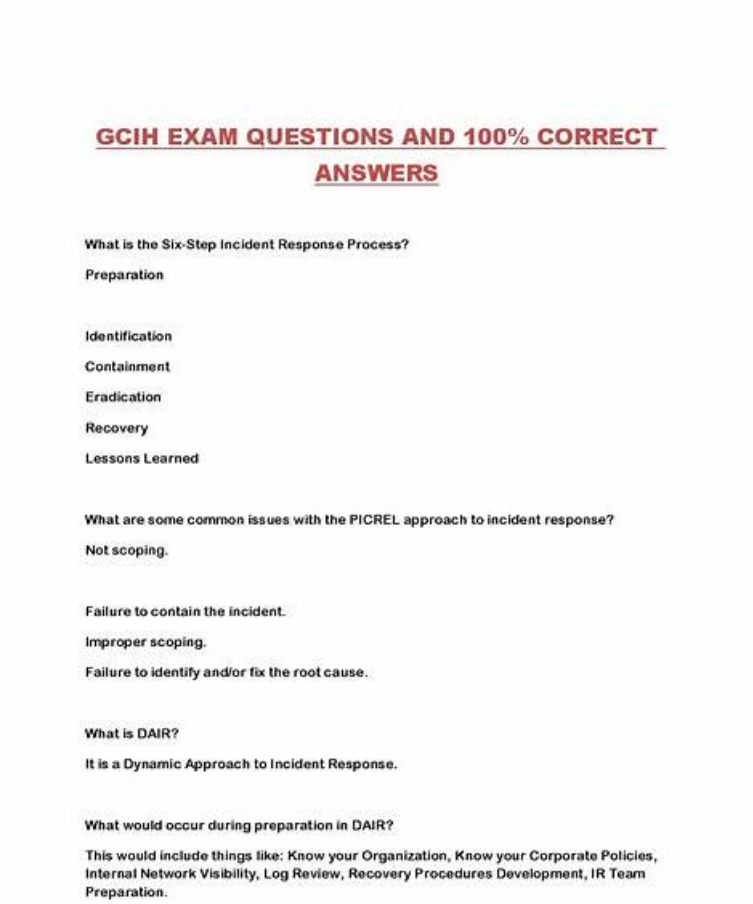
GCIH Exam Actual Questions, Exam GCIH Tests


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.

P.S. Free & New GCIH dumps are available on Google Drive shared by Test4Sure: https://drive.google.com/open?id=1zh5YMrGq7P-vLuVZBk2GrdEOSfTf08nk

The experts in our company have been focusing on the GCIH examination for a long time and they never overlook any new knowledge. The content of our GCIH study materials has always been kept up to date. Don't worry if any new information comes out after your purchase of our GCIH Practice Braindumps. We will inform you by E-mail when we have a new version and send it to you right away. So as long as you buy our GCIH learning guide, you can always have the latest exam questions and answers.

The GCIH Certification is recognized as a standard in the cybersecurity industry and is highly respected by employers worldwide. It is an advanced-level certification that requires individuals to have a solid understanding of incident handling techniques, tools, and methodologies. To obtain the certification, candidates are required to pass a rigorous exam that tests their knowledge of incident handling and response.

>> GCIH Exam Actual Questions <<

Exam GCIH Tests, GCIH Positive Feedback

This product is enough to get ready for the GCIH test on the first attempt. Three formats are easy to use and meet the needs of every GIAC Certified Incident Handler (GCIH) test applicant. The GIAC GCIH practice material's three formats are Desktop practice test software, web-based practice exam, and PDF.

GIAC Certified Incident Handler Sample Questions (Q64-Q69):

NEW QUESTION # 64

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

- A. SNMP enumeration
- B. IIS buffer overflow
- C. NetBIOS NULL session
- D. DNS zone transfer

Answer: B

NEW QUESTION # 65
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

NEW QUESTION # 66
Which of the following can be used to perform session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

- A. Session fixation
- B. Cross-site scripting
- C. Session sidejacking
- D. ARP spoofing

Answer: A,B,C

NEW QUESTION # 67
Which of the following statements are true about worms?
Each correct answer represents a complete solution. Choose all that apply.

- A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- B. One feature of worms is keystroke logging.
- C. Worms replicate themselves from one system to another without using a host file.
- D. Worms can exist inside files such as Word or Excel documents.

Answer: A,C,D

Explanation:
Section: Volume A

NEW QUESTION # 68
You discover that your network routers are being flooded with broadcast packets that have the return address of one of the servers on your network. This is resulting in an overwhelming amount of traffic going back to that server and flooding it. What is this called?

- A. IP spoofing

- B. Smurf attack
- C. Syn flood
- D. Blue jacking

Answer: B

Explanation:
Section: Volume B
Explanation

NEW QUESTION # 69
.....

Our company is considerably cautious in the selection of talent and always hires employees with store of specialized knowledge and skills on our GCIH exam questions. All the members of our experts and working staff maintain a high sense of responsibility, which is why there are so many people choose our GCIH Exam Materials and to be our long-term partner. Believe in our GCIH study guide, and you will have a brighter future!

Exam GCIH Tests: https://www.test4sure.com/GCIH-pass4sure-vce.html

- GIAC GCIH Exam Actual Questions | Useful GIAC Exam GCIH Tests: GIAC Certified Incident Handler □ Download [GCIH] for free by simply searching on ➤ www.torrentvce.com □ □Practice GCIH Online
- GCIH Exam Questions Dumps, GIAC Certified Incident Handler VCE Collection □ Search for { GCIH } and download it for free on ➽ www.pdfvce.com □ website □Reliable GCIH Exam Price
- GIAC GCIH Exam Actual Questions | Useful GIAC Exam GCIH Tests: GIAC Certified Incident Handler □ Search for （ GCIH ） on □ www.pdfdumps.com □ immediately to obtain a free download □Actual GCIH Test Answers
- Valid GCIH Vce □ Actual GCIH Test Answers □ Valid GCIH Exam Bootcamp □ { www.pdfvce.com } is best website to obtain 「 GCIH 」 for free download □Exam GCIH Blueprint
- Valid GCIH Exam Format □ New GCIH Dumps Ppt □ Valid GCIH Exam Format □ Open □ www.practicevce.com □ enter 【 GCIH 】 and obtain a free download □Practice GCIH Exams
- High-quality GCIH Exam Actual Questions - Pass GCIH Once - Complete Exam GCIH Tests □ Go to website ➽ www.pdfvce.com □ open and search for □ GCIH □ to download for free □Exam GCIH Simulator Fee
- GCIH Exam Questions Dumps, GIAC Certified Incident Handler VCE Collection □ Search for ⇛ GCIH ⇚ and obtain a free download on 《 www.examcollectionpass.com 》 □Exam GCIH Simulator Fee
- GCIH Exam Questions Dumps, GIAC Certified Incident Handler VCE Collection □ Search for ▸ GCIH ◂ and download it for free immediately on ▸ www.pdfvce.com ◂ □GCIH Reliable Cram Materials
- Valid GCIH Exam Bootcamp □ GCIH Latest Exam Answers □ Exam GCIH Simulator Fee □ Search for ➠ GCIH □ □ and obtain a free download on ⇛ www.prep4away.com ⇚ □GCIH Test Pattern
- Reliable GCIH Exam Price □ Practice GCIH Online □ Exam GCIH Simulator Fee □ Open ➥ www.pdfvce.com □ enter □ GCIH □ and obtain a free download □GCIH Test Pattern
- Training GCIH Materials □ Actual GCIH Test Answers □ Reliable GCIH Exam Price □ Search for ➤ GCIH □ and download it for free immediately on （ www.examcollectionpass.com ） ↕Exam GCIH Simulator Fee
- bbs.t-firefly.com, 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, 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, training.oraclis.co.za, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, leveleservices.com, Disposable vapes

BTW, DOWNLOAD part of Test4Sure GCIH dumps from Cloud Storage: https://drive.google.com/open?id=1zh5YMrGq7P-vLuVZBk2GrdEOSfTf08nk