Valid EC-COUNCIL 212-89 Exam Materials - Certification 212-89 Cost


Exam : 212-89

Title : EC Council Certified Incident Handler (ECIH v2) Exam

Vendor : Eccouncil

Version : V12.35

P.S. Free & New 212-89 dumps are available on Google Drive shared by Exam4Free: https://drive.google.com/open?id=1RtzPGS3oL07pa0Q5XPKqrtkU8hDaysDm

Exam4Free is fully aware of the fact that preparing successfully for the EC-COUNCIL 212-89 exam in one go is a necessity because of the expensive registration fee. For applicants like you, success in the EC Council Certified Incident Handler (ECIH v3) exam on the first attempt is crucial to saving money and time. Our Free EC-COUNCIL 212-89 Exam Questions will help you decide fast to buy the premium ones.

The EC-Council 212-89 Exam measures the knowledge and competence of the candidates in identifying, analyzing, and rectifying hazards to prevent any future reoccurrences. The interested individuals who pass this certification test will gain the fundamental skills in responding and handling computer security incidents within an information system. A certified applicant is a skilled professional with the ability to handle different incident types, risk assessment methodologies, as well as different policies and laws associated with incident handling. So, if you want to become one of these experts, you will need to know a lot of details.

The EC-Council Certified Incident Handler (ECIH v2) certification exam is a globally recognized certification that validates the skills and knowledge of an individual in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification exam is ideal for security professionals who want to advance their career in incident handling and response and IT professionals who are responsible for protecting their organization's critical assets. EC Council Certified Incident Handler (ECIH v3) certification exam is comprehensive, covers all aspects of incident handling and response, and is available online in multiple languages.

>> Valid EC-COUNCIL 212-89 Exam Materials <<

Certification 212-89 Cost - Mock 212-89 Exam

Exam4Free's senior team of experts has developed training materials for EC-COUNCIL 212-89 exam.Through Exam4Free's training and learning passing EC-COUNCIL certification 212-89 exam will be very simple. Exam4Free can 100% guarantee you pass your first time to participate in the EC-COUNCIL Certification 212-89 Exam successfully. And you will find that our practice questions will appear in your actual exam. When you choose our help, Exam4Free can not only give you the accurate and comprehensive examination materials, but also give you a year free update service.

To become certified in ECIH v2, candidates must pass a rigorous certification exam that tests their knowledge, skills, and abilities in the areas of incident handling and response. 212-89 exam consists of 100 multiple-choice questions, and candidates have 3 hours to complete the exam. 212-89 Exam is designed to test the candidate's knowledge of incident handling and response techniques, as well as their ability to analyze and respond to security incidents.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q39-Q44):

NEW QUESTION # 39
Rinni is an incident handler and she is performing memory dump analysis.
Which of following tools she can use in order to perform memory dump analysis?

- A. iNetSim
- B. Scylla and OllyDumpEx
- C. Procmon and ProcessExplorer
- D. OllyDbg and IDA Pro

Answer: B

Explanation:
For memory dump analysis, tools like Scylla and OllyDumpEx are more suited. These tools are designed to analyze and extract information from memory dumps, which can be crucial for understanding the state of a system at the time of an incident. Scylla is used for reconstructing imports in dumped binaries, while OllyDumpEx is an OllyDbg plugin used for dumping process memory. Both tools are valuable for incident handlers like Rinni who are performing memory dump analysis to uncover evidence or understand the behavior of malicious software.

NEW QUESTION # 40
Which of the following tools helps incident responders effectively contain a potential cloud security incident and gather required forensic evidence?

- A. Alert Logic
- B. Cloud Passage Halo
- C. Qualys Cloud Platform
- D. CloudPassage Quarantine

Answer: A

NEW QUESTION # 41
QualTech Solutions is a leading security services enterprise. Dickson works as an incident responder with this firm. He is performing vulnerability assessment to identify the security problems in the network, using automated tools to identify the hosts, services, and vulnerabilities present in the enterprise network.
Based on the above scenario, identify the type of vulnerability assessment performed by Dickson.

- A. Passive assessment
- B. Active assessment
- C. Internal assessment
- D. External assessment

Answer: D

Explanation:
An active assessment involves using automated tools to scan and probe the network actively to identify hosts, services, and vulnerabilities. This type of assessment directly interacts with the network components to gather information about the existing security posture, unlike passive assessments, which analyze traffic without sending packets to the target systems. Dickson's approach, employing automated tools to identify the network's hosts, services, and vulnerabilities, fits the definition of an active assessment. This method provides a more immediate understanding of the network's vulnerabilities, allowing for timely remediation actions.
References:The ECIH v3 program includes discussions on vulnerability assessment techniques, highlighting the differences between active and passive assessments and their applicability in identifying network security issues.

NEW QUESTION # 42
A large multinational enterprise recently integrated a digital HR onboarding system to streamline applicant submissions and document collection. During a cybersecurity audit, it was revealed that attackers had set up a phishing site mimicking the official HR document submission portal. Several employees and new hires uploaded their resumes and downloaded pre-filled form templates, believing them to be legitimate. Upon opening the downloaded Word documents, the system silently connected to external servers and fetched additional template data without any user consent or visible macro execution warnings. This bypassed email gateway filters and endpoint antivirus tools, leading to lateral malware spread across systems used by HR, finance, and legal departments.
Digital forensic analysis showed that the documents did not contain visible scripts or macros but relied on hidden structural definitions to retrieve malicious payloads dynamically from attacker-controlled servers.
Which of the following web-based malware distribution techniques best explains the observed behavior?

- A. Distribution of malware through remotely hosted RTF injection.
- B. Distribution of malware through peer-to-peer file propagation mechanisms within internal networks.
- C. Distribution of malware through spear-phishing emails that impersonate social media contacts.
- D. Distribution of malware through compromised browser extensions embedded in PDF rendering engines.

Answer: A

Explanation:
This incident demonstrates a document-based web malware delivery mechanism, specifically leveraging remotely hosted Rich Text Format (RTF) injection, which is explicitly discussed in ECIH web and malware handling modules. RTF documents can reference external objects or templates, allowing malicious payloads to be fetched dynamically when the document is opened-without requiring macros or user interaction.
Option A is correct because the behavior described aligns precisely with remote template injection. The absence of macros, the silent external connections, and the use of structural document elements are classic indicators of RTF-based malware delivery. ECIH highlights this as a high-risk technique because it bypasses traditional macro-based detection and user warning mechanisms.
Option B is incorrect because the payload was delivered via downloaded documents, not email impersonation of social contacts.
Option C references browser extensions and PDFs, which are not involved. Option D describes lateral spread, not initial delivery.
ECIH emphasizes that modern web-based attacks increasingly abuse trusted document formats and remote object references to evade controls. Understanding these techniques enables responders to improve document sanitization, outbound traffic monitoring, and content disarm and reconstruction (CDR) controls.

NEW QUESTION # 43
Which of the following is not a countermeasure to eradicate cloud security incidents?

- A. Disable security options such as two factor authentication and CAPTCHA
- B. Patch the database vulnerabilities and improve the isolation mechanism
- C. Remove the malware files and traces from the affected components
- D. Check for data protection at both design and runtime

Answer: A

NEW QUESTION # 44
.....

Certification 212-89 Cost: https://www.exam4free.com/212-89-valid-dumps.html

- Pass Guaranteed 212-89 - EC Council Certified Incident Handler (ECIH v3) Authoritative Valid Exam Materials □ Download ☀ 212-89 □☀□ for free by simply searching on " www.troytecdumps.com " □Valid 212-89 Exam Cost
- Unparalleled Valid 212-89 Exam Materials - Win Your EC-COUNCIL Certificate with Top Score □ Search for ➡ 212-89 □□□ and download it for free on { www.pdfvce.com } website □212-89 Latest Questions
- EC-COUNCIL 212-89 Overview of the Problems Faced in Preparation Exam Questions □ Easily obtain [212-89] for free download through ➤ www.practicevce.com □ □Certification 212-89 Exam Cost
- Valid 212-89 Exam Prep □ Interactive 212-89 Course □ 212-89 New Dumps Book □ Open ▸ www.pdfvce.com ◂ enter 《 212-89 》 and obtain a free download □212-89 Reliable Test Syllabus
- 100% Pass Quiz 2026 212-89: EC Council Certified Incident Handler (ECIH v3) Perfect Valid Exam Materials □ The page for free download of 「 212-89 」 on { www.pass4test.com } will open immediately □Valid 212-89 Exam Cost
- Efficient EC-COUNCIL - Valid 212-89 Exam Materials ☃ Enter ➡ www.pdfvce.com □□□ and search for [212-89] to download for free ✏Valid 212-89 Exam Cost
- 212-89 Exam Braindumps: EC Council Certified Incident Handler (ECIH v3) -amp; 212-89 Actual Test Questions □ ☀ www.verifieddumps.com □☀□ is best website to obtain （ 212-89 ） for free download □212-89 New Dumps Book
- 212-89 Reliable Test Syllabus □ 212-89 Valid Test Dumps □ Valid 212-89 Exam Prep □ Enter ✔ www.pdfvce.com □✔□ and search for ➠ 212-89 □ to download for free □212-89 Valid Test Dumps
- Fantastic EC-COUNCIL Valid 212-89 Exam Materials Are Leading Materials - Authorized 212-89: EC Council Certified Incident Handler (ECIH v3) □ Search for { 212-89 } and download it for free immediately on ➡ www.validtorrent.com □□□ □Exam 212-89 Cram
- Reliable 212-89 Exam Braindumps □ 212-89 Exam Duration □ Interactive 212-89 Course □ Search for ⇛ 212-89 ⇚ and download it for free immediately on ➤ www.pdfvce.com □ □Valid 212-89 Exam Cost
- Verified Valid 212-89 Exam Materials | First-Grade Certification 212-89 Cost and Well-Prepared Mock EC Council Certified Incident Handler (ECIH v3) Exam □ Search for " 212-89 " and easily obtain a free download on ➡ www.vceengine.com □□□ □Exam 212-89 Cram
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, albsaer.alalawidesigner.com, www.tttttt456.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, 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.810706.cn, www.stes.tyc.edu.tw, www.1pge.cc, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Download part of Exam4Free 212-89 dumps for free: https://drive.google.com/open?id=1RtzPGS3oL07pa0Q5XPKqrtkU8hDaysDm