312-49

(Computer Hacking Forensic Investigator)

Total Questions: 75

Last Updated: Jan 01, 2009

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' 312-49 study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: **refund@techeXams.ws**. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: **feedback@techeXams.ws**

Copyright

Question: 1

When an investigator contacts by telephone the domain administrator or controller listed by a whois lookup to request all e-mails sent and received for a user account be preserved, what
U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)

Answer: D

Question: Item 2

If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip coordinates several honeypots
B. A sheepdip computer is another name for a honeypot
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer defers a denial of service attack

Answer: C

Question: 3

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. rules of evidence
B. law of probability
C. chain of custody
D. policy of separation

Answer: C

Question: 4

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 128
B. 64
C. 32
D. 16

Answer: C

Question: 5

To calculate the nu

A. number of circl ector
B. number of cylin r sector
C. number of cells or
D. number of cylin r sector

lback@TechExams.ws

Question: 6

What does the supe

A. file system nam
B. available space
C. location of the f
D. disk geometry

Answer: B, C, D

Question: 7

A honey pot deploy attacker . Given below is an excerpt the activity carried out by the attacker ed to infer only what is explicit in th cepts learnt during passive OS fingerpri lity to read packet signatures from a sr

A. The attacker ha
B. The attacker ha

Answer: A