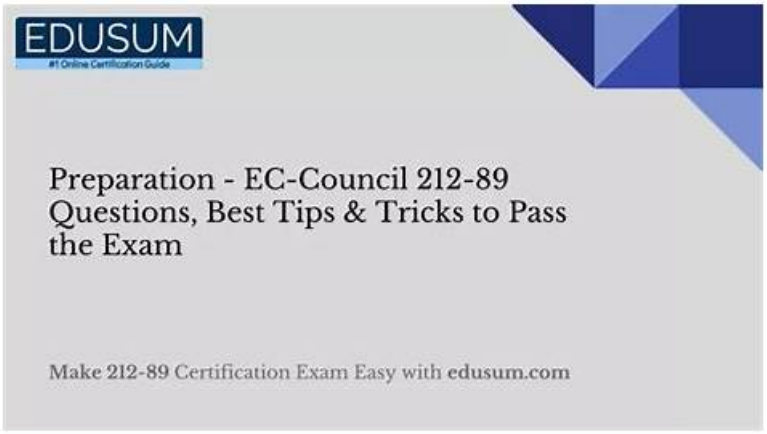
Valid New 212-89 Test Duration & Fast Download 212-89 Exam Sample & Latest Test 212-89 Collection Pdf



DOWNLOAD the newest Prep4sures 212-89 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1cxZ9BqdG3N5oPtGZc7fNr5H7nOA4MTyQ

We can promise that we are going to provide you with 24-hours online efficient service after you buy our EC Council Certified Incident Handler (ECIH v3) guide torrent. If you purchase our 212-89 test guide, we are going to answer your question immediately, because we hope that we can help you solve your problem about our 212-89 exam questions in the shortest time. We can promise that our online workers will be online every day. If you buy our 212-89 Test Guide, we can make sure that we will offer you help in the process of using our 212-89 exam questions. You will have the opportunity to enjoy the best service from our company.

The ECIH v2 certification exam is aimed at individuals who work in the field of cybersecurity and are responsible for detecting, responding to, and preventing security incidents. 212-89 exam is also suitable for individuals who aspire to work in this field. EC Council Certified Incident Handler (ECIH v3) certification is vendor-neutral, which means that it is not specific to any particular technology or product. This makes it a valuable certification for individuals who work in different environments and with different technologies.

The ECIH v2 certification exam is a comprehensive exam that tests the candidate's knowledge and skills in incident handling. 212-89 Exam consists of 100 multiple-choice questions and has a time limit of three hours. 212-89 exam covers topics such as incident management, risk assessment, incident response, and forensic analysis. Candidates must score at least 70% to pass the exam and earn the certification.

>> New 212-89 Test Duration <<

212-89 Exam Sample - Test 212-89 Collection Pdf

Do you want to spend the least time to pass your exam? If you do, then we will be your bets choice. 212-89 training materials are compiled by experienced experts who are quite familiar with the exam center, so the quality can be guaranteed. In addition, 212-89 exam materials contain most of the knowledge points for the exam, and you can have a good command of these knowledge points through practicing. In order to strengthen your confidence for the 212-89 Exam Braindumps, we are pass guarantee and money back guarantee if you fail to pass the exam. The money will be returned to your payment account.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q152-Q157):

NEW QUESTION # 152
Marley was asked by his incident handing and response (IH&R) team lead to collect volatile data such as system information and network information present in the registries, cache, and RAM of victim's system.
Identify the data acquisition method Marley must employ to collect volatile data.

- A. Live data acquisition

- B. Remote data acquisition
- C. Static data acquisition
- D. Validate data acquisition

Answer: A

NEW QUESTION # 153
Eric is an incident responder and is working on developing incident-handling plans and procedures. As part of this process, he is performing an analysis on the organizational network to generate a report and develop policies based on the acquired results. Which of the following tools will help him in analyzing his network and the related traffic?

- A. Wireshark
- B. Whois
- C. Burp Suite
- D. FaceNiff

Answer: A

Explanation:
Wireshark is a widely used network protocol analyzer that helps in capturing and interactively browsing the traffic on a network. It is an essential tool for incident responders like Eric who are developing incident- handling plans and procedures. By analyzing network traffic, Wireshark allows users to see what is happening on their network at a microscopic level, making it invaluable for troubleshooting network problems, analyzing security incidents, and understanding network behavior. Whois is used for querying databases that store registered users or assignees of an Internet resource. Burp Suite is a tool for testing web application security, and FaceNiff is used for session hijacking within a WiFi network, which makes Wireshark the best choice for analyzing network traffic.
References:ECIH v3 certification materials often reference Wireshark as a fundamental tool for network analysis, crucial for incident handlers in the analysis phase of incident response.

NEW QUESTION # 154
In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:

- A. Honey Pots
- B. Zombies
- C. Relays
- D. Handlers

Answer: B

NEW QUESTION # 155
In which of the following types of insider threats an insider who is uneducated on potential security threats or simply bypasses general security procedures to meet workplace efficiency?

- A. Malicious insider
- B. Compromised insider
- C. Professional insider
- D. Negligent insider

Answer: D

Explanation:
A negligent insider is an individual within an organization who, due to a lack of knowledge on security threats or in an attempt to increase workplace efficiency, inadvertently bypasses security procedures or makes errors that compromise security. This type of insider threat is not malicious in intent; rather, it stems from carelessness, oversight, or a lack of proper security training. Such insiders might click on phishing links, mishandle sensitive information, or use unsecured networks for work-related tasks, thereby exposing the organization to potential security breaches. This contrasts with compromised insiders (who are manipulated by external parties), professional insiders (who misuse their access for personal gain), and malicious insiders (who intentionally aim to harm the

organization).
References:The Incident Handler (ECIH v3) courses and study guides discuss different types of insider threats, emphasizing the importance of security awareness training to mitigate the risks associated with negligent insiders.

NEW QUESTION # 156
Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

- A. Correlating known patterns of suspicious and malicious behavior
- B. Making is compulsory for employees to sign a none disclosure agreement
- C. Protecting computer systems by implementing proper controls
- D. Categorizing information according to its sensitivity and access rights

Answer: A

NEW QUESTION # 157
.....

We keep a close watch at the change of the popular trend among the industry and the latest social views so as to keep pace with the times and provide the clients with the newest 212-89 study materials resources. Our service philosophy and tenet is that clients are our gods and the clients' satisfaction with our 212-89 Guide material is the biggest resource of our happiness. So why you still hesitated? Go and buy our 212-89 guide questions now. With our 212-89 learning guide, you will be able to pass the 212-89 exam without question.

https://drive.google.com/open?id=1cxZ9BqdG3N5oPtGZc7fNr5H7nOA4MTyQ