212-89 Q&As

EC-Council Certified Incident Handler

Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/212-89.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The state of incident response preparedness that enables an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation is called:

A. Computer Forensics

B. Digital Forensic Analysis

C. Forensic Readiness

D. Digital Forensic Policy

Correct Answer: C

QUESTION 2

Incident Response Plan requires

A. Financial and Management support

B. Expert team composition

C. Resources

D. All the above

Correct Answer: D

QUESTION 3

Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

A. Evidence Supervisor

B. Evidence Documenter

C. Evidence Manager

D. Evidence Examiner/ Investigator

Correct Answer: D

QUESTION 4

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

A. Snort

B. Wireshark

C. Cain and Able

D. nmap

Correct Answer: B

QUESTION 5

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

A. An insider intentionally deleting files from a workstation

B. An attacker redirecting user to a malicious website and infects his system with Trojan

C. An attacker infecting a machine to launch a DDoS attack

D. An attacker using email with malicious code to infect internal workstation

Correct Answer: A