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

In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called: A. Honey Pots

B. Relays

C. Zombies

D. Handlers

Correct Answer: C

QUESTION 2

Which of the following is a correct statement about incident management, handling and response:

A. Incident response is on the functions provided by incident handling

B. Incident handling is on the functions provided by incident response

C. Triage is one of the services provided by incident response

D. Incident response is one of the services provided by triage

Correct Answer: A

QUESTION 3

Adam calculated the total cost of a control to protect 10,000 $ worth of data as 20,000 $. What do you advise Adam to do?

A. Apply the control

B. Not to apply the control

C. Use qualitative risk assessment

D. Use semi-qualitative risk assessment instead

Correct Answer: B

QUESTION 4

A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency\\'s reporting timeframe guidelines, this incident should be reported within two

(2)

HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

A.

CAT 5

B.

CAT 1

C.

CAT 2

D.

CAT 6

Correct Answer: C

QUESTION 5

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

A. To restore the original site, tests systems to prevent the incident and terminates operations

B. To define the notification procedures, damage assessments and offers the plan activation

C. To provide the introduction and detailed concept of the contingency plan

D. To provide a sequence of recovery activities with the help of recovery procedures

Correct Answer: A

212-89 Practice Test 212-89 Study Guide 212-89 Braindumps