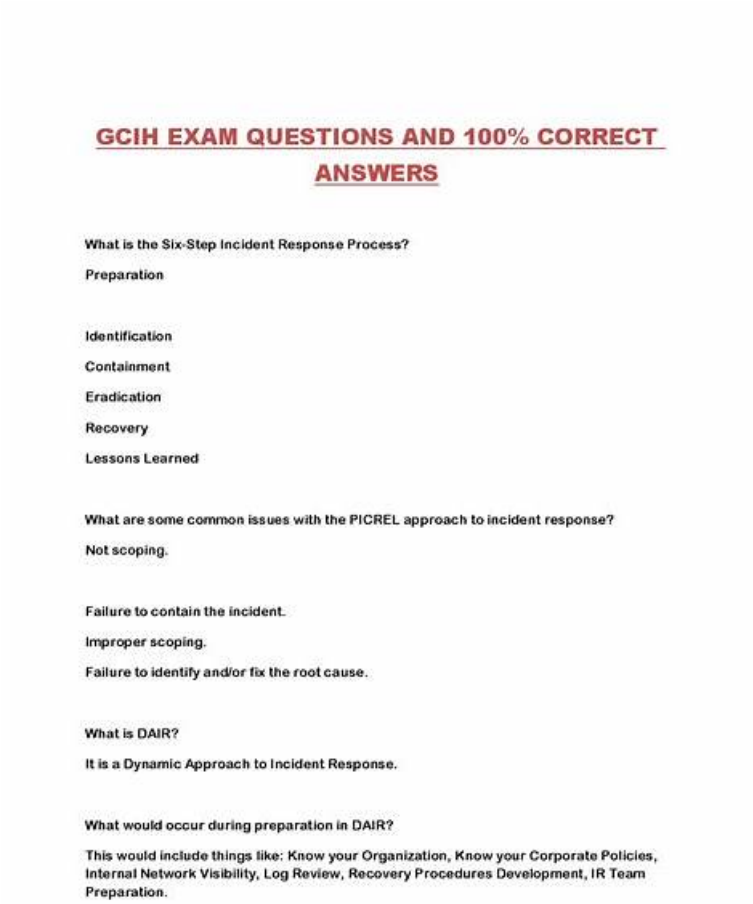
Valid Test GCIH Experience | GCIH Training Questions


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.

BTW, DOWNLOAD part of Dumps4PDF GCIH dumps from Cloud Storage: https://drive.google.com/open?id=13415G8SV2SapyeWkYeocznc0xlnrgQIT

If candidates are going to buy GCIH test dumps, they may consider the problem of the fund safety. If you are thinking the same question like this, our company will eradicate your worries. We choose the international third party to ensure the safety of the fund. The GCIH Test Dumps are effective and conclusive, you just need to use the least time to pass it. I f you choose us, it means you choose the pass.

GIAC GCIH (GIAC Certified Incident Handler) Certification Exam is an excellent way for individuals to demonstrate their expertise in incident handling and advance their careers in cybersecurity. With the right training and preparation, candidates can successfully pass the exam and join the ranks of certified incident handlers around the world.

GIAC GCIH certification exam is a computer-based exam that consists of 150 multiple-choice questions. The time allotted for the exam is four hours. GCIH Exam is designed to test the candidate's knowledge of incident handling, threat intelligence, network security, and forensics. GCIH exam fee is $1,899, and it is available in English language only. GCIH exam can be taken either at a Pearson VUE testing center or online.

>> Valid Test GCIH Experience <<

100% Valid GIAC GCIH Dumps PDF Updated Questions- Dumps4PDF

The GIAC job market has become so competitive and challenging. To stay competitive in the market as an experienced GIAC professional you have to upgrade your skills and knowledge with the GIAC Certified Incident Handler (GCIH) certification exam. With the GIAC GCIH exam dumps you can easily prove your skills and upgrade your knowledge. To do this you just need to enroll

in the GIAC Certified Incident Handler (GCIH) certification exam and put all your efforts to pass this challenging GCIH exam with good scores. However, you should keep in mind that to get success in the GCIH certification exam is not a simple and easy task.

GIAC GCIH certification exam is not easy and requires a lot of preparation and dedication. Candidates must have a deep understanding of the topics covered in the exam and must be able to apply that knowledge in real-world situations. GCIH Exam is designed to test the practical knowledge of the candidate rather than just their theoretical understanding.

GIAC Certified Incident Handler Sample Questions (Q139-Q144):

NEW QUESTION # 139
Which of the following types of malware can an antivirus application disable and destroy?
Each correct answer represents a complete solution. Choose all that apply.

- A. Trojan
- B. Adware
- C. Crimeware
- D. Virus
- E. Rootkit
- F. Worm

Answer: A,D,E,F

NEW QUESTION # 140
Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason. Which of the following mistakes made by Jason helped the Forensic Investigators catch him?

- A. Jason did not perform a vulnerability assessment.
- B. Jason did not perform foot printing.
- C. Jason did not perform covering tracks.
- D. Jason did not perform port scanning.
- E. Jason did not perform OS fingerprinting.

Answer: C

Explanation:
Section: Volume A
Explanation/Reference:

NEW QUESTION # 141
John works as a Penetration Tester in a security service providing firm named you-are-secure Inc. Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:
<script>alert('Hi, John')</script>
After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John." Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

- A. CSRF attack
- B. Replay attack
- C. Buffer overflow attack
- D. XSS attack

Answer: D

NEW QUESTION # 142
Maria works as a professional Ethical Hacker. She is assigned a project to test the security of www.we-are-secure.com. She wants to test a DoS attack on the We-are-secure server. She finds that the firewall of the server is blocking the ICMP messages, but it is not checking the UDP packets. Therefore, she sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the We-are-secure server. Which of the following DoS attacks is Maria using to accomplish her task?

- A. Smurf DoS attack
- B. Ping flood attack
- C. Teardrop attack
- D. Fraggle DoS attack

Answer: D

NEW QUESTION # 143
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

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

Answer: A

NEW QUESTION # 144
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.jyotishadda.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, myportal.utt.edu.tt, www.ted.com, www.stes.tyc.edu.tw, eduderma.info, Disposable vapes

BONUS!!! Download part of Dumps4PDF GCIH dumps for free: https://drive.google.com/open?id=13415G8SV2SapyeWkYeocznc0xlnrgQIT