212-89Q&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.pass2lead.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

QUESTION 1

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim\\'s system is called:

A. Trojan

B. Worm

C. Virus

D. RootKit

Correct Answer: A

QUESTION 2

The main difference between viruses and worms is:

A. Worms require a host file to propagate while viruses don\\'t

B. Viruses require a host file to propagate while Worms don\\'t

C. Viruses don\\'t require user interaction; they are self-replicating malware

D. Viruses and worms are common names for the same malware

Correct Answer: B

QUESTION 3

Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:

A. Outsider threats

B. Social Engineers

C. Insider threats

D. Zombies

Correct Answer: C

QUESTION 4

Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

A. Correlating known patterns of suspicious and malicious behavior

B. Protecting computer systems by implementing proper controls

C. Making is compulsory for employees to sign a none disclosure agreement

D. Categorizing information according to its sensitivity and access rights

Correct Answer: A

QUESTION 5

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

Correct Answer: B