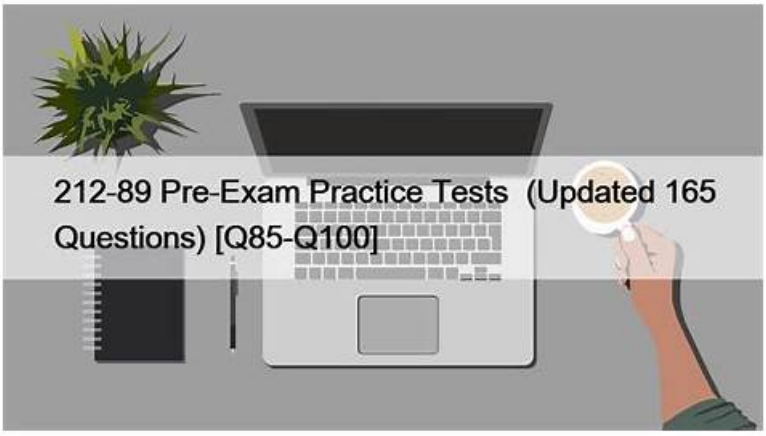
Real 212-89 are uploaded by Real Users which provide 212-89 Practice Tests Solutions.



P.S. Free & New 212-89 dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1I0bTRos2VAs3KEHV6Vsj8iPFJfAA3FqT

We are confident about our EC-COUNCIL 212-89 braindumps tested by our certified experts who have great reputation in IT certification. These 212-89 exam pdf offers you a chance to get high passing score in formal test and help you closer to your success. Valid 212-89 Test Questions can be access and instantly downloaded after purchased and there are free 212-89 pdf demo for you to check.

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 Learning Engine <<

212-89 Exam Tips & Latest 212-89 Dumps Ppt

The web-based 212-89 practice test is accessible via any browser. This 212-89 mock exam simulates the actual EC-COUNCIL 212-89 exam and does not require any software or plugins. Compatible with iOS, Mac, Android, and Windows operating systems, it provides all the features of the desktop-based 212-89 Practice Exam software.

ECCouncil 212-89 Exam

The Incident Manager Certification certified by the EC Council is designed to provide the fundamental skills to manage and respond to cybersecurity incidents in an information system. A certified accident controller is a qualified professional who can handle various types of accidents, risk assessment methodologies, and various accident management laws and policies. A certified incident controller will be capable to generate an incident response and management policies and control various types of computer security incidents, such as network security incidents, malicious code incidents, and threats of internal attacks.

The ECIH certification is ideal for individuals who are responsible for incident handling and response in their organizations. This includes security professionals, network administrators, IT managers, and incident response team members. With this certification, individuals can demonstrate their expertise in incident handling and response, and become more valuable to their organizations.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q94-Q99):

NEW QUESTION # 94
Eve's is an incident handler in ABC organization. One day, she got a complaint about email hacking incident from one of the employees of the organization. As a part of incident handling and response process, she must follow many recovery steps in order to recover from incident impact to maintain business continuity.

What is the first step that she must do to secure employee account?

- A. Enable scanning of links and attachments in all the emails
- B. Restore the email services and change the password
- C. Enable two-factor authentication
- D. Disabling automatic file sharing between the systems

Answer: B

Explanation:
The first step in securing an employee's account following an email hacking incident involves restoring access to the email services if necessary and immediately changing the password to prevent unauthorized access. This action ensures that the attacker is locked out of the account as quickly as possible. While enabling two-factor authentication, scanning links and attachments, and disabling automatic file sharing are important security measures, they come into play after ensuring that the compromised account is first secured by changing its password to halt any ongoing unauthorized access.References:The ECIH v3 certification materials cover the initial steps to be taken when responding to incidents involving compromised accounts, emphasizing the importance of quickly changing passwords to secure the accounts against further unauthorized access.

NEW QUESTION # 95
Daniel, a SOC analyst, detects multiple incoming TCP requests to the organization's mail server from different IPs. However, none of the requests complete the handshake. He suspects a potential attempt to exhaust server resources and confirms this with netstat logs. Which type of protocol-level incident is Daniel identifying?

- A. DNS cache poisoning
- B. SYN flood attack
- C. TCP session hijacking
- D. UDP reflection

Answer: B

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario describes a SYN flood attack, a classic protocol-level Denial-of-Service technique covered in the ECIH Network Security Incidents module. In a SYN flood, attackers send a large volume of TCP SYN packets but never complete the three-way handshake, leaving the server waiting for responses and exhausting connection resources.
Option D is correct because incomplete TCP handshakes, half-open connections, and resource exhaustion are defining characteristics of SYN flood attacks. The presence of multiple source IPs further suggests a distributed attack.
Option A involves taking over an existing session, not exhausting resources. Option B applies to UDP-based amplification attacks. Option C affects DNS resolution, not TCP handshakes.
ECIH stresses that early identification of SYN floods allows defenders to deploy SYN cookies, rate limiting, and upstream filtering. Recognizing handshake anomalies is therefore critical in protecting service availability.

NEW QUESTION # 96
Rica works as an incident handler for an international company. As part of her role, she must review the present security policy implemented. Upon inspection, Rica finds that the policy is wide open, and only known dangerous services/attacks or behaviors are blocked.
Which of the following is the current policy that Rica identified?

- A. Permissive policy
- B. Paranoid policy
- C. Promiscuous policy
- D. Prudent policy

Answer: A

NEW QUESTION # 97
You area systems administrator for a company. You are accessing your fileserver remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the

file server either.
You can ping the file server but not connect to it via RD. You check the Active Directory Server, and all is well.
You check the email server and find that emails are sent and received normally.
What is the most likely issue?

- A. The fileserver has shutdown
- B. An admin account issue
- C. A denial-of-service issue
- D. An email service issue

Answer: C

NEW QUESTION # 98
What command does a Digital Forensic Examiner use to display the list of all IP addresses and their associated MAC addresses on a victim computer to identify the machines that were communicating with it:

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

Answer: B

NEW QUESTION # 99
.....

BTW, DOWNLOAD part of PassExamDumps 212-89 dumps from Cloud Storage: https://drive.google.com/open?id=1I0bTRos2VAs3KEHV6Vsj8iPFJfAA3FqT