

Enjoy EC-COUNCIL 212-89 Exam Questions Free Updates At 30% Discount



DOWNLOAD the newest TestsDumps 212-89 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=16jziVyG-rPM0hvDsMlrZiqXg1wJnoJX5>

With our 212-89 practice test software, you can simply assess yourself by going through the 212-89 practice tests. We highly recommend going through the 212-89 answers multiple times so you can assess your preparation for the EC Council Certified Incident Handler (ECIH v3). Make sure that you are preparing yourself for the 212-89 test with our practice test software as it will help you get a clear idea of the real 212-89 exam scenario. By passing the exams multiple times on practice test software, you will be able to pass the real 212-89 test in the first attempt.

Many candidates find the EC-COUNCIL 212-89 exam preparation difficult. They often buy expensive study courses to start their EC Council Certified Incident Handler (ECIH v3) (212-89) certification exam preparation. However, spending a huge amount on such resources is difficult for many EC-COUNCIL exam applicants. The latest EC-COUNCIL 212-89 Exam Dumps are the right option for you to prepare for the 212-89 certification test at home. TestsDumps has launched the 212-89 exam dumps with the collaboration of world-renowned professionals.

>> 212-89 Latest Test Discount <<

Hot 212-89 Questions | Reliable 212-89 Test Experience

If you are very busy, you can only take two or three hours a day to study our 212-89 study engine. Then I tell you this is enough! After ten days you can go to the exam. With such an efficient product, you really can't find the second one! In any case, many people have passed the exam after using 212-89 Training Materials. This is a fact that you must see. As long as you are still a sensible person, you will definitely choose 212-89 practice quiz. Don't hesitate! Time does not wait!

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q143-Q148):

NEW QUESTION # 143

Rose is an incident-handling person and she is responsible for detecting and eliminating any kind of scanning attempts over the

network by any malicious threat actors. Rose uses Wireshark tool 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==0X029`
- B. `tcp.dstport==7`
- C. `tcp.flags==0X000`
- D. `tcp.flags.reset==1`

Answer: A

NEW QUESTION # 144

Which of the following incidents are reported under CAT -5 federal agency category?

- A. Denial of Service DoS
- B. **Scans/ probes/ Attempted Access**
- C. Malicious code
- D. Exercise/ Network Defense Testing

Answer: B

NEW QUESTION # 145

Which of the following is a characteristic of adware?

- A. Replicating
- B. **Displaying popups**
- C. Gathering information
- D. Intimidating users

Answer: B

NEW QUESTION # 146

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

Answer: B

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 # 147

Preventing the incident from spreading and limiting the scope of the incident is known as:

- A. Incident Classification
- B. Incident Eradication
- **C. Incident Containment**
- D. Incident Protection

Answer: C

NEW QUESTION # 148

.....

Many job-hunters want to gain the competition advantages and become the hottest people which the companies rush to get. But if they want to realize that they must boost some valuable 212-89 certificate to raise their values and positions. The 212-89 certificate enjoys a high reputation among the labor market circle and is widely recognized as the proof of excellent talents and if you are one of them and you want to pass the test smoothly you can choose our 212-89 Practice Questions.

Hot 212-89 Questions: https://www.testsdumps.com/212-89_real-exam-dumps.html

And if you buy our 212-89 training materials, you will find you can have it in 5 to 10 minutes, EC-COUNCIL 212-89 Latest Test Discount We are more than just an exam dump provider, we are your guides to a passing score, and we are always here to help you, To help our candidate solve the difficulty of 212-89 real exam, we prepared the most reliable questions and answers for the exam preparation, which comes in three versions, Although a lot of people participate in EC-COUNCIL 212-89 exam, the pass rate is not very high.

Work with the Table of Contents in a Pages Document, Charting Utilities from Jon Peltier, And if you buy our 212-89 training materials, you will find you can have it in 5 to 10 minutes.

We are more than just an exam dump provider, we are 212-89 your guides to a passing score, and we are always here to help you, To help our candidate solve the difficulty of 212-89 real exam, we prepared the most reliable questions and answers for the exam preparation, which comes in three versions.

Quiz EC-COUNCIL - 212-89 Pass-Sure Latest Test Discount

Although a lot of people participate in EC-COUNCIL 212-89 exam, the pass rate is not very high, Once download and installed on your PC, you can practise test questions, review 212-89 Latest Test Discount your questions & answers using two different options 'practice exam' and 'virtual exam'.

- Exam 212-89 Book Vce 212-89 Free 212-89 Reliable Dumps Ebook Simply search for « 212-89 » for free download on www.examcollectionpass.com New 212-89 Exam Topics
- 212-89 Latest Test Discount | 100% Free the Best Hot EC Council Certified Incident Handler (ECIH v3) Questions Search for 212-89 on www.pdfvce.com immediately to obtain a free download 212-89 Reliable Study Questions
- 212-89 Sample Questions Pdf 212-89 Test Voucher New 212-89 Test Camp Immediately open www.prepawayete.com and search for 212-89 to obtain a free download 212-89 New Study Plan
- Excellent 212-89 Latest Test Discount by Pdfvce Open www.pdfvce.com enter 212-89 and obtain a free download 212-89 Exam Dumps Demo
- Pass Guaranteed 2026 212-89: EC Council Certified Incident Handler (ECIH v3) –Valid Latest Test Discount Easily obtain free download of 212-89 by searching on www.prepawaypdf.com Exam 212-89 Book
- 212-89 Premium Exam Exam 212-89 Tests Simulation 212-89 Questions Search on www.pdfvce.com for 212-89 to obtain exam materials for free download Vce 212-89 Free
- 212-89 New Study Plan 212-89 Test Certification Cost 212-89 Latest Exam Question Copy URL www.easy4engine.com open and search for 212-89 to download for free 212-89 Sample Questions Pdf
- 212-89 Test Certification Cost 212-89 Latest Exam Question 212-89 Reliable Study Questions Easily obtain (212-89) for free download through www.pdfvce.com 212-89 Test Certification Cost
- Free PDF Trustable EC-COUNCIL - 212-89 - EC Council Certified Incident Handler (ECIH v3) Latest Test Discount Search for 212-89 and download it for free immediately on www.troytecdumps.com Exam 212-89 Tests
- 212-89 Latest Test Discount Pass Certify High-quality Hot 212-89 Questions: EC Council Certified Incident Handler (ECIH v3) Search for (212-89) on www.pdfvce.com immediately to obtain a free download 212-89 Valid

Exam Book

DOWNLOAD the newest TestsDumps 212-89 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=16jziVyG-rPM0hvDsMrZiqXg1wJnoJX5>