Useful GCIH - Latest Study GIAC Certified Incident Handler Questions


GCIH (GIAC Certified Incident Handler) 3
Exam Questions And Answers

Server-Side Request Forgery (SSRF) - ANS Allows the threat actor to read the source code of the software/server (EX: CRM software exposed to internet). Gets around logins

Command Injection - ANS allow ability to run arbitrary commands without needing to be logged in.

PICERL - ANS 6 step Incident Response process
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

DIAR - ANS A frame work that is more dynamic for incident response, is the one with a circle in the middle of the line.

Get-CimInstance - ANS CIM is the Common Information Model part of WMI and lets us interrogate detailed information about the windows host. It can tell you the process ID, name, command line details and more.

BONUS!!! Download part of TopExamCollection GCIH dumps for free: https://drive.google.com/open?id=18UN9W_5k3AvOFWRjl9vDN4QWXPIlAliP

TopExamCollection has collected the frequent-tested knowledge into our GCIH practice materials for your reference according to our experts' years of diligent work. So our GCIH exam materials are triumph of their endeavor. By resorting to our GCIH practice materials, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our GCIH training engine, the passing rate is 98-100 percent. So your chance of getting success will be increased greatly by our GCIH exam questions.

GIAC GCIH certification is a valuable asset for professionals in the information security industry, as it demonstrates their expertise and commitment to the field of incident handling and response. It is also a valuable credential for organizations looking to hire security professionals, as it provides assurance that the candidate has the necessary skills and knowledge to effectively respond to security incidents. The GCIH Certification is widely recognized as a benchmark for incident handlers and is highly respected in the information security community.

>> Latest Study GCIH Questions <<

Achieve an Excellent Score in Your GIAC GCIH Exam with TopExamCollection

Our company has worked on the GCIH study material for more than 10 years, and we are also in the leading position in the industry, we are famous for the quality and honesty. The pass rate of our company is also highly known in the field. If you fail to pass it after buying the GCIH Exam Dumps, money back will be guaranteed for your lost or you will get another free GCIH exam dumps. Our company will ensure the fundamental interests of our customers.

GIAC Certified Incident Handler Sample Questions (Q224-Q229):

NEW QUESTION # 224
Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:

Which of the following actions will this command take?

- A. Dumps the SAM password file to pwd.txt
- B. Dumps the Active Directory password hashes to pwd.txt
- C. The password history file is transferred to pwd.txt
- D. Dumps the SAM password hashes to pwd.txt

Answer: D

Explanation:
Section: Volume B

NEW QUESTION # 225
You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the wearesecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.
What may be the reason?

- A. The zombie computer is the system interacting with some other system besides your computer.
- B. The firewall is blocking the scanning process.
- C. Hping does not perform idle scanning.
- D. The zombie computer is not connected to the we-are-secure.com Web server.

Answer: A

NEW QUESTION # 226
Which of the following is a version of netcat with integrated transport encryption capabilities?

- A. Nikto
- B. Cryptcat
- C. Socat
- D. Encat

Answer: B

Explanation:
Section: Volume B

NEW QUESTION # 227
Which of the following protocol loggers is used to detect ping sweep?

- A. ippl
- B. lppi
- C. pitl
- D. dpsl

Answer: A

NEW QUESTION # 228
Which of the following provides packet-level encryption between hosts in a LAN?

- A. PPTP
- B. PFS
- C. IPsec
- D. Tunneling protocol

Answer: C

NEW QUESTION # 229
.....

One thing has to admit, more and more certifications you own, it may bring you more opportunities to obtain better job, earn more salary. This is the reason that we need to recognize the importance of getting the test GCIH certifications. More qualified certification for our future employment has the effect to be reckoned with, only to have enough qualification certifications to prove their ability, can we win over rivals in the social competition. Therefore, the GCIH Guide Torrent can help users pass the qualifying examinations that they are required to participate in faster and more efficiently.

- academia.thisismusic.ec, daotao.wisebusiness.edu.vn, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ncon.edu.sa, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

2025 Latest TopExamCollection GCIH PDF Dumps and GCIH Exam Engine Free Share: https://drive.google.com/open?id=18UN9W_5k3AvOFWRjl9vDN4QWXPIlAliP