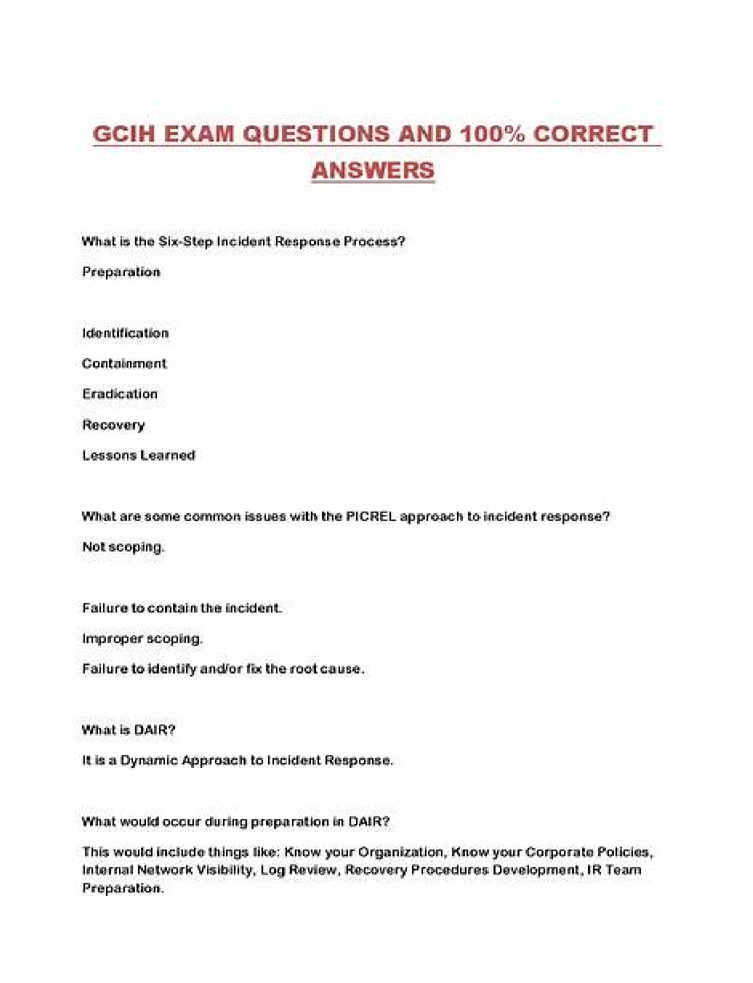
GCIH Guaranteed Questions Answers, GCIH Dumps Free Download



GCIH EXAM QUESTIONS AND 100% CORRECT ANSWERS

What is the Six-Step Incident Response Process?

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

What are some common issues with the PICREL approach to incident response?

Not scoping.

Failure to contain the incident.

Improper scoping.

Failure to identify and/or fix the root cause.

What is DAIR?

It is a Dynamic Approach to Incident Response.

What would occur during preparation in DAIR?

This would include things like: Know your Organization, Know your Corporate Policies, Internal Network Visibility, Log Review, Recovery Procedures Development, IR Team Preparation.

What's more, part of that DumpsFree GCIH dumps now are free: https://drive.google.com/open?id=1pHXym6uiXjf0b63u3BvxXbkLfRDKeDPt

Entering a strange environment, we will inevitably be very nervous. And our emotions will affect our performance. That is why some of the condidats fail in their real exam. But if you buy our GCIH exam questions, then you won't worry about this problem. Our GCIH study guide has arranged a mock exam to ensure that the user can take the exam in the best possible state. We simulated the most realistic examination room environment so that users can really familiarize themselves with the examination room. And our GCIH Practice Engine can give you 100% pass guarantee.

The GCIH Certification is designed for professionals who are responsible for incident handling and response, including security analysts, incident responders, network administrators, and IT security managers. GIAC Certified Incident Handler certification demonstrates that an individual has the technical skills and knowledge required to detect, respond to, and recover from security incidents, as well as the ability to develop and implement incident response plans.

>> GCIH Guaranteed Questions Answers <<

2026 GCIH Guaranteed Questions Answers | Accurate GIAC Certified Incident Handler 100% Free Dumps Free Download

We don't want you to prepare and practice the old questions and waste time. Therefore, our team of certified experts includes updated GIAC Certified Incident Handler GCIH Exam Questions as soon as they are released. DumpsFree provides up-to-date GIAC exam questions.

GIAC Certified Incident Handler Sample Questions (Q126-Q131):

NEW QUESTION # 126
Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone.
Which of the following methods has the attacker used to crack Andrew's password?
Each correct answer represents a complete solution. Choose all that apply.

- A. Social engineering
- B. Brute force attack
- C. Denial-of-service (DoS) attack
- D. Zero-day attack
- E. Password guessing
- F. Dictionary-based attack
- G. Buffer-overflow attack
- H. Rainbow attack

Answer: A,B,E,F,H

NEW QUESTION # 127
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?

- A. Denial-of-Service
- B. Injection
- C. Virus
- D. Internal attack

Answer: A

NEW QUESTION # 128
John works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user-defined URLs?

- A. Code red worm
- B. Hybrid attacks
- C. Morris worm
- D. PTC worms and mutations

Answer: D

Explanation:
Section: Volume B

NEW QUESTION # 129
Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?
Each correct answer represents a complete solution. Choose two.

- A. Teardrop attack
- B. Land attack
- C. SYN flood attack
- D. Ping of Death attack

Answer: A,D

NEW QUESTION # 130
Which of the following functions can be used as a countermeasure to a Shell Injection attack?
Each correct answer represents a complete solution. Choose all that apply.

- A. regenerateid()
- B. mysql_real_escape_string()
- C. escapeshellcmd()
- D. escapeshellarg()

Answer: C,D

NEW QUESTION # 131
......

Some people are not good at operating computers. So you might worry about that the GCIH certification materials are not suitable for you. Try to believe us. Our experts have taken your worries seriously. They have made it easy to operate for all people. Even if you know little about computers, you can easily begin to do exercises of the GCIH real exam dumps. Also, we have invited for many volunteers to try our study materials. The results show our products are suitable for them. In addition, the system of our GCIH test training is powerful. You will never come across system crashes. The system we design has strong compatibility. High speed running completely has no problem at all.