EC1-349$^{Q\&As}$

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.geekcert.com/ec1-349.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the goal of forensic science?

A. To determine the evidential value of the crime scene and related evidence

B. Mitigate the effects of the information security breach

C. Save the good will of the investigating organization

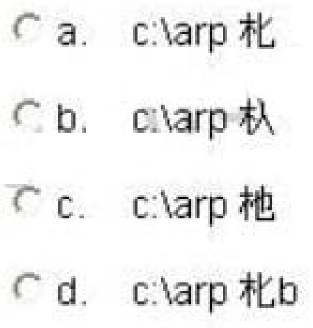
D. It is a disciple to deal with the legal processes

Correct Answer: A

QUESTION 2

The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.

The ARP table can be accessed using the __________command in Windows 7.



○ a. c:\arp 朼

○ b. c:\arp 朳

○ c. c:\arp 杝

○ d. c:\arp 朼b

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 3

John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf?John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched

B. It is not necessary to scan the virtual memory of a computer

C. It contains the times and dates of all the system files

D. Hidden running processes

Correct Answer: D

QUESTION 4

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Dig

B. Ping sweep

C. Netcraft

D. Nmap

Correct Answer: C

QUESTION 5

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

A. .email

B. .mail

C. .pst

D. .doc

Correct Answer: C