EC-COUNCIL 212-89

EC-Council ECIH Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

212-89

EC-Council Certified Incident Handler

100 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Discover More about the 212-89 Certification 2

EC-Council 212-89 ECIH Certification Details:...................2

212-89 Syllabus:...2

Broaden Your Knowledge with EC-Council 212-89 Sample Questions: 3

Avail the Study Guide to Pass EC-Council 212-89 ECIH Exam: 6

Career Benefits: 6

Discover More about the 212-89 Certification

Are you interested in passing the EC-Council 212-89 exam? First discover, who benefits from the 212-89 certification. The 212-89 is suitable for a candidate if he wants to learn about Specialist. Passing the 212-89 exam earns you the EC-Council Certified Incident Handler title.

While preparing for the 212-89 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 212-89 PDF contains some of the most valuable preparation tips and the details and instant access to useful **212-89 study materials just at one click**.

EC-Council 212-89 ECIH Certification Details:

Exam Name	EC-Council Certified Incident Handler (ECIH)
Exam Code	212-89
Exam Price	$250 (USD)
Duration	180 mins
Number of Questions	100
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**Pearson VUE** OR **ECC Exam Center**
Sample Questions	**EC-Council ECIH Sample Questions**
Practice Exam	**EC-Council 212-89 Certification Practice Exam**

212-89 Syllabus:

Topic
Introduction to Incident Handling and Response
Incident Handling and Response Process
Forensic Readiness and First Response
Handling and Responding to Malware Incidents
Handling and Responding to Email Security Incidents
Handling and Responding to Network Security Incidents
Handling and Responding to Web Application Security Incidents
Handling and Responding to Cloud Security Incidents
Handling and Responding to Insider Threats

Broaden Your Knowledge with EC-Council 212-89 Sample Questions:

Question: 1

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

a) The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information
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) All access rights of the employee to physical locations, networks, systems, applications and data should be disabled

Answer: d

Question: 2

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

Answer: c

Question: 3

Rinni is an incident handler and she is performing memory dump analysis. Which of following tools she can use in order to perform a memory dump analysis?

a) Proc mon and Process Explorer
b) iNetSim
c) Security breach
d) OllyDbg and IDA Pro

Answer: d

Question: 4

Unusual logins, accessing sensitive information not used for the job role, and the use of personal external storage drives on company assets are all signs of which of the following?

a) Security breach
b) Over-working
c) Insider threat
d) Lack of job rotation

Answer: c

Question: 5

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

a) "netstat -an" command
b) "dd" command
c) "arp" command
d) "ifconfig" command

Answer: a

Question: 6

In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:

a) System characterization
b) System classification
c) Asset valuation
d) Asset Identification

Answer: a

Question: 7

What is the best staffing model for an incident response team if current employees' expertise is very low?

a) Fully insourced
b) Fully outsourced
c) Partially outsourced
d) All the above

Answer: b

Question: 8

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues.

Which of the following documents helps in protecting evidence from physical or logical damage?

a) Chain-of-Precedence
b) Chain-of-Custody
c) Network and host log records
d) Forensic analysis report

Answer: b

Question: 9

Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS). In case of a malware incident in your customer's database, who is responsible for eradicating the malicious software?

a) Your company
b) The customer
c) The PaaS provider
d) Building management

Answer: a

Question: 10

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) SURFnet-CERT
b) NET-CERT
c) Funet CERT
d) DFN-CERT

Answer: a

Avail the Study Guide to Pass EC-Council 212-89 ECIH Exam:

- Find out about the 212-89 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **212-89 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 212-89 training. Joining the EC-Council provided training for 212-89 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **212-89 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 212-89 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the 212-89 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the 212-89 Certification

EduSum.Com is here with all the necessary details regarding the 212-89 exam. We provide authentic practice tests for the 212-89 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **212-89 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the EC-Council Certified Incident Handler.

Start Online practice of 212-89 Exam by visiting URL
https://www.edusum.com/ec-council/212-89-ec-council-certified-incident-handler