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

QUESTION 1

One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers\\' security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:

A. Interactive approach

B. Introductive approach

C. Proactive approach

D. Qualitative approach

Correct Answer: C

QUESTION 2

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

A. Snort

B. Wireshark

C. Cain and Able

D. nmap

Correct Answer: B

QUESTION 3

An information security incident is

A. Any real or suspected adverse event in relation to the security of computer systems or networks

B. Any event that disrupts normal today\\'s business functions

C. Any event that breaches the availability of information assets

D. All of the above

Correct Answer: D

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

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

A. Scenario testing

B. Facility testing

C. Live walk-through testing

D. Procedure testing

Correct Answer: D