

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Incident Response Plan requires

- A. Financial and Management support
- B. Expert team composition
- C. Resources
- D. All the above

Correct Answer: D

QUESTION 2

According to US-CERT; if an agency is unable to successfully mitigate a DOS attack it must be reported within:

- A. One (1) hour of discovery/detection if the successful attack is still ongoing
- B. Two (2) hours of discovery/detection if the successful attack is still ongoing
- C. Three (3) hours of discovery/detection if the successful attack is still ongoing
- D. Four (4) hours of discovery/detection if the successful attack is still ongoing

Correct Answer: B

QUESTION 3

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 4

The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

- A. SAM service

- B. POP3 service
- C. SMTP service
- D. Echo service

Correct Answer: D

QUESTION 5

The typical correct sequence of activities used by CSIRT when handling a case is:

- A. Log, inform, maintain contacts, release information, follow up and reporting
- B. Log, inform, release information, maintain contacts, follow up and reporting
- C. Log, maintain contacts, inform, release information, follow up and reporting
- D. Log, maintain contacts, release information, inform, follow up and reporting

Correct Answer: A

QUESTION 6

The product of intellect that has commercial value and includes copyrights and trademarks is called:

- A. Intellectual property
- B. Trade secrets
- C. Logos
- D. Patents

Correct Answer: A

QUESTION 7

A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

- A. The risk must be urgently mitigated
- B. The risk must be transferred immediately
- C. The risk is not present at this time
- D. The risk is accepted

Correct Answer: C

QUESTION 8

Risk management consists of three processes, risk assessment, mitigation and evaluation. Risk assessment determines the extent of the potential threat and the risk associated with an IT system through its SDLC. How many primary steps does NIST's risk assessment methodology involve?

- A. Twelve
- B. Four
- C. Six
- D. Nine

Correct Answer: C

QUESTION 9

Common name(s) for CSIRT is(are)

- A. Incident Handling Team (IHT)
- B. Incident Response Team (IRT)
- C. Security Incident Response Team (SIRT)
- D. All the above

Correct Answer: D

QUESTION 10

The data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?

- A. Containment
- B. Eradication
- C. Incident recording
- D. Incident investigation

Correct Answer: A

QUESTION 11

Which of the following is a characteristic of adware?

- A. Gathering information
- B. Displaying popups
- C. Intimidating users
- D. Replicating

Correct Answer: B

QUESTION 12

The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:

- A. Incident Management
- B. Incident Response
- C. Incident Recovery
- D. Incident Handling

Correct Answer: C

QUESTION 13

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 14

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 15

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

- A. Incident Manager
- B. Incident Analyst
- C. Incident Handler
- D. Incident coordinator

Correct Answer: B

[212-89 VCE Dumps](#)

[212-89 Practice Test](#)

[212-89 Exam Questions](#)