



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

Which test is conducted to determine the incident recovery procedures effectiveness?

- A. Live walk-throughs of procedures
- B. Scenario testing
- C. Department-level test
- D. Facility-level test

Correct Answer: A

QUESTION 2

Incident response team must adhere to the following: A. Stay calm and document everything

- B. Assess the situation
- C. Notify appropriate personnel
- D. All the above

Correct Answer: D

QUESTION 3

Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

- A. (Probability of Loss) X (Loss)
- B. (Loss) / (Probability of Loss)
- C. (Probability of Loss) / (Loss)
- D. Significant Risks X Probability of Loss X Loss

Correct Answer: A

QUESTION 4

The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:

- A. Incident Management
- B. Incident Response



C. Incident Recovery

D. Incident Handling

Correct Answer: C

QUESTION 5

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

A. Network and host log records

B. Chain-of-Custody

C. Forensic analysis report

D. Chain-of-Precedence

Correct Answer: B

[Latest 212-89 Dumps](#)

[212-89 Practice Test](#)

[212-89 Study Guide](#)