412-79$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

QUESTION 1

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

A. All sites that link to ghttech.net

B. Sites that contain the code: link:www.ghttech.net

C. All sites that ghttech.net links to

D. All search engines that link to .net domains

Correct Answer: A

QUESTION 2

In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available

B. The longer a disk is inuse, the less likely it is that deleted files will be overwritten

C. While booting, the machine may create temporary files that can delete evidence

D. Secure delete programs work by completely overwriting the file in one go

Correct Answer: CD

QUESTION 3

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 t preview them

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

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

Correct Answer: A

QUESTION 4

Windows identifies which application to open a file with by examining which of the following?

A. The File extension

B. The file attributes

C. The file Signature at the end of the file

D. The file signature at the beginning of the file

Correct Answer: A

QUESTION 5

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

A. Encryption of agent communications will conceal the presence of the agents

B. Alerts are sent to the monitor when a potential intrusion is detected

C. An intruder could intercept and delete data or alerts and the intrusion can go undetected

D. The monitor will know if counterfeit messages are being generated because they will not be encrypted

Correct Answer: D