Vendor: EC-Council

Exam Code: 312-49v11

Exam Name: Computer Hacking Forensic Investigator (CHFI-v11)

Version: DEMO

QUESTION 1
Forensic Investigator Alex has to collect data from a suspect's large drive in a time-bound investigation. The court would allow him to retain the original drive. Considering these factors, what should be Alex's primary considerations to ensure a forensically sound data acquisition?

A. Using Microsoft disk compression tools and validating the data acquisition process
B. Sanitizing the target media using the (German) VSITR method and acquiring volatile data
C. Enabling write protection on the evidence media and prioritizing data acquisition based on evidentiary value
D. Utilizing lossless compression tools and creating a bit-stream copy using a reliable acquisition tool

Answer: D

QUESTION 2
An investigator is analyzing EXIF metadata in a case involving cybercrime. She finds that the timestamp data has been modified, potentially misleading the investigation. What is the best next step she should take in her forensic examination?

A. Accept the tampered EXIF metadata as it's the only information available
B. Change the focus of the investigation, as tampered EXIF metadata indicates a false lead
C. Validate the EXIF metadata with other sources of information to corroborate its accuracy
D. Discard the EXIF metadata as it has been tampered with and is no longer useful

Answer: C

QUESTION 3
A Computer Hacking Forensic Investigator (CHFI) is conducting an analysis of malware obtained from a Darknet source. The CHFI is preparing to run the malware in a controlled environment and plans to record the malware's behavior for further investigation. Based on the available supporting tools, which combination would best suit the CHFI's needs in this scenario?

A. Virtual Box for virtualization, QualNet for network simulation, and Camtasia for screen capture and recording
B. Parallels Desktop 16 for virtualization, ns-3 for network simulation, and Ezvid for screen capture and recording
C. VMware vSphere Hypervisor for virtualization, Riverbed Modeler for network simulation, and Genie Backup Manager Pro for OS backup and imaging
D. Virtual Box for virtualization, NetSim for network simulation, and Snagit for screen capture and recording

Answer: D

QUESTION 4
A digital forensic investigator examines a Windows system to identify suspicious activity related to a recent cyber incident. She has collected volatile and non-volatile registry hives for analysis. The investigator has noticed modifications in a user's profile settings, including changes in desktop wallpaper and screen colors. Which hive and component cells in the registry should she examine more closely for further evidence of user-specific activity?

A. Examine HKEY_CLASSES_ROOT; focus on security descriptor cells and value cells
B. Examine HKEY_LOCAI MACHINE; focus on value cells and subkey list cells
C. Examine HKEY_CURRENT_CONFIG: focus on subkey list cells and value cells
D. Examine HKEY_CURRENT_USER; focus on key cells and value list cells

Answer: D

QUESTION 5
An investigator is examining a compromised system and comes across some files that have been compressed with a packer. The investigator knows that these files contain malicious content, but cannot access them due to a password protection mechanism. The investigator does not have the password. Which approach is the most suitable for accessing the contents of the packed files?

A. The investigator should attempt static analysis on the packed file
B. The investigator should run the packed executable in a controlled environment for dynamic analysis
C. The investigator should attempt to crack the password using a brute force attack
D. The investigator should attempt to reverse engineer the packed file in an attempt to bypass password protection

Answer: B

QUESTION 6
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 directly handed the original hardware containing the evidence
B. The new team member should be allowed to bring his own hardware and software tools to the lab for investigation
C. The new team member should be given immediate access to the lab without maintaining a visitor's log register
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

QUESTION 7
In a high-profile digital forensics investigation, a Computer Hacking Forensic Investigator (CHFI) has successfully secured digital evidence from the crime scene. The investigator must now preserve this evidence for further analysis. Which of the following actions should the investigator prioritize to ensure evidence integrity?

A. Use a tag to uniquely identify the evidence and create a chain of custody record
B. Brief the press about the types of evidence collected to maintain transparency
C. Immediately send the evidence to the forensic laboratory for detailed analysis
D. Print out a copy of all digital files to keep as a backup

Answer: A

QUESTION 8
A forensic investigator encounters a suspicious executable on a compromised system, believed to be packed using a known program packer, and is password-protected. The investigator has knowledge of the tool used for packing and has the corresponding unpacking tool. What should be the next best course of action to examine the executable?

A. Use the unpacking tool to decompress the executable, without dealing with the password
B. Run a dynamic analysis on the packed executable in a controlled environment
C. Decrypt the password to unpack the executable before analyzing
D. Use reverse engineering to understand the attack tool hidden inside

Answer: B

QUESTION 9
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. Execution of the Linuxrc program to generate the real file system for the kernel
B. Detecting the device that contains the file system and loading the necessary modules
C. Loading the kernel into memory
D. Loading the Linux kernel and optional initial RAM disk

Answer: A

QUESTION 10
In a forensic investigation on an Android device, a Computer Hacking Forensics Investigator is required to extract information from the SQLite database. They aim to recover the user's web browsing history. Which is the correct SQLite database path that the investigator should focus on?

A. \data\com.android.providers.calendar\databases\calendar.db
B. \data\data\com.android.browser\databases\browser2.db
C. \data\data\com.android.providers.telephony\databases\mmssms.db
D. \data\data\com.android.providers.contacts\databases\contacts2.db

Answer: B

QUESTION 11
After an unexpected shutdown of a company's database server, the IT forensics team is tasked with collecting data from the Database Plan Cache to investigate potential issues. What query should they use to retrieve the SQL text of all cached entries and acquire additional aggregate performance statistics?

A. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_plan_attributes(plan_handle) followed by: select * from sys.dm_exec_query_stats

B. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) followed by: select * from sys.dm_exec_plan_attributes(plan_handle)
C. Use: select * from sys.dm_exec_sql_text(plan_handle) cross apply sys.dm_exec_cached_plans followed by: select * from sys.dm_exec_query_stats
D. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) followed by: select * from sys.dm_exec_query_stats

Answer: D

QUESTION 12
An attorney requests a Computer Hacking Forensics Investigator to check for Dropbox installation on a suspect's hard drive, suspected to contain stolen intellectual property. Given the complexity of the investigation, which of the following steps should be the investigator's primary approach?

A. The investigator should skip hypothesis formulation and move directly to an experimental design
B. The investigator should use multiple open-source tools regardless of their market value to start the investigation immediately
C. The investigator should immediately begin the search for Dropbox installation artifacts without considering the Operating System (OS)
D. The investigator should formulate a hypothesis considering the Operating System (OS) and the probable Dropbox installation artifacts location in directories: C:\Users\Admin\AppData\Roaming\ or C:\Program Files (x86) or C:\Program Files

Answer: D

QUESTION 13
While investigating a potential SQL Injection Attack on a Windows-based server, a CHFI has found the following IIS log entry:

"2023-05-14 15:05:02 10.10.10.55 GET /products.php id=ORD-001%27%20or%201=l;-- 80 bob 10.10.10.12 HTTP/1.1
Mozilla/5.0+(X11;+Ubuntu;+Linux+x86_64;+rv:67.0)+Gecko/20100101+Firefox/67.0
http://www.luxurytreats.com/products.php 200 0 0 510"

Based on this log entry, which of the following is a correct assertion?

A. The attacker tried to manipulate the user login functionality of the website
B. The attacker was unsuccessful, as the HTTP 200 status code indicated
C. The attacker could execute a stored procedure on the MS SQL server
D. The attacker tried to bypass authentication using a Linux machine

Answer: D

QUESTION 14
During a recent network intrusion investigation, a CHFI received logs from Juniper IDS, Check Point IPS, and a Kippo Honeypot. Which log provides information about the network traffic and bandwidth adjustment, aiding in business risk valuation?

A. Kippo Honeypot
B. Juniper IDS
C. None of the above

D. Check Point IPS

Answer: B

QUESTION 15
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. Contact local law enforcement in the country where the attack originated
B. Gather system data before an intruder can alter it
C. Begin documenting all the traces and records of the attack in the system
D. Notify all jurisdictions involved about the breach

Answer: B

QUESTION 16
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 corresponds with the Protect America Act of 2007 which permits the surveillance of individuals who are thought to be residing outside the United States
B. This measure breaches the Privacy Act of 1974, involving the unauthorized revelation of private data
C. This measure corresponds with the Foreign Intelligence Surveillance Act of 1978, permitting the surveillance of US individuals suspected of participating in espionage
D. This measure breaches the Foreign Intelligence Surveillance Act of 1978 as no compelling evidence suggests criminal involvement

Answer: C

QUESTION 17
In a situation where an investigator needs to acquire volatile data from a live Linux system, the physical access to the suspect machine is either restricted or unavailable. Which of the following steps will be the most suitable approach to perform this task?

A. The investigator should use the Belkasoft Live RAM Capturer on the forensic workstation, then remotely execute the tool on the suspect machine to acquire the RAM image
B. The investigator should initiate a listening session on the forensic workstation using 'netcat', then execute a 'dd' command on the suspect machine and pipe the output using 'netcat'
C. The investigator should leverage OSXPMem to remotely parse the physical memory in the Linux machine and create AFF4 format images for analysis
D. The investigator should employ the LiME tool and 'netcat', starting a listening session using tcp:port on the suspect machine and then establishing a connection from the forensic workstation using 'netcat'

Answer: D

QUESTION 18
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. InnoDB storage engine, because it supports traditional ACID and crash recovery, and is used in online transaction processing systems
B. Memory storage engine, because it offers in-memory tables and implements a hashing mechanism for faster data retrieval
C. MyISAM storage engine, because it offers unlimited data storage and high-speed data loads
D. BDB storage engine, because it provides an alternative to InnoDB and supports additional transaction methods such as COMMIT and ROLLBACK

Answer: A

QUESTION 19
As part of an ongoing cyber investigation in a rapidly expanding organization, the Computer Hacking Forensic Investigator (CHFI) has to choose the most effective Security Information and Event Management (SIEM) tool for the company's ever-growing IT infrastructure. This SIEM tool must efficiently collect, index, and alert real-time machine data and offer functionalities for rapid detection and response to both internal and external threats. Additionally, the tool should be capable of leveraging AI-powered machine learning for actionable insights. Based on these requirements, the investigator should consider the following:

A. Splunk Enterprise Security (ES) only
B. Both Splunk ES and IBM QRadar, but IBM QRadar has an edge due to prebuilt reports and templates
C. Both Splunk ES and IBM QRadar, but Splunk ES has an edge due to AI-powered machine learning capabilities
D. IBM QRadar only

Answer: C

QUESTION 20
An organization is concerned about potential attacks using steganography to hide malicious data within image files. After a recent breach, the incident response team found that an attacker had managed to sneak past their defenses by hiding a keylogger inside a legitimate image. Given that the attacker has knowledge of the organization's steganography detection techniques, which method of steganalysis would likely be the most effective in detecting such a steganographic attack in the future?

A. Chi-square attack, where the analyst performs probability analysis to test whether the stego object and original data are identical
B. Known-message attack, where the analyst has a known hidden message in the corresponding stego-image and looks for patterns that arise from hiding the message
C. Known-stego attack, where the analyst knows both the steganography algorithm and original and stego-object

D. Chosen-message attack, where the analyst uses a known message to generate a stego-object in order to find the steganography algorithm used

Answer: D

QUESTION 21
Following an advanced persistent threat attack, a CHFI investigator is called in to acquire data from the compromised system. Given the wide range of potential data sources, the investigator needs to prioritize the order of data collection based on volatility. Which of the following would be the correct order to collect data in this scenario?

A. Archival media, physical configuration, network topology, disk or other storage media, temporary file systems, routing table, process table, kernel statistics, registers and processor cache
B. Archival media, disk or other storage media, temporary file systems, routing table, process table, and kernel statistics, registers and processor cache, physical configuration, and network topology
C. Registers and processor cache, routing table, process table, kernel statistics, temporary file systems, disk or other storage media, physical configuration, and network topology, archival media
D. Physical configuration, network topology, archival media, disk or other storage media, temporary file systems, routing table, process table, kernel statistics, registers and processor cache

Answer: C

QUESTION 22
During an international cybercrime investigation, your team discovers an intercepted email with a sequence of special characters. Believing that the Unicode standard might have been used in encoding the message, which of the following elements could serve as the strongest indicator of this suspicion?

A. The presence of characters from multiple modern and historic scripts
B. The presence of over 128.000 different characters in the intercepted email
C. The presence of a unique number for each character, irrespective of the platform, program, and language
D. The presence of characters from a single non-English script

Answer: C

QUESTION 23
A forensic investigator is examining an attack on a MySQL database. The investigator has been given access to a server, but the physical MySQL data files are encrypted, and the database is currently inaccessible. The attacker seems to have tampered with the data. Which MySQL utility program would most likely assist the investigator in determining the changes that occurred during the attack?

A. Mysqlbinlog, because it reads the binary log files directly and displays them in text format
B. Myisamchk, because it views the status of the MyISAM table or checks, repairs, and optimizes them
C. Mysqldump, because it allows dumping a database for backup purposes
D. Mysqlaccess, because it checks the access privileges defined for a hostname or username

Answer: A

QUESTION 24
A company is investigating an issue with one of their Windows servers that fails to boot up. The IT forensics team is called upon to determine the cause of the issue. According to the standard Windows Boot Process (BIOS-MBR method), what is the likely issue if the system fails right after the BIOS completes the power-on self-test (POST) and before the master boot record (MBR) is loaded?

A. Failure in loading the OS kernel ntoskrnl.exe
B. The system boot disk is not detected
C. Failure of the Boot Configuration Data (BCD)
D. Failure of the Bootmgr.exe

Answer: B

QUESTION 25
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. Immediately searching the dark web for similar malware signatures
B. Creating a list of IoCs from other machines in the network to check for malware presence
C. Setting up a controlled malware analysis lab to study the behavior of the malware
D. Sending a copy of the malware to anti-virus companies for urgent signature development

Answer: C

QUESTION 26
During a forensic investigation, an attorney requested a forensic investigator to check if Dropbox was installed on the suspect's hard drive. The investigator finds traces of Dropbox artifacts in C:\Users\Admin\AppData\Roaming\, C:\Program Files (x86) and C:\Program Files directories. If the hypothesis is that the operating system installed is Windows 10, and Dropbox installation is confirmed by its artifacts in the mentioned directories, which assertion is the investigator most likely to make?

A. The Dropbox was installed on the suspect's machine using the open-source version of the installation package
B. The Dropbox application was most likely installed on the system running Windows 10
C. The Dropbox artifacts were manually moved to the mentioned directories on the suspect's hard drive
D. The Dropbox installation occurred using Windows 10's built-in installation manager

Answer: B

QUESTION 27
As a Computer Hacking Forensics Investigator, you are analyzing a TCP dump of network traffic during a suspected breach. During the investigation, you noticed that the 揚ackets dropped by kernel?count was unusually high. Given that the network has a high load, what could be the most

probable reason for this situation?

A. The Tcpdump tool was run without the -c flag, causing it to capture packets indefinitely
B. The TCP packets were not matching the input expression of Tcpdump
C. The Boolean expression used with Tcpdump was too restrictive, missing some packets
D. The buffer space in the OS running Tcpdump was insufficient, leading to dropped packets

Answer: D

QUESTION 28
A Computer Hacking Forensics Investigator is analyzing a malware sample named "payload.exe". They have run the malware on a test workstation, and used a tool named WhatChanged Portable to monitor host integrity by capturing the system state before and after the malware execution. After comparing these two snapshots, the investigator observes that an entry named CjNWWyUJ has been created under the Run registry key with value C:\Users\\AppData\Local\Temp\xKNkeLQI.vbs. Given this information, what conclusion can the investigator draw?

A. The malware has corrupted the Windows registry
B. The malware is performing a denial of service attack
C. The malware creates a persistent connection with the machine on startup
D. The malware has deleted system files on the workstation

Answer: C

QUESTION 29
During a digital forensics investigation, you discovered an SQL injection attack that occurred on a MySQL database using the MyISAM storage engine. You found the '.MYD' and '.MYI' files for the attacked table in the MySQL data directory. You also identified the type of SQL injection attack as a UNION-based attack. Which of the following steps would be the most effective in your investigation?

A. Analyzing the MySQL error log (HOSTNAME.err) for irregularities
B. Checking the '.MYD' file to find evidence of the attack in the table data
C. Investigating the '.MYI' file to inspect the index of the attacked table
D. Inspecting the Binary log (HOSTNAME-bin.nnnnnn) for unusual transactions

Answer: D

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**