Vendor: EC-Council

Exam Code: 312-49v10

Exam Name: Computer Hacking Forensic Investigator (CHFI-v10)

Version: DEMO

QUESTION 1
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams.
Which of the following commands would you Issue to display the contents of a data stream?

A. echo text > program: source_file
B. myfile.dat: st ream 1
C. C:\MORE < myfile.txt:siream1
D. C:\>ECHO text_message > myfile.txt:stream1

Answer: A

QUESTION 2
Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

A. Data Protection Act of 2018
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Electronic Communications Privacy Act
D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Answer: D

QUESTION 3
In a Fllesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

A. /sbin
B. /proc
C. /mm
D. /media

Answer: A

QUESTION 4
Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?

A. Ollydbg
B. oledump
C. HashCalc
D. BinText

Answer: A

QUESTION 5

A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

A. Helix
B. R-Studio
C. NetCat
D. Wireshark

Answer: B

QUESTION 6
In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

A. init
B. Media server
C. Zygote
D. Daemon

Answer: C

QUESTION 7
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court."
Which ACPO principle states this?

A. Principle 1
B. Principle 3
C. Principle 4
D. Principle 2

Answer: D

QUESTION 8
_____allows a forensic investigator to identify the missing links during investigation.

A. Evidence preservation
B. Chain of custody
C. Evidence reconstruction
D. Exhibit numbering

Answer: C

QUESTION 9
An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies

upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?

A. BitLocker
B. Data duplication tool
C. Backup tool
D. Write blocker

Answer: D

QUESTION 10
During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
What does the first four digits (89 and 44) In the ICCID represent?

A. TAC and industry identifier
B. Country code and industry identifier
C. Industry identifier and country code
D. Issuer identifier number and TAC

Answer: C

QUESTION 11
Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

A. Stream Detector
B. TimeStomp
C. Autopsy
D. analyzeMFT

Answer: A

QUESTION 12
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. Denial-of-Service (DoS) attack
B. Malware attack
C. Ransomware attack
D. Phishing

Answer: C

QUESTION 13
When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

A. 7680
B. 49667/49668
C. 9150/9151
D. 49664/49665

Answer: C

QUESTION 14
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. PWdump7
B. HashKey
C. Nuix
D. FileMerlin

Answer: A

QUESTION 15
William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000) "GET / HTTP/1.1" 200 1861.
Which of the following logs does the log entry belong to?

A. The combined log format of Apache access log
B. The common log format of Apache access log
C. Apache error log
D. IIS log

Answer: A

QUESTION 16
What happens lo the header of the file once It Is deleted from the Windows OS file systems?

A. The OS replaces the first letter of a deleted file name with a hex byte code: E5h
B. The OS replaces the entire hex byte coding of the file.
C. The hex byte coding of the file remains the same, but the file location differs
D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

Answer: A

QUESTION 17
Sally accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored. To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?

A. Password sniffing
B. Anti-forensics

C. Brute-force attack
D. Network intrusion

Answer: B

QUESTION 18
Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

A. Block clones cannot be created with solid-state drives
B. Write blockers were used while cloning the evidence
C. John did not document the chain of custody
D. John investigated the clone instead of the original evidence itself

Answer: C

QUESTION 19
Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?

A. BMP
B. GIF
C. ASCII
D. JPEG

Answer: D

QUESTION 20
Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from client that has undergone a cyberattack. Brian ran the executable file In the virtual environment to see what it would do. What type of analysis did Brian perform?

A. Static malware analysis
B. Status malware analysis
C. Dynamic malware analysis
D. Static OS analysis

Answer: C

QUESTION 21
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. Cross-site scripting attack
D. SQL injection attack

Answer: C

QUESTION 22
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. Swap space
B. Cluster space
C. Slack space
D. Sector space

Answer: D

QUESTION 23
Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite
B. Bulk Extractor
C. Belkasoft Live RAM Capturer and AccessData FTK imager
D. Hex Editor

Answer: C

QUESTION 24
Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase
B. First Response is a part of the post-investigation phase
C. First Response is a part of the pre-investigation phase
D. First Response is neither a part of pre-investigation phase nor a part of investigation phase. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

Answer: A

QUESTION 25

Consider a scenario where the perpetrator of a dark web crime has unlnstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?

A. Swap files
B. Files in Recycle Bin
C. Security logs
D. Prefetch files

Answer: A

QUESTION 26
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 remain in its original clusters until it is overwritten
B. The data will be moved to new clusters in unallocated space
C. The data will become corrupted, making it unrecoverable
D. The data will be overwritten with zeroes

Answer: A

QUESTION 27
Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

A. Volatility
B. Autopsy
C. RAM Mapper
D. Memcheck

Answer: A

QUESTION 28
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. Dead data acquisition
B. Static data acquisition
C. Non-volatile data acquisition
D. Live data acquisition

Answer: C

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**