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.passapply.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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers

QUESTION 1

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of one

B. Firewalk sets all packets with a TTL of zero

C. Firewalk cannot pass through Cisco firewalls

D. Firewalk cannot be detected by network sniffers

Correct Answer: A

QUESTION 2

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. 127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200 2326

B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test

C. http://victim.com/scripts/..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af./..%c0%af ./..%c0%af./../winnt/system32/cmd.exe?/c+di r+c:\wintt\system32\Logfiles\W3SVC1

D. 127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0\\' 200 2326

Correct Answer: B

QUESTION 3

Where does Encase search to recover NTFS files and folders?

A. MBR

B. MFT

C. Slack space

D. HAL

Correct Answer: B

QUESTION 4

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A. 8

B. 1

C. 4

D. 2

Correct Answer: C

QUESTION 5

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

Latest EC1-349 Dumps   EC1-349 Study Guide   EC1-349 Exam Questions