Proven and Instant Method to Pass EC-COUNCIL 212-89 Exam

BTW, DOWNLOAD part of LatestCram 212-89 dumps from Cloud Storage: https://drive.google.com/open?id=1sAuwTum8Tau-64nAbYv3wB1zjJ0l0-kF

EC-COUNCIL 212-89 practice braindumps will be worthy of purchase, and you will get manifest improvement. So you have a comfortable experience with our 212-89 study guide this time. By using our 212-89 Preparation materials, we are sure you will pass your exam smoothly and get your dreamed certification.

The ECIH v2 exam covers a wide range of topics related to incident handling, including incident response and management, vulnerability assessment and management, network security, and forensic analysis. 212-89 Exam also includes hands-on labs that allow candidates to practice their skills in a simulated environment. This practical approach ensures that candidates not only understand the theory behind incident handling, but also have the necessary skills to apply that knowledge in real-world scenarios.

Following are the requirements of ECCouncil 212-89 Exam

- Candidates with at least 1 year of work experience in the sector who wish to apply for admission
- Have the right to E | CIH, the candidate must:
- A direct exam without attending training is required to pay the registration fee of 100 USD.
- If the candidate is under 18, they are not allowed to take a formal training course or certification exam, unless they provide written accreditation to the training center / EC Council accredited by their parents / legal guardian and a letter of support from your higher education institution. Only candidates from a nationally accredited institution of higher education will be considered.
- The age required to follow the training or take the exam is limited to all candidates who are at least 18 years old.

>> Valid 212-89 Test Practice <<

212-89 Exam Braindumps: EC Council Certified Incident Handler (ECIH v3) & 212-89 Certification Training

The experts in our company are always keeping a close eye on even the slightest change on the 212-89 exam questions in the field. Therefore, we can assure that you will miss nothing needed for the 212-89 exam. What's more, the latest version of our 212-89 Study Materials will be a good way for you to broaden your horizons as well as improve your skills. You will certainly obtain a great chance to get a promotion in your company.

The content of the exam for the EC-Council Certified Incident Handler certification revolves around nine domains. They all have different weights in the content. The specific knowledge and skills as well as percentage share of questions related to each subject area of EC-Council 212-89 are outlined below:

- **Process Handling (14%).** Within this domain, the applicants need to demonstrate competency in security auditing; incident handling and response; incident readiness; forensic investigation; security incidents; eradication and recovery.
- **Malware Incidents (8%).** In the framework of this area, the students are required to be aware of malware, malware incident triage, as well as malicious code.
- **Application Level Incidents (8%).** The objective entails your knowledge of web application threats and vulnerabilities; web attacks; eradication of web applications.
- **Email Security Incidents (10%).** Here the examinees need to show good comprehension of email security as well as familiarity with deceptive and suspicious email; email incident; phishing email.
- **Forensic Readiness and First Response (13%).** This subject area encompasses an understanding of digital evidence; forensic readiness; computer forensics; volatile evidence; preservation of electronic evidence anti-forensics; static evidence.
- **Insider Threats (7%).** To deal with the questions from this domain, the learners should be conversant with insider threats; eradication; employee monitoring tools; detecting and preventing insider threats.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q31-Q36):

NEW QUESTION # 31
Common name(s) for CSIRT is(are)

- A. Incident Response Team (IRT)
- B. All the above
- C. Incident Handling Team (IHT)
- D. Security Incident Response Team (SIRT)

Answer: B

NEW QUESTION # 32
Alice is a disgruntled employee. She decided to acquire critical information from her organization for financial benefit. To acccomplish this, Alice started running a virtual machine on the same physical host as her victim's virtual machine and took advantage of shared physical resources (processor cache) to steal data (cryptographic key/plain text secrets) from the victim machine. Identify the type of attack Alice is performing in the above scenario.

- A. Service hijacking
- B. Side channel attack
- C. Man-in-the-cloud attack
- D. SQL injection attack

Answer: B

NEW QUESTION # 33
The open source TCP/IP network intrusion prevention and detection system (IDS/IPS), uses a rule-driven language, performs real-time traffic analysis and packet logging is known as:

- A. Snort
- B. Nessus
- C. Wireshark
- D. SAINT

Answer: A

NEW QUESTION # 34
Which policy recommends controls for securing and tracking organizational resources:

- A. Access control policy
- B. Administrative security policy
- C. Asset control policy
- D. Acceptable use policy

Answer: C

Explanation:
Explanation/Reference:

NEW QUESTION # 35
Lena, a SOC analyst, observes a pattern of unusual login attempts originating from multiple foreign IP addresses tied to shared drive links circulating within the organization. These links were embedded in emails appearing to come from the HR department and marked with urgent subject lines. Upon deeper inspection, Lena finds multiple similar messages still pending in the mail server's delivery queue. To prevent widespread exposure, she takes immediate action to eliminate these messages before they reach employees' inboxes.
Which incident response action best describes Lena's action?

- A. Isolating compromised mailboxes from the email relay
- B. Preemptively purging queued phishing emails from the server
- C. Initiating forensic triage on suspicious attachments
- D. Flagging login anomalies for correlation in the SIEM

Answer: B

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario demonstrates a preventive containment action during an email security incident. The ECIH Email Security Incident Handling module emphasizes that once phishing is identified, responders should immediately prevent further delivery to reduce organizational exposure.
Option A is correct because Lena removes malicious emails from the mail server's delivery queue before users receive them. This action directly reduces risk by preventing additional users from clicking malicious links or submitting credentials. ECIH identifies email purging as a critical containment technique during active phishing campaigns.
Option B is an investigative action, not containment. Option C applies after delivery and compromise. Option D addresses already compromised accounts rather than preventing exposure.
By stopping malicious emails before delivery, Lena aligns with ECIH best practices for rapid containment of email-based threats.

NEW QUESTION # 36
.....

- 212-89 Latest Learning Material □ Instant 212-89 Download □ 212-89 New Practice Materials □ Download { 212-89 } for free by simply searching on ➽ www.vce4dumps.com □ □212-89 Training For Exam
- www.4shared.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, 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, k12.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by LatestCram: https://drive.google.com/open?id=1sAuwTum8Tau-64nAbYv3wB1zjJ0l0-kF