Exam : EC-Council 312-49

Title : Computer Hacking Forensic Investigator

Version : Demo

Important Note, Please Read Carefully

Other examsoon products

All examsoon IT Exam Products

Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

examsoon Testing Engine

Guarantee

Examsoon provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!.

Features

1. Comprehensive questions with complete details
2. Instant Downloadable in PDF form.
3. Verified Answers Researched by Industry Experts
4. Questions accompanied by exhibits
5. Drag and Drop questions as experienced in the Actual Exams.
6. These questions and answers are backed by our GUARANTEE.
7. Questions updated on regular basis.
8. Like actual certification exams our product is in multiple-choice questions (MCQs).

1. As a CHFI professional, which of the following is the most important to your professional reputation?

A. Your Certifications

B. The correct, successful management of each and every case

C. The free that you charge

D. The friendship of local law enforcement officers

Answer: B

2. In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation.

What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you

D. ISP's never maintain log files so they would be of no use to your investigation

Answer: B

3. You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

A. ARP Poisoning

B. DNS Poisoning

C. HTTP redirect attack

D. IP Spoofing

Answer: B

4. You are working as an independent computer forensics investigator and receive 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 proceedings?

A. Bit-stream Copy

B. Robust Copy

C. Full backup Copy

D. Incremental Backup Copy

Answer: A

5. Law enforcement officers are conducting a legal search for which a valid warrant was obtained. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine

B. Corpus delicti

C. Locard Exchange Principle

D. Ex Parte Order

Answer: A

6. Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email

B. .mail

C. .pst

D. .doc

Answer: C

7. The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection

B. Hearsay

C. Spoliation

D. Discovery

Answer: D

8. The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost

B. All running processes will be lost

C. The /tmp directory will be flushed

D. Power interruption will corrupt the pagefile

Answer: AB

9. You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files

D. Email Header

Answer: D

10. Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for

loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY_LOCAL_MACHINE\hardware\windows\start

B. HKEY_LOCAL_USERS\Software|Microsoft\old\Version\Load

C. HKEY_CURRENT_USER\Microsoft\Default

D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

Answer: D

Examsoon.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, Juniper, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

You can reach us at any of the email addresses listed below.

E-MAIL: examsoon(at)hotmail.Com