



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

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

- A. "arp" command
- B. "netstat ?n" command
- C. "dd" command
- D. "ifconfig" command

Correct Answer: B

QUESTION 2

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 3

Incidents are reported in order to:

- A. Provide stronger protection for systems and data
- B. Deal properly with legal issues
- C. Be prepared for handling future incidents
- D. All the above

Correct Answer: D

QUESTION 4

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?



- A. Links the appropriate technology to the incident to ensure that the foundation's offices are returned to normal operations as quickly as possible
- B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
- C. Applies the appropriate technology and tries to eradicate and recover from the incident
- D. Focuses on the incident and handles it from management and technical point of view

Correct Answer: B

QUESTION 5

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

[212-89 PDF Dumps](#)

[212-89 Exam Questions](#)

[212-89 Braindumps](#)