Latest 212-89 VCE Torrent & 212-89 Pass4sure PDF & 212-89 Latest VCE

What's more, part of that ExamDumpsVCE 212-89 dumps now are free: https://drive.google.com/open?id=1FCQJnTg1MLb488zB84d9g-t2_oDKMIfb

We provide you with free update for one year for 212-89 study guide, that is to say, there no need for you to spend extra money on update version. The update version for 212-89 exam materials will be sent to your email automatically. In addition, 212-89 exam dumps are compiled by experienced experts who are quite familiar with the exam center, therefore the quality can be guaranteed. You can use the 212-89 Exam Materials at ease. We have online and offline service, and if you have any questions for 212-89 training materials, don't hesitate to consult us.

The ECIH certification exam is based on the latest version of the ECIH v2 courseware. 212-89 courseware covers a wide range of topics such as incident handling process, incident handling procedures, communication and documentation, and various types of incidents, including network security incidents, web application security incidents, and malware incidents. 212-89 courseware also covers the legal and ethical issues related to incident handling and response.

>> Valid 212-89 Study Guide <<

High Pass-Rate Valid 212-89 Study Guide to Obtain EC-COUNCIL Certification

If you unluckily fail to pass your exam, don't worry, because we have created a mechanism for economical compensation. You just need to give us your test documents and transcript, and then our EC Council Certified Incident Handler (ECIH v3) prep torrent will

immediately provide you with a full refund, you will not lose money. More importantly, if you decide to buy our 212-89 Exam Torrent, we are willing to give you a discount, you will spend less money and time on preparing for your exam.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q50-Q55):

NEW QUESTION # 50
Finn is working in the eradication phase, wherein he is eliminating the root cause of an incident that occurred in the Windows operating system installed in a system. He ran a tool that can detect missing security patches and install the latest patches on the system and networks. Which of the following tools did he use to detect the missing security patches?

- A. Microsoft Cloud App Security
- B. Offico360 Advanced Throat Protection
- C. Microsoft Baseline Security Analyzer
- D. Microsoft Advanced Threat Analytics

Answer: C

Explanation:
The Microsoft Baseline Security Analyzer (MBSA) is a tool designed to assess a computer or network's security state by checking for missing security updates and common security misconfigurations. In the scenario with Finn, who is working in the eradication phase of an incident response process, the use of MBSA makes sense. The tool's ability to detect missing security patches and recommend the installation of the latest patches is crucial for eliminating vulnerabilities in the Windows operating system that could be the root cause of the incident.
MBSA scans the system for missing security updates, misconfigurations, and other vulnerabilities and provides detailed reports and recommendations for remediation. This step is vital in the eradication phase, where the goal is to remove the root causes of the incident and secure the system against future attacks. By ensuring that all necessary patches are applied, Finn is addressing any security gaps that could be exploited by attackers.
References:EC-Council's ECIH v3 program discusses various tools and techniques for securing systems and networks, including the importance of patch management and the use of tools like the Microsoft Baseline Security Analyzer for identifying and applying necessary security updates as part of the incident response process.

NEW QUESTION # 51
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 security 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 application, 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. Promiscuous policy
- B. Paranoid policy
- C. Prudent policy
- D. Permissive policy

Answer: B

Explanation:
A permissive security policy is one that allows employees broad freedoms in terms of internet access, application downloads, and remote access capabilities. In the scenario described, the incident response team identifies that the lack of restrictions is a significant security threat that could be exploited by attackers, indicating that the current policy is permissive. Modifying this policy would involve implementing more stringent controls on what sites can be visited, what applications can be downloaded, and how remote access is granted, moving towards a more controlled and secure environment. This approach contrasts with paranoic, prudent, and promiscuous policies, each of which has its own characteristics and applications in cybersecurity frameworks.
References:The ECIH v3 certification materials often discuss security policies within the context of organizational security posture, emphasizing how varying degrees of restrictiveness impact security and risk.

NEW QUESTION # 52

Darwin is an attacker within an organization and is performing network sniffing by running his system in promiscuous mode. He is capturing and viewing all the network packets transmitted within the organization. Edwin is an incident handler in the same organization.
In the above situation, which of the following Nmap commands Edwin must use to detect Darwin's system that is running in promiscuous mode?

- A. nmap -sU -p 500
- B. nmap -sV -T4 -O -F -version-light
- C. nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
- D. nmap --script host map

Answer: C

NEW QUESTION # 53
Jason is setting up a computer forensics lab and must perform the following steps: 1. physical location and structural design considerations; 2. planning and budgeting; 3. work area considerations; 4. physical security recommendations; 5. forensic lab licensing; 6. human resource considerations. Arrange these steps in the order of execution.

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

Answer: A

NEW QUESTION # 54
Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always turn out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network.
Which step of IR did you just perform?

- A. Detection and analysis (or identification)
- B. Remediation
- C. Recovery
- D. Preparation

Answer: A

NEW QUESTION # 55
.....

] by searching on ➤ www.pdfdumps.com □ □212-89 Latest Braindumps Sheet

- Test 212-89 Pattern □ 212-89 Valid Exam Pdf □ Test 212-89 Lab Questions □ Search for " 212-89 " and download it for free on □ www.pdfvce.com □ website □PDF 212-89 VCE
- 2026 Trustable Valid 212-89 Study Guide | 100% Free Examcollection 212-89 Dumps Torrent □ Copy URL 「 www.vce4dumps.com 」 open and search for □ 212-89 □ to download for free □212-89 Braindumps Pdf
- Training 212-89 Pdf □ Free 212-89 Dumps □ 212-89 Real Dumps ✳ Search on ➥ www.pdfvce.com □ for □ 212-89 □ to obtain exam materials for free download □Test 212-89 Lab Questions
- 2026 Trustable Valid 212-89 Study Guide | 100% Free Examcollection 212-89 Dumps Torrent □ Search for □ 212-89 □ and download exam materials for free through ✔ www.prepawayete.com □✔□ □Real 212-89 Braindumps
- 212-89 Exam Experience □ Trustworthy 212-89 Exam Torrent □ 212-89 Valid Exam Pdf □ Immediately open ➽ www.pdfvce.com □ and search for □ 212-89 □ to obtain a free download □212-89 Valid Exam Pdf
- 212-89 Valid Exam Pdf □ Test 212-89 Pattern □ 212-89 Valid Exam Pdf □ Go to website □ www.pdfdumps.com □ open and search for 【 212-89 】 to download for free □Test 212-89 Lab Questions
- 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, 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, ncon.edu.sa, study.stcs.edu.np, 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, Disposable vapes

BONUS!!! Download part of ExamDumpsVCE 212-89 dumps for free: https://drive.google.com/open?id=1FCQJnTg1MLb488zB84d9g-t2_oDKMIfb