EDUSUM

#1 Online Certification Guide

EC-COUNCIL 212-89

EC-Council ECIH Certification Questions & Answers

Exam Summary – Syllabus –Questions

212-89

EC-Council Certified Incident Handler (ECIH)

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

Table of Contents:

Know Your 212-89 Certification Well:

The 212-89 is best suitable for candidates who want to gain knowledge in the EC-Council Specialist. Before you start your 212-89 preparation you may struggle to get all the crucial ECIH materials like 212-89 syllabus, sample questions, study guide.

But don't worry the 212-89 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 212-89 syllabus?
- How many questions are there in the 212-89 exam?
- Which Practice test would help me to pass the 212-89 exam at the first attempt?

Passing the 212-89 exam makes you EC-Council Certified Incident Handler (ECIH). Having the ECIH certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

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	Details	Weights
Incident Response and Handling	- Information Security - Computer Security - Threat intelligence - Risk Management - Incident Handling - Security Policies	16%
Process Handling	- Incident Handling and Response - Incident Readiness - Security Auditing - Security Incidents - Forensic Investigation - Eradication and Recovery	14%
Forensic Readiness and First Response	- Computer Forensics - Digital Evidence - Forensic Readiness - Preservation of Electronic Evidence - Volatile Evidence - Static Evidence - Anti-forensics	13%
Email Security Incidents	- Email Security - Deceptive and Suspicious Email - Email Incidents - Phishing email	10%
Application Level Incidents	- Web Application Threats & Vulnerabilities - Web Attack - Eradication of Web Applications	8%
Network & Mobile Incidents	- Network Attacks - Unauthorized Access - Inappropriate Usage - Denial-of-Service - Wireless Network - Mobile Platform Vulnerabilities and Risks - Eradication of Mobile Incidents & Recovery	16%
Insider Threats	- Insider Threats - Eradication - Detecting and Preventing Insider Threats - Employee Monitoring Tools	7%

Topic	Details	Weights
Malware Incidents	- Malware - Malware Incident Triage - Malicious Code	8%
Incidents Occurred in a Cloud Environment	- Cloud Computing Threats - Security in Cloud Computing - Eradication - Recovery in Cloud	8%

EC-Council 212-89 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 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

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: 8

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: 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

Study Guide to Crack EC-Council ECIH 212-89 Exam:

- Getting details of the 212-89 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 212-89 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the EC-Council provided training for 212-89 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 212-89 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 212-89 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 212-89 Certification

Make EduSum.com your best friend during your EC-Council Certified Incident Handler exam preparation. We provide authentic practice tests for the 212-89 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 212-89 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 212-89 exam.

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