High 212-89 Quality | Valid 212-89 Test Dumps

What's more, part of that Getcertkey 212-89 dumps now are free: https://drive.google.com/open?id=13q672rBe-Qbhx4YanzqMH-ptu_sp3_E_

But the helpful feature is that it works without a stable internet service. What makes your EC-COUNCIL Certification Exams preparation super easy is it imitates the exact syllabus and structure of the actual EC-COUNCIL 212-89 Certification Exam. Getcertkey never leaves its customers in the lurch.

EC-COUNCIL 212-89 Exam Syllabus Topics:

Section	Weight	Objectives
Handling and Responding to Network Security Incidents	15%	- Response and mitigation strategies • 1. Blocking malicious traffic • 2. Securing network infrastructure - Network attacks and threats • 1. Network intrusion techniques • 2. DDoS, man-in-the-middle, SQL injection - Network incident detection and analysis • 1. Monitoring network traffic • 2. Using IDS/IPS tools
Handling and Responding to Malware Incidents	18%	- Malware analysis techniques • 1. Static and dynamic analysis • 2. Identifying malware behavior - Malware incident response procedures • 1. Removing malware and recovering • 2. Isolating infected systems - Types of malware and attack vectors • 1. Viruses, worms, trojans, ransomware • 2. Social engineering and phishing

Incident Handling Process	15%	- Detection and analysis phase • 1. Classifying and prioritizing incidents • 2. Identifying security incidents - Containment, eradication, and recovery • 1. Strategies for containment • 2. Restoring systems and services • 3. Eradicating threats and vulnerabilities - Preparation phase • 1. Developing incident response policies • 2. Building incident response teams
Handling and Responding to Cloud Security Incidents	10%	- Cloud computing concepts and risks • 1. Cloud-specific threats • 2. Cloud service models and deployment models - Cloud incident response process • 1. Detecting and analyzing cloud incidents • 2. Responding in multi-tenant environments
Post-Incident Activities and Reporting	7%	- Lessons learned and improvement • 1. Updating policies and procedures • 2. Conducting post-incident reviews - Incident documentation and reporting • 1. Communicating with stakeholders • 2. Creating incident reports
Introduction to Incident Handling and Response	12%	- Legal and ethical aspects • 1. Compliance requirements • 2. Privacy and data protection - Fundamentals of incident handling and response • 1. Incident response lifecycle • 2. Key concepts and terminology
Handling and Responding to Endpoint Security Incidents	13%	- Endpoint incident response • 1. Investigating compromised endpoints • 2. Remediation and hardening - Endpoint threats and vulnerabilities • 1. Endpoint attack vectors • 2. Unpatched systems, misconfigurations

Three High-in-Demand Getcertkey EC-COUNCIL 212-89 Practice Questions Formats

Do you want to double your salary in a short time? Yes, it is not a dream. Our 212-89 latest study guide can help you. IT field is becoming competitive; a EC-COUNCIL certification can help you do that. If you get a certification with our 212-89 latest study guide, maybe your career will change. A useful certification will bring you much outstanding advantage when you apply for any jobs about EC-COUNCIL company or products. Just only dozens of money on 212-89 Latest Study Guide will assist you 100% pass exam and 24-hours worm aid service.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q195-Q200):

NEW QUESTION # 195
As a Certified Incident Handler at a multinational corporation, you are notified of a possible data breach incident in one of the departments. During the initial investigation, you confirmed that one workstation was used to execute the malicious activity. You need to ensure the integrity of the evidence for further forensic analysis. What should your first response action be regarding the affected workstation?

- A. Shut down the workstation immediately to stop potential data loss.
- B. Use an antivirus to scan the workstation and delete any detected malware.
- C. Immediately disconnect the workstation from the network but leave it running.
- D. Photograph the workstation and document the hardware configuration.

Answer: C

NEW QUESTION # 196
What is the name of the type of malicious software or malware designed to deny access to a computer system or data until money is paid?

- A. Adware
- B. Ransomware
- C. Virus
- D. Spyware

Answer: B

NEW QUESTION # 197
When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

- A. The access requests granted to an employee should be documented and vetted by the supervisor
- B. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
- C. The organization should enforce separation of duties
- D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

Answer: B

NEW QUESTION # 198
ZYX company experienced a DoS/DDoS attack on their network. Upon investigating the incident, they concluded that the attack is an application-layer attack. Which of the following attacks did the attacker use?

- A. SYN flood attack
- B. UDP flood attack
- C. Ping of ceath
- D. Slowloris attack

Answer: D

Explanation:
The Slowloris attack is a type of application-layer attack that targets the web server by establishing and maintaining many

simultaneous HTTP connections to the target server. Unlike traditional network-layer DoS /DDoS attacks such as UDP flood or SYN flood, Slowloris is designed to hold as many connections to the target web server open for as long as possible. It does so by sending partial requests, which are never completed, and periodically sending subsequent HTTP headers to keep the connections open. This consumes the server's resources, leading to denial of service as legitimate users cannot establish connections. The Slowloris attack is effective even against servers with a high bandwidth because it targets the server's connection pool, not its network bandwidth.
References:Incident Handler (ECIH v3) courses and study guides particularly emphasize understanding different types of attacks, including application-layer attacks like Slowloris, as part of the incident handling and response process.

NEW QUESTION # 199
Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS).
In case of a malware incident in your customer's database, who is responsible for eradicating the malicious software?

- A. Your company
- B. The PaaS provider
- C. Building management
- D. The customer

Answer: A

NEW QUESTION # 200
.....

Perhaps now you are one of the candidates of the EC-COUNCIL 212-89 exam, perhaps now you are worried about not passing the exam smoothly. Now we have good news for you: our 212-89 study materials will solve all your worries and help you successfully pass it. With the high pass rate as 98% to 100%, you will find that we have the best EC Council Certified Incident Handler (ECIH v3) 212-89 learning braindumps which contain the most accurate real exam questions.

Valid 212-89 Test Dumps: https://www.getcertkey.com/212-89_braindumps.html

- Latest Released EC-COUNCIL High 212-89 Quality: EC Council Certified Incident Handler (ECIH v3) - Valid 212-89 Test Dumps □ Search on [www.pdfdumps.com] for [212-89] to obtain exam materials for free download □212-89 Latest Materials
- High 212-89 Quality - Quiz EC-COUNCIL 212-89 First-grade Valid Test Dumps □ Search for ▹ 212-89 ◃ and obtain a free download on 「 www.pdfvce.com 」 □212-89 Latest Materials
- New 212-89 Exam Answers □ 212-89 High Passing Score □ 212-89 Latest Materials □ Enter " www.prepawaypdf.com " and search for ⇛ 212-89 ⇚ to download for free □212-89 Reliable Mock Test
- EC-COUNCIL - High Hit-Rate High 212-89 Quality □ Open ▹ www.pdfvce.com ◃ enter " 212-89 " and obtain a free download □Exam 212-89 Exercise
- Instant 212-89 Access □ 212-89 Latest Exam Book □ 212-89 Latest Materials □ Enter 「 www.prepawayete.com 」 and search for ➡ 212-89 □□□ to download for free □212-89 Latest Materials
- EC-COUNCIL 212-89 Dumps - Hassle-Free Accomplishment □ Open 【 www.pdfvce.com 】 enter ⇛ 212-89 ⇚ and obtain a free download □Latest 212-89 Exam Cram
- EC-COUNCIL - High Hit-Rate High 212-89 Quality □ Search for 《 212-89 》 and obtain a free download on 《 www.practicevce.com 》 □Exam 212-89 Exercise
- Earn the Credential of EC-COUNCIL 212-89 Exam □ Search for ▹ 212-89 ◃ on ⇛ www.pdfvce.com ⇚ immediately to obtain a free download □New 212-89 Test Answers
- High 212-89 Quality - Quiz EC-COUNCIL 212-89 First-grade Valid Test Dumps □ " www.prepawayete.com " is best website to obtain □ 212-89 □ for free download □New 212-89 Test Answers
- Test 212-89 Vce Free ～ Braindump 212-89 Pdf □ Instant 212-89 Access □ Search for [212-89] and obtain a free download on ➤ www.pdfvce.com □ □212-89 High Passing Score
- High 212-89 Quality - Quiz EC-COUNCIL 212-89 First-grade Valid Test Dumps □ Search for □ 212-89 □ and download it for free immediately on { www.examcollectionpass.com } □New 212-89 Test Answers
- 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, www.stes.tyc.edu.tw, 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, 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, letterboxd.com, Disposable vapes

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by Getcertkey: https://drive.google.com/open?id=13q672rBe-Qbhx4YanzqMH-ptu_sp3_E_