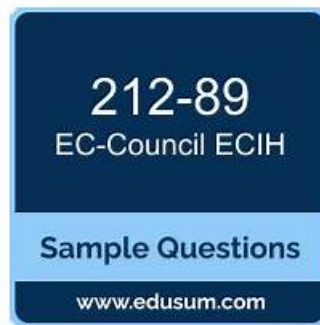


Free PDF Quiz 2026 EC-COUNCIL 212-89 Pass-Sure New Exam Sample



2026 Latest ActualtestPDF 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=1pkLJPCvSvioMWUQc4Gx2s4ZPtMF7Z_bg

Additionally, students can take multiple EC-COUNCIL 212-89 exam questions, helping them to check and improve their performance. Three formats are prepared in such a way that by using them, candidates will feel confident and crack the EC Council Certified Incident Handler (ECIH v3) (212-89) actual exam. These three formats suit different preparation styles of 212-89 test takers.

The EC-Council Certified Incident Handler (ECIH) v2 certification exam is a highly respected credential in the IT security industry. EC Council Certified Incident Handler (ECIH v3) certification exam is designed to test the knowledge, skills, and abilities of individuals who are responsible for handling and responding to computer security incidents. EC Council Certified Incident Handler (ECIH v3) certification exam is intended for professionals who want to demonstrate their expertise in handling incidents and managing network security operations.

>> New 212-89 Exam Sample <<

212-89 Valid Exam Sample, 212-89 Reliable Test Prep

In fact, the overload of learning seems not to be a good method, once you are weary of such a studying mode, it's difficult for you to regain interests and energy. Therefore, we should formulate a set of high efficient study plan to make the 212-89 exam dumps easier to operate. Here our products strive for providing you a comfortable study platform and continuously upgrade 212-89 Test Prep to meet every customer's requirements. Under the guidance of our 212-89 test braindumps, 20-30 hours' preparation is enough to help you obtain the EC-COUNCIL certification, which means you can have more time to do your own business as well as keep a balance between a rest and taking exams.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q75-Q80):

NEW QUESTION # 75

Which of the following digital evidence is temporarily stored on a digital device that requires a constant power supply and is deleted if the power supply is interrupted?

- A. Slack space
- **B. Process memory**
- C. Swap file
- D. Event logs

Answer: B

NEW QUESTION # 76

Which of the following is not the responsibility of first responders?

- A. Identifying the crime scene
- B. Protecting the crime scene
- **C. Preserving temporary and fragile evidence and then shut down or reboot the victim's computer**
- D. Packaging and transporting the electronic evidence

Answer: C

Explanation:

The responsibility of first responders does not include shutting down or rebooting the victim's computer as a measure to preserve temporary and fragile evidence. In fact, such actions can potentially alter or destroy volatile data that could be crucial for the investigation. The primary responsibilities of first responders include protecting and identifying the crime scene, and ensuring the preservation of evidence in its original state as much as possible, which may involve isolating affected systems from the network but not necessarily shutting them down or rebooting them without proper forensic readiness and consideration.

NEW QUESTION # 77

An organization implemented an encoding technique to eradicate SQL injection attacks. In this technique, if a user submits a request using single-quote and some values, then the encoding technique will convert it into numeric digits and letters ranging from a to f. This prevents the user request from performing SQL injection attempt on the web application.

Identify the encoding technique used by the organization.

- A. Unicode encoding
- B. URL encoding
- **C. Hex encoding**
- D. Base64 encoding

Answer: C

Explanation:

Hex encoding (also known as hexadecimal encoding) involves converting binary data into hexadecimal representation. In the context described, when a user submits a request with potentially malicious input (such as a single quote and other characters in an attempt to perform SQL injection), the encoding technique converts this input into a string of hexadecimal digits (ranging from 0 to 9 and A to F). This prevents the direct interpretation of the input as SQL commands by the database, thereby mitigating the risk of SQL injection attacks. This method is a form of input sanitization that helps ensure that user input cannot be used to manipulate database queries directly.

References: The use of hex encoding as a technique to prevent SQL injection attacks is discussed in the ECIH v3 course materials. This includes an explanation of how encoding user input can protect web applications from injection and other forms of attacks by ensuring that inputs are treated as data rather than executable code.

NEW QUESTION # 78

A colleague wants to minimize their security responsibility because they are in a small organization. They are evaluating a new application that is offered in different forms. Which form would result in the least amount of responsibility for the colleague?

- A. On-prom installation
- B. PaaS
- C. IaaS

- Answer: D**

The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.

- Answer: B**

• • • • •

212-89 Valid Exam Sample: <https://www.actualtestpdf.com/EC-COUNCIL/212-89-practice-exam-dumps.html>

- BTW, DOWNLOAD part of ActualtestPDF 212-89 dumps from Cloud Storage: https://drive.google.com/open?id=1pkLJPCySvioMWUQc4Gx2s4ZPtMF7Z_bg