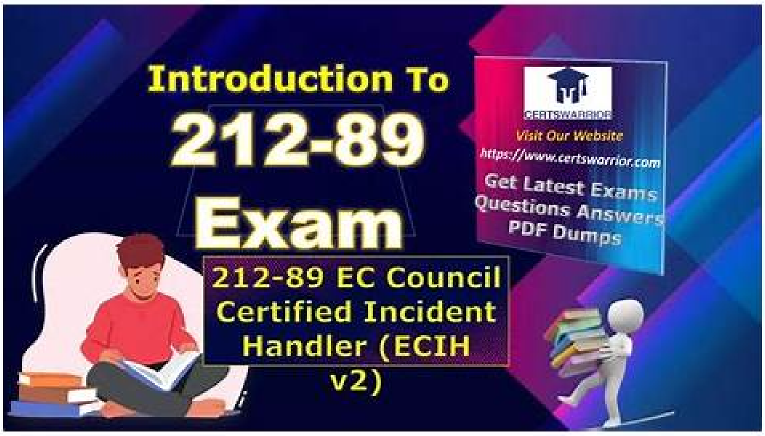
212-89 Valid Real Exam 100% Pass | High-quality 212-89 Test Assessment: EC Council Certified Incident Handler (ECIH v3)


Introduction To
212-89
Exam
212-89 EC Council Certified Incident Handler (ECIH v2)
CERTSWARRIOR
Visit Our Website
https://www.certswarrior.com
Get Latest Exams Questions Answers PDF Dumps

2025 Latest Itcertking 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=1YMdHoFvVnqescdNsukLZWulX0aOzkvYT

If you have been very panic sitting in the examination room, our 212-89 actual exam allows you to pass the exam more calmly and calmly. After you use our products, our 212-89 study materials will provide you with a real test environment before the 212-89 Exam. After the simulation, you will have a clearer understanding of the exam environment, examination process, and exam outline. And our 212-89 learning guide will be your best choice.

The EC-Council Certified Incident Handler (ECIH v2) certification exam is suitable for IT professionals who want to specialize in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification is ideal for security professionals, network administrators, system administrators, and IT professionals who want to advance their careers in incident handling and response.

>> 212-89 Valid Real Exam <<

212-89 Test Assessment, 212-89 Latest Braindumps Ppt

Our 212-89 exam guide have also set a series of explanation about the complicated parts certificated by the syllabus and are based on the actual situation to stimulate exam circumstance in order to provide you a high-quality and high-efficiency user experience. In addition, the 212-89 exam guide function as a time-counter, and you can set fixed time to fulfill your task, so that promote your efficiency in real test. The key strong-point of our 212-89 Test Guide is that we impart more important knowledge with fewer questions and answers, with those easily understandable 212-89 study braindumps, you will find more interests in them and experience an easy learning process.

The ECIH certification program is ideal for security personnel, network administrators, system administrators, security consultants, and IT managers who are responsible for incident handling or responding to security incidents. EC Council Certified Incident Handler (ECIH v3) certification program provides professionals with the knowledge and skills required to effectively detect, respond, and resolve security incidents in an organization. The ECIH certification is recognized globally and is an industry-standard certification for incident handling professionals. It is a valuable certification for professionals who want to enhance their career prospects in the field of cybersecurity.

EC-COUNCIL 212-89, also known as the EC Council Certified Incident Handler (ECIH v2), is a certification exam designed to assess the knowledge and skills of professionals in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification is offered by the International Council of E-Commerce Consultants (EC-Council) and is recognized globally as a standard for incident handling professionals.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q163-Q168):

NEW QUESTION # 163

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

- A. "arp" command
- B. "ifconfig" command
- C. "netstat -an" command
- D. "dd" command

Answer: C

NEW QUESTION # 164

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

Answer: D

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 # 165

Alice is a disgruntled employee. She decided to acquire critical information from her organization for financial benefit. To acccomplish this, Alice started running a virtual machine on the same physical host as her victim's virtual machine and took advantage of shared physical resources (processor cache) to steal data (cryptographic key/plain text secrets) from the victim machine. Identify the type of attack Alice is performing in the above scenario.

- A. SQL injection attack
- B. Side channel attack
- C. Service hijacking
- D. Man-in-the-cloud attack

Answer: B

Explanation:
A side channel attack, as described in the scenario, involves an attacker using indirect methods to gather information from a system. In this case, Alice is exploiting the shared physical resources, specifically the processor cache, of a virtual machine host to steal data from another virtual machine on the same host. This type of attack does not directly breach the system through conventional means like breaking encryption but instead takes advantage of the information leaked by the physical implementation of the system, such as timing information, power consumption, electromagnetic leaks, or, as in this case, shared resource utilization, to infer the secret data.
References:The EC-Council's Certified Incident Handler (ECIH v3) program covers various types of cyber attacks, including advanced techniques like side channel attacks, highlighting the need for comprehensive security strategies that consider both direct and indirect attack vectors.

NEW QUESTION # 166

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

- A. Chain-of-Precedence

- B. Network and host log records
- C. Forensic analysis report
- D. Chain-of-Custody

Answer: D

NEW QUESTION # 167

Stenley is an incident handler working for Texa Corp. located in the United States. With the growing concern of increasing emails from outside the organization, Stenley was asked to take appropriate actions to keep the security of the organization intact. In the process of detecting and containing malicious emails, Stenley was asked to check the validity of the emails received by employees. Identify the tools he can use to accomplish the given task.

- A. EventLog Analyzer
- B. PointofMail
- C. Email Dossier
- D. PoliteMail

Answer: C

NEW QUESTION # 168

......

212-89 Test Assessment: https://www.itcertking.com/212-89_exam.html

- 212-89 Valid Practice Materials □ Certification 212-89 Test Answers □ Pass 212-89 Test Guide □ Download ☀ 212-89 □☀□ for free by simply searching on □ www.examcollectionpass.com □ □Test 212-89 Pattern
- 212-89 exam study guide □ Search on ➽ www.pdfvce.com □ for ▹ 212-89 ◃ to obtain exam materials for free download □Certification 212-89 Test Answers
- Latest 212-89 Exam Pdf □ Latest 212-89 Exam Pdf □ PDF 212-89 Download □ Easily obtain free download of □ 212-89 □ by searching on □ www.testsdumps.com □ □Pass 212-89 Test Guide
- PDF 212-89 Download □ Latest 212-89 Exam Pdf □ Latest 212-89 Exam Pdf □ ⇛ www.pdfvce.com ⇚ is best website to obtain “ 212-89 ” for free download □212-89 Valid Practice Materials
- Useful 212-89 Valid Real Exam, Ensure to pass the 212-89 Exam □ Easily obtain free download of “ 212-89 ” by searching on ✔ www.passtestking.com □✔□ □212-89 Latest Guide Files
- Free PDF Quiz 2025 212-89: Reliable EC Council Certified Incident Handler (ECIH v3) Valid Real Exam □ Easily obtain 《 212-89 》 for free download through 「 www.pdfvce.com 」 □Online 212-89 Bootcamps
- 212-89 exam study guide □ Open website （ www.real4dumps.com ） and search for □ 212-89 □ for free download □ □Dump 212-89 Torrent
- 2025 Latest 212-89: EC Council Certified Incident Handler (ECIH v3) Valid Real Exam □ Search for ▸ 212-89 ◂ and download exam materials for free through ✔ www.pdfvce.com □✔□ □Latest 212-89 Exam Pdf
- Dump 212-89 Torrent □ 212-89 Reliable Test Prep □ 212-89 Latest Guide Files □ Search for □ 212-89 □ on □ www.examdiscuss.com □ immediately to obtain a free download □PDF 212-89 Download
- 2025 212-89 Valid Real Exam | Efficient EC-COUNCIL 212-89: EC Council Certified Incident Handler (ECIH v3) 100% Pass □ Search for ☀ 212-89 □☀□ on ➥ www.pdfvce.com □ immediately to obtain a free download □Exam 212-89 Actual Tests
- Pass 212-89 Test Guide □ Latest 212-89 Exam Pdf □ Test 212-89 Pattern □ Open □ www.passcollection.com □ enter ➤ 212-89 □ and obtain a free download □Dump 212-89 Torrent
- shufaii.com, nogorweb.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, kareyed271.snack-blog.com, provcare.com.au, tedcole945.win-blog.com, korodhsoaqoon.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, tutor.mawgood-eg.com, tedcole945.worldblogged.com, Disposable vapes

P.S. Free & New 212-89 dumps are available on Google Drive shared by Itcertking: https://drive.google.com/open?id=1YMdHoFvVnqescdNsukLZWulX0aOzkvYT