212-89 Reliable Exam Sample - 212-89 Latest Exam Cost

What's more, part of that Real4dumps 212-89 dumps now are free: https://drive.google.com/open?id=1jtHwZpE1btC7OSncMg0hCYQAJuz68Jrh

As you may see the data on the website, our sales volumes of our 212-89 exam questions are the highest in the market. You can browse our official websites to check our sales volumes. At the same time, many people pass the exam for the first time under the guidance of our 212-89 Practice Exam. And there is no exaggeration that our pass rate for our 212-89 study guide is 98% to 100% which is proved and tested by our loyal customers.

EC-COUNCIL 212-89 Exam is a certification program designed for professionals in the field of incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification is globally recognized and is considered one of the most prestigious certifications in the field of cybersecurity. The EC-COUNCIL 212-89 exam is also known as the EC Council Certified Incident Handler (ECIH v2) certification exam.

Who Is ECIH 212-89 Test Intended for?

This exam is designed for the individuals who work as incident handlers, penetration testers, risk assessment administrators, cyber forensic investigators, system administrators, firewall administrators, IT professionals, IT managers, etc. Those who want to pursue their career in incident response and handling can also apply for this certification exam as it will enhance your skills and abilities to perform tasks in the ECIH sector.

>> 212-89 Reliable Exam Sample <<

Hot 212-89 Reliable Exam Sample 100% Pass | Latest 212-89 Latest Exam Cost: EC Council Certified Incident Handler (ECIH v3)

Success in acquiring the 212-89 is seen to be crucial for your career growth. But preparing for the EC Council Certified Incident Handler (ECIH v3) (212-89) exam in today's busy routine might be difficult. This is where actual EC-COUNCIL 212-89 Exam Questions offered by Real4dumps come into play. For those candidates, who want to clear the 212-89 certification exam in a short time, we offer updated and real exam questions.

EC-Council Certified Incident Handler (ECIH) is a certification program designed to equip individuals with the necessary skills to handle and respond to various types of security incidents. The ECIH program is globally recognized and accredited by the American National Standards Institute (ANSI). The program covers a broad range of topics, including incident handling process, types of incidents, and incident reporting, among others. 212-89 course is ideal for IT and security professionals who want to enhance their skills in handling and responding to security incidents.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q159-Q164):

NEW QUESTION # 159
The region where the CSIRT is bound to serve and what does it and give service to is known as:

- A. Consistency
- B. None of the above
- C. Constituency
- D. Confidentiality

Answer: C

NEW QUESTION # 160
Bonney's system has been compromised by a gruesome malware.
What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

- A. Call the legal department in the organization and inform about the incident
- B. Complaint to police in a formal way regarding the incident
- C. Turn off the infected machine
- D. Leave it to the network administrators to handle

Answer: A

NEW QUESTION # 161
Mr. Smith is a lead incident responder of a small financial enterprise having few branches in Australia. Recently, the company suffered a massive attack losing USD 5 million through an inter-banking system. After in-depth investigation on the case, it was found out that the incident occurred because 6 months ago the attackers penetrated the network through a minor vulnerability and maintained the access without any user being aware of it. Then, he tried to delete users' fingerprints and performed a lateral movement to the computer of a person with privileges in the inter-banking system.
Finally, the attacker gained access and did fraudulent transactions.
Based on the above scenario, identify the most accurate kind of attack.

- A. Ransomware attack
- B. Denial-of-service attack
- C. APT attack
- D. Phishing

Answer: C

Explanation:
The scenario described fits the characteristics of an Advanced Persistent Threat (APT) attack. APTs are sophisticated, stealthy, and continuous computer hacking processes often orchestrated by groups targeting a specific entity. These attackers penetrate the network through vulnerabilities, maintain access without detection, and achieve their objectives, such as data exfiltration or financial theft, over an extended period.
The fact that attackers exploited a minor vulnerability, maintained access for six months, and performed lateral movements to access critical systems for fraudulent transactions highlights the strategic planning and persistence typical of APT attacks.
References:Incident Handler (ECIH v3) certification materials discuss APTs in detail, including their methodologies, objectives, and the importance of comprehensive security strategies to detect and mitigate such threats.

NEW QUESTION # 162
Which of the following is an attack that occurs when a malicious program causes a user's browser to perform man unwanted action on a trusted site for which the user is currently authenticated?

- A. Insecure direct object references
- B. Cross-site scripting
- C. SQL injection
- D. Cross-site request forgery

Answer: D

NEW QUESTION # 163
During the vulnerability assessment phase, the incident responders perform various steps as below:
1. Run vulnerability scans using tools
2. Identify and prioritize vulnerabilities
3. Examine and evaluate physical security
4. Perform OSINT information gathering to validate the vulnerabilities
5. Apply business and technology context to scanner results
6. Check for misconfigurations and human errors
7. Create a vulnerability scan report
Identify the correct sequence of vulnerability assessment steps performed by the incident responders.

- A. 2-->1-->4->7->5->6-->3
- B. 1-->3-->2->4->5->6-->7
- C. 3-->6-->1->2->5->4-->7
- D. 4-->1-->2->3->6->5-->7

Answer: C

NEW QUESTION # 164
......

id=1jtHwZpE1btC7OSncMg0hCYQAJuz68Jrh