# 212-89 Certification Exam | 212-89 Exam Revision Plan


What's more, part of that TopExamCollection 212-89 dumps now are free: https://drive.google.com/open?id=1IEDXnfl1ZO3rRRLexzdkeVr14y_KGzpi

We are quite confident that all these EC-COUNCIL 212-89 exam dumps feature you will not find anywhere. Just download the EC-COUNCIL 212-89 and start this journey right now. For the well and quick 212-89 exam dumps preparation, you can get help from EC-COUNCIL 212-89 which will provide you with everything that you need to learn, prepare and pass the EC Council Certified Incident Handler (ECIH v3) (212-89) certification exam.

The ECIH v2 certification is ideal for professionals who are responsible for managing and responding to security incidents, such as security analysts, network security administrators, and incident response team members. EC Council Certified Incident Handler (ECIH v3) certification is also suitable for individuals who want to enhance their skills and knowledge in incident handling and response. With the increasing prevalence of cyber threats and security breaches, the demand for incident handling professionals with ECIH v2 certification is on the rise.

**>> 212-89 Certification Exam <<**

## 212-89 Certification Exam - 100% Pass Quiz 2026 212-89: EC Council Certified Incident Handler (ECIH v3) First-grade Exam Revision Plan

Generally speaking, reviewing what you have learned is important, since it will help you have a good command of the knowledge points. 212-89 Online test engine has testing history and performance review, so that you can have a general review of what you have learned before next learning. In addition, 212-89 exam dumps is convenient and easy to study, it supports all web browsers and Android and iOS etc. You can also practice offline if you like. We provide you with free update for 365 days for 212-89 Exam Materials, so that you can get the latest information for the exam timely. And the latest information for 212-89 exam dumps will be auto sent to you.

## EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q227-Q232):

**NEW QUESTION # 227**
Which of the following is an attack that occurs when a malicious program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated?

- A. Cross-site request forgery
- B. SQL injection
- C. Cross-site scripting
- D. Insecure direct object references

**Answer: A**

**NEW QUESTION # 228**
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 compromised browser extensions embedded in PDF rendering engines.
- 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 remotely hosted RTF injection.

**Answer: D**

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
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 # 229**
Rose is an incident-handler and is responsible for detecting and eliminating any kind of scanning attempts over the network by malicious threat actors. Rose uses Wire shark 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==0X 000
- B. tcp.flags.reset== 1
- C. tcp.flags==0X 029
- D. tcp.dstport== 7

**Answer: C**

**NEW QUESTION # 230**
CSIRT can be implemented at:

- A. All the above
- B. Internal enterprise level
- C. Vendor level
- D. National, government and military level

**Answer: A**

**NEW QUESTION # 231**

Shiela is working at night as an incident handler. During a shift, servers were affected by a massive cyberattack. After she classified and prioritized the incident, she must report the incident, obtain necessary permissions, and perform other incident response functions. What list should she check to notify other responsible personnel?

- A. Email list
- B. HR log book
- C. Point of contact
- D. Phone number list

**Answer: C**

**NEW QUESTION # 232**
.....

When you decide to prepare for the EC-COUNCIL certification, you must want to pass at first attempt. Now, make a risk-free investment in training and certification with the help of 212-89 practice torrent. Our 212-89 test engine allows you to practice until you think it is ok. Our 212-89 Questions are the best relevant and can hit the actual test, which lead you successfully pass. Please feel confident about your 212-89 preparation with our 100% pass guarantee.



P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by TopExamCollection: https://drive.google.com/open?id=1IEDXnfl1ZO3rRRLexzdkeVr14y_KGzpi