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 incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

A. Incident recording

B. Reporting

C. Containment

D. Identification

Correct Answer: D

QUESTION 2

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

A. Digital evidence

B. Computer Emails

C. Digital investigation

D. Digital Forensic Examiner

Correct Answer: A

QUESTION 3

A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to propagate is called:

A. Trojan

B. Worm

C. Virus

D. RootKit

Correct Answer: C

QUESTION 4

Business Continuity planning includes other plans such as:

A. Incident/disaster recovery plan

B. Business recovery and resumption plans

C. Contingency plan

D. All the above

Correct Answer: D

QUESTION 5

An estimation of the expected losses after an incident helps organization in prioritizing and formulating their incident response. The cost of an incident can be categorized as a tangible and intangible cost. Identify the tangible cost associated with virus outbreak?

A. Loss of goodwill

B. Damage to corporate reputation

C. Psychological damage

D. Lost productivity damage

Correct Answer: D