN-SPAM-related issues, but they do not match the facts as closely. A missing postal address can be a compliance problem, and false header information is also a separate violation, but the question repeatedly emphasizes the missing or nonworking unsubscribe mechanism. The involvement of a hacker is not the issue being examined here.
From a CHFI legal-awareness perspective, investigators must be able to identify the regulatory issue most directly supported by the evidence. Since the complaints are specifically about customers being unable to stop future emails, the most accurate conclusion is that the company is being investigated for failing to honor or properly provide opt-out functionality , which violates the CAN-SPAM Act.

NEW QUESTION: 266
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution.
Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
A. gwcheck.db
B. PRIV.STM
C. PUB.EDB
D. PRIV.EDB
Answer: (SHOW ANSWER)

NEW QUESTION: 267
During a forensic investigation, an investigator opens a file using a hex editor and examines the binary data. While analyzing the content, the investigator observes the presence of both "00" and
"FF" byte values spread across different sections of the file. These byte sequences appear repeatedly, filing large areas of the file. What might these values signify in the context of file analysis?
A. File padding or unused data, often used to ensure the file reaches a required size or alignment.
B. File compression, indicating the presence of compressed data or blocks of repeated patterns.
C. Encrypted data, where these byte values represent encoded content that can only be decrypted with the proper key.
D. Data corruption, suggesting the file may be damaged or incomplete.
Answer: A (LEAVE A REPLY)
Repeated "00" and "FF" byte values commonly indicate padding or unused space within a file, used for alignment or to fill allocated storage regions rather than representing meaningful data.

NEW QUESTION: 268
Software firewalls work at which layer of the OSI model?
A. Application
B. Network
C. Transport
D. Data Link
Answer: A (LEAVE A REPLY)

NEW QUESTION: 269

In an investigation involving a corporate data breach, the forensic investigator is tasked with recovering deleted files from a suspect's hard drive. The investigator is careful to confirm that the hard drive remains untouched and reliable, so they create aforensic imageof the device and store it in a secure location to maintain its integrity for future analysis. This step is crucial to guarantee that the original data remains unaltered during the investigative process.

Which responsibility of a forensic investigator is being fulfilled in this scenario?

A. Ensuring appropriate handling and preservation of evidence.

B. Engaging with law enforcement and stakeholders during the investigation.

C. Creating structured reports for the court of law.

D. Reconstructing the damaged storage devices to recover hidden information.

Answer: (SHOW ANSWER)

According to theCHFI v11 Computer Forensics Fundamentalsmodule, one of thecore responsibilities of a forensic investigatoris to ensure theproper handling, preservation, and integrity of digital evidence. This responsibility is foundational to the entire forensic process and directly impacts theadmissibility of evidence in court.

In the given scenario, the investigator creates aforensic imageof the suspect's hard drive rather than working directly on the original media. CHFI v11 explicitly states that investigators must always perform analysis on a bit-by-bit forensic copywhile preserving the original evidence in a secure, controlled environment. This practice prevents accidental modification, contamination, or destruction of original data and ensures compliance with thebest evidence ruleandchain of custody requirements.

The act of securely storing the original drive and working only on the forensic image demonstrates strict adherence to evidence preservation principles. While recovering deleted files is an investigative goal, the scenario emphasizesmaintaining integrity and preventing alteration, which aligns directly with evidence handling and preservation-not reporting, stakeholder engagement, or device reconstruction.

CHFI v11 consistently reinforces that failure to preserve evidence properly can lead tolegal challenges, evidence exclusion, or case dismissal, regardless of the quality of the technical analysis performed.

Therefore, the responsibility being fulfilled in this scenario-fully aligned with CHFI v11-isensuring appropriate handling and preservation of evidence, makingOption Athe correct answer.

NEW QUESTION: 270

At a multi-agency digital-forensics laboratory in Denver, Colorado, investigators must extract evidence from a drone, a smart TV, and a wearable device as part of a joint investigation. The devices span heterogeneous consumer and embedded platforms, and the team requires a single forensic solution capable of performing both low-level and filesystem-level acquisition across this mixed environment without switching between specialized tools. Which tool best meets these requirements?

A. MD-NEXT
B. MOBILedit Smartwatch Kit
C. MD-Drone
D. IoT Inspector
Answer: A (LEAVE A REPLY)
MD-NEXT is designed for forensic acquisition and analysis across heterogeneous embedded and IoT-type devices. It supports both low-level and filesystem-level acquisition, making it suitable for extracting evidence from mixed devices such as drones, smart TVs, and wearables without relying on separate specialized tools.

NEW QUESTION: 271
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. Memory storage engine, because it offers in-memory tables and implements a hashing mechanism for faster data retrieval
B. BDB storage engine, because it provides an alternative to InnoDB and supports additional transaction methods such as COMMIT and ROLLBACK
C. MyISAM storage engine, because it offers unlimited data storage and high-speed data loads
D. InnoDB storage engine, because it supports traditional ACID and crash recovery, and is used in online transaction processing systems
Answer: D (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 272
While reviewing Cisco IOS logs for suspicious network traffic, an administrator encounters a log message with the mnemonic " %SEC-6-IPACCESSLOGP.,' The message indicates that a packet matching the log criteria for the given access list has been detected, either for TCP or UDP traffic. Which of the following describes the log entry?

A. A packet matching the criteria defined in an access list has been allowed or denied, and it was logged for monitoring.
B. A system-level error has occurred, related to excessive network traffic.
C. A packet has been dropped due to an access control list (ACL) rule.
D. A failed connection attempt was detected on the network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 273
John, a forensic examiner, has been tasked with analyzing an evidence image file acquired from a suspect machine. While conducting his investigation, he discovered a file that appeared to be suspicious.
He opened the file in a Hex Editor and found the hex value of the file starting with "89 50 4E". Based on his analysis, which file type does this hex value correspond to?
A. PDF
B. JPEG
C. BMP
D. PNG
Answer: D (LEAVE A REPLY)
This question aligns with CHFI v11 objectives under Operating System Forensics and File Type and Encoding Analysis . In digital forensics, file signature analysis-also known as magic number analysis -is a critical technique used to identify the true file type regardless of its extension. Attackers often rename or disguise files to evade detection, making hex-level inspection essential during forensic examinations.
Each file format begins with a unique hexadecimal header that identifies its structure. The hex value "89 50
4E 47" corresponds to the ASCII representation of ‰PNG , which is the standard file signature for Portable Network Graphics (PNG) files. CHFI v11 specifically emphasizes the use of hex editors to analyze file headers and detect file extension mismatches during investigations.
The other options have different signatures: PDF files start with 25 50 44 46 (%PDF) , JPEG files typically begin with FF D8 FF , and BMP files start with 42 4D (BM) . Since the observed hex value matches the PNG signature, the correct identification is PNG. This technique is vital for uncovering hidden or obfuscated evidence and ensuring accurate file classification in forensic investigations.

NEW QUESTION: 274
What will the following command accomplish in Linux?
fdisk /dev/hda
A. Fill the disk with zeros
B. Format the hard drive
C. Delete all files under the /dev/hda folder

D. Partition the hard drive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 275
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?
A. Network credentials of the database
B. Operating system of the system
C. Name of the Database
D. Name of SQL Server
Answer: (SHOW ANSWER)

NEW QUESTION: 276
Which of the following techniques can be used to beat steganography?
A. Cryptanalysis
B. Encryption
C. Steganalysis
D. Decryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 277
James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the Investigation, he recovered certain deleted files from Recycle Bin to Identify attack clues.
Identify the location of Recycle Bin in Windows XP system.
A. Drive:\RECYCLER\
B. local/sha re/Trash
C. DriveARECYCLED
D. Drive:\$Recycle.Bin\
Answer: A (LEAVE A REPLY)

NEW QUESTION: 278
A digital forensics team is investigating a case involving the potential tampering of electronic evidence in a cybercrime investigation. In adherence to ENFSI Best Practices for Forensic Examination of Digital Technology , what would be their primary concern?
A. Analyzing cyberattack origin via IP tracking.
B. Employing advanced techniques for file recovery.
C. Determining cybercriminal motive for evidence tampering.
D. Verifying forensic imaging tools for accuracy.
Answer: (SHOW ANSWER)

According to the CHFI v11 syllabus under Standards and Best Practices Related to Computer Forensics , the ENFSI (European Network of Forensic Science Institutes) Best Practices for Forensic Examination of Digital Technology place strong emphasis on the reliability, accuracy, and validation of forensic tools and methods . When investigating potential evidence tampering, the foremost concern is ensuring that the tools used to acquire, image, and analyze digital evidence are forensically sound and produce repeatable, verifiable results .
Verifying forensic imaging tools for accuracy ensures that the data acquired is an exact and complete representation of the original evidence , with no alteration introduced during the acquisition or analysis process. This directly supports evidence integrity, chain of custody, and legal admissibility-core principles repeatedly highlighted in CHFI v11. Tool validation also helps investigators defend their findings in court by demonstrating that industry-recognized, tested, and approved tools were used.
The other options do not align with ENFSI's primary focus. IP tracking (Option A) relates to attribution, not evidence integrity. File recovery techniques (Option B) are investigative actions but secondary to tool reliability. Determining criminal motive (Option C) falls under criminal profiling rather than forensic examination standards.
Therefore, consistent with CHFI v11 objectives and ENFSI best practices , verifying the accuracy and reliability of forensic imaging tools is the primary concern when addressing potential evidence tampering

NEW QUESTION: 279
Detective Patel is investigating a cross-border cybercrime that impacted victims in the United States and Europe. To obtain timely evidence and coordinate actions across jurisdictions, which primary function of international agencies is most critical in this scenario?
A. Investigation
B. Collaboration
C. Policy and Regulation
D. Jurisdictional Response
Answer: B (LEAVE A REPLY)
International agencies primarily support cross-border cybercrime cases by enabling collaboration among countries, law enforcement bodies, and legal authorities. This coordination helps investigators obtain evidence, share intelligence, and synchronize actions across jurisdictions.

NEW QUESTION: 280
Camila, a system administrator, is tasked with investigating web traffic logs on a Windows-based server running IIS (Internet Information Services). She needs to find the location of the IIS log files in order to analyze the requests made to the server. Which of the following paths should Camila check to find the IIS log files?

A. /usr/local/etc/apache22/httpd.conf
B. /etc/httpd/conf/httpd.conf
C. /etc/apache2/apache2.conf
D. %SystemDrive%\inetpub
Answer: D (LEAVE A REPLY)
According to the CHFI v11 objectives under Web Application Forensics and Log Analysis, investigators must know the default log storage locations of commonly used web servers. On Windows-based systems, Internet Information Services (IIS) stores its web server logs within the inetpub directory, which resides on the system drive by default. The standard path used by IIS for logging HTTP and HTTPS requests is:
%SystemDrive%\inetpub\logs\LogFiles
In this question, the option %SystemDrive%\inetpub correctly points to the parent directory that contains IIS-related content, including the LogFiles directory where forensic-relevant web access logs are stored. These logs record critical details such as client IP addresses, request methods, requested URLs, HTTP status codes, timestamps, and user agents--key artifacts for reconstructing web-based attacks such as SQL injection, directory traversal, brute-force attempts, and malicious file uploads.

NEW QUESTION: 281
During an internal audit following suspected misuse of privileged credentials at a technology services firm, investigators must review detailed activity records related to configuration changes, API calls, and access attempts made across cloud-hosted resources. The organization operates entirely within a single cloud provider's infrastructure, and the investigation requires a native service that records management-plane actions with precise timestamps, source addresses, and request parameters for later reconstruction of user activity. Which platform would investigators rely on to reconstruct this activity timeline?
A. Google Workspace Logs Explorer
B. AWS CloudTrail
C. Azure Monitor Logs
D. Microsoft Sentinel
Answer: B (LEAVE A REPLY)
AWS CloudTrail records management-plane activity across AWS resources, including API calls, configuration changes, access attempts, timestamps, source IP addresses, and request details.
These records allow investigators to reconstruct user and service activity within an AWS environment.

NEW QUESTION: 282
You are a cybersecurity analyst tasked with performing dynamic malware analysis on a suspicious file received by your organization. Your objective is to understand the behavior

of the malware by running it in a controlled environment and monitoring its actions without allowing it to propagate to the production network.
As a cybersecurity analyst conducting dynamic malware analysis, what is a key aspect of designing the testing environment to ensure the safety of the production network?
A. Implementing host integrity monitoring to track system changes caused by the malware.
B. Disabling antivirus software to prevent interference with the malware's execution.
C. Running the malware on physical machines to minimize the risk of network propagation.
D. Using outdated operating systems to reduce compatibility issues with the malware.
Answer: A (LEAVE A REPLY)
According to theCHFI v11 Malware Forensics and Malware Analysis objectives, dynamic malware analysis must be performed in acontrolled, isolated, and well-monitored environmentto both observe malicious behavior and prevent unintended spread to production systems. A key requirement of such an environment is the ability tomonitor and record all system-level changesmade by the malware during execution.
Host Integrity Monitoring (HIM)plays a critical role in dynamic malware analysis by tracking modifications tofiles, registry keys, services, processes, startup locations, system calls, and configuration settings. CHFI v11 emphasizes system behavior analysis as a core component of malware forensics, including monitoring registry artifacts, file system changes, persistence mechanisms, and process activity. HIM enables investigators to safely analyze malware impact while maintaining forensic visibility and containment.
The other options are not aligned with CHFI v11 best practices.Disabling antivirus softwareweakens security controls but does not ensure containment or safety.Running malware on physical machines increases the risk of permanent damage and network propagation, which contradicts CHFI guidelines favoring sandboxed or virtualized environments.Using outdated operating systemsdoes not contribute to safety and may introduce irrelevant vulnerabilities.
CHFI v11 strongly advocatescontrolled malware analysis labswith monitoring mechanisms that capture behavioral indicators without exposing production assets. Therefore, implementinghost integrity monitoring is a key design aspect that supports bothsafe containment and effective behavioral analysis, makingOption Athe correct and CHFI-verified answer.

NEW QUESTION: 283
A forensic investigator is assigned to investigate a data leak involving the distribution of sensitive corporate information across multiple online platforms. The suspect is believed to have shared the data discreetly through various public channels. To uncover evidence, the investigator needs to collect posts, photos, videos, and user interactions from multiple networks. The investigator requires a tool that can efficiently gather, organize, and analyze this data, ensuring the integrity of the evidence for further investigation. Which tool would be best suited for this task?
A. LiME

B. Elastic Stack
C. Social Network Harvester
D. Guymager
Answer: C (LEAVE A REPLY)
This scenario aligns with CHFI v11 objectives under Network and Web Attacks and Social Media Forensics , where investigators are required to collect and analyze digital evidence from online platforms while preserving evidentiary integrity. When sensitive data is leaked through public or semi-public online channels, social media and online network artifacts such as posts, multimedia content, comments, likes, and user relationships become critical sources of evidence.
Social Network Harvester is specifically designed for social media and online platform investigations. It allows forensic investigators to systematically collect data such as posts, images, videos, timestamps, usernames, and interaction metadata from multiple social networks. CHFI v11 emphasizes the importance of using purpose-built tools that support structured collection, proper documentation, and evidence preservation to maintain chain of custody and admissibility.
LiME is a volatile memory acquisition tool, Elastic Stack is primarily used for log aggregation and analysis, and Guymager is a forensic disk imaging tool. None of these are suitable for harvesting social media content.
Therefore, Social Network Harvester is the most appropriate CHFI-aligned tool for efficiently gathering, organizing, and analyzing social network evidence in data leakage investigations.

NEW QUESTION: 284
A digital forensics lab is working on a high-profile cybercrime case. The director has decided to include a new team member in the investigation team for his specialized expertise. Which of the following considerations should be considered in the context of maintaining the lab's integrity, based on the given information?
A. The new team member should be allowed to bring his own hardware and software tools to the lab for investigation
B. The new team member should be given immediate access to the lab without maintaining a visitor's log register
C. The new team member should be directly handed the original hardware containing the evidence
D. The new team member should be provided with an electronic sign-in pass, and his entry should be logged in the register
Answer: D (LEAVE A REPLY)

NEW QUESTION: 285
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. Master File Table
B. Volume Boot Record
C. GUID Partition Table
D. Master Boot Record
Answer: A (LEAVE A REPLY)

NEW QUESTION: 286
A large corporation hired an independent marketing firm to manage its email advertising campaign. Subsequently, it was found that the firm was sending commercial emails without including necessary information about how to stop receiving emails in the future. In addition, they failed to honor the opt-out requests of the recipients within 10 business days. Under the CAN- SPAM Act, which of the following is true?
A. Neither the corporation nor the marketing firm would be held legally responsible for the violation
B. Only the corporation would be held legally responsible for the violation
C. The marketing firm alone would be held legally responsible for the violation
D. Both the corporation and the marketing firm could be held legally responsible for the violation
Answer: D (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 287
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. Squatting
C. Phreaking
D. Pretexting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 288
Emily, a system administrator, is tasked with automating the deployment of a custom service on a group of Windows servers in her organization. She has developed a script that will be used to add the new service to each server. The service will run a custom executable file that provides specific functionality for internal applications. To ensure that the service is created correctly, Emily needs to know which SrvMan command she should use to deploy the service to the system. Which of the following SrvMan commands should Emily use to create the new service?
A. srvman.exe add [service name] [display name] [/type:][/start:] [/interactive:no] [/overwrite:yes]
B. srvman.exe delete
C. srvman.exe stop [/nowait] [/delay:]
D. srvman.exe run [service name] [/copy:yes] [/overwrite:no] [/stopafter:]
Answer: (SHOW ANSWER)
The add command in SrvMan is used to create and install a new Windows service. It allows specifying the service name, display name, and configuration parameters such as startup type and behavior, which are required for deploying a custom service.

NEW QUESTION: 289
On the heels of a massive coordinated cyberattack, a multinational corporation called upon the services of veteran forensic investigator, Lisa. The attack infiltrated their MSSQL servers, and Lisa suspected the breach was a result of a sophisticated SQL Injection method that was executed from multiple sources and locations simultaneously. To determine the attack's origin, Lisa needs to not only collect but also examine the evidence files on the MSSQL server. To cope with the breach's scale and sophistication, which tool should Lisa rely on?
A. Nessus
B. EnCase
C. SQLsus
D. Sqlmap
Answer: D (LEAVE A REPLY)

NEW QUESTION: 290
What encryption technology is used on Blackberry devices Password Keeper?
A. AES
B. RC5
C. 3DES
D. Blowfish
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
A forensic team at a multinational corporation is investigating an alleged data breach. After thoroughly reviewing the system logs, the team discovers consistent outbound traffic from an internal system to a suspicious IP address linked with dark web activity. Upon inspecting the concerned system, they identify that the user had been using TOR for unsanctioned activities. To gather further evidence of TOR usage, which of the following techniques is least likely to yield substantial results?
A. Inspecting the Windows Registry for TOR-related entries.
B. Analyzing Command Prompt history for traces of TOR related commands.
C. Scanning Prefetch files for instances of TOR execution.
D. Monitoring real-time network traffic to identify connections to TOR nodes.
Answer: (SHOW ANSWER)

NEW QUESTION: 292
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. Packers
B. Password crackers
C. Emulators
D. Botnets
Answer: A (LEAVE A REPLY)

NEW QUESTION: 293
A regional bank, operating across several cities, recently discovered discrepancies in account balances following routine audits. The issues were noticed across various branches, prompting an internal investigation. Upon deeper analysis, it was revealed that someone with prior authorization had altered financial records. The investigation uncovered that a former employee, whose credentials had not been deactivated after leaving the company, had retained full control over critical systems. This oversight allowed the individual to modify transactional data, leading to inaccurate financial reports and potential harm to the bank ' s reputation. The adjustments made by the former employee were intentional and impacted customer accounts. Despite the employee no longer being employed, the lack of action to revoke their permissions allowed these changes to occur without any barriers. What classification of cybercrimes best fits this event?
A. An impersonation attempt using credential stuffing techniques.
B. A breach caused by external actors bypassing firewalls.
C. An authentication flaw due to expired password policies.
D. An abuse of role-based access from within the network.
Answer: D (LEAVE A REPLY)

Option D is the best answer because the scenario describes misuse of previously authorized internal access rather than an external intrusion. CHFI v11 explicitly includes Types of Computer Crimes , Cyber Crime Investigation , and Insider Threat and Identity Theft Forensics as important areas of study. It also emphasizes forensic readiness, investigative challenges, and the role of investigators in examining misuse of legitimate access.
The former employee still had active credentials and was able to alter transactional records because their permissions were not revoked. That makes this an insider-style abuse of role-based access , even though the individual was no longer officially employed. The key factor is that the attacker did not need to bypass perimeter defenses or crack authentication through brute-force methods; instead, they exploited existing trusted access that remained available inside the environment.
Option A would involve stolen credentials used through credential stuffing, which is not what the question states. B incorrectly frames the event as an external breach. C is too narrow and does not describe the intentional misuse of privileged access. Therefore, under CHFI's insider threat and cybercrime classification concepts, this event is best classified as abuse of role-based access from within the network .

NEW QUESTION: 294
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 X509 Address
B. The SMTP reply Address
C. The Host Domain Name
D. The E-mail Header
Answer: D (LEAVE A REPLY)

NEW QUESTION: 295
As a digital forensics expert at a cybersecurity company, you're knee-deep in a case involving a data breach. You're tasked with scrutinizing the Windows Registry of a client's computer which you believe might be harboring malware related to the breach. Which part of the registry should be your main focus in order to spot potential malware entries?
A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_USER
D. HKEY_USERS
Answer: (SHOW ANSWER)
HKEY_LOCAL_MACHINE contains system-wide configuration settings, including startup entries, services, and drivers that apply to all users. Malware often establishes persistence here to ensure it runs at system startup across the entire machine.

NEW QUESTION: 296
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
A. Technical material related to forensics
B. Judging the character of defendants/victims
C. No particular field
D. Legal issues
Answer: (SHOW ANSWER)

NEW QUESTION: 297
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well- tested hardware write-blocking device to _____
A. Automate collection from image files
B. Avoiding copying data from the boot partition
C. Acquire data from the host-protected area on a disk
D. Prevent contamination to the evidence drive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 298
During a late-night investigation at a tech firm ' s office in Seattle, the first responder arrives to find multiple computers displaying active sessions. To ensure a comprehensive record that supports later evidence recreation, which action should the first responder prioritize at the crime scene?
A. Maintain a log of all actions taken during every investigation phase
B. Document witness statements along with other relevant information if identified
C. Take a photograph of the computer monitor screen and note what is seen
D. Note the location where the evidence is securely stored for further examination
Answer: C (LEAVE A REPLY)
The correct answer is C because when a live system is found displaying an active session, the first responder should immediately preserve what is visible on the screen before that information changes or disappears.
CHFI v11 places strong emphasis on first response, documenting the electronic crime scene, and preserving volatile or transient evidence. A screen may show logged-in users, running applications, chats, remote sessions, command windows, or other live artifacts that can vanish if the user session locks, the system sleeps, or the machine is powered down. Photographing the monitor and noting what is displayed creates an early evidentiary snapshot that helps reconstruct the scene later. Option A is good general practice, but it is broader and less urgent than capturing the live display. Option B may matter if witnesses exist, and option D is a later evidence-handling concern. The question asks what should be

prioritized at the scene to support later reconstruction, and CHFI-style reasoning favors recording the immediate visual state of active systems before that state changes. That makes photographing the monitor and noting observations the best first-response action.

NEW QUESTION: 299
As a newly appointed Quality Manager in a digital forensics lab. you are reviewing the lab's current Quality Assurance Manual. You notice that the last update to the Quality Management System was four years ago. Which immediate action should you take to ensure compliance with best practices in the industry?
A. Update and document the Quality Management System
B. Validate and document the lab equipment
C. Schedule a proficiency test for investigators
D. Start the process for ASCLD/LAB accreditation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 300
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 48
B. 64
C. 16
D. 32
Answer: D (LEAVE A REPLY)

NEW QUESTION: 301
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)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected**

get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 302
In the realm of web accessibility, there are three layers: the Surface Web, which is easily accessible and indexed by standard search engines; the Deep Web, which contains unindexed content such as confidential databases and private portals; and the Dark Web, a clandestine environment often associated with illegal activities like drug trafficking and cybercrime, accessible through specialized browsers such as Tor.
What distinguishes the Dark Web from the Surface and Deep Web?
A. It contains legal dossiers and financial records.
B. It enables complete anonymity through encryption.
C. It requires authorization to access.
D. It is indexed by search engines.
Answer: B (LEAVE A REPLY)
According to the CHFI v11 Dark Web Forensics objectives, the defining characteristic that distinguishes the Dark Web from both the Surface Web and the Deep Web is its ability to provide strong anonymity through layered encryption and anonymization techniques. The Dark Web is intentionally designed to conceal the identities and locations of users, services, and hosting infrastructure.
Access to the Dark Web typically requires specialized software such as the Tor Browser, which routes traffic through multiple encrypted relay nodes (entry, middle, and exit relays). This process, known as onion routing, ensures that no single node knows both the source and destination of the communication. CHFI v11 explicitly highlights that this encryption-based anonymity is what makes the Dark Web attractive for activities such as cybercrime marketplaces, illegal trade, anonymous communications, and covert operations.

NEW QUESTION: 303
In a supply chain attack investigation at an automotive supplier in Detroit, Michigan, the forensics team examines alerts from endpoint antivirus systems indicating suspicious file downloads and network IDS sensors reporting anomalous outbound DNS queries. Independently, the alerts provide limited insight. The team consolidates these sources to identify relationships and reconstruct the broader compromise sequence.
What event-correlation approach does this consolidation demonstrate?
A. Route Correlation
B. Cross-domain Event Correlation
C. Multivariate Correlation
D. Topology-based Event Correlation
Answer: (SHOW ANSWER)

Answer B fits best because the investigators are correlating evidence from different security domains, in this case endpoint protection data and network intrusion-detection telemetry. Cross-domain event correlation is used when analysts combine events from separate domains or control layers to uncover a wider incident pattern that is not obvious when each alert stream is reviewed alone. The CHFI v11 blueprint specifically includes event correlation approaches, prerequisites of event correlation, and reconstruction of incident timelines. That is exactly what is happening here: antivirus alerts show suspicious activity on hosts, while IDS alerts reveal related outbound DNS behavior on the network. Together, these data sources can expose malware staging, command-and-control attempts, or data exfiltration paths. Route correlation and topology- based correlation do not fit as well because the question does not emphasize pathing through infrastructure topology. Multivariate correlation usually refers more broadly to statistical relationships across variables, not the explicit joining of alerts from separate investigative domains. Therefore, the strongest CHFI-aligned interpretation is cross-domain event correlation.

NEW QUESTION: 304
During a cybersecurity investigation, logs from a Cisco switch, VPN, and DNS server are collected. These logs contain valuable information about network activities and potential security breaches.
In digital forensics, what role do Cisco switch, VPN, and DNS server logs play when analyzing network incidents?
A. Provides insights on network traffic, device connections, and security incidents.
B. Tracks website visits and browser history exclusively.
C. Not pertinent to digital forensics.
D. Details user activities within the local network.
Answer: A (LEAVE A REPLY)
This question aligns with CHFI v11 objectives under Network and Web Attacks and Network Log Analysis. In digital forensics, network infrastructure logs are critical sources of evidence for detecting, analyzing, and reconstructing network-based attacks. CHFI v11 specifically emphasizes the forensic value of logs generated by network devices such as Cisco switches, VPN gateways, and DNS servers.
Cisco switch logs provide information about device connections, port activity, MAC address mappings, VLAN assignments, and potential unauthorized access within the internal network.
VPN logs reveal details about remote connections, including authentication attempts, user identities, IP addresses, session durations, and encrypted tunnel activity--crucial for identifying compromised credentials or unauthorized remote access. DNS server logs record domain name queries and responses, which help investigators detect command-and-control communication, data exfiltration attempts, malware beaconing, and access to malicious domains.

NEW QUESTION: 305
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased.
They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?
A. They examined the actual evidence on an unrelated system
B. They tampered with evidence by using it
C. They attempted to implicate personnel without proof
D. They called in the FBI without correlating with the fingerprint data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 306
Rachel, a computer forensic investigator, is investigating a case of data theft at a law firm. She needs to capture and analyze the data present in a specific computer which is believed to be the source of the data leak.
However, the computer is continuously being used for critical tasks. Rachel is considering her options for data acquisition. Given the urgency of the situation, which type of data acquisition should Rachel choose?
A. Differential Acquisition
B. Live Acquisition
C. Remote Acquisition
D. Static Acquisition
Answer: B (LEAVE A REPLY)
Option B. Live Acquisition is the best answer because the computer is actively in use for critical tasks , which means shutting it down for a static or dead acquisition would disrupt operations and may also destroy volatile evidence. In CHFI methodology, when a system is running and immediate evidence preservation is necessary, live acquisition is the appropriate approach.
A live acquisition enables the investigator to capture both volatile and non-volatile evidence while the machine remains operational. This is especially important in data theft cases, where active sessions, memory- resident artifacts, current network connections, running processes, and open documents may be crucial to understanding how the leak occurred. Since the computer is continuously used and the situation is urgent, this method best balances evidentiary need with operational reality.
Differential acquisition is not the right concept here because the question is about choosing the overall acquisition mode. Remote acquisition may be possible in some environments, but it is not the primary answer to the problem described. Static acquisition generally

requires the system to be inactive. Therefore, under CHFI data acquisition principles, the correct choice is Live Acquisition .

NEW QUESTION: 307
The offset in a hexadecimal code is:
A. The last byte after the colon
B. The 0x at the end of the code
C. The first byte after the colon
D. The 0x at the beginning of the code
Answer: D (LEAVE A REPLY)

NEW QUESTION: 308
A forensic investigator discovers an Android smartwatch at the crime scene during an investigation. The investigator realizes the smartwatch was potentially involved in the crime, but the device associated with it was not found at the scene. What is the most suitable initial step for the investigator to retrieve meaningful data from the smartwatch?
A. The investigator should start by understanding the smartwatch's basic framework, including its APIs
B. The investigator should directly analyze data stored on the smartwatch using IoT forensics tools
C. The investigator should first physically dismantle the smartwatch to access its internal storage
D. The investigator should immediately turn off the smartwatch to prevent data manipulation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 309
During a post-incident investigation at an energy company, analysts are tasked with identifying coordinated malicious activity by examining security data generated from multiple control points, including network defenses and server systems. The investigation requires a platform that can ingest diverse event sources, relate activity across those sources as it occurs, and surface actionable findings to support analyst-led investigation through a unified interface. How should analysts enable this type of real-time, cross-source event analysis and investigation?
A. ELK Stack Elasticsearch, Logstash, Kibana
B. ManageEngine EventLog Analyzer
C. OSSEC HIDS
D. IBM QRadar
Answer: (SHOW ANSWER)
The correct answer is D because IBM QRadar is built around real-time ingestion, normalization, and correlation of events and flows from many different sources, then

presenting those results through a unified investigative interface. The CHFI v11 blueprint includes centralized logging, SIEM solutions, and event correlation approaches, so the exam expects candidates to identify tools that can combine diverse evidence streams into actionable security findings. IBM documentation states that QRadar consolidates log source and network flow data, performs immediate normalization and correlation, and provides dashboards, offenses, log activity, and network activity views for analysts. That lines up closely with the scenario's need for real-time, cross-source analysis. ELK can aggregate and visualize data effectively, but the question stresses built-in correlation of activity across sources as it occurs. OSSEC is host-focused, and EventLog Analyzer is more centered on log monitoring and analysis rather than the broader SIEM-style cross-source correlation platform described here. For CHFI-style tool selection, a requirement for unified, real-time event correlation across network and system telemetry points most directly to IBM QRadar.

NEW QUESTION: 310
In an investigation into a cyber-attack incident, you are a Computer Hacking Forensics Investigator tasked with gathering digital evidence. The targeted system has been turned off unexpectedly, and you know the system was running a crucial process during the attack. Which types of evidence might be lost due to the system being switched off?
A. Non-volatile data such as event logs and hidden files, but not volatile data like command history and process-to-port mapping
B. Neither volatile data, such as command history and process-to-port mapping, nor non-volatile data, like event logs and hidden files
C. Both volatile data, such as command history and process-to-port mapping, and non-volatile data, like event logs and hidden files
D. Volatile data such as command history and process-to-port mapping, but not non-volatile data like event logs and hidden files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 311
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security- auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas.
After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room.
What type of attack has the technician performed?
A. Man trap attack
B. Tailgating

C. Fuzzing
D. Backtrapping
Answer: (SHOW ANSWER)

NEW QUESTION: 312
What is the name of the standard Linux command that can be used to create bit-stream images?
A. image
B. dd
C. mcopy
D. MD5
Answer: (SHOW ANSWER)

NEW QUESTION: 313
During a forensic investigation of a misconfiguration breach in a Microsoft Azure deployment, investigators observe that the client organization manages user identities, endpoint devices, and data, while Microsoft handles physical hosts, networking, and datacenter operations. Which cloud service model best represents this shared-responsibility division?
A. On-premises deployment
B. Software as a Service SaaS
C. Infrastructure as a Service IaaS
Answer: (SHOW ANSWER)
The correct answer is C because the responsibility split described in the question aligns most closely with Infrastructure as a Service. Microsoft's Azure shared responsibility documentation explains that responsibilities differ depending on whether the service model is SaaS, PaaS, or IaaS. In IaaS, the provider is responsible for the physical datacenter, physical hosts, networking fabric, and core infrastructure, while the customer remains responsible for significant portions of what runs in the environment, including identities, endpoints, data, operating systems, and workload configuration. That matches the scenario much more closely than SaaS, where Microsoft would handle substantially more of the stack. On-premises deployment would place nearly all responsibility on the organization itself, which also does not fit. CHFI v11 includes cloud computing service models, cloud threats, and cloud forensics, so candidates are expected to connect a forensic scenario to the correct service model by examining who manages which layers. Since Microsoft handles the physical cloud infrastructure while the customer manages core usage-side components and data, the best answer is Infrastructure as a Service.

NEW QUESTION: 314
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and

vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA
B. IANA
C. CVE
D. RIPE
Answer: C (LEAVE A REPLY)

NEW QUESTION: 315
Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Brute force attack
B. Hybrid attack
C. Syllable attack
D. Rule-based attack
Answer: (SHOW ANSWER)

NEW QUESTION: 316
A rogue/unauthorized access point is one that Is not authorized for operation by a particular firm or network

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

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 317
During a cross-border fraud investigation at a financial analytics company in Chicago, forensic responders suspect an Amazon EC2 instance has been compromised. To ensure

evidence integrity while preserving the system state, which step should the forensic team perform immediately before taking a snapshot of the instance?

A. Isolate the compromised EC2 instance from the production environment

B. Create evidence volume from the snapshot

C. Attach the evidence volume to the forensic workstation

D. Provision and launch forensic workstation

Answer: A (LEAVE A REPLY)

The correct answer is A because isolating the compromised EC2 instance helps preserve its state and reduces the chance that the attacker, users, or normal production traffic will continue altering evidence before the snapshot is taken. Current AWS guidance describes incident-response and forensics workflows that isolate affected instances as part of preserving artifacts and protecting the integrity of later acquisition. AWS documentation on forensic orchestration notes that affected EC2 instances are isolated and then disk and memory acquisition actions proceed. AWS incident-response guidance also recommends isolating potentially compromised EC2 instances by associating an isolation security group. The other options happen later in the forensic workflow. Creating an evidence volume, attaching it to a forensic workstation, and provisioning an analysis host are post-snapshot or downstream examination steps. CHFI v11 includes cloud forensics and data acquisition in the cloud, so the exam logic is to stabilize and preserve the source system first, then acquire evidence from that preserved state. Therefore, the immediate step before snapshotting is to isolate the compromised EC2 instance.

NEW QUESTION: 318

In a sophisticated cloud attack, assailants strategically deploy virtual machines (VMs) in close proximity to target servers. Leveraging shared physical resources, they execute side-channel attacks, extracting sensitive data through timing vulnerabilities. Subsequently, they exploit stolen credentials to impersonate legitimate users, posing a grave security risk. How do attackers compromise cloud security by exploiting the proximity of virtual machines (VMs) to target servers?

A. Targeted VM Overloading for Side-Channel Attacks

B. Cloud Infrastructure Breach via DNS Hijacking

C. Exploitation of Shared Resources for Side-Channel Attacks

D. Application Layer Exploitation for SQL Injection

Answer: C (LEAVE A REPLY)

According to the CHFI v11 Cloud Forensics objectives, cloud environments rely heavily on virtualization, where multiple virtual machines share the same underlying physical hardware such as CPU caches, memory, storage, and network interfaces. Attackers can exploit this shared- resource model by intentionally placing malicious VMs on the same physical host as the victim VM, a technique often referred to as co-residency attacks. Once co-residency is achieved, attackers perform side-channel attacks that analyze indirect

indicators such as cache timing, memory access patterns, or CPU usage to infer sensitive information.
This scenario precisely describes the exploitation of shared resources for side-channel attacks.
Timing vulnerabilities in shared CPU caches or memory buses allow attackers to extract cryptographic keys, credentials, or other sensitive data without directly breaching the target system. After obtaining credentials, attackers may impersonate legitimate users, escalating the impact of the attack.

NEW QUESTION: 319
During an insider-threat investigation at a technology firm in San Jose, California, network monitoring reveals that security staff captured the contents of employee emails and chat messages in transit and accessed copies stored on the company mail server. To ensure the collection and review of these communications complies with U.S. law, which statute is most directly applicable?
A. Electronic Communications Privacy Act ECPA of 1986
B. Privacy Act of 1974
C. Foreign Intelligence Surveillance Act
D. Protect America Act of 2007
Answer: (SHOW ANSWER)
The correct answer is A because the Electronic Communications Privacy Act of 1986 is the main U.S. statute that addresses both interception of electronic communications and access to stored electronic communications. The scenario involves two separate but related activities: capturing messages in transit and reviewing copies stored on a mail server. Justice Department materials explain that ECPA includes protections for intercepted electronic communications under the Wiretap Act and for stored communications under the Stored Communications Act. That makes it the most directly applicable law for this type of email and chat evidence handling. The Privacy Act of 1974 focuses on federal agency records rather than general workplace monitoring of electronic communications. FISA and the Protect America Act deal with foreign intelligence and national security contexts, not standard corporate insider-threat investigations. CHFI v11 covers legal issues, privacy issues, and legal compliance affecting digital investigations, so candidates are expected to identify the statute that governs electronic communications content both in transit and in storage.
For that reason, ECPA is the strongest and most defensible answer.

NEW QUESTION: 320
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 5th Amendment
B. The 10th Amendment
C. The 4th Amendment
D. The 1st Amendment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 321
In a smart city surveillance breach at a municipal agency in Chicago, Illinois, investigators identify anomalous data flows from field sensors to cloud services, where intermediate processing for data aggregation, data filtering, access control, and device information discovery would reveal policy violations.
Which IoT architecture layer, acting as an interface between hardware and applications, should be the focus?
A. Edge Technology Layer
B. Middleware Layer
C. Application Layer
D. Access Gateway Layer
Answer: B (LEAVE A REPLY)
The correct answer is B because the middleware layer in IoT architecture sits between devices and applications and is responsible for functions such as data aggregation, filtering, transformation, access handling, and information discovery. References describing IoT middleware note that it manages heterogeneous IoT components and provides the software layer that connects hardware-side activity to the application layer. That matches the scenario exactly, since investigators are interested in the intermediate processing stage where policy violations could be exposed through aggregation, filtering, access control, and device discovery behavior. CHFI v11 includes IoT architecture, IoT threats, and IoT forensic analysis, so candidates are expected to identify which layer performs coordination and processing between devices and higher-level services. The application layer is where user-facing services reside, while edge and gateway concepts may participate in communication, but the broad interface and processing responsibilities listed in the question align most clearly with middleware. Therefore, the best answer is the middleware layer.

NEW QUESTION: 322
The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies.

What is preventing the police from breaking down the suspect door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?
A. The USA Patriot Act
B. The Fourth Amendment
C. The Federal Rules of Evidence
D. The Good Samaritan Laws
Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
When operating systems mark a cluster as used but not allocated, the cluster is considered as

_____
A. Corrupt
B. Lost
C. Unallocated
D. Bad
Answer: B (LEAVE A REPLY)

NEW QUESTION: 324
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. Detecting the device that contains the file system and loading the necessary modules
C. Execution of the Linuxrc program to generate the real file system for the kernel
D. Loading the kernel into memory
Answer: C (LEAVE A REPLY)

NEW QUESTION: 325
A financial institution experiences a cyber incident in which customer financial records are exposed, stored data is modified without authorization, and access to critical systems is temporarily disrupted. The incident results in regulatory scrutiny and operational concerns due to the compromise of sensitive organizational information. Which impact on organizational information security is most directly demonstrated by this incident?
A. Theft of sensitive information, such as financial and corporate information
B. Loss of customer and stakeholder trust; reputational damage; and stolen intellectual property
C. Loss of confidentiality, integrity, and availability of information stored in organizational systems

D. Disruption of normal business operations leading to huge financial losses

Answer: C (LEAVE A REPLY)

The correct answer is C because the scenario explicitly affects all three core security properties at once.

Customer records were exposed, which means confidentiality was lost. Stored data was modified without authorization, which means integrity was compromised. Access to critical systems was disrupted, which means availability was affected. This three-part impact is the classic confidentiality, integrity, and availability model that underpins organizational information security analysis. CHFI v11 includes the impact of cybercrimes at the organizational level and expects candidates to identify not only business consequences, but also the underlying security principles directly harmed by an incident. The other choices describe real downstream effects, such as theft, reputational harm, and financial disruption, but they are consequences rather than the most direct information-security impact demonstrated by the facts in the question. In exam reasoning, when a single incident simultaneously exposes data, alters it, and interrupts access, the most accurate answer is the loss of confidentiality, integrity, and availability of information stored in organizational systems. That is the clearest conceptual match to the evidence described.

NEW QUESTION: 326

A digital forensics examiner is investigating a suspected case of corporate espionage involving the theft of sensitive intellectual property from a company's servers. In adherence to ENFSI Best Practices for Forensic Examination of Digital Technology, what would be the examiner's primary concern?

A. Complying with GDPR data privacy rules.

B. Following ISO/IEC 17025 standards in forensic labs.

C. Establishing secure evidence-handling protocols.

D. Implementing ISO/IEC 27001 for information security.

Answer: C (LEAVE A REPLY)

This question maps directly to CHFI v11 objectives underComputer Forensics FundamentalsandStandards and Best Practices Related to Computer Forensics, specifically theENFSI Best Practices for the Forensic Examination of Digital Technology. ENFSI (European Network of Forensic Science Institutes) guidelines focus primarily on ensuring that digital evidence is handled in asecure, reliable, and forensically sound mannerso that it remains admissible and defensible in legal proceedings.

The examiner's primary concern under ENFSI best practices is thesecure handling of digital evidence, which includes proper acquisition, preservation, documentation, storage, and chain of custody management.

These practices ensure evidence integrity, prevent contamination or alteration, and allow results to be independently verified. CHFI v11 emphasizes that forensic investigators must be able to demonstrate that evidence has not been tampered with and that standardized procedures were followed throughout the investigation lifecycle.

While GDPR, ISO/IEC 17025, and ISO/IEC 27001 are important regulatory and security frameworks, they are not the core focus of ENFSI forensic examination guidelines. ENFSI is evidence-centric, prioritizing secure evidence handling and methodological consistency. Therefore, establishing secure evidence-handling protocols is the correct and CHFI-aligned answer.

NEW QUESTION: 327
Ethan, a forensic investigator, is analyzing a suspect ' s computer and finds a suspicious file that may be related to a cybercrime. Upon examining the file ' s metadata, Ethan discovers that the file has been modified several times and was last accessed shortly before the crime took place. Which of the following forensic methods would be most useful for Ethan to determine whether the file was tampered with or manipulated?
A. Review the file ' s file system logs
B. Look for hidden attributes or alternate data streams
C. Check the file ' s access control list (ACL)
D. Examine the file ' s hash value
Answer: D (LEAVE A REPLY)
Within the CHFI v11 curriculum, verifying the integrity of digital evidence is a core responsibility of a forensic investigator. The most reliable method to determine whether a file has been tampered with is by examining its cryptographic hash value . A hash value (such as MD5 or SHA-256) is a fixed-length digital fingerprint generated from the file's contents. Even the smallest change to the file-whether intentional or accidental-will produce a completely different hash value, making hash comparison a definitive method for detecting manipulation.
File system logs (Option A) can help reconstruct timelines by showing access or modification events, but logs can be deleted, altered, or incomplete and do not directly validate file content integrity. Hidden attributes or alternate data streams (Option B) are indicators of possible anti-forensics techniques, yet their presence does not confirm that the primary file data was altered. Access Control Lists (Option C) only describe permission settings and ownership, not whether the file itself was modified.
According to the CHFI v11 objectives under Digital Evidence , Data Acquisition , and Evidence Validation
, investigators must calculate and verify hash values during acquisition and analysis to maintain chain of custody , ensure evidence integrity , and support legal admissibility . This makes hash examination the most appropriate and forensically sound choice in this scenario

NEW QUESTION: 328
Which of the following Perl scripts will help an investigator to access the executable image of a process?
A. Lspm.pl

B. Lspi.pl
C. Lpsi.pl
D. Lspd.pl
Answer: B (LEAVE A REPLY)

NEW QUESTION: 329
When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?
A. 49664/49665
B. 9150/9151
C. 7680
D. 49667/49668
Answer: (SHOW ANSWER)

NEW QUESTION: 330
Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks.
The source, nature, and time of the attack can be determined by _____of the compromised system.
A. Analyzing SAM file
B. Analyzing hard disk boot records
C. Analyzing rainbow tables
D. Analyzing log files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 331
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. Use the netstat -ano command to check the active network connections
B. Look for the 'State' file in the \Tor Browser\Browser\TorBrowser\Data\Tor\ directory
C. Examine the registry key: HKEY_USERS\\SOFTWARE\Mozilla\Firefox\Launcher for path information
D. Check the prefetch files using a tool such as WinPrefetchView
Answer: D (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 332
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. Both lower and higher ASCII codes primarily contain alphanumeric characters and punctuation
C. 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
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: D (LEAVE A REPLY)
Standard ASCII (0-127) includes control characters at the very low end and printable characters (letters, digits, punctuation). "Higher ASCII" commonly refers to extended codes (128-255 in many code pages), often used for accented characters, symbols, and simple graphics, depending on encoding.

NEW QUESTION: 333
What method of copying should always be performed first before carrying out an investigation?
A. MS-DOS disc copy
B. System level copy
C. Parity-bit copy
D. Bit-stream copy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
To which phase of the Computer Forensics Investigation Process does the 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: 335
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 start retrieving the stolen data from the compromised systems immediately to minimize further damage
B. They should power down the compromised systems to prevent further attacks
C. They should launch a preliminary investigation into the breach before the forensics team arrives
D. They should isolate the affected systems and document every detail relevant to the incident without tampering with them
Answer: D (LEAVE A REPLY)

NEW QUESTION: 336
In the course of a criminal investigation involving a suspect ' s mobile devices, the forensic investigation team needs to analyze digital evidence from both Android and iOS smartphones. Each platform presents unique challenges and methodologies for forensic analysis.
To effectively extract and examine digital evidence from these devices, which of the following statements regarding Android and iOS forensic analysis is most accurate?
A. iOS offers robust open-source forensic tools for comprehensive digital evidence extraction, while Android relies on manual extraction due to limited forensic software support.
B. Both Android and iOS devices use the FAT32 file system, facilitating cross-platform compatibility and straightforward forensic analysis with widely available tools.
C. Android: Single partition aids forensic analysis; iOS: Sandbox, encryption complexities hinder data extraction.
D. Android devices use Ext4 for straightforward file extraction with standard forensic tools; iOS devices, however, require specialized techniques due to APFS (Apple File System) encryption and complexity.
Answer: D (LEAVE A REPLY)
Option D is the most accurate answer because CHFI v11 explicitly includes Android and iOS forensic analysis , logical and physical acquisition of Android and iOS devices ,

Android and iOS file systems , and APFS file system analysis as major mobile-forensics objectives.
Android devices are commonly associated in forensic contexts with Ext4-based storage structures , while iOS devices use APFS , which introduces additional complexity due to Apple's security model, sandboxing, and strong encryption protections. That makes iOS extraction and examination more dependent on specialized methods and tools. This matches the CHFI view that mobile platforms require different forensic strategies rather than one uniform method.
Option A reverses the practical situation. B is incorrect because FAT32 is not the shared native forensic file- system answer for both platforms. C contains a partially plausible idea about iOS complexity, but it is less precise and less aligned to the file-system-focused wording than D . Therefore, based on CHFI mobile- forensics objectives, the strongest answer is that Android commonly uses Ext4 , while iOS uses APFS and often requires more specialized forensic handling.

NEW QUESTION: 337
Emily, a seasoned digital forensics investigator, has been tasked with conducting an investigation on a Linux system running the ext2 file system. The system was involved in a suspected data exfiltration incident, and Emily needs to gather detailed information about the metadata of a specific file that may have been accessed or modified during the attack. After reviewing the system's file system structure, Emily aims to focus on the source that contains the file's metadata, such as timestamps, permissions, and file size. Which of the following would be the best source for this critical information?
A. The dentry cache
B. The inode table
C. The file's data blocks
D. The superblock
Answer: B (LEAVE A REPLY)
In ext2, an inode stores a file's metadata, including timestamps, permissions, ownership, and size. The inode table holds these structures, making it the primary source for detailed file metadata.

NEW QUESTION: 338
A top-tier forensic investigation bureau within the United States is handling a major case related to espionage. They have started electronic monitoring of a permanent lawful inhabitant of the nation suspected of participating in the case. Yet, there seems to be no compelling evidence suggesting the individual's criminal involvement. How does this measure correspond with existing laws?
A. This measure breaches the Foreign Intelligence Surveillance Act of 1978 as no compelling evidence suggests criminal involvement

B. This measure corresponds with the Foreign Intelligence Surveillance Act of 1978, permitting the surveillance of US individuals suspected of participating in espionage
C. This measure breaches the Privacy Act of 1974, involving the unauthorized revelation of private data
D. This measure corresponds with the Protect America Act of 2007 which permits the surveillance of individuals who are thought to be residing outside the United States
Answer: B (LEAVE A REPLY)

NEW QUESTION: 339
During an incident-response project at a biotech company in San Diego, California, the team must move 600 TB of research datasets from an isolated lab network to Google Cloud, but the site has limited bandwidth and no direct peering. They need a secure, offline method to ship the data to Google for upload into Cloud Storage. Which Google Cloud service fits this requirement?
A. Data Transfer Services
B. Transfer Appliance
C. Cloud Storage for Firebase
D. Google Cloud Backup and DR
Answer: B (LEAVE A REPLY)
The correct answer is B because Google Transfer Appliance is specifically designed for large-scale offline data movement into Google Cloud when network bandwidth is limited or impractical. Google documents it as a high-capacity storage appliance that customers load on-premises and then securely ship to a Google upload facility, where the data is transferred into Cloud Storage. That matches the scenario exactly: the site is isolated, the bandwidth is constrained, and the volume is extremely large at 600 TB. In CHFI v11, cloud forensics includes understanding cloud platforms and evidence acquisition approaches, so recognizing the difference between online transfer services and offline shipping methods is important. Data Transfer Services generally rely on network-based transfers and are not the best choice when direct connectivity is a bottleneck.
Cloud Storage for Firebase is unrelated to bulk evidence migration, and Backup and DR is intended for protection and recovery workflows rather than secure offline ingestion. When the exam scenario stresses secure shipment of very large datasets into Google Cloud without relying on available bandwidth, Transfer Appliance is the only option that cleanly fits the operational requirement.

NEW QUESTION: 340
Sophia, a forensic investigator, has been working on a significant corporate data theft case. The suspect, an IT employee, allegedly downloaded hundreds of confidential files onto his laptop before resigning abruptly. Sophia obtained a search and seizure warrant, and during the execution, she found the suspect's laptop, a desktop computer, and several

storage devices. To ensure she maintains the chain of custody and abides by the ACPO principles of digital evidence, what should be her next step?
A. She should immediately begin analyzing the digital devices on-site.
B. She should ask the suspect for the passwords to the devices to expedite the investigation.
C. She should only seize the personal laptop as per the information on the warrant.
D. She should seize all the devices and send them to a forensic lab for analysis.
Answer: D (LEAVE A REPLY)
Following proper forensic procedures and ACPO principles, all relevant devices should be seized, documented, and transported to a controlled forensic lab environment for analysis. This ensures evidence integrity, proper handling, and maintenance of the chain of custody.

NEW QUESTION: 341
Which of the following tool enables data acquisition and duplication?
A. DriveSpy
B. Xplico
C. Colasoft's Capsa
D. Wireshark
Answer: A (LEAVE A REPLY)

NEW QUESTION: 342
During a forensic investigation into a recent cyberattack, analysts discovered a piece of malware that had been deliberately disguised to avoid detection. The malware was wrapped in a layer of encryption, making its contents unreadable to typical security software. Once the layer was removed using decryption techniques, the true malicious functionality of the malware became visible. Which of the following components is most likely responsible for this obfuscation?
A. Packer
B. Exploit
C. Payload
D. Dropper
Answer: A (LEAVE A REPLY)
Option A. Packer is the correct answer because CHFI v11 explicitly identifies program packers as an anti- forensics technique and also covers program packers unpacking tools as a way to reverse that concealment during analysis.
A packer is used to wrap or obfuscate an executable so that its real content is hidden from straightforward inspection. This often makes the malware appear unreadable or significantly harder to analyze until the packed layer is removed or unpacked. That fits the scenario exactly: the malicious functionality only became clear after the outer encrypted or packed layer was removed.

An exploit is code used to take advantage of a vulnerability, not primarily to hide malware. A payload is the malicious function delivered or executed after infection. A dropper is designed to install or deliver other malware components, but it is not the best term for the specific concealment layer described here. Therefore, within CHFI's anti-forensics framework, the component most responsible for this type of obfuscation is a packer .

NEW QUESTION: 343
A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be identified as _____.
A. Slack space
B. Swap space
C. Sector space
D. Cluster space
Answer: (SHOW ANSWER)

NEW QUESTION: 344
A medium-sized company's IT department noticed a sudden surge in network traffic and peculiar DNS requests originating from their internal servers. Realizing it could be a malware attack, they recruited Lisa, a seasoned forensic investigator, to probe into the situation. Lisa decided to use a tool to analyze this unusual network behavior and particularly focus on monitoring DNS requests.
What tool should Lisa use for this?
A. Snort
B. Wireshark
C. Nmap
D. Nessus
Answer: B (LEAVE A REPLY)
Wireshark captures and analyzes network traffic in detail, including DNS queries, allowing investigators to inspect packets and identify suspicious patterns or anomalies in real time.

NEW QUESTION: 345
As the lead of the forensic department in a well-known multinational bank, John has been tasked with updating the company's forensic readiness plan. The bank has faced several minor cyber incidents over the past year but managed to tackle them promptly without any significant impact.
However, the upper management has emphasized the need for more robust preparedness. John already has an incident response plan in place and has ensured that the SOC is adequately equipped with the necessary resources. Given this situation, what could be a valuable addition to John's forensic readiness plan to further strengthen the bank's ability to deal with future cyber incidents?

A. Establishing a detailed procedure for evidence collection and analysis.
B. Integrating the SOC with an AI-based threat detection system.
C. Organizing a monthly review of the bank's network infrastructure.
D. Implementing a zero-trust network architecture.
Answer: A (LEAVE A REPLY)
A forensic readiness plan focuses on the ability to efficiently collect, preserve, and analyze digital evidence in a legally sound manner. Establishing detailed procedures for evidence collection and analysis ensures that, when incidents occur, evidence is handled properly and can be used effectively for investigation and legal purposes.

NEW QUESTION: 346
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house.
Daryl packs all the items found in his van and takes them back to his lab for further examination.
At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?
A. Three
B. Four
C. One
D. Two
Answer: (SHOW ANSWER)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 347
Which of the following is an iOS Jailbreaking tool?
A. Kingo Android ROOT
B. Towelroot
C. One Click Root

D. Redsn0w
Answer: D (LEAVE A REPLY)

NEW QUESTION: 348
Forming a specialized cybercrime investigation team for a multinational corporation. Roles assigned include photographer, incident responder, evidence examiner, and attorney. External support is enlisted for complex cases. The goal is to identify perpetrators, gather evidence, and ensure justice.
What is a crucial step in forming a specialized cybercrime investigation team?
A. Providing legal advice
B. Enlisting external support
C. Conducting digital forensics analysis
D. Assigning roles to team members
Answer: D (LEAVE A REPLY)
According to the CHFI v11 Computer Forensics Fundamentals and Investigation Process , one of the most critical steps in forming a specialized cybercrime investigation team is clearly assigning roles and responsibilities to team members . This step ensures that every aspect of the investigation is handled efficiently, lawfully, and without overlap or conflict.
CHFI v11 emphasizes that cybercrime investigations are multidisciplinary by nature and require role-based coordination . Typical roles include first responders, incident responders, forensic examiners, evidence handlers, photographers, documentation specialists, and legal advisors. Clearly defining these roles at the outset ensures proper evidence handling, adherence to legal procedures, and effective incident response .
It also supports maintaining the chain of custody , minimizing contamination of evidence, and ensuring accountability throughout the investigation lifecycle.
While legal advice and external support are important, they are supplementary functions that support the investigation after the core team structure is established. Conducting digital forensics analysis is an operational activity that occurs later in the forensic process, not during team formation.
CHFI v11 explicitly highlights building the investigation team and assigning responsibilities as foundational steps before evidence collection and analysis begin. Without clearly defined roles, investigations risk procedural errors, legal challenges, and inefficiencies.
Therefore, the most crucial step in forming a specialized cybercrime investigation team-fully aligned with CHFI v11 objectives-is assigning roles to team members , making Option D the correct answer.

NEW QUESTION: 349
A forensic investigator is assigned to a cybercrime investigation where they need to document critical evidence from a powered-on computer located at the crime scene. The computer is suspected to contain important files or programs that are part of the ongoing investigation, upon arriving at the scene, the investigator observes that the monitor of the

computer is displaying a screensaver, which is obscuring any active programs or open files. The forensic team is under pressure to preserve the integrity of the evidence without modifying or tampering with any data on the machine.
The investigator needs to capture a clear image of the programs running on the screen to document the evidence properly. However, they are uncertain about how to proceed in this situation to avoid potentially altering any information on the computer. What should the investigator do to capture the active programs on the screen and document the evidence effectively?
A. Reboot the machine to force the system to show the programs running after the restart.
B. Move the mouse slightly and slowly to wake up the screen from the screensaver, then photograph the active programs and document them.
C. Unplug the computer ' s main power cord to reset the system and clear any volatile data.
D. Disconnect the network cable to prevent any remote access while documenting the evidence.
Answer: B (LEAVE A REPLY)
Option B is the best answer because the investigator's immediate goal is to document what is currently displayed or active on a powered-on system while causing the least possible disturbance . CHFI v11 emphasizes best practices for handling digital evidence , preserving evidence , collecting volatile information , and understanding the consequences of actions taken on a live system.
A slight movement of the mouse to wake the screen is the least disruptive way among the listed options to reveal the active display and allow proper photographic documentation.
Rebooting or unplugging the machine would destroy volatile evidence and significantly alter the system state. Disconnecting the network cable may sometimes be considered in other operational contexts, but it does not solve the immediate issue of documenting the active on-screen evidence hidden by the screensaver.
From a CHFI standpoint, documentation at the scene should preserve the evidence as found as much as possible while minimizing changes. Therefore, the correct response is to gently wake the screen and photograph/document the visible programs without taking destructive actions that would compromise volatile evidence.

NEW QUESTION: 350
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 to reverse engineer the packed file in an attempt to bypass password protection
B. The investigator should attempt to crack the password using a brute force attack

C. The investigator should attempt static analysis on the packed file
D. The investigator should run the packed executable in a controlled environment for dynamic analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 351
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. Phishing
B. Malware attack
C. Ransomware attack
D. Denial-of-Service (DoS) attack
Answer: D (LEAVE A REPLY)
A denial-of-service attack disrupts the availability of a device, network, or service by overwhelming it with excessive traffic or resource requests, preventing legitimate users from accessing systems or services.

NEW QUESTION: 352
E-mail logs contain which of the following information to help you in your investigation? (Select up to 4)
A. contents of the e-mail message
B. attachments sent with the e-mail message
C. user account that was used to send the account
D. unique message identifier
E. date and time the message was sent
Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 353
The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.
A. Gramm-Leach-Bliley Act
B. Sarbanes-Oxley 2002
C. California SB 1386
D. HIPAA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 354
During a digital forensics investigation, an investigator is tasked with collecting data from servers and shared drives within an organization's infrastructure. The investigator

accesses and retrieves relevant electronic evidence from these central storage locations to assist in the investigation.
This data collection includes files, user logs, and other system artifacts necessary for understanding the scope of the incident. Which eDiscovery collection methodology is the investigator employing in this scenario?
A. The investigator uses network collection to gather data directly from internal repositories and organizational data hubs across the network.
B. The investigator uses cloud-based collection to retrieve data from cloud storage and platforms.
C. The investigator uses email collection to extract relevant communications and attachments from email systems.
D. The investigator uses mobile device collection to retrieve data from smartphones, tablets, or other mobile devices.
Answer: A (LEAVE A REPLY)
Under the CHFI v11 objectives related to the eDiscovery process, investigators must understand and correctly apply various eDiscovery collection methodologies based on where data resides and how it is accessed. In this scenario, the investigator is collecting evidence from internal servers and shared drives that are part of the organization's on-premises infrastructure. These repositories typically store centralized data such as user files, audit logs, access records, and application artifacts.
This approach directly aligns with network collection, an eDiscovery methodology in which data is acquired remotely over the organizational network from file servers, database servers, shared storage, and internal repositories. Network collection is commonly used in enterprise investigations because it allows investigators to gather large volumes of data efficiently without physically seizing individual endpoint devices.
Cloud-based collection (Option B) applies only when data is hosted on third-party cloud platforms such as AWS, Azure, or Google Cloud. Email collection (Option C) is limited to mail servers and messaging systems, while mobile device collection (Option D) focuses on smartphones and tablets. None of these accurately describe the centralized, internal infrastructure outlined in the scenario.
The CHFI v11 Exam Blueprint emphasizes eDiscovery collection methodologies as part of forensic readiness and investigation workflows, highlighting network collection as the appropriate technique for acquiring evidence from organizational servers and shared drives while maintaining integrity and chain of custody

NEW QUESTION: 355
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. Phishing

B. Denial-of-Service (DoS) attack
C. Malware attack
D. Ransomware attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 356
As a Computer Hacking Forensic Investigator, you're working on a case involving the unauthorized alteration of financial records within a major bank. The network administrators have identified a specific terminal where they believe the alterations originated. You have been tasked with examining this workstation. The administrators inform you that the machine has been powered down for fear of further alterations. In this scenario, which of the following would be your first step?
A. Create a bootable copy of the hard drive to analyze on a separate, secure machine.
B. Connect the machine to a separate network and use a network packet analyzer to monitor any ongoing traffic.
C. Leave the system powered down, and initiate the forensic imaging process for further offline analysis.
D. Power up the machine and perform a live analysis to identify any running processes that might have been involved in the unauthorized alterations.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 357
A renowned global retail corporation recently underwent a sophisticated cyber attack leading to a significant loss of data. The company had invested heavily in its Security Operations Center (SOC) which was expected to act as the first line of defense against such cyber threats. However, the SOC was unable to detect the attack until it was too late. In retrospect what aspect of the SOC ' s role in computer forensics might have been overlooked in this scenario?
A. SOC's role in continuously monitoring and analyzing network traffic.
B. SOC ' s role in preserving evidence for forensic investigations.
C. SOC ' s role in conducting a forensic investigation
D. SOC ' s role in maintaining and securing log data.
Answer: A (LEAVE A REPLY)
Option A is the best answer because the problem described is a failure to detect the attack in time , which points most directly to a lapse in the SOC's continuous monitoring and analysis function. CHFI v11 explicitly includes the Role of SOC in Computer Forensics , centralized logging using SIEM solutions , incident detection and examination with SIEM tools , and the analysis of network and log data to identify attacks and suspicious behavior. A SOC's first-line defensive role depends heavily on ongoing visibility into the environment, including network traffic, logs, alerts, and correlations that can reveal malicious activity before major damage occurs. If the attack was only discovered after significant loss, the

most likely overlooked function was not primarily evidence preservation or post-incident investigation, but timely monitoring and analysis .
Preserving evidence and maintaining logs are important forensic responsibilities, and the SOC may contribute to investigations, but those do not most directly explain the initial detection failure described in the scenario. Therefore, under CHFI's view of the SOC as part of forensic readiness and incident detection, the strongest answer is continuous monitoring and analysis of network activity .

NEW QUESTION: 358
Rule 1002 of Federal Rules of Evidence (US) talks about _____.
A. Requirement of original
B. Admissibility of duplicates
C. Admissibility of other evidence of contents
D. Admissibility of original
Answer: A (LEAVE A REPLY)

NEW QUESTION: 359
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 642
B. Event ID 644
C. Event ID 624
D. Event ID 612
Answer: C (LEAVE A REPLY)
In classic Windows Security auditing (pre-Vista style event IDs commonly referenced in many exam banks), Event ID 624 corresponds to user account created. Since the sequence begins with account creation, 624 is the key starting point for correlation, followed by modification and group membership events.

NEW QUESTION: 360
An investigator is assigned to a complex cybercrime case involving unauthorized access to sensitive and confidential data stored on a corporate server. The investigation is being conducted in a jurisdiction with strict privacy laws and digital evidence guidelines, while the suspect is located in a different jurisdiction that adheres to its own set of privacy and evidence laws. The investigator must gather and preserve evidence from the suspect's devices using specialized digital forensic tools. However, the investigator faces significant

challenges as they navigate the differing legal frameworks that govern the collection and handling of digital evidence across the two jurisdictions.
As part of the investigation, the investigator uses forensic tools to create forensic images of the suspect's devices and to gather data from the breached systems. Due to the differences in legal requirements, the investigator is unsure of how to ensure compliance with both jurisdictions' laws while maintaining the integrity of the evidence. Which legal challenge might the investigator face in this case when handling the evidence?
A. The challenge of using outdated forensic tools that are not compatible with newer file systems and devices.
B. The requirement to use the same forensic tool across all devices involved to ensure uniformity in evidence handling.
C. The need for forensic tools to have encryption capabilities to secure the evidence during transport.
D. The need to ensure that the forensic tools used during the investigation are validated according to the regulations of both regions involved.
Answer: D (LEAVE A REPLY)
In multi-jurisdictional investigations, different regions may require that forensic tools be tested, validated, and accepted according to their own legal standards. Ensuring that the tools used meet the evidentiary requirements of both jurisdictions is essential for maintaining admissibility and compliance.

NEW QUESTION: 361
Which of the following information is displayed when Netstat is used with -ano switch?
A. Contents of IP routing table
B. Details of TCP and UDP connections
C. Details of routing table
D. Ethernet statistics
Answer: B (LEAVE A REPLY)

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 362

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

NEW QUESTION: 363
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. Immediately start examining the suspect's computer with any readily available digital forensic tool
B. Rely on your past experience and intuition to confirm or disprove the installation of Dropbox without formulating any hypothesis
C. Formulate a hypothesis and design an experiment to test the hypothesis on a similar system before examining the suspect's machine
D. Use the most expensive commercial tool to guarantee a thorough investigation and reliable findings
Answer: (SHOW ANSWER)

NEW QUESTION: 364
As an experienced forensic analyst, you ' ve been called upon to examine a Linux server suspected of being compromised. You are performing file system analysis using The Sleuth Kit (TSK) to discover any anomalies. While conducting the analysis, you notice that there ' s a huge amount of data and manually checking each file would be impractical. What feature of TSK should you use to automate the process and identify potential evidence more effectively?
A. File carving
B. Hash database lookup
C. File system timeline
D. Disk imaging
Answer: B (LEAVE A REPLY)
Option B. Hash database lookup is the best answer because the question is specifically about automating the review of a very large number of files and identifying potential evidence more efficiently. CHFI v11 includes hash analysis , identifying suspicious or known files through hashes , and the use of forensic tools to streamline evidence examination across large datasets.

A hash database lookup allows the investigator to compare file hashes against known-good or known-bad sets, quickly filtering out benign system files and highlighting files that are suspicious, altered, or already associated with malicious activity. This is exactly the kind of automation that reduces manual effort in a large- scale file-system analysis.
File carving is useful for recovering deleted content, but it does not primarily automate file triage. File system timeline helps reconstruct activity order, and disk imaging is an acquisition task rather than a feature for rapidly identifying potential evidence. Therefore, under CHFI forensic-analysis principles, the most effective TSK feature for automating identification of relevant evidence is hash database lookup .

Valid 312-49v11 Dumps shared by PrepPdf.com for Helping Passing 312-49v11 Exam! PrepPdf.com now offer the **newest 312-49v11 exam dumps**, the PrepPdf.com 312-49v11 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v11 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v11-prepaway-exam-dumps.html (**637** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)