GCIH Practice Test Questions and Answers

1. What is the primary focus of incident handling and response?

A) Preventing all security incidents

B) Containing, analyzing, and recovering from security incidents

C) Installing security software

D) Training end users

2. Which phase comes first in the incident response process?

A) Recovery

B) Preparation

C) Containment

D) Investigation

3. What is the main purpose of preserving digital evidence during incident response?

A) To speed up recovery

B) To maintain chain of custody for potential legal proceedings

C) To reduce storage costs

D) To improve system performance

4. Which tool is commonly used for network traffic analysis during incident response?

A) Microsoft Word

B) Wireshark

C) Adobe Photoshop

D) Web browser

Answers: 1-B 2-B 3-B 4-B