DUMPSARENA

Computer Hacking Forensic Investigator (CHFI-v10)

ECCouncil 312-49v10

Version Demo

Total Demo Questions: 12

Total Premium Questions: 714

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

A. Physical block

B. Operating system block

C. Hard disk block

D. Logical block

ANSWER: A

QUESTION NO: 2

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

QUESTION NO: 3

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

A. Civil Investigation

B. Administrative Investigation

C. Both Civil and Criminal Investigations

D. Criminal Investigation

ANSWER: B

QUESTION NO: 4

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable

B. Administratively Blocked

C. Port Unreachable

D. Protocol Unreachable

ANSWER: B

QUESTION NO: 5

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame.

What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

QUESTION NO: 6

In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Chosen-message attack

B. Known-cover attack

C. Known-message attack

D. Known-stego attack

ANSWER: A

Explanation:

Reference: https://www.giac.org/paper/gsec/707/steganalysis-overview/101589 (3)

QUESTION NO: 7

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To control the room temperature

B. To strengthen the walls, ceilings, and floor

C. To avoid electromagnetic emanations

D. To make the lab sound proof

ANSWER: D

QUESTION NO: 8

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)

B. Integrated Circuit Code (ICC)

C. Manufacturer Identification Code (MIC)

D. Device Origin Code (DOC)

ANSWER: A

QUESTION NO: 9

When investigating a Windows System, it is important to view the contents of the page or swap file because:

A. Windows stores all of the systems configuration information in this file

B. This is file that windows use to communicate directly with Registry

C. A Large volume of data can exist within the swap file of which the computer user has no knowledge

D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

ANSWER: C

QUESTION NO: 10

Which U.S. Federal law requires financial institutions that offer consumers financial products or services to protect their customers' private information?

A. Payment Card Industry Data Security Standard (PCI DSS)

B. Federal Information Security Management Act of 2002 (FISMA)

C. Health insurance Portability and Accountability Act of 1996 (HIPAA)

D. Gramm-Leach-Bliley Act (GLBA)

ANSWER: A

QUESTION NO: 11

What is the first step taken in an investigation for laboratory forensic staff members?

A. Packaging the electronic evidence

B. Securing and evaluating the electronic crime scene

C. Conducting preliminary interviews

D. Transporting the electronic evidence

ANSWER: B

QUESTION NO: 12

"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court" - this principle Is advocated by which of the following?

A. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

B. Locard's exchange principle

C. Scientific Working Group on Imaging Technology (SWGIT)

D. FBI Cyber Division

ANSWER: A