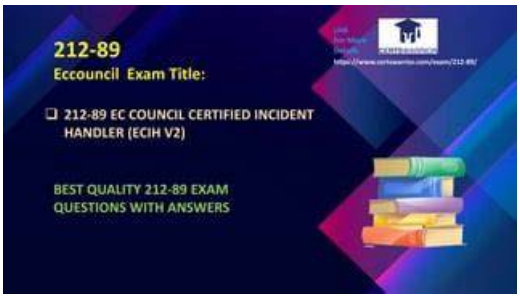
Pass Guaranteed Quiz EC-COUNCIL - 212-89 - EC Council Certified Incident Handler (ECIH v3)–Trustable Reliable Test Prep



P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by PDFVCE: https://drive.google.com/open?id=1IbpxO1UykS4UH-jzOPfo39eVRzxnZz6i

You have tried all kinds of exam questions when others are still looking around for 212-89 exam materials, which means you have stayed one step ahead of other IT exam candidates. 212-89 Exam software provided by our PDFVCE consists of full exam resources will offer you a simulation of the real exam atmosphere of 212-89.

EC-COUNCIL 212-89 Exam Overview:

Certification Vendor:	EC-Council
Exam Name:	EC Council Certified Incident Handler (ECIH v3) Exam
Exam Number:	212-89
Passing Score:	70%
Real Exam Qty:	100
Exam Duration:	180 minutes
Exam Format:	Multiple Choice Questions (MCQ), Scenario-based questions
Related Certifications:	EC-Council Certified Ethical Hacker (CEH) EC-Council Computer Hacking Forensic Investigator (CHFI)
Exam Price:	$450 USD
Available Languages:	English, Japanese, Korean, Simplified Chinese
Certificate Validity Period:	3 years
Recommended Training:	EC-Council Online Self-Paced Training Official ECIH v3 Instructor-Led Training
Exam Registration:	EC-Council Official Registration Pearson VUE
Sample Questions:	EC-COUNCIL 212-89 Sample Questions
Exam Way:	Online remote proctored or onsite at Pearson VUE test centers
Pre Condition:	No mandatory prerequisites; recommended 1 year of information security experience or completion of official ECIH training
Official Syllabus URL:	https://www.eccouncil.org/programs/certified-incident-handler-ecih/

>> 212-89 Reliable Test Prep <<

Valid 212-89 Vce | Updated 212-89 Dumps

You must hold an optimistic belief for your life. There always have solutions to the problems. We really hope that our 212-89 study materials will greatly boost your confidence. In fact, many people are confused about their future and have no specific aims. Then our 212-89 practice quiz can help you find your real interests. Just think about that you will get more oppotunities to bigger enterprise and better position in your career with the 212-89 certification. It is quite encouraging!

The ECIH certification exam is a 2-hour, computer-based exam that consists of 100 multiple-choice questions. 212-89 Exam is designed to test an individual's knowledge and skills in incident handling and response. 212-89 exam covers various topics such as incident handling process, incident handling procedures, communication and documentation, and various types of incidents. To pass the ECIH certification exam, an individual must score at least 70% on the exam.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q400-Q405):

NEW QUESTION # 400
Stanley is an incident handler working for TexaCorp., a United States based organization. With the growing concern of increasing emails from outside the organization, Stanley was asked to take appropriate actions to keep the security of the organization intact. In the process of detecting and containing malicious emails, Stanley was asked to check the validity of the emails received by employees. Identify the tool Stanley can use to accomplish this task.

- A. Point of Mail
- B. Event Log Analyzer
- C. Email Dossier
- D. Polite Mail

Answer: A

NEW QUESTION # 401
Shall y, an incident handler, works for a company named Texas Pvt.Ltd.based in Florida. She was asked to work on an incident response plan. As part of the plan, she decided to enhance and improve the security infrastructure of the enterprise. She incorporated a security strategy that allows security professionals to use several protection layers throughout their information system. Owing to multiple-layer protection, this security strategy assists in preventing direct attacks against the organization's information system as a break in one layer only leads the attacker to the next layer.
Which of the following security strategies did Shall y incorporate in the incident response plan?

- A. Defense-in-depth
- B. Exponential back off algorithm
- C. Three-way handshake
- D. Covert channels

Answer: A

NEW QUESTION # 402
GlobalCorp, a leading software development company, recently launched a cloud-based CRM application.
However, within a week, customers reported unauthorized access incidents. On investigation, it was discovered that the vulnerability was due to improper session management, allowing session fixation attacks.
How should GlobalCorp address this vulnerability?

- A. Increase the complexity of user passwords.
- B. Rotate session tokens after successful login.
- C. Store session IDs in encrypted cookies.
- D. Implement CAPTCHA on all login pages.

Answer: B

Explanation:
This scenario involves a session fixation vulnerability, a well-known web application attack where an attacker forces or predicts a session identifier and then tricks a user into authenticating with that session. According to the ECIH web application security module, proper session management is essential to prevent such attacks.
Option B is correct because rotating or regenerating session tokens immediately after successful authentication ensures that any session identifier known to an attacker becomes invalid. This breaks the attack chain inherent in session fixation attacks. ECIH explicitly identifies session regeneration as a primary mitigation control.
Option A helps against automated abuse but does not address session reuse. Option C strengthens authentication but does not prevent session hijacking. Option D improves confidentiality but does not prevent fixation if the same session ID remains valid.

ECIH stresses that authentication and session management must be treated as distinct security controls. Even strong passwords cannot protect against flawed session handling. Therefore, regenerating session tokens post- login is the correct and most effective remediation.

NEW QUESTION # 403
Sophia, an incident handler at a cloud hosting provider, is investigating reports of intermittent web server slowdowns and timeouts. Upon analyzing router logs, she finds an unusually high number of incomplete connection attempts, causing the server's memory and CPU resources to spike. Suspecting a form of resource exhaustion attack, she applies a protective configuration to the router that allows it to validate connection requests before they reach the server. Soon after this change, the number of partial connections decreases, and the server regains stable performance. What was the purpose of this action?

- A. To scan for malicious payloads
- B. To prevent brute-force logins
- C. To monitor port scans
- D. To block SYN flood attempts

Answer: D

Explanation:
The described symptoms-numerous incomplete TCP connections consuming server resources-are characteristic of a SYN flood attack, a denial-of-service technique targeting the transport layer. In such attacks, attackers send SYN packets without completing the TCP handshake, leaving servers overwhelmed with half-open connections.
ECIH network incident handling guidance emphasizes rapid identification and containment of DoS conditions to preserve service availability. By configuring the router to validate connection requests (for example, using SYN cookies or proxy validation), illegitimate handshake attempts are filtered before reaching the server.
Option A involves payload inspection, which is irrelevant here. Option B relates to authentication attacks, which require completed connections. Option D is a detection activity, not mitigation.
Therefore, the purpose of Sophia's action was to block SYN flood attempts, making Option C correct.

NEW QUESTION # 404
An organization named Sam Morison Inc. decided to use cloud-based services to reduce the cost of their maintenance. They first identified various risks and threats associated with cloud .. adoption and migrating critical business data to third-party systems. Hence, the organization decided to deploy cloud-based security tools to prevent upcoming threats. Which of the following tools would help the organization to secure cloud resources and services?

- A. Nmap
- B. Wireshark
- C. Alert Logic
- D. Burp Suite

Answer: C

NEW QUESTION # 405
.....

- 212-89 Valid Braindumps Ppt □ 212-89 Testking □ 212-89 Valid Exam Papers □ Open [www.pdfvce.com] enter 【 212-89 】 and obtain a free download □Valid 212-89 Test Camp
- Prepare with EC-COUNCIL 212-89 PDF Questions [2026]-Best Preparation Materials □ Search for ➡ 212-89 □□□ and download it for free on 「 www.vceengine.com 」 website □212-89 Valid Braindumps Ppt
- Quiz EC-COUNCIL - Valid 212-89 Reliable Test Prep □ Easily obtain free download of ➥ 212-89 □ by searching on ⇛ www.pdfvce.com ⇚ ✈New 212-89 Practice Questions
- 212-89 Reliable Exam Preparation □ 212-89 Reliable Exam Preparation □ 212-89 Valid Exam Papers □ Download ➥ 212-89 □ for free by simply entering □ www.practicevce.com □ website □212-89 Valid Braindumps Ppt
- 212-89 Learning materials: EC Council Certified Incident Handler (ECIH v3) - 212-89 Exam Preparation □ Download 【 212-89 】 for free by simply entering ➥ www.pdfvce.com □ website □212-89 Valid Braindumps Files
- Free PDF 2026 EC-COUNCIL The Best 212-89: EC Council Certified Incident Handler (ECIH v3) Reliable Test Prep □ Go to website " www.exam4labs.com " open and search for ➥ 212-89 □ to download for free □212-89 Test King
- willysforsale.com, zenwriting.net, hashnode.com, www.longisland.com, connect.garmin.com, knowyourmeme.com, www.fotor.com, divisionmidway.org, ronorp.net, learn.csisafety.com.au, Disposable vapes

DOWNLOAD the newest PDFVCE 212-89 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1IbpxO1UykS4UH-jzOPfo39eVRzxnZz6i