EDUSUM

#1 Online Certification Guide

EC-COUNCIL 212-89 STUDY GUIDE PDF

Grab the EC-Council ECIH Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

212-89

EC-Council Certified Incident Handler (ECIH)

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

Table of Contents:

Get an Overview of the 212-89 Certification:

Who should take the **212-89 exam**? This is the first question that comes to a candidate's mind when preparing for the ECIH certification. The 212-89 certification is suitable for candidates who are keen to earn knowledge on the Specialist and grab their EC-Council Certified Incident Handler (ECIH). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But 212-89 study guide PDF is here to solve the problem. 212-89 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the EC-Council 212-89 Certification?

There are several reasons why one should grab the 212-89 certification.

- The ECIH certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **EC-Council Certified Incident Handler (ECIH)** is a powerful qualification for a prosperous career.

What is the EC-Council 212-89 ECIH Certification Exam Structure?

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**

Enhance Knowledge with 212-89 Sample Questions:

Question: 1

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

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

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: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

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

What Study Guide Works Best in acing the EC-Council 212-89 ECIH Certification?

The 212-89 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the ECIH exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don’t like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the EC-Council 212-89 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the EC-Council 212-89 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, 212-89 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven 212-89 Practice Test for Success!!!

Do you want to pass the 212-89 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your EC-Council Certified Incident Handler preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **212-89 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.