

KTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.ktest.jp>

1年で無料進級することに提供する

Exam : **212-89**

Title : EC Council Certified
Incident Handler (ECIH v2)

Version : DEMO

1.Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?”

- A. Risk
- B. Vulnerability
- C. Threat
- D. Incident Response

Answer: A

2.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

Answer: B

3.The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost.

Which of the following does NOT constitute a goal of incident response?

- A. Dealing with human resources department and various employee conflict behaviors.
- B. Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.
- C. Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.
- D. Dealing properly with legal issues that may arise during incidents.

Answer: A

4.An organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization’s incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness.

How would you categorize such information security incident?

- A. High level incident
- B. Middle level incident
- C. Ultra-High level incident
- D. Low level incident

Answer: A

5.Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy.

Identify the plan which is mandatory part of a business continuity plan?

- A. Forensics Procedure Plan
- B. Business Recovery Plan
- C. Sales and Marketing plan
- D. New business strategy plan

Answer: B