212-89$^{\text{Q\&As}}$

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.passapply.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

Removing or eliminating the root cause of the incident is called:

A. Incident Eradication

B. Incident Protection

C. Incident Containment

D. Incident Classification

Correct Answer: A

QUESTION 2

When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled

B. The organization should enforce separation of duties

C. The access requests granted to an employee should be documented and vetted by the supervisor

D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

Correct Answer: A

QUESTION 3

In which of the steps of NIST\\'s risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

A. Likelihood Determination

B. Control recommendation

C. System characterization

D. Control analysis

Correct Answer: C

QUESTION 4

The program that helps to train people to be better prepared to respond to emergency situations in their communities is known as:

A. Community Emergency Response Team (CERT)

B. Incident Response Team (IRT)

C. Security Incident Response Team (SIRT)

D. All the above

Correct Answer: A

QUESTION 5

________________ attach(es) to files

A. adware

B. Spyware

C. Viruses

D. Worms

Correct Answer: C

QUESTION 6

An adversary attacks the information resources to gain undue advantage is called:

A. Defensive Information Warfare

B. Offensive Information Warfare

C. Electronic Warfare

D. Conventional Warfare

Correct Answer: B

QUESTION 7

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

A. Computer Security Incident Response Team CSIRT

B. Security Operations Center SOC

C. Digital Forensics Examiner

D. Vulnerability Assessor

Correct Answer: A

QUESTION 8

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 9

Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

A. NET-CERT

B. DFN-CERT

C. Funet CERT

D. SURFnet-CERT

Correct Answer: D

QUESTION 10

The very well-known free open source port, OS and service scanner and network discovery utility is called:

A. Wireshark

B. Nmap (Network Mapper)

C. Snort

D. SAINT

Correct Answer: B

QUESTION 11

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 12

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following steps focus on limiting the scope and extent of an incident?

A. Eradication

B. Containment

C. Identification

D. Data collection

Correct Answer: B

QUESTION 13

Incident Response Plan requires

A. Financial and Management support

B. Expert team composition

C. Resources

D. All the above

Correct Answer: D

QUESTION 14

Digital evidence must:

A. Be Authentic, complete and reliable

B. Not prove the attackers actions

C. Be Volatile

D. Cast doubt on the authenticity and veracity of the evidence

Correct Answer: A

QUESTION 15

Which of the following is NOT a digital forensic analysis tool:

A. Access Data FTK

B. EAR/ Pilar

C. Guidance Software EnCase Forensic

D. Helix

Correct Answer: B