Vendor:EC-COUNCIL

Exam Code:312-49

Exam Name:ECCouncil Computer Hacking Forensic Investigator (V9)

Version: Demo

QUESTION 1

Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it

B. Give the Operating System a minimal amount of memory, forcing it to use a swap file

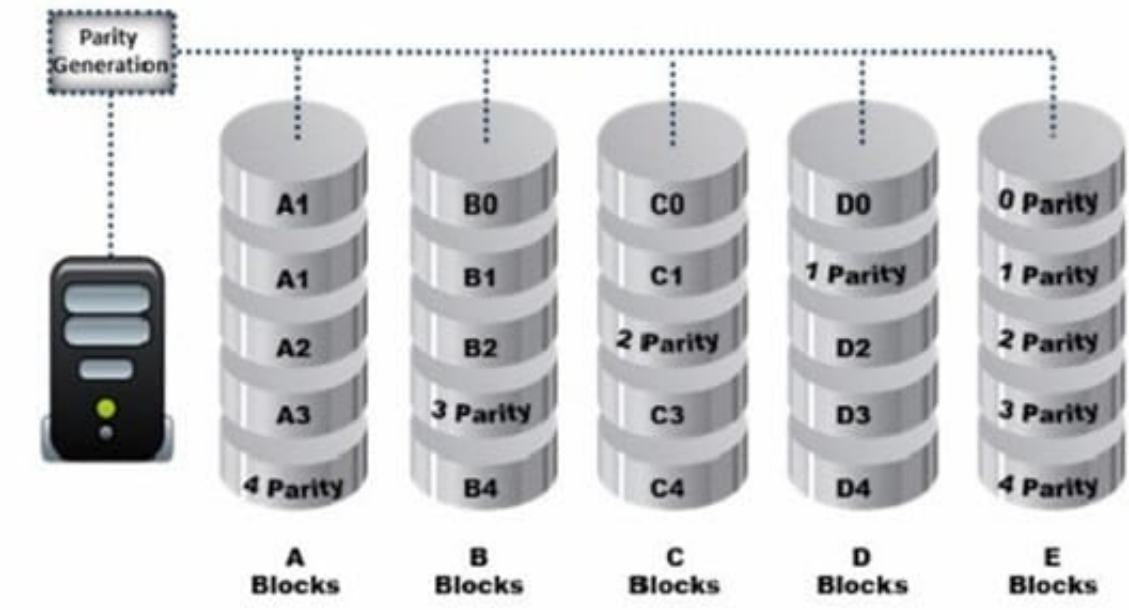
C. Create a Separate partition of several hundred megabytes and place the swap file there

D. Use intrusion forensic techniques to study memory resident infections

Correct Answer: C

QUESTION 2

Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

A. RAID Level 0

B. RAID Level 5

C. RAID Level 3

D. RAID Level 1

Correct Answer: B

QUESTION 3

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator

B. Network Administrator

C. Director of Information Technology

D. Director of Administration

Correct Answer: B

QUESTION 4

Jacky encrypts her documents using a password. It is known that she uses her daughter\\'s year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Rule-based attack

B. Brute force attack

C. Syllable attack

D. Hybrid attack

Correct Answer: A

QUESTION 5

Which of the following is a device monitoring tool?

A. Capsa

B. Driver Detective

C. Regshot

D. RAM Capturer

Correct Answer: A

QUESTION 6

Who is responsible for the following tasks?

Secure the scene and ensure that is maintained in a secure state until the Forensic Team advises Make notes about the

scene that will eventually be handed over to the Forensic Team

A. Non-forensics staff

B. Lawyers

C. System administrators

D. Local managers or other non-forensic staff

Correct Answer: A

QUESTION 7

Paraben Lockdown device uses which operating system to write hard drive data?

A. Mac OS

B. Red Hat

C. Unix

D. Windows

Correct Answer: D

QUESTION 8

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A. logical

B. anti-magnetic

C. magnetic

D. optical

Correct Answer: D

QUESTION 9

George is a senior security analyst working for a state agency in Florida. His state\\'s congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection

B. Pattern matching

C. Real-time anomaly detection

D. Statistical-based anomaly detection

Correct Answer: C

QUESTION 10

What does the command "C:\>wevtutil gl " display?

A. Configuration information of a specific Event Log

B. Event logs are saved in .xml format

C. Event log record structure

D. List of available Event Logs

Correct Answer: A

QUESTION 11

Which of the following setups should a tester choose to analyze malware behavior?

A. A virtual system with internet connection

B. A normal system without internet connect

C. A normal system with internet connection

D. A virtual system with network simulation for internet connection

Correct Answer: D

QUESTION 12

Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

A. Written Formal Report

B. Verbal Formal Report

C. Verbal Informal Report

D. Written Informal Report

Correct Answer: B