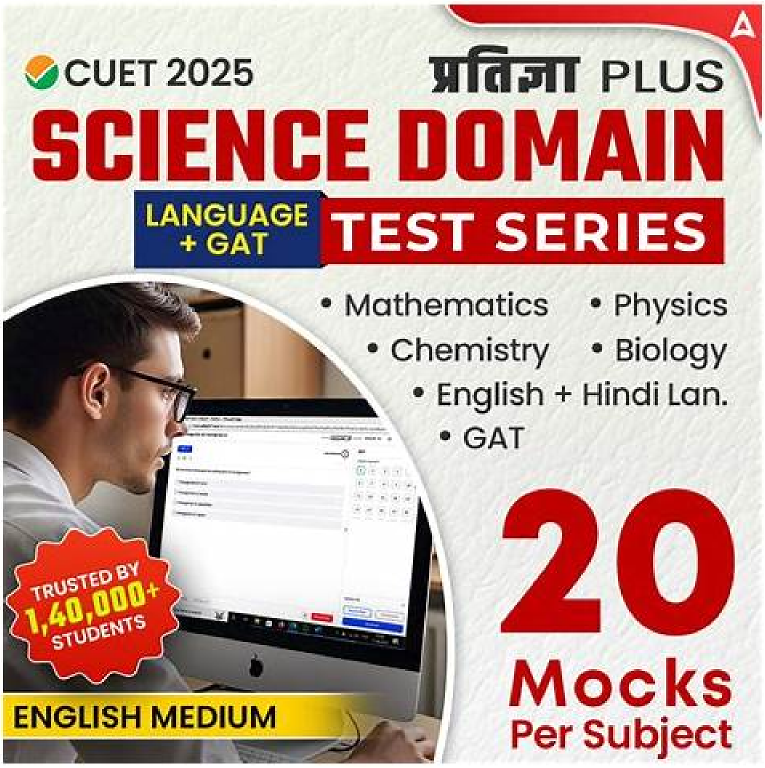
New 212-89 Mock Test - Latest Version



P.S. Free & New 212-89 dumps are available on Google Drive shared by ActualCollection: https://drive.google.com/open?id=12BCASu_fzL378IEC0Ea3qPon7Pzo7H_y

ActualCollection has been designing and offering real EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) exam dumps for many years. We regularly update our valid EC-COUNCIL 212-89 certification test preparation material to keep them in line with the current EC Council Certified Incident Handler (ECIH v3) (212-89) exam content and industry standards. Professionals from different countries give us their valuable feedback to refine 212-89 actual dumps even more.

The EC-Council Certified Incident Handler (ECIH v2) certification exam is designed for professionals who are responsible for incident handling or response. EC Council Certified Incident Handler (ECIH v3) certification verifies that the candidate possesses the skills and knowledge necessary to effectively respond to various types of security incidents. 212-89 exam covers a wide range of topics, including incident handling process, forensic readiness, and network traffic analysis.

The ECIH v2 certification exam is a comprehensive exam that covers all aspects of incident handling and response. 212-89 Exam consists of 100 multiple-choice questions, and candidates have two hours to complete the exam. EC Council Certified Incident Handler (ECIH v3) certification exam is available online, making it convenient for professionals to take the exam from anywhere in the world. 212-89 exam is also available in multiple languages, including English, Spanish, and Chinese.

>> New 212-89 Mock Test <<

212-89 Valid Test Cost | 212-89 Free Practice

Do you want to get more respects from other people? Do you long to become a powerful people? Our 212-89 exam torrent is compiled by professional experts that keep pace with contemporary talent development and makes every learner fit in the needs of the society. If you choose our 212-89 Study Materials, you will pass 212-89 exam successful in a short time. There is no doubt that our 212-89 exam question can be your first choice for your relevant knowledge accumulation and ability enhancement.

EC-Council Certified Incident Handler (ECIH v2) is an industry recognized certification that validates an individual's expertise in detecting, responding and resolving computer security incidents. 212-89 Exam is designed to assess the candidate's knowledge of the incident handling process, including the identification, containment, eradication, and recovery of a security breach. The ECIH certification is an excellent way for IT professionals to demonstrate their knowledge and skills in the area of incident handling.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q231-Q236):

NEW QUESTION # 231
Zaimasoft, a prominent IT organization, was attacked by perpetrators who directly targeted the hardware and caused irreversible damage to the hardware. In result, replacing or reinstalling the hardware was the only solution.
Identify the type of denial-of-service attack performed on Zaimasoft.

- A. DRDoS
- B. ddos
- C. PDoS
- D. DoS

Answer: C

Explanation:
A Permanent Denial-of-Service (PDoS) attack, also known as "phlashing," is a form of attack that targets hardware, causing irreversible damage to the hardware components, thereby making the device unusable without a replacement or significant hardware intervention. In the scenario described with Zaimasoft, the attackers' actions leading to the damage of hardware components align with the characteristics of a PDoS attack. Unlike Distributed Denial-of-Service (DDoS) or Denial-of-Service (DoS) attacks, which generally aim to overwhelm a system's resources temporarily, or DRDoS (Distributed Reflection Denial of Service), which involves amplification techniques using third-party servers, aPDoS attack directly damages the physical hardware, necessitating its replacement or reinstallation. This makes PDoS particularly severe due to its permanent impact on the targeted organization's hardware infrastructure.References:Incident Handler (ECIH v3) educational resources detail various types of denial-of-service attacks, including PDoS, highlighting the distinct nature of each attack and its implications on the affected systems, with PDoS being noted for its physical, irreparable impact on hardware components.

NEW QUESTION # 232
Bran is an incident handler who is assessing the network of the organization. In the process, he wants to detect ping sweep attempts on the network using Wireshark tool.
Which of the following Wireshark filter he must use to accomplish this task?

- A. icmp.type==8
- B. icmp.redir_gw
- C. icmp.ident
- D. icmp.seq

Answer: A

Explanation:
In Wireshark, the filtericmp.type==8is used to detect ping sweep attempts. ICMP type 8 messages are echo requests, which are used in ping operations to check the availability of a network device. A ping sweep involves sending ICMP echo requests to multiple addresses to discover active devices on a network. By filtering for ICMP type 8 messages in Wireshark, Bran can identify these echo requests, helping to pinpoint ping sweep activities on the network.
References:Wireshark, as a network protocol analyzer, is frequently discussed in the ECIH v3 program, with particular emphasis on its utility in detecting network reconnaissance activities like ping sweeps through specific filter usage.

NEW QUESTION # 233
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. 1-->3-->2-->4-->5-->6-->7
- B. 3-->6-->1-->2-->5-->4-->7
- C. 4-->1-->2-->3-->6-->5-->7
- D. 2-->1-->4-->7-->5-->6-->3

Answer: C

Explanation:
The correct sequence of steps performed by incident responders during the vulnerability assessment phase is as follows:
* Perform OSINT information gathering to validate the vulnerabilities (4):Initially, Open Source Intelligence (OSINT) is used to gather information about the organization's digital footprint and
* potential vulnerabilities.
* Run vulnerability scans using tools (1):Next, specialized tools are employed to scan the organization's networks and systems for vulnerabilities.
* Identify and prioritize vulnerabilities (2):The identified vulnerabilities are then analyzed and prioritized based on their severity and potential impact on the organization.
* Examine and evaluate physical security (3):Physical security assessments are also crucial as they can impact the overall security posture and protection of digital assets.
* Check for misconfigurations and human errors (6):This step involves looking for misconfigurations in systems and networks, as well as potential human errors that could lead to vulnerabilities.
* Apply business and technology context to scanner results (5):The results from the scans are evaluated within the context of the business and its technology environment to accurately assess risks.
* Create a vulnerability scan report (7):Finally, a comprehensive report is created, detailing the vulnerabilities, their severity, and recommended mitigation strategies.
This sequence ensures a thorough assessment, prioritizing vulnerabilities that pose the greatest risk and providing actionable insights for mitigation.References:ECIH v3 courses and study guides elaborate on the vulnerability assessment process, detailing the steps involved in identifying, evaluating, and addressing security vulnerabilities within an organization's IT infrastructure.

NEW QUESTION # 234
An adversary attacks the information resources to gain undue advantage is called:

- A. Conventional Warfare
- B. Defensive Information Warfare
- C. Offensive Information Warfare
- D. Electronic Warfare

Answer: C

NEW QUESTION # 235
A cloud service provider's IH&R team faces huge volumes of cloud-native logs after anomalous activity. To ensure swift and effective incident triage, what should be the primary course of action?

- A. Focus only on cloud-native logging, ignoring third-party logging tools.
- B. Immediately isolate all affected cloud instances regardless of customer impact.
- C. Implement an incident response automation/orchestration tool for cloud environments to correlate logs and prioritize alerts.
- D. Notify all clients to back up data and prepare for disruptions.

Answer: C

Explanation:
Explanation (cloud triage at scale):
Cloud environments generate massive telemetry across services, accounts, regions, and tenants. The limiting factor is not "more logs," but correlation and prioritization: connecting identity events, network flows, workload behaviors, API calls, and configuration changes into a coherent incident timeline and severity assessment. Automation/orchestration (A) supports rapid triage by correlating alerts, deduplicating noise, enriching with context (asset criticality, ownership, exposure), and driving consistent playbook actions (ticket creation, isolation steps, snapshotting, token revocation) with approvals.
(B) may be overbroad and can create major outages and contractual harm; it's containment without validated scope. (C) is premature; customer communication should be accurate and proportional, usually after initial scoping and legal review. (D) is the opposite of best practice-third-party logs can be essential (EDR, CASB, SIEM, SaaS audit logs).

So (A) is the best first step because it makes triage fast, consistent, and scalable, which is exactly what you need when log volume is the main operational barrier.

NEW QUESTION # 236

......

212-89 Valid Test Cost: https://www.actualcollection.com/212-89-exam-questions.html

- Exam 212-89 Simulator Online □ 212-89 Valid Test Blueprint □ 212-89 Exam Dumps Demo □ Open website □ www.examdiscuss.com □ and search for ⇛ 212-89 ⇚ for free download □Exam 212-89 Simulator Online
- Reliable 212-89 Test Pass4sure □ 212-89 Certification Sample Questions □ Valid Study 212-89 Questions □ Open website [www.pdfvce.com] and search for □ 212-89 □ for free download □212-89 Valid Test Blueprint
- Valid Study 212-89 Questions ❤ 212-89 Reliable Exam Questions □ Reliable 212-89 Test Bootcamp □ 【 www.practicevce.com 】 is best website to obtain 《 212-89 》 for free download □New 212-89 Real Exam
- EC-COUNCIL New 212-89 Mock Test: EC Council Certified Incident Handler (ECIH v3) - Pdfvce High Pass Rate □ Enter 《 www.pdfvce.com 》 and search for ▸ 212-89 ◂ to download for free □Reliable 212-89 Test Bootcamp
- Excellent New 212-89 Mock Test - Pass 212-89 Exam □ Search for 「 212-89 」 on ➤ www.practicevce.com □ immediately to obtain a free download □212-89 Valid Test Blueprint
- Valid 212-89 Exam Testking □ Reliable 212-89 Test Cost □ New 212-89 Exam Answers □ Easily obtain free download of □ 212-89 □ by searching on ▸ www.pdfvce.com ◂ □Reliable 212-89 Test Bootcamp
- Reliable 212-89 Braindumps Free □ Reliable 212-89 Test Cost □ Reliable 212-89 Braindumps Free □ Open ▹ www.pdfdumps.com ◃ and search for ➻ 212-89 □ to download exam materials for free □Valid 212-89 Exam Testking
- Quiz 2026 EC-COUNCIL 212-89: Pass-Sure New EC Council Certified Incident Handler (ECIH v3) Mock Test □ Download ☀ 212-89 □☀□ for free by simply searching on 【 www.pdfvce.com 】 □Reliable 212-89 Test Bootcamp
- 212-89 Valid Test Blueprint □ Reliable 212-89 Test Pass4sure □ Reliable 212-89 Braindumps Free □ Enter 「 www.examdiscuss.com 」 and search for ✔ 212-89 □✔□ to download for free □212-89 Valid Exam Answers
- Valid Study 212-89 Questions □ 212-89 Reliable Exam Questions □ Reliable 212-89 Test Bootcamp 🗟 Open ▹ www.pdfvce.com ◃ enter ➤ 212-89 □ and obtain a free download □212-89 Valid Test Sims
- Excellent New 212-89 Mock Test - Pass 212-89 Exam □ Search on ⇛ www.examcollectionpass.com ⇚ for □ 212-89 □ to obtain exam materials for free download □Reliable 212-89 Braindumps Free
- 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, learn.csisafety.com.au, 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, www.haogebbk.com, 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, www.kickstarter.com, 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, Disposable vapes

P.S. Free & New 212-89 dumps are available on Google Drive shared by ActualCollection: https://drive.google.com/open?id=12BCASu_fzL378IEC0Ea3qPon7Pzo7H_y