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.geekcert.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

An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:

A. It helps calculating intangible losses to the organization due to incident

B. It helps tracking individual actions and allows users to be personally accountable for their actions

C. It helps in compliance to various regulatory laws, rules,and guidelines

D. It helps in reconstructing the events after a problem has occurred

Correct Answer: A

QUESTION 2

Business Continuity provides a planning methodology that allows continuity in business operations:

A. Before and after a disaster

B. Before a disaster

C. Before, during and after a disaster

D. During and after a disaster

Correct Answer: C

QUESTION 3

Incidents such as DDoS that should be handled immediately may be considered as:

A. Level One incident

B. Level Two incident

C. Level Three incident

D. Level Four incident

Correct Answer: C

QUESTION 4

A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

A. Trojans

B. Zombies

C. Spyware

D. Worms

Correct Answer: B

QUESTION 5

Which of the following is a risk assessment tool:

A. Nessus

B. Wireshark

C. CRAMM

D. Nmap

Correct Answer: C