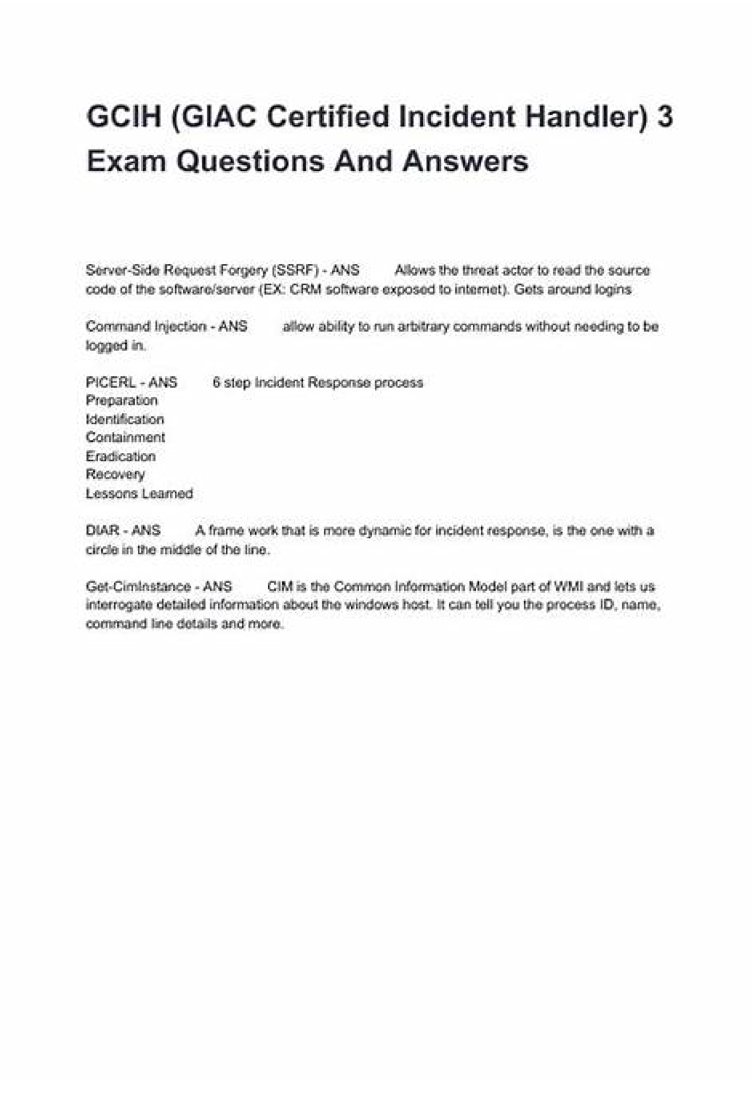
Exam GIAC GCIH Vce | GCIH Relevant Answers



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.

Possessing GIAC certification will be a standard to test IT workers' qualifications. GCIH reliable exam preparation will be a key to a certification. If you want to apply for a senior management position, one certification will be an outstanding advantage. I advise people pass exams and get certifications with GCIH Reliable Exam Preparation as soon as possible so that you will be one step ahead while facing better job opportunities.

GIAC GCIH (GIAC Certified Incident Handler) Exam is a professional certification exam that validates the skills and knowledge of individuals in incident handling and response. GCIH exam is designed to test the ability of the candidates to detect, respond to, and resolve security incidents effectively. GIAC Certified Incident Handler certification is globally recognized and is highly respected in the cybersecurity industry. It is an essential credential for professionals who are looking to advance their careers in incident response and handling.

>> Exam GIAC GCIH Vce <<

GCIH Relevant Answers - GCIH Brain Dump Free

We have professional technicians to examine the website at times, so that we can offer you a clean and safe shopping environment for you if you choose the GCIH study materials of us. Besides, GCIH exam dumps contain both questions and answers, and you can have a quickly check after practicing, and so that you can have a better understanding of your training mastery. We have free update for one year, so that you can know the latest information about the GCIH Study Materials, and you can change your learning strategies in accordance with the new changes.

GIAC GCIH (GIAC Certified Incident Handler) exam is a highly respected certification that validates a candidate's ability to detect, respond to, and resolve computer security incidents. GIAC Certified Incident Handler certification is designed for professionals who have some experience in the field of computer security and want to develop their skills further. The GCIH certification is globally recognized and is highly regarded by employers as a benchmark for incident handling skills.

To prepare for the GIAC GCIH Certification Exam, candidates can enroll in training courses offered by GIAC or other training providers. These training courses cover the topics and skills required for the certification exam. Candidates can also use study materials such as books, practice exams, and online resources to prepare for the exam. It is recommended that candidates have at least one year of experience in incident handling and response before taking the exam.

GIAC Certified Incident Handler Sample Questions (Q84-Q89):

NEW QUESTION # 84
Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

- A. Win32/Conflicker
- B. WMA/TrojanDownloader.GetCodec
- C. Win32/Agent
- D. Win32/PSW.OnLineGames

Answer: A

NEW QUESTION # 85
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. Reduce the range of the network to avoid attacks into wireless networks.
- B. Use tools such as StackGuard and Immunix System to avoid attacks.
- C. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
- D. Use encrypted protocols for all communications.

Answer: A,C,D

NEW QUESTION # 86
Which of the following types of attacks slows down or stops a server by overloading it with requests?

- A. Vulnerability attack
- B. Network attack
- C. Impersonation attack
- D. DoS attack

Answer: D

Explanation:
Section: Volume C

NEW QUESTION # 87
Which of the following can be used as a Trojan vector to infect an information system?
Each correct answer represents a complete solution. Choose all that apply.

- A. Spywares and adware
- B. ActiveX controls, VBScript, and Java scripts
- C. Any fake executable
- D. NetBIOS remote installation

Answer: A,B,C,D

NEW QUESTION # 88

Which of the following actions is performed by the netcat command given below?
nc 55555 < /etc/passwd

- A. It grabs the /etc/passwd file when connected to UDP port 55555.
- B. It fills the incoming connections to /etc/passwd file.
- C. It changes the /etc/passwd file when connected to the UDP port 55555.
- D. It resets the /etc/passwd file to the UDP port 55555.

Answer: A

Explanation:
Section: Volume B
Explanation

NEW QUESTION # 89

......

GCIH Relevant Answers: https://www.vceprep.com/GCIH-latest-vce-prep.html