EC0-349

ECCouncil

Computer Hacking Forensic Investigator

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your EC0-349 exam in first attempt and also get high scores to acquire ECCouncil certification.

If you use OfficialCerts EC0-349 Certification questions and answers, you will experience actual EC0-349 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ECCouncil exam prep covers over 95% of the questions and answers that may be appeared in your EC0-349 exam. Every point from pass4sure EC0-349 PDF, EC0-349 review will help you take ECCouncil EC0-349 exam much easier and become ECCouncil certified.

Here's what you can expect from the OfficialCerts ECCouncil EC0-349 course:

** Up-to-Date ECCouncil EC0-349 questions as experienced in the real exam.*
** 100% correct ECCouncil EC0-349 answers you simply can't find in other EC0-349 courses.*
** All of our tests are easy to download. Your file will be saved as a EC0-349 PDF.*
** ECCouncil EC0-349 brain dump free content featuring the real EC0-349 test questions.*

ECCouncil EC0-349 certification exam is of core importance both in your Professional life and ECCouncil certification path. With ECCouncil certification you can get a good job easily in the market and get on your path for success. Professionals who passed ECCouncil EC0-349 exam training are an absolute favorite in the industry. You will pass ECCouncil EC0-349 certification test and career opportunities will be open for you.

http://www.officialcerts.com/exams.asp?examcode=EC0-349

EC0-349

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 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 number of bytes on a disk, the formula is: CHS**

A. number of circles x number of halves x number of sides x 512 bytes per sector
B. number of cylinders x number of halves x number of shims x 512 bytes per sector
C. number of cells x number of heads x number of sides x 512 bytes per sector
D. number of cylinders x number of halves x number of shims x 512 bytes per sector

Answer:

QUESTION 6:

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

A. 0:1000, 150
B. 0:1709, 150
C. 1:1709, 150
D. 0:1709-1858

Answer: B

QUESTION 7:

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt. (Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23678634 2878772
=+=
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104
Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c............
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....
3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost
=+=
+
03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168
TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF
AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23679878 2880015
63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;
69 64 3B id;

A. The attacker has conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow
C. The attacker has used a Trojan on port 32773
D. The attacker has installed a backdoor

Answer: A

QUESTION 8:

The newer Macintosh Operating System is based on:

A. OS/2
B. BSD Unix
C. Linux
D. Microsoft Windows

Answer: B

QUESTION 9:

Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness

Answer: D

QUESTION 10:

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google