

312-49 Practice Test

EC-COUNCIL Computer Hacking Forensic Investigator

312-49: Computer Hacking Forensic Investigator

Practice Exam: 312-49 Exams

Exam Number/Code: 312-49

Exam Name: Computer Hacking Forensic Investigator

Questions and Answers: 141 Q&As

(Certified Ethical Hacker)



Exam : [312-49](#)

For candidates making preparation for the EC-COUNCIL 312-49 questions and answers, what they most desire is to easily pass the 312-49 (Computer Hacking Forensic Investigator) exam. ItCertHome 312-49 includes 141 questions and answers, which are collected and collated by experts of EC-COUNCIL. With our 312-49 study materials, you can successfully take EC-COUNCIL certification of 312-49 exam and go further on EC-COUNCIL career path.

Free 312-49 Demo

we provide EC-COUNCIL 312-49 demo exam for free (in PDF format) before you decide to purchase it. Thus,you can know better about the quality of our practice exam and then make your right decision.

ItCertHome Test tool's advantages:

High Quality and Value of 312-49 exam

ItCertHome EC-COUNCIL Certified Ethical Hacker 312-49 Practice Questions is developed and finished by EC-COUNCIL technical team , cover every field of the exam . Besides, we have verified 312-49 answers,almost 100% correct.

100% Guarantee to Pass 312-49 Exam

We promise to give you FULL REFUND if you fail the Certified Ethical Hacker 312-49 certification(EC-COUNCIL Certified Network Associate) with the use of our ItCertHome testing engine.

312-49 Self Test Mode

ItCertHome provides a simulated and interactive environment where you can test your knowledge and skills about 312-49 to ensure enough assurance in real testing center.

Periodic Updates of ItCertHome 312-49

Once there is some change on EC-COUNCIL 312-49 exam, we will update it timely, and the product you buy will be updated within 90 days for free.

Professional and Efficient Service

We offer 7*24 customer support via diverse channels: LIVE CHAT,MAIL.Expecting the communication with you about IT certification.

The Questions & Answers cover the latest real test and with all the correct answer.we promise the Q&A for **EC-COUNCIL Certified Ethical Hacker 312-49** examination of original title complete coverage.ItCertHome **312-49 Braindumps** Questions & Answers help you pass the exam. Otherwise,we will give you a full refund.

We promised that use ItCertHome Q&A ensure you pass the exam at your first try.

1. The Q&A are from cooperation exam center of the real original title,summaried by our professional team and collated by senior IT lectured in co-training center to make sure the professional quality of the Q&A.The correctly of the Q&A is 100%, the coverage of 312-49 Q&A are more than 96%.All you need to study the whole 312-49 Q&A before you participate the certification exam,it should be possible to easily complete the exam and pass the

certification.

2. ItCertHome to all the Q&A, we promised "do not pass the exam give you a full refund". If you buy our 312-49 Q&A and did not pass the exam at the first try. You can take the examination report card that stamped with PROMETRIC or VUE test centers Seal. we will refund your full cost of 312-49 Q&A, absolutely guarantee you interests have no losses.(For a full refund details)

3. ItCertHome professional IT Q&A vendors, we provide well after-sale service. To all the customers buy the Q&A, we provide track service. when you buy the Q&A with in one year. you can enjoy the upgrade Q&A service for free. If in this period, the certified test center change the 312-49 Q&A, we will update the Q&A in the first time, and provide you the download update for free.

EC-COUNCIL 312-49 Test belongs to one of the Certified Ethical Hacker certified test, if needs to obtain the Certified Ethical Hacker certificate, you also need to participate in other related test, the details you may visit the Certified Ethical Hacker certified topic, in there, you will see all related Certified Ethical Hacker certified subject of examination.

312-49

ItCertHome professional provide Certified Ethical Hacker 312-49 the newest Q&A, completely covers 312-49 test original topic. With our complete Certified Ethical Hacker resources, you will minimize your Certified Ethical Hacker cost and be ready to pass your 312-49 tests on Your First Try, 100% Money Back Guarantee included!

This 312-49 PDF demo do not include the questions and answers's picture:

Exam : EC-Council 312-49

Title : Computer Hacking Forensic Investigator

1. 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

2. 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_MACHINEhardwarewindowsstart
- B. HKEY_LOCAL_USERSSoftware|MicrosoftoldVersionLoad
- C. HKEY_CURRENT_USERMicrosoftDefault
- D. HKEY_LOCAL_MACHINESoftwareMicrosoftCurrentVersionRun

Answer: D

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

- A. .email
- B. .mail
- C. .pst

D. .doc

Answer: C

4. 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

5. 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

6. 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 fees that you charge

D. The friendship of local law enforcement officers

Answer: B

7. The efforts to obtain information before a trial 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. 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

9. 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

10. 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

More [312-49 practice test](#)

Related 312-49 Exams

[EC0-350](#) *ethical hacking and countermeasures*

[312-49](#) *Computer Hacking Forensic Investigator*

[312-50](#) *Ethical Hacking and Countermeasures (CEHv6)*

[EC0-349](#) *Computer Hacking Forensic Investigator*

Other EC-COUNCIL Exams

[EC0-350](#)

[EC0-232](#)

[EC0-479](#)

[312-50](#)

[412-79](#)

[312-49](#)

[EC0-349](#)