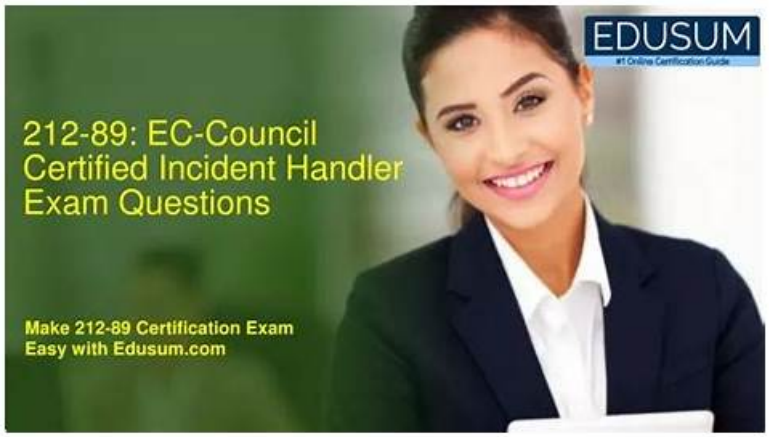
Latest 212-89 Exam Forum & 212-89 Study Center



What's more, part of that Pass4sures 212-89 dumps now are free: https://drive.google.com/open?id=1ibb2LMFIQjBt1qqSqcJKE1Av-s5PT-iA

When we are not students, we have more responsibility. The time we can be dedicated to learning is less, but if you want to have a better development in the IT industry, it is very important to pass the international recognized IT certification exam such as 212-89 exam. However, the IT elite our Pass4sures make efforts to provide you with the quickest method to help you Pass 212-89 Exam. We provide three type version of 212-89 exam materials: PDF, online and software version, and each version has its unique benifit. You can combine what you like and to choose a free trial of our demo.

The ECIH v2 exam covers a wide range of topics related to incident handling and response, including incident management, vulnerability management, threat intelligence, and forensic analysis. Participants will learn how to identify and respond to various types of cyber incidents, such as malware attacks, denial-of-service (DoS) attacks, and network intrusions. They will also be able to implement best practices for incident response, such as incident reporting, containment, eradication, and recovery.

>> Latest 212-89 Exam Forum <<

EC-COUNCIL 212-89 Study Center & 212-89 Real Testing Environment

As we all know, a lot of efforts need to be made to develop a 212-89 learning prep. Firstly, a huge amount of first hand materials are essential, which influences the quality of the compilation about the 212-89 actual test guide. We have tried our best to find all reference books. Then our experts have carefully summarized all relevant materials of the 212-89 exam. Also, annual official test is also included. They have built a clear knowledge frame in their minds before they begin to compile the 212-89 Actual Test guide. It is a long process to compilation. But they stick to work hard and never abandon. Finally, they finish all the compilation because of their passionate and persistent spirits. So you are lucky to come across our 212-89 exam questions.

To be eligible to take the EC-Council Certified Incident Handler (ECIH v2) certification exam, candidates must have a minimum of two years of experience in the IT security field. They must also have completed an EC-Council-approved training course or have equivalent knowledge and skills. EC Council Certified Incident Handler (ECIH v3) certification exam is a multiple-choice exam that consists of 100 questions, and candidates have two hours to complete the exam.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q76-Q81):

NEW QUESTION # 76
Which of the following is the ECIH phase that involves removing or eliminating the root cause of an incident and closing all attack vectors to prevent similar incidents in the future?

- A. Containment
- B. Vulnerability management phase
- C. Eradication
- D. Recovery

Answer: C

Explanation:
Eradication is the phase in the incident response process where the root cause of an incident is removed or eliminated, and all attack vectors are closed to prevent similar incidents in the future. This step follows the containment phase, where the immediate threat is isolated to prevent further damage, and precedes the recovery phase, where normal operations are restored. Eradication involves thoroughly removing malware, unauthorized access mechanisms, or any other elements used in the attack, and securing any vulnerabilities that were exploited. The goal is to ensure that the threat cannot re-emerge and that the systems are secure before they are returned to operational status.
References:The EC-Council's Incident Handler (ECIH v3) certification guide outlines the incident response process, including the specific tasks involved in the eradication phase, to ensure that incident handlers are prepared to effectively remove threats from an organization's environment.

NEW QUESTION # 77
Ikeo Corp.hired an incident response team to assess the enterprise security. As part of the incident handling and response process, the IR team is reviewing the current se cunty policies implemented by the enterprise. The IR team finds that employees of the organization do not have any restrictions on Internet access: they are allowed to visit any site, download any appl cation, and access a computer or network from a remote location. Considering this as the main security threat, the IR team plans to change this policy as it can be easily exploited by attackers.
Which of the following security policies is the IR team planning to modify?

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

Answer: B

NEW QUESTION # 78
Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall. They then use any software or hardware access point to perform an attack. Which of the following is this type of attack?

- A. Malware attack
- B. Password-based attack
- C. Rogue- access point attack
- D. Email infection

Answer: C

Explanation:
A rogue-access point attack occurs when attackers or insiders install an unsecured access point within a trusted network, typically behind a firewall, to create a backdoor. This allows them to bypass network security measures and perform various malicious activities undetected. The use of any software or hardware access point to gain unauthorized access and conduct an attack characterizes a rogue-access point attack. This contrasts with password-based attacks, malware attacks, and email infections, which involve different methodologies and objectives, such as stealing credentials, distributing malicious software, or propagating through email systems, respectively.References:The ECIH v3 certification materials discuss various types of network attacks, including rogue-access point attacks, highlighting the risk they pose by providing unauthorized network access to attackers.

NEW QUESTION # 79
The sign of incident that may happen in the future is called:

- A. A Precursor
- B. A Reactive
- C. A Proactive
- D. An Indication

Answer: A

NEW QUESTION # 80
Frederick is in the eradication process in one of the incidents he is handing.
Which of the following is NOT an eradication process?

- A. Analyze the security model of the cloud provider interface.
- B. Monitor the client's traffic for any malicious activities.
- C. Conduct vulnerability scanning and configuration audits.
- D. CCs must train a few of their employees to use the cloud securely.

Answer: D

NEW QUESTION # 81
......

212-89 Study Center: https://www.pass4sures.top/ECIH-Certification/212-89-testking-braindumps.html

- 212-89 Exam Materials are the Most Excellent Path for You to Pass 212-89 Exam □ Copy URL 【 www.testkingpass.com 】 open and search for ➽ 212-89 □ to download for free □212-89 Practice Exams
- Valid EC-COUNCIL 212-89 test questions - 212-89 braindumps files - 212-89 test engine □ Copy URL □ www.pdfvce.com □ open and search for ➽ 212-89 □ to download for free □Exam Vce 212-89 Free
- Valid 212-89 Study Notes ↘ 212-89 Examcollection Dumps Torrent □ 212-89 Practice Exams □ Copy URL " www.prepawaypdf.com " open and search for （ 212-89 ） to download for free □212-89 Detailed Study Dumps
- 212-89 Complete Exam Dumps □ Valid 212-89 Study Notes □ 212-89 Examcollection Dumps Torrent □ Easily obtain free download of ➽ 212-89 □ by searching on ➽ www.pdfvce.com □ □212-89 Real Torrent
- Valid EC-COUNCIL 212-89 test questions - 212-89 braindumps files - 212-89 test engine □ Easily obtain free download of ➤ 212-89 □ by searching on " www.exam4labs.com " □212-89 Pass Exam
- Valid 212-89 Study Notes □ 212-89 Examcollection Dumps Torrent □ New 212-89 Exam Test □ The page for free download of （ 212-89 ） on ☀ www.pdfvce.com □☀□ will open immediately □Valid 212-89 Exam Sample
- 212-89 Pass Exam □ New 212-89 Exam Dumps □ Test 212-89 Voucher □ Copy URL ☀ www.verifieddumps.com □☀□ open and search for ➤ 212-89 □ to download for free □212-89 Examcollection Dumps Torrent
- New Latest 212-89 Exam Forum 100% Pass | High Pass-Rate 212-89: EC Council Certified Incident Handler (ECIH v3) 100% Pass □ Simply search for ➤ 212-89 □ for free download on □ www.pdfvce.com □ □212-89 Exam Blueprint
- Valid EC-COUNCIL 212-89 test questions - 212-89 braindumps files - 212-89 test engine □ Download ⇛ 212-89 ⇚ for free by simply searching on ➡ www.troytecdumps.com □□□ □Test 212-89 Voucher
- Valid 212-89 Exam Discount □ 212-89 Reliable Exam Labs □ Test 212-89 Voucher □ Search for ➡ 212-89 □□□ and easily obtain a free download on [www.pdfvce.com] □212-89 Complete Exam Dumps
- Prepare with Confidence Using www.verifieddumps.com EC-COUNCIL 212-89 Exam Questions □ Open 【 www.verifieddumps.com 】 enter ➽ 212-89 □ and obtain a free download □212-89 Practice Exams
- raeverieacademy.com, myportal.utt.edu.tt, 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.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.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, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Pass4sures 212-89 dumps for free: https://drive.google.com/open?id=1ibb2LMFIQjBt1qqSqcJKE1Av-s5PT-iA