212-89 exam collection: EC Council Certified Incident Handler (ECIH v3) & 212-89 torrent VCE

BONUS!!! Download part of Exam4Docs 212-89 dumps for free: https://drive.google.com/open?id=1nOA7L1yFhptw8ETe_0t3zOEOQiaHjoOH

The certification is necessary to get a job in your desired EC-COUNCIL company. Success in the test gives you an edge over the others because you will have certified skills that will make a good impression on the interviewer. Most people preparing for the EC Council Certified Incident Handler (ECIH v3) (212-89) exam are confused about preparation. How will they get real and updated EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions? In the case of studying with outdated EC Council Certified Incident Handler (ECIH v3) (212-89) practice questions, you will fail and lose your resources.

The ECIH v2 certification exam covers a wide range of topics related to incident handling, including incident response and recovery, threat intelligence and analysis, vulnerability assessment, and risk management. 212-89 exam is designed to test the candidate's ability to identify, contain, and mitigate security incidents and to manage the incident response process. 212-89 Exam is also designed to test the candidate's knowledge of best practices for incident handling, including how to communicate effectively with stakeholders, how to document incidents, and how to maintain the integrity and confidentiality of sensitive information.

>> Exam 212-89 Format <<

2026 Exam 212-89 Format | Professional 212-89 100% Free Practice Exam Pdf

Education degree does not equal strength, and it does not mean ability. Education degree just mean that you have this learning experience only. And the real ability is exercised in practice, it is not necessarily linked with the academic qualifications. Do not feel that you have no ability, and don't doubt yourself. When you choose to participate in the EC-COUNCIL 212-89 Exam, it is necessary to pass it. If you are concerned about the test, however, you can choose Exam4Docs's EC-COUNCIL 212-89 exam training materials. No matter how low your qualifications, you can easily understand the content of the training materials. And you can pass the exam successfully.

The EC Council Certified Incident Handler (ECIH v2) exam is a comprehensive and practical certification that is designed to help IT professionals develop the skills and knowledge needed to effectively detect, analyze, and respond to security incidents. Earning this certification is a valuable asset for anyone looking to advance their career in the field of cybersecurity.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q107-Q112):

NEW QUESTION # 107
SWA Cloud Services added PKI as one of their cloud security controls. What does PKI stand for?

- A. Private key infrastructure
- B. Public key infrastructure
- C. Public key information
- D. Private key in for ma lion

Answer: B

NEW QUESTION # 108
Rose is an incident-handling person and she is responsible for detecting and eliminating any kind of scanning attempts over the network by any malicious threat actors. Rose uses Wireshark tool to sniff the network and detect any malicious activities going on. Which of the following Wireshark filters can be used by her to detect TCP Xmas scan attempt by the attacker?

- A. tcp.flags.reset==1
- B. tcp.dstport==7
- C. tcp.flags==0X000
- D. tcp.flags==0X029

Answer: D

NEW QUESTION # 109
Joseph is an incident handling and response (IH&R) team lead in Toro Network Solutions Company. As a part of IH&R process, Joseph alerted the service providers, developers, and manufacturers about the affected resources.
Identify the stage of IH&R process Joseph is currently in.

- A. Recovery
- B. Eradication
- C. Incident triage
- D. Containment

Answer: D

Explanation:
When Joseph, the IH&R team lead, alerted service providers, developers, and manufacturers about the affected resources, he was engaged in the Containment stage of the Incident Handling and Response (IH&R) process.
Containment involves taking steps to limit the spread or impact of an incident and to isolate affected systems to prevent further damage. Alerting relevant stakeholders, including service providers and developers, is part of containment efforts to ensure that the threat does not escalate and that measures are taken to protect unaffected resources. This stage precedes eradication and recovery, focusing on immediate response actions to secure the environment.References:The ECIH v3 certification program outlines the IH&R process stages, explaining the roles and actions involved in containment, including communication with external and internal stakeholders to manage and mitigate the incident's effects.

NEW QUESTION # 110
Patrick is performing a cyber forensic investigation. He is in the process of collect ng physical evidence at the crime scene.
Which of the following elements must he consider while collecting physical evidence?

- A. Removable media, cables, and publications
- B. DNS information including domains and subdomains
- C. Published nameservers and web-application source code
- D. Open ports, services, and operating system (OS) vulnerabilities

Answer: A

NEW QUESTION # 111
BadGuy Bob hid files in the slack space, changed the file headers, hid suspicious files in executables, and changed the metadata for all types of files on his hacker laptop. What has he committed?

- A. Adversarial mechanics
- B. Anti-forensics
- C. Felony
- D. Legal hostility

Answer: B

Explanation:
Anti-forensics refers to techniques used to hinder the forensic analysis of a computer system. By hiding files in slack space, changing file headers, embedding suspicious files in executables, and altering metadata, BadGuy Bob is attempting to make it difficult for forensic analysts to find, analyze, and attribute the malicious activities and data on his laptop. These actions are designed to conceal evidence, manipulate digital artifacts, and obstruct investigations, making them clear examples of anti-forensic techniques. While such actions could be part of broader criminal activities, constituting a felony, and could be seen as adversarial mechanics or legal hostility in specific contexts, the most accurate classification of these techniques is anti-forensics.References:The ECIH v3 certification program includes discussions on forensic analysis and the challenges posed by anti-forensic techniques, teaching incident handlers how to recognize and counteract attempts to obstruct investigations.

NEW QUESTION # 112
.....