

Free GCIH Exam Questions Updates By VCE4Dumps



BTW, DOWNLOAD part of VCE4Dumps GCIH dumps from Cloud Storage: https://drive.google.com/open?id=1HrkfKQUd0BaP_8wkt0cjXHHp8cdaJ8WR

Our experts are researchers who have been engaged in professional qualification GCIH exams for many years and they have a keen sense of smell in the direction of the examination. Therefore, with our GCIH study materials, you can easily find the key content of the exam and review it in a targeted manner so that you can successfully pass the GCIH Exam. We have free demos of the GCIH exam materials that you can try before payment.

If you have the certification the exam, you can enter a better company, and your salary will also be doubled. GCIH training materials can help you pass the exam and obtain corresponding certification successfully. GCIH exam materials are edited by experienced experts, and they possess the professional knowledge for the exam, and you can use it with ease. We have online and offline chat service, they possess the professional knowledge for the exam, and you can consult them any questions that bothers you. We offer you free update for one year for GCIH Exam Dumps, and our system will send the latest version to you automatically.

>> Test GCIH Dumps Free <<

GCIH Latest Exam Cram, GCIH New Dumps Sheet

We have three formats of study materials for your leaning as convenient as possible. Our GCIHquestion torrent can simulate the real operation test environment to help you pass this test. You just need to choose suitable version of our GCIH guide question you want, fill right email then pay by credit card. It only needs several minutes later that you will receive products via email. After your purchase, 7*24*365 Day Online Intimate Service of GCIH question torrent is waiting for you. We believe that you don't encounter failures anytime you want to learn our GCIH guide torrent.

GIAC Certified Incident Handler Sample Questions (Q143-Q148):

NEW QUESTION # 143

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it with chess.exe. Which of the following tools are required in such a scenario?

Each correct answer represents a part of the solution. Choose three.

- A. Chess.exe
- B. Yet Another Binder
- C. NetBus
- D. Absinthe

Answer: A,B,C

NEW QUESTION # 144

Which of the following steps can be taken as countermeasures against sniffer attacks?
Each correct answer represents a complete solution. Choose all that apply.

- A. Use encrypted protocols for all communications.
- B. Reduce the range of the network to avoid attacks into wireless networks.
- C. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
- D. Use tools such as StackGuard and Immunix System to avoid attacks.

Answer: A,B,C

Explanation:

Section: Volume C

NEW QUESTION # 145

Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.

- A. tcp wrapper protects a Linux server from IP address spoofing.
- B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
- C. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
- D. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.

Answer: B,C,D

NEW QUESTION # 146

Which of the following commands can be used for port scanning?

- A. nc -t
- B. nc -w
- C. nc -g
- D. nc -z

Answer: D

Explanation:

Section: Volume A

NEW QUESTION # 147

John works as an Ethical Hacker for PassGuide Inc. He wants to find out the ports that are open in PassGuide's server using a port scanner. However, he does not want to establish a full TCP connection.

Which of the following scanning techniques will he use to accomplish this task?

- A. TCP SYN
- B. TCP FIN
- C. TCP SYN/ACK
- D. Xmas tree

Answer: A

NEW QUESTION # 148

.....

We try our best to provide the most efficient and intuitive learning methods to the learners and help them learn efficiently. Our GCIH study materials provide the instances, simulation and diagrams to the clients so as to they can understand them intuitively. Based on

