Wonderful 212-89 Exam Questions: EC Council Certified Incident Handler (ECIH v3) Exhibit the Most Useful Training Guide- Actual4Exams

2026 Latest Actual4Exams 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=16WfFQ6hEka8p9LzWDEo6yCYV4xwqUVwl

Actual4Exams will provide you with actual EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions in pdf to help you crack the 212-89 exam. So, it will be a great benefit for you. If you want to dedicate your free time to preparing for the EC Council Certified Incident Handler (ECIH v3) (212-89) exam, you can check with the soft copy of pdf questions on your smart devices and study when you get time. On the other hand, if you want a hard copy, you can print 212-89 exam questions.

Exam Topic Areas

All in all, the ECIH 212-89 Exam will cover the following topic areas:

- Malware Incidents;
- Email Security Incidents;
- Incidents Occurred in a Cloud Environment.
- Application-Level Incidents;
- Network & Mobile Incidents;
- Process Handling;
- Incident Response and Handling;

>> 212-89 Reliable Exam Question <<

Free PDF Quiz 2026 EC-COUNCIL High-quality 212-89: EC Council Certified Incident Handler (ECIH v3) Reliable Exam Question

Passing an exam requires diligent practice, and using the right study EC-COUNCIL Certification Exams material is crucial for optimal performance. With this in mind, Actual4Exams has introduced a range of innovative 212-89 Practice Test formats to help candidates prepare for their 212-89.

EC-COUNCIL 212-89 (EC Council Certified Incident Handler (ECIH v2)) Certification Exam is recognized by many organizations and businesses worldwide, and it is a valuable certification for anyone interested in a career in information security. EC Council Certified Incident Handler (ECIH v3) certification is an excellent way to demonstrate your expertise in incident handling and response, and it can help you advance your career in the field. EC Council Certified Incident Handler (ECIH v3) certification is also an excellent way to stay up-to-date with the latest developments in incident handling and response, ensuring that you are always prepared to tackle any security challenges that may arise.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample

Questions (Q73-Q78):

NEW QUESTION # 73
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. SMTP service
- B. SAM service
- C. POP3 service
- D. Echo service

Answer: D

NEW QUESTION # 74
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. Asset Identification
- B. Asset valuation
- C. System classification
- D. System characterization

Answer: D

NEW QUESTION # 75
In the wake of a sophisticated cyber attack at a global financial institution involving encrypted data exfiltration, an incident handler must preserve volatile memory for forensic investigation. What should be the incident handler's immediate action?

- A. Isolate the network segment and power down machines.
- B. Conduct preliminary documentation before any evidence preservation.
- C. Deploy forensic tools to capture volatile memory using trusted tools.
- D. Prioritize capturing system memory immediately, then secure the scene.

Answer: D

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
Volatile memory contains critical artifacts such as encryption keys, running processes, and network connections. The ECIH Forensic Readiness module emphasizes that volatile evidence must be captured immediately before it is lost.
Option C is correct because capturing memory first preserves irreplaceable evidence, followed by securing the scene to prevent contamination. Powering down systems before memory capture would destroy volatile data.
Options A and D are incomplete without prioritization. Option B is incorrect due to evidence loss.
Thus, immediate memory capture followed by scene security is the correct action.

NEW QUESTION # 76
An organization implemented an encoding technique to eradicate SQL injection attacks. In this technique, if a user submits a request using single-quote and some values, the encoding technique will convert it into numeric digits and letters ranging from "a" to "f". This prevents the user request from performing a SQL injection attempt on the web application.
Identify the encoding technique used by the organization.

- A. Unicode encoding
- B. URL encoding
- C. Hex encoding
- D. Base 64 encoding

Answer: C

NEW QUESTION # 77
Francis is an incident handler and security expert. He works at MorisonTech Solutions based in Sydney, Australia. He was assigned a task to detect phishing/spam mails for the client organization.
Which of the following tools can assist Francis to perform the required task?

- A. Cain and Abel
- B. Nessus
- C. Netcraft
- D. BTCrack

Answer: C

Explanation:
Netcraft is a tool that provides internet security services, including the detection of phishing and spam emails.
It offers a range of services that can help organizations identify fraudulent websites and phishing activities by analyzing web content and email messages for known phishing signatures and heuristics. This makes it a useful tool for incident handlers like Francis, who is tasked with detecting phishing and spam emails for clientorganizations. Other options listed, such as Nessus (a vulnerability scanner), BTCrack (a Bluetooth pin and link-key cracker), and Cain and Abel (a password recovery tool), do not specialize in detecting phishing or spam emails but serve different purposes in cybersecurity.References:The Incident Handler (ECIH v3) curriculum includes discussions on tools and methodologies for detecting and mitigating various cyber threats, including phishing and spam, highlighting tools like Netcraft for their utility in these areas.

NEW QUESTION # 78
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Actual4Exams 212-89 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=16WfFQ6hEka8p9LzWDEo6yCYV4xwqUVwl