EC0-349 Q&As

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/ec0-349.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

![Pass2Lead](https://Pass2Lead.com)
QUESTION 1

What does mactime, an essential part of the coroner\\\'s toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is too specific to the MAC OS and forms a core component of the toolkit

Correct Answer: A

QUESTION 2

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field

B. TCP header field

C. IP header field

D. UDP header field

Correct Answer: B

QUESTION 3

From the following spam mail header, identify the host IP that sent this spam?

From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001 Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT) Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT) Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web" To: "Shlam" Subject: SHANGHAI (HILTON HOTEL) PACKAGE Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0 X-Priority: 3 X-MSMail-Priority: Normal Reply-To: "china hotel web"

A. 137.189.96.52

B. 8.12.1.0

C. 203.218.39.20

D. 203.218.39.50

Correct Answer: C

QUESTION 4

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

Correct Answer: C

QUESTION 5

Sectors in hard disks typically contain how many bytes?

A. 256

B. 512

C. 1024

D. 2048

Correct Answer: B

Latest EC0-349 Dumps   EC0-349 Practice Test   EC0-349 Braindumps