![Leads4Pass logo]

212-89 ^{Q&As}
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.leads4pass.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 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 2

The policy that defines which set of events needs to be logged in order to capture and review the important data in a timely manner is known as:

A. Audit trail policy

B. Logging policy

C. Documentation policy

D. Evidence Collection policy

Correct Answer: B

QUESTION 3

A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

A. Trojans

B. Zombies

C. Spyware

D. Worms

Correct Answer: B

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

According to US-CERT; if an agency is unable to successfully mitigate a DOS attack it must be reported within:

A. One (1) hour of discovery/detection if the successful attack is still ongoing

B. Two (2) hours of discovery/detection if the successful attack is still ongoing

C. Three (3) hours of discovery/detection if the successful attack is still ongoing

D. Four (4) hours of discovery/detection if the successful attack is still ongoing

Correct Answer: B

[212-89 PDF Dumps](link)   [212-89 Practice Test](link)   [212-89 Exam Questions](link)