EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

NEW QUESTION 1
- (Exam Topic 1)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments.
What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Bit-stream Copy
B. Robust Copy
C. Full backup Copy
D. Incremental Backup Copy

Answer: C

NEW QUESTION 2
- (Exam Topic 2)
Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

A. Identifying File Dependencies
B. Strings search
C. Dynamic analysis
D. File obfuscation

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
Printing under a Windows Computer normally requires which one of the following files types to be created?

A. EME
B. MEM
C. EMF
D. CME

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Perform a zone transfer
D. Enumerate all the users in the domain

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
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. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Data link layer firewall

Answer: C

NEW QUESTION 6
- (Exam Topic 1)
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A. The manufacturer of the system compromised
B. The logic, formatting and elegance of the code used in the attack
C. The nature of the attack
D. The vulnerability exploited in the incident

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Answer: A

NEW QUESTION 8
- (Exam Topic 4)
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 Second Amendment of the U.
B. Constitution
C. Compliance with the Third Amendment of the U.
D. Constitution
E. None of these
F. Compliance with the Fourth Amendment of the U.
G. Constitution

Answer: D

NEW QUESTION 9
- (Exam Topic 4)
To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

A. Post-investigation phase
B. Reporting phase
C. Pre-investigation phase
D. Investigation phase

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:

A. Threat hunting
B. Threat analysis
C. Static analysis
D. Dynamic analysis

Answer: B

NEW QUESTION 11
- (Exam Topic 4)
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

NEW QUESTION 12
- (Exam Topic 3)
Which list contains the most recent actions performed by a Windows User?

A. MRU
B. Activity
C. Recents
D. Windows Error Log

Answer: A

NEW QUESTION 13
- (Exam Topic 3)
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

A. DependencyWalker
B. SysAnalyzer
C. PEiD
D. ResourcesExtract

Answer: A

NEW QUESTION 14
- (Exam Topic 3)
One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. The file header
B. The File Allocation Table
C. The file footer
D. The sector map

Answer: A

NEW QUESTION 15
- (Exam Topic 3)
Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe
B. pmdump.exe
C. processdump.exe
D. pdump.exe

Answer: B

NEW QUESTION 16
- (Exam Topic 3)
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness
B. Evidence Examiner
C. Forensic Examiner
D. Defense Witness

Answer: A

NEW QUESTION 17
- (Exam Topic 2)
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

A. Microsoft Outlook
B. Eudora
C. Mozilla Thunderbird
D. Microsoft Outlook Express

Answer: D

NEW QUESTION 18
- (Exam Topic 2)
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 a doc file deleted in seventh sequential order
B. RIYG6VR.doc is the name of the doc file deleted from the system
C. It is file deleted from R drive
D. It is a deleted doc file

Answer: D

NEW QUESTION 19
- (Exam Topic 2)
Which of the following Event Correlation Approach checks and compares all the fields systematically and
intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Rule-Based Approach
B. Automated Field Correlation
C. Field-Based Approach
D. Graph-Based Approach

Answer: B

NEW QUESTION 20
- (Exam Topic 2)
Which of the following tools will help the investigator to analyze web server logs?

A. XRY LOGICAL
B. LanWhois
C. Deep Log Monitor
D. Deep Log Analyzer

Answer: D

NEW QUESTION 21
......