# 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

2 / 3

## QUESTION 1

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 2

Which is the incorrect statement about Anti-keyloggers scanners: A. Detect already installed Keyloggers in victim machines

B. Run in stealthy mode to record victims online activity

C. Software tools

Correct Answer: B

## QUESTION 3

Digital evidence must:

A. Be Authentic, complete and reliable

B. Not prove the attackers actions

C. Be Volatile

D. Cast doubt on the authenticity and veracity of the evidence

Correct Answer: A

## QUESTION 4

Preventing the incident from spreading and limiting the scope of the incident is known as:

A. Incident Eradication

B. Incident Protection

C. Incident Containment

D. Incident Classification

Correct Answer: C

---

**QUESTION 5**

What command does a Digital Forensic Examiner use to display the list of all IP addresses and their associated MAC addresses on a victim computer to identify the machines that were communicating with it:

A. "arp" command

B. "netstat ?n" command

C. "dd" command

D. "ifconfig" command

Correct Answer: A