

# TestHorse

Certified IT practice exam authority

---

Accurate study guides, High passing rate!  
Testhorse provides update free of charge in one year!



**Exam** : **312-49v9**

**Title** : EC Council Computer  
Hacking Forensic  
Investigator (V9)

**Version** : DEMO

1.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 to preview them
- C. The tools scans for i-node information, which is used by other tools in the tool kit
- D. It is too specific to the MAC OS and forms a core component of the toolkit

**Answer: A**

2.Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities.

Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

- A. Closed
- B. Open
- C. Stealth
- D. Filtered

**Answer: B**

3.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

**Answer: A**

4.When conducting computer forensic analysis, you must guard against \_\_\_\_\_ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

- A. Hard Drive Failure
- B. Scope Creep
- C. Unauthorized expenses
- D. Overzealous marketing

**Answer: B**

5.After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

- A. Enable direct broadcasts
- B. Disable direct broadcasts
- C. Disable BGP
- D. Enable BGP

**Answer: B**