# GCIH Übungsfragen: GIAC Certified Incident Handler & GCIH Dateien Prüfungsunterlagen


P.S. Kostenlose und neue GCIH Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar: https://drive.google.com/open?id=1WLS6yqFfo9zd_eMrF7eEQmFZDjHKDR6M

Sich für IT-Branche interessierend Sie bereiten sich jetzt auf die wichtige GIAC GCIH Prüfung? Lassen wir DeutschPrüfung Ihnen helfen! Was wir Ihnen garantieren ist, dass Sie nicht nur die GIAC GCIH Prüfung bestehen können, sondern auch Sie der leichte Vorbereitungsprozess und guter Kundendienst genießen.

Wenn Sie die Fragen und Antworten zur GIAC GCIH Prüfung von DeutschPrüfung kaufen, können Sie ihre wichtige Vorbereitung im leben treffen und die Fragenkataloge von guter Qualität bekommen. Kaufen Sie unsere Produkte heute, dann öffnen Sie sich eine Tür, um eine bessere Zukunft zu haben. Sie können auch mit weniger Mühe den großen Erfolg erzielen.

**>> GCIH Trainingsunterlagen <<**

## GCIH Online Test, GCIH Prüfung

Die Fragenkataloge zur GIAC GCIH Prüfung von DeutschPrüfung sind die besten im Vergleich zu den anderen Materialien. Wenn Sie Fragenkataloge suchen, wählen Sie doch die Fragenkataloge zur GIAC GCIH Prüfung von DeutschPrüfung. Und Sie würden viel davonprofitieren. Sonst würden Sie bereuen.

Die GIAC GCIH -Zertifizierung ist in der Informationssicherheitsbranche hoch angesehen und von Arbeitgebern weltweit anerkannt. Das Halten dieser Zertifizierung zeigt das Wissen und die Fähigkeiten des Kandidaten in der Behandlung und Reaktion des Vorfalls, was eine begehrte Fähigkeit in der Cybersicherheitsbranche darstellt. Einige der beruflichen Rollen, die von dieser Zertifizierung profitieren können, umfassen Analysten, Sicherheitsanalysten, Netzwerksicherheitsingenieure und Cybersicherheitsberater.

## GIAC Certified Incident Handler GCIH Prüfungsfragen mit Lösungen (Q205-Q210):

**205. Frage**
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing

department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?

- A. Recovery
- B. Eradication
- C. Containment
- D. Identification

**Antwort: C**

Begründung:
Section: Volume C

**206. Frage**
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

- A. Man-in-the-middle
- B. ARP spoofing
- C. Port scanning
- D. Session hijacking

**Antwort: B**

Begründung:
Section: Volume C

**207. Frage**
Which of the following tools can be used to perform brute force attack on a remote database?
Each correct answer represents a complete solution. Choose all that apply.

- A. FindSA
- B. SQLDict
- C. SQLBF
- D. nmap

**Antwort: A,B,C**

Begründung:
Section: Volume A

**208. Frage**
Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.
After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for (( i = 0;i<11;i++ )); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done Which of the following actions does Adam want to perform by the above command?

- A. Wiping the contents of the hard disk with zeros.
- B. Infecting the hard disk with polymorphic virus strings.
- C. Making a bit stream copy of the entire hard disk for later download.
- D. Deleting all log files present on the system.

**Antwort: A**

**209. Frage**
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 to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:
C:\WINDOWS>netstat -an | find "UDP" UDP IP_Address:31337 *:*
Now you check the following registry address:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
In the above address, you notice a 'default' key in the 'Name' field having " .exe" value in the corresponding 'Data' field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

- A. Back Orifice
- B. Tini
- C. Donald Dick
- D. Qaz

**Antwort: A**

**210. Frage**
.....

Unsere GIAC GCIH Prüfungsunterlage (GIAC Certified Incident Handler) enthalten alle echten, originalen und richtigen Fragen und Antworten. Die Abdeckungsrate unserer GIAC GCIH Unterlagen (Fragen und Antworten) (GIAC Certified Incident Handler) ist normalerweise mehr als 98%.



P.S. Kostenlose und neue GCIH Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar: https://drive.google.com/open?id=1WLS6yqFfo9zd_eMrF7eEQmFZDjHKDR6M