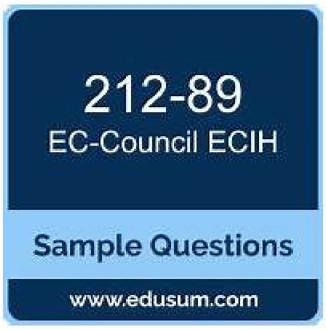
# Sample 212-89 Questions Answers - Latest 212-89 Dumps Ebook



DOWNLOAD the newest Exams4Collection 212-89 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1j2FhKwS-67a3GKYivM53qAl6T46JMDUi

Our 212-89 exam questions can meet your needs to the maximum extent, and our 212-89 learning materials are designed to the greatest extent from the customer's point of view. So you don't have to worry about the operational complexity. As soon as you enter the learning interface of our system and start practicing our 212-89 Learning Materials on our Windows software, you will find small buttons on the interface. These buttons show answers, and you can choose to hide answers during your learning of our 212-89 exam quiz so as not to interfere with your learning process. Every espect is perfect.

The ECIH v2 exam is an ideal certification for security professionals who want to enhance their skills and knowledge in incident handling and response. It is also a valuable certification for IT managers and executives who want to ensure that their organization is well-prepared to handle various types of security incidents. EC Council Certified Incident Handler (ECIH v3) certification is recognized globally, and it is highly valued by employers in the information security industry.

**>> Sample 212-89 Questions Answers <<**

## Latest 212-89 Dumps Ebook & 212-89 Free Exam Questions

In today’s society, there are increasingly thousands of people put a priority to acquire certificates to enhance their abilities. With a total new perspective, 212-89 study materials have been designed to serve most of the office workers who aim at getting a 212-89 certification. Our 212-89 Test Guide keep pace with contemporary talent development and makes every learner fit in the needs of the society. There is no doubt that our 212-89 latest question can be your first choice for your relevant knowledge accumulation and ability enhancement.

EC-COUNCIL 212-89 (EC Council Certified Incident Handler (ECIH v2)) certification exam is a globally recognized certification program that tests the knowledge and skills of individuals in the field of incident handling and response. It covers various topics such as incident management, risk assessment, vulnerability assessment, and incident reporting. EC Council Certified Incident Handler (ECIH v3) certification is ideal for security professionals, incident handlers, IT managers, network administrators, and anyone interested in enhancing their knowledge and skills in the field of incident handling and response.

# EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q165-Q170):

**NEW QUESTION # 165**
QualTech Solutions is a leading security services enterprise. Dickson works as an incident responder with this firm. He is performing vulnerability assessment to identify the security problems in the network, using automated tools to identify the hosts, services, and vulnerabilities present in the enterprise network.
Based on the above scenario, identify the type of vulnerability assessment performed by Dickson.

- A. External assessment
- B. Active assessment
- C. Passive assessment
- D. Internal assessment

**Answer: A**

Explanation:
An active assessment involves using automated tools to scan and probe the network actively to identify hosts, services, and vulnerabilities. This type of assessment directly interacts with the network components to gather information about the existing security posture, unlike passive assessments, which analyze traffic without sending packets to the target systems. Dickson's approach, employing automated tools to identify the network's hosts, services, and vulnerabilities, fits the definition of an active assessment. This method provides a more immediate understanding of the network's vulnerabilities, allowing for timely remediation actions.
References:The ECIH v3 program includes discussions on vulnerability assessment techniques, highlighting the differences between active and passive assessments and their applicability in identifying network security issues.

**NEW QUESTION # 166**
Farheen is an incident responder at reputed IT Firm based in Florida. Farheen was asked to investigate a recent cybercrime faced by the organization. As part of this process, she collected static data from a victim system.
She used DD tool command to perform forensic duplication to obtain an NTFS image of the original disk. She created a sector-by-sector mirror imaging of the disk and saved the output image file as image.dd.
Identify the static data collection process step performed by Farheen while collecting static data.

- A. System preservation
- B. Physical presentatio
- C. Administrative consideration
- D. Comparison

**Answer: A**

Explanation:
Farheen's activity of using the DD tool to create a sector-by-sector mirror image of the original disk is an example of system preservation. This process is crucial in digital forensics for creating an exact copy of a storage device to ensure that the original data remains unchanged during the investigation. By making a forensic duplication, or image, of the disk, Farheen ensures that the static data on the disk is preserved in its current state for thorough analysis, without altering the original evidence. This step allows investigators to work with a precise replica of the data, protecting the integrity of the original evidence.References:The Incident Handler (ECIH v3) certification materials discuss various methods and tools for data acquisition and preservation, highlighting the importance of system preservation in the initial stages of forensic analysis.

**NEW QUESTION # 167**
Your manager hands you several items of digital evidence and asks you to investigate them in the order of volatility. Which of the following is the MOST volatile?

- A. Disk
- B. Temp files
- C. Cache
- D. Emails

**Answer: C**

Explanation:
In the context of digital evidence investigation, volatility refers to how quickly data can change or be lost when power is removed or systems are altered. Among the options provided, cache is the most volatile because it is temporary storage that is designed to speed up access to data and is frequently overwritten. Cache data resides in RAM and includes things like memory buffers, system and network information, and process execution data, which are lost upon reboot or power loss. This contrasts with disks, emails, and temp files, which are considered less volatile because they are stored on permanent or semi-permanent media and are less likely to be immediately lost or overwritten.References:The Incident Handler (ECIH v3) curriculum includes principles of digital evidence handling, which emphasizes the importance of collecting evidence in descending order of volatility to ensure that the most ephemeral data is preserved before it's lost.

**NEW QUESTION # 168**
Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always turn out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network. Which step of IR did you just perform?

- A. Remediation
- B. Recovery
- C. Detection anc analysis (or identification)
- D. Preparation

**Answer: C**

**NEW QUESTION # 169**
Alex is an incident handler in QWERTY Company. He identified that an attacker created a backdoor inside the company's network by installing a fake AP inside a firewall. Which of the following attack types did the attacker use?

- A. Wardriving
- B. Ad hoc associations
- C. AP misconfiguration
- D. Rogue access point

**Answer: D**

**NEW QUESTION # 170**
......

**Latest 212-89 Dumps Ebook**: https://www.exams4collection.com/212-89-latest-braindumps.html

- Quiz EC-COUNCIL - Perfect 212-89 - Sample EC Council Certified Incident Handler (ECIH v3) Questions Answers □ Search for ✔ 212-89 □✔□ and obtain a free download on □ www.prepawaypdf.com □ □Free 212-89 Practice
- Real EC-COUNCIL 212-89 Exam Questions [2026] - Secret To Pass Exam In First Attempt □ Go to website 【 www.pdfvce.com 】 open and search for □ 212-89 □ to download for free □212-89 Boot Camp
- Free PDF 212-89 - EC Council Certified Incident Handler (ECIH v3) –High Pass-Rate Sample Questions Answers □ Simply search for “ 212-89 ” for free download on ▸ www.troytecdumps.com ◂ □Downloadable 212-89 PDF
- Real EC-COUNCIL 212-89 Exam Questions [2026] - Secret To Pass Exam In First Attempt □ Simply search for 《 212-89 》 for free download on ➽ www.pdfvce.com □ □Exam 212-89 Pass Guide
- 212-89 Download Free Dumps □ Free 212-89 Practice □ 212-89 Original Questions □ Open 【 www.vce4dumps.com 】 enter ➽ 212-89 □ and obtain a free download 👆212-89 Latest Exam Practice
- Download 212-89 Pdf □ 212-89 Latest Braindumps □ 212-89 Books PDF □ ✔ www.pdfvce.com □✔□ is best website to obtain { 212-89 } for free download □212-89 Test Score Report
- Pass Guaranteed Quiz 2026 EC-COUNCIL 212-89 Accurate Sample Questions Answers □ Open website （ www.torrentvce.com ） and search for □ 212-89 □ for free download □Download 212-89 Free Dumps
- 212-89 Original Questions □ 212-89 Exam Quizzes □ 212-89 Original Questions □ Open 「 www.pdfvce.com 」 enter ➥ 212-89 □ and obtain a free download □Download 212-89 Free Dumps

- 212-89 Training Materials □ Valid Exam 212-89 Preparation □ 212-89 Books PDF □ Search for 「212-89」 and download it for free on ➽ www.prepawayete.com □ website □Free 212-89 Practice
- Pass Guaranteed Quiz 2026 EC-COUNCIL 212-89 Accurate Sample Questions Answers □ Open ▹ www.pdfvce.com ◃ and search for ➡ 212-89 □□□ to download exam materials for free □Download 212-89 Free Dumps
- Quiz EC-COUNCIL - Perfect 212-89 - Sample EC Council Certified Incident Handler (ECIH v3) Questions Answers □ ▹ www.prepawayete.com ◃ is best website to obtain " 212-89 " for free download □Valid Exam 212-89 Preparation
- 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.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, onlyfans.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pastebin.com, Disposable vapes

What's more, part of that Exams4Collection 212-89 dumps now are free: https://drive.google.com/open?id=1j2FhKwS-67a3GKYivM53qAl6T46JMDUi