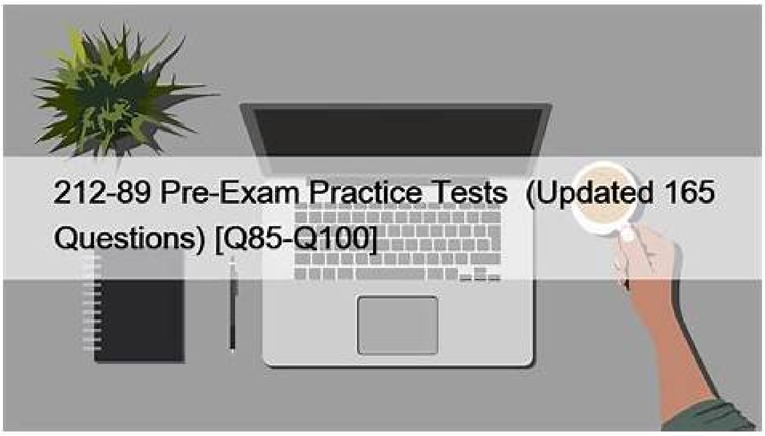
212-89 Latest Exam Experience - 212-89 Practice Exam Fee


212-89 Pre-Exam Practice Tests (Updated 165 Questions) [Q85-Q100]

BONUS!!! Download part of RealValidExam 212-89 dumps for free: https://drive.google.com/open?id=17obJ13bVkq9JQEtQtHV894AT29LOqyCb

Owning RealValidExam is to have a key to pass 212-89 exam certification. RealValidExam's 212-89 exam certification training materials is the achievement that our IT elite team take advantage of their own knowledge and experience, and grope for rapid development and achievements of the IT industry. Its authority is undeniable. Before purchase RealValidExam's 212-89 Braindumps, you can download 212-89 free demo and answers on probation on RealValidExam.COM.

Exam Topic Areas

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

- Application-Level Incidents;
- Incidents Occurred in a Cloud Environment.
- Email Security Incidents;
- Incident Response and Handling;
- Network & Mobile Incidents;
- Process Handling;
- Insider Threats;
- Forensic Readiness and First Response;

EC-COUNCIL 212-89: EC Council Certified Incident Handler (ECIH v2) exam is a certification test that measures the candidate's ability to handle various security incidents that may affect an organization's network infrastructure. 212-89 exam is designed to provide IT professionals with the necessary knowledge and skills required to identify, manage, and respond to security incidents.

EC-COUNCIL 212-89 Exam Syllabus Topics:

Topic	Details
Topic 1	• Handling and Responding to Email Security Incidents: This part evaluates Cybersecurity Analysts on their ability to detect and mitigate email-based threats. It explores preparation, analysis, and containment measures in response to email-related incidents, as well as post-incident recovery steps. Candidates must interpret case studies and apply best practices for protecting enterprise email systems.
Topic 2	• Handling and Responding to Malware Incidents:In this domain, IT Security Operations Managers are tested on their capacity to respond to malware incidents effectively. The focus lies on planning, detecting, containing, and analyzing malware threats. It also includes strategies for eradication and recovery, alongside evaluating real-world malware case studies and identifying applicable best practices to avoid recurrence.

Topic 3	- Introduction to Incident Handling and Response: This section of the exam measures the competency of Cybersecurity Analysts in understanding the core concepts of information security threats, vulnerabilities, and various attack and defense frameworks. It covers foundational knowledge of incidents, their classification, and the incident management lifecycle. Candidates are expected to be familiar with automation and orchestration in response efforts, industry standards, security best practices, and legal compliance frameworks relevant to incident handling.
Topic 4	- Handling and Responding to Endpoint Security Incidents: This section measures the abilities of IT Security Operations Managers to protect various endpoint devices, including mobile, IoT, and operational technologies. It addresses the identification and mitigation of endpoint threats, with applied case examples to evaluate readiness and response capacity in complex technical environments.
Topic 5	- Incident Handling and Response Process: This part evaluates IT Security Operations Managers on their understanding of the structured incident handling and response process. It includes the recording, assignment, and triage of incidents, as well as the procedures for notifying stakeholders and containing threats. The module also examines capabilities in forensic evidence gathering, eradication and recovery strategies, post-incident review activities, and the significance of inter-organizational information sharing.
Topic 6	- First Response: This section of the exam assesses Cybersecurity Analysts in their ability to carry out effective first response procedures. It includes securing and documenting crime scenes, evidence collection methodologies, and guidelines for preserving, packaging, and transporting digital and physical evidence in a way that maintains chain of custody and forensic integrity.

>> 212-89 Latest Exam Experience <<

212-89 Practice Exam Fee - 212-89 Latest Version

Owing to our high-quality 212-89 real dump sand high passing rate, our company has been developing faster and faster and gain good reputation in the world. Our education experts are adept at designing and researching exam questions and answers of 212-89 study materials. What’s more, we can always get latest information resource. Our high passing rate is the leading position in this field. We are the best choice for candidates who are eager to Pass 212-89 Exam and acquire the certification.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q151-Q156):

NEW QUESTION # 151
Oscar receives an email from an unknown source containing his domain name oscar.com. Upon checking the link, he found that it contains a malicious URL that redirects to the website evil site.org.
What type of vulnerability is this?

- A. Unvalidated redirects and forwards
- B. Malware
- C. Botnet
- D. SQL injection

Answer: A

NEW QUESTION # 152
XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and removed the malware completely. Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident.
Which of the following stages in IH&R process is James working on?

- A. Post-incident activities
- B. Notification
- C. Eradication
- D. Evidence gathering and forensics analysis

Answer: A

Explanation:
James is working on the post-incident activities stage of the Incident Handling and Response (IH&R) process.
After containing the spread of the infection and removing the malware, the focus shifts to assessing the impact of the incident on the organization and preparing a detailed report. This phase involves analyzing the extent of the damage, determining the cost of the attack, evaluating how well the incident was managed, and identifying lessons learned to improve future response efforts. The objective is to restore systems to normal operation, ensure no remnants of the threat remain, and implement measures to prevent recurrence.
References:Incident Handler (ECIH v3) courses and study guides outline the IH&R process, emphasizing the importance of post-incident activities for organizational recovery and improvement of future security measures.

NEW QUESTION # 153
Bran is an incident handler who is assessing the network of the organization. In the process, he wants to detect ping sweep attempts on the network using Wireshark tool.
Which of the following Wireshark filter he must use to accomplish this task?

- A. icmp.ident
- B. icmp.redir_gw
- C. icmp.type==8
- D. icmp.seq

Answer: C

NEW QUESTION # 154
Identify the network security incident where intended or authorized users are prevented from using system, network, or applications by flooding the network with a high volume of traffic that consumes all existing network resources.

- A. Denial-of-service
- B. SQL injection
- C. URL manipulation
- D. XSS attack

Answer: A

Explanation:
A Denial-of-Service (DoS) attack is characterized by flooding the network with a high volume of traffic to consume all available network resources, preventing intended or authorized users from accessing system, network, or applications. This type of attack aims to overwhelm the target's capacity to handle incoming requests, causing a denial of access to legitimate users. Unlike XSS (Cross-Site Scripting) attacks, URL manipulation, or SQL injection, which exploit vulnerabilities in web applications for unauthorized data access or manipulation, a DoS attack specifically targets the availability of services.
References:Incident Handler (ECIH v3) courses and study guides cover various types of network security incidents, including Denial-of-Service attacks, detailing their impact on network resources and services.

NEW QUESTION # 155
Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify
the reaction of the procedures that are implemented to handle such situations?

- A. Procedure testing
- B. Live walk-through testing
- C. Facility testing
- D. Scenario testing

Answer: A

NEW QUESTION # 156
......

Now there are many IT training institutions which can provide you with EC-COUNCIL certification 212-89 exam related training material, but usually through these website examinees do not gain detailed material. Because the materials they provide are specialized for EC-COUNCIL Certification 212-89 Exam, so they didn't attract the examinee's attention.

212-89 Practice Exam Fee: https://www.realvalidexam.com/212-89-real-exam-dumps.html

- Excel in Your 212-89 Exam with www.vce4dumps.com: The Quick Solution for Success □ Open website ➻ www.vce4dumps.com □ and search for ➥ 212-89 □ for free download □Exam 212-89 Book
- Valid 212-89 Exam Pass4sure □ Latest 212-89 Exam Pattern □ 212-89 Online Training □ Search for { 212-89 } and download exam materials for free through □ www.pdfvce.com □ □Valid Braindumps 212-89 Ebook
- 212-89 Related Certifications □ 212-89 Test Study Guide □ Valid 212-89 Exam Pass4sure □ Search on " www.practicevce.com " for □ 212-89 □ to obtain exam materials for free download □212-89 Test Topics Pdf
- 212-89 Related Certifications □ 212-89 Passed □ 212-89 Latest Test Cost □ Copy URL □ www.pdfvce.com □ open and search for 【 212-89 】 to download for free □Valid 212-89 Exam Pass4sure
- Quiz EC-COUNCIL First-grade 212-89 - EC Council Certified Incident Handler (ECIH v3) Latest Exam Experience □ Open website 《 www.practicevce.com 》 and search for 「 212-89 」 for free download □212-89 Test Guide
- Quiz EC-COUNCIL First-grade 212-89 - EC Council Certified Incident Handler (ECIH v3) Latest Exam Experience □ Easily obtain ⇛ 212-89 ⇚ for free download through 「 www.pdfvce.com 」 □Latest 212-89 Exam Registration
- Quiz EC-COUNCIL First-grade 212-89 - EC Council Certified Incident Handler (ECIH v3) Latest Exam Experience □ Go to website ⇛ www.dumpsquestion.com ⇚ open and search for " 212-89 " to download for free □212-89 Latest Test Cost
- 212-89 actual test, Test VCE dumps for EC Council Certified Incident Handler (ECIH v3) □ Search for ⇛ 212-89 ⇚ and easily obtain a free download on □ www.pdfvce.com □ □Reliable 212-89 Exam Simulator
- 2026 100% Free 212-89 –Perfect 100% Free Latest Exam Experience | 212-89 Practice Exam Fee □ Search for [212-89] and easily obtain a free download on □ www.prep4sures.top □ ℹ212-89 Latest Examprep
- Exam 212-89 Book □ Valid 212-89 Exam Pass4sure □ 212-89 Online Training ✈ Immediately open ➤ www.pdfvce.com □ and search for □ 212-89 □ to obtain a free download □212-89 Test Topics Pdf
- 212-89 Test Topics Pdf □ Reliable 212-89 Exam Simulator □ 212-89 Vce Files □ Easily obtain free download of 「 212-89 」 by searching on □ www.vce4dumps.com □ □Exam 212-89 Book
- www.stes.tyc.edu.tw, hashnode.com, www.stes.tyc.edu.tw, 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, www.peiyuege.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mecabricks.com, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of RealValidExam 212-89 dumps from Cloud Storage: https://drive.google.com/open?id=17obJ13bVkq9JQEtQtHV894AT29LOqyCb