



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.pass4itsure.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 data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?

- A. Containment
- B. Eradication
- C. Incident recording
- D. Incident investigation

Correct Answer: A

QUESTION 2

Which of the following is NOT a digital forensic analysis tool:

- A. Access Data FTK
- B. EAR/ Pilar
- C. Guidance Software EnCase Forensic
- D. Helix

Correct Answer: B

QUESTION 3

The type of relationship between CSIRT and its constituency have an impact on the services provided by the CSIRT. Identify the level of the authority that enables members of CSIRT to undertake any necessary actions on behalf of their constituency?

- A. Full-level authority
- B. Mid-level authority
- C. Half-level authority
- D. Shared-level authority

Correct Answer: A

QUESTION 4

Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to



damage company assets:

- A. Gain privileged access, install malware then activate
- B. Install malware, gain privileged access, then activate
- C. Gain privileged access, activate and install malware
- D. Activate malware, gain privileged access then install malware

Correct Answer: A

QUESTION 5

The most common type(s) of intellectual property is(are):

- A. Copyrights and Trademarks
- B. Patents
- C. Industrial design rights and Trade secrets
- D. All the above

Correct Answer: D

[Latest 212-89 Dumps](#)

[212-89 PDF Dumps](#)

[212-89 Study Guide](#)