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.pass4itsure.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 state of incident response preparedness that enables an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation is called:

A. Computer Forensics

B. Digital Forensic Analysis

C. Forensic Readiness

D. Digital Forensic Policy

Correct Answer: C

QUESTION 2

Which of the following is NOT one of the common techniques used to detect Insider threats:

A. Spotting an increase in their performance

B. Observing employee tardiness and unexplained absenteeism

C. Observing employee sick leaves

D. Spotting conflicts with supervisors and coworkers

Correct Answer: A

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

A computer forensic investigator must perform a proper investigation to protect digital evidence. During the investigation, an investigator needs to process large amounts of data using a combination of automated and manual methods. Identify the computer forensic process involved:

A. Analysis

B. Preparation

C. Examination

D. Collection

Correct Answer: C

QUESTION 5

To whom should an information security incident be reported?

A. It should not be reported at all and it is better to resolve it internally

B. Human resources and Legal Department

C. It should be reported according to the incident reporting and handling policy

D. Chief Information Security Officer

Correct Answer: C

QUESTION 6

Incident prioritization must be based on:

A. Potential impact

B. Current damage

C. Criticality of affected systems

D. All the above

Correct Answer: D

QUESTION 7

The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:

A. Tripwire

B. HijackThis

C. Stinger

D. F-Secure Anti-virus

Correct Answer: B

QUESTION 8

Which test is conducted to determine the incident recovery procedures effectiveness?

A. Live walk-throughs of procedures

B. Scenario testing

C. Department-level test

D. Facility-level test

Correct Answer: A

QUESTION 9

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.

Correct Answer: A

QUESTION 10

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

Correct Answer: A

QUESTION 11

Electronic evidence may reside in the following:

A. Data Files

B. Backup tapes

C. Other media sources

D. All the above

Correct Answer: D

QUESTION 12

Incidents such as DDoS that should be handled immediately may be considered as:

A. Level One incident

B. Level Two incident

C. Level Three incident

D. Level Four incident

Correct Answer: C

QUESTION 13

The open source TCP/IP network intrusion prevention and detection system (IDS/IPS), uses a rule-driven language, performs real-time traffic analysis and packet logging is known as:

A. Snort

B. Wireshark

C. Nessus

D. SAINT

Correct Answer: A

QUESTION 14

A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so

B. The message from a known email id is caught by SPAM filters due to change of filter settings

C. The message warns to delete certain files if the user does not take appropriate action

D. The message prompts the user to install Anti-Virus

Correct Answer: A

QUESTION 15

A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

A. adware (spelled all lower case)

B. Trojan

C. RootKit

D. Virus

E. Worm

Correct Answer: A