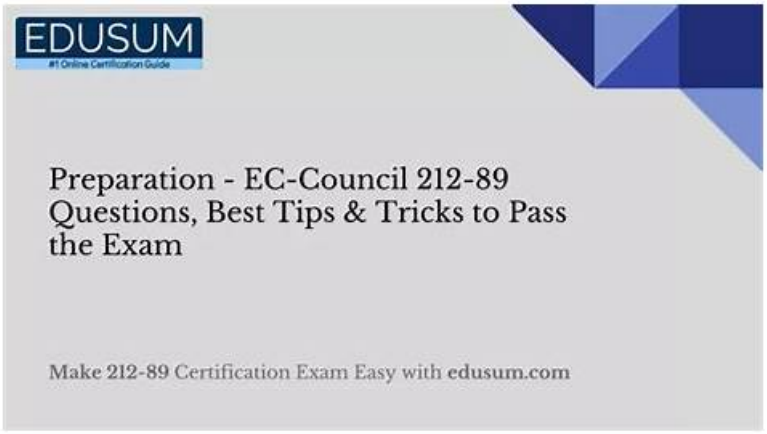
212-89 Latest Braindumps Book - Real 212-89 Testing Environment



P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by PrepPDF: https://drive.google.com/open?id=1cx8V0_mKPg1LW52Oc_OzC-pmXnFNp1Jk

Our 212-89 study questions in every year are summarized based on the test purpose, every answer is a template, there are subjective and objective 212-89 exams of two parts, we have in the corresponding modules for different topic of deliberate practice. To this end, our 212-89 training materials in the qualification exam summarize some problem- solving skills, and induce some generic templates. The user can scout for answer and scout for score based on the answer templates we provide, so the universal template can save a lot of precious time for the user to study and pass the 212-89 Exam.

The ECIH v2 certification exam is conducted by the EC-Council, a global leader in the field of cybersecurity. The EC-Council is known for its range of certifications and training programs that are designed to enhance the skills of cybersecurity professionals. The ECIH v2 certification exam is based on the latest industry standards and best practices, which ensures that individuals who pass the exam have the necessary knowledge and skills to handle security incidents.

>> 212-89 Latest Braindumps Book <<

Real 212-89 Testing Environment | Dump 212-89 Check

Free demo for 212-89 learning materials is available, you can try before buying, so that you can have a deeper understanding of what you are going to buy. We also recommend you to have a try before buying. In addition, 212-89 training materials contain both questions and answers, and it's convenient for you to check answers after practicing. 212-89 Exam Dumps cover most of the knowledge points for the exam, and you can have a good command of the knowledge points by using 212-89 exam dumps. We have online and offline chat service, if you have any questions, you can consult us.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q185-Q190):

NEW QUESTION # 185
In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:

- A. Asset Identification
- B. System characterization
- C. System classification
- D. Asset valuation

Answer: B

NEW QUESTION # 186
Which of the following is not called volatile data?

- A. Open sockets er open ports
- B. State of the network interface
- C. Creation dates of files
- D. The dale a no Lime of the system

Answer: C

Explanation:
Volatile data refers to information that is stored temporarily and is lost when a computer is turned off or restarted, such as RAM contents, including open sockets and open ports, the date and time of the system, and the state of the network interface. The creation dates of files, however, are considered non-volatile data because they are preserved on the hard drive and remain available after the system is restarted or turned off.
Non-volatile data is stored on persistent storage mediums like hard drives, SSDs, and magnetic tapes, where it remains until it is deleted or overwritten.
References:The Incident Handler (ECIH v3) certification emphasizes the distinction between volatile and non- volatile data in the context of digital forensics and incident response, highlighting the importance of understanding what data may be lost upon system shutdown and what data persists.

NEW QUESTION # 187
Which of the following techniques helps incident handlers to detect man-in-the-middle attack by finding the new APs and trying to connect an already established channel, even if the spoofed AP consists similar IP and MAC addresses as of the original AP?

- A. Access point monitoring
- B. Network traffic monitoring
- C. Wireless client monitoring
- D. General wireless traffic monitoring

Answer: A

Explanation:
Access point monitoring is the technique that helps incident handlers to detect man-in-the-middle (MitM) attacks by continuously observing and managing the wireless access points (APs) within a network. This includes identifying unauthorized or new APs attempting to connect to the network or mimic existing APs, even if they present similar IP and MAC addresses to legitimate access points. Through access point monitoring, incident handlers can quickly identify and mitigate spoofed APs, thus preventing MitM attacks that exploit wireless networks by intercepting and manipulating communications.
References:Incident Handler (ECIH v3) courses and study materials discuss network security monitoring strategies, including the importance of monitoring access points to detect and prevent MitM attacks and other threats to wireless networks.

NEW QUESTION # 188
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. Procmon and ProcessExplorer
- B. OllyDbg and IDA Pro
- C. Scylla and OllyDumpEx
- D. iNetSim

Answer: B

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 # 189
Identify the network security incident where intended or authorized users are prevented from using system, network, or applications by flooding the network with a high volume of traffic that consumes all existing network resources.

- A. URL manipulation
- B. SQL injection
- C. Denial-of-service
- D. XSS attack

Answer: C

Explanation:
A Denial-of-Service (DoS) attack is characterized by flooding the network with a high volume of traffic to consume all available network resources, preventing intended or authorized users from accessing system, network, or applications. This type of attack aims to overwhelm the target's capacity to handle incoming requests, causing a denial of access to legitimate users. Unlike XSS (Cross-Site Scripting) attacks, URL manipulation, or SQL injection, which exploit vulnerabilities in web applications for unauthorized data access or manipulation, a DoS attack specifically targets the availability of services.References:Incident Handler (ECIH v3) courses and study guides cover various types of network security incidents, including Denial-of-Service attacks, detailing their impact on network resources and services.

NEW QUESTION # 190
.....

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, 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, Disposable vapes

P.S. Free & New 212-89 dumps are available on Google Drive shared by PrepPDF: https://drive.google.com/open?id=1cx8V0_mKPg1LW52Oc_OzC-pmXnFNp1Jk