Accurate GIAC GCIH Study Material | GCIH Vce Free

GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[illegible]

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

What's more, part of that Pass4Test GCIH dumps now are free: https://drive.google.com/open?id=1HzvikjIHX2NmAdOqi2LkBu-b1jsgPD1F

Pass4Test offers GIAC GCIH practice tests for the evaluation of GIAC Certified Incident Handler exam preparation. GIAC GCIH practice test is compatible with all operating systems, including iOS, Mac, and Windows. Because this is a browser-based GCIH Practice Test, there is no need for installation.

GIAC GCIH (GIAC Certified Incident Handler) certification exam is a highly sought-after certification for professionals who are involved in the incident response and handling process. GIAC Certified Incident Handler certification is specifically designed for individuals who are responsible for detecting, responding to, and resolving security incidents within their organization. GCIH exam is created by the Global Information Assurance Certification (GIAC) organization, which is known for providing the highest level of certification in the field of cybersecurity.

The GCIH certification program is offered by the Global Information Assurance Certification (GIAC), which is one of the leading organizations in the field of information security. The GCIH Exam is designed to test the knowledge of candidates in various areas of incident handling, such as incident response and management, network security, malware analysis, and digital forensics. GIAC Certified Incident Handler certification program is recognized by companies and organizations worldwide, and GCIH certified professionals are in high demand in the information security industry.

>> Accurate GIAC GCIH Study Material <<

Download Latest Accurate GCIH Study Material and Pass GCIH Exam

The Pass4Test team regularly revises the GIAC Certified Incident Handler (GCIH) PDF version to add new questions and update

GIACmation, so candidates are always up-to-date. We provide candidates with comprehensive GIAC Certified Incident Handler (GCIH) exam questions with up to 1 year of free updates. If you are doubtful, feel free to download a free demo of Pass4Test GIAC Certified Incident Handler (GCIH) PDF dumps, desktop practice exam software, and web-based GIAC Certified Incident Handler (GCIH) practice exam. Don't wait. Purchase GIAC Certified Incident Handler (GCIH) exam dumps at an affordable price and start preparing for the updated GIAC GCIH certification exam today.

GIAC Certified Incident Handler Sample Questions (Q90-Q95):

NEW QUESTION # 90
John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.
Which of the following worms has attacked the computer?

- A. Code red
- B. Nimda
- C. Ramen
- D. LoveLetter

Answer: C

NEW QUESTION # 91
You run the following PHP script:
<?php $name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]); ?>
What is the use of the mysql_real_escape_string() function in the above script.
Each correct answer represents a complete solution. Choose all that apply.

- A. It can be used to mitigate a cross site scripting attack.
- B. It can be used as a countermeasure against a SQL injection attack.
- C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".
- D. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

Answer: B,D

Explanation:
Section: Volume C

NEW QUESTION # 92
Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property.
The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.
The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.
Which of the following actions can Adam perform to prevent such attacks from occurring in future?

- A. Apply different security policy to make passwords of employees more complex
- B. Allow VPN access but replace the standard authentication with biometric authentication
- C. Disable VPN access to all employees of the company from home machines
- D. Replace the VPN access with dial-up modem access to the company's network

Answer: C

NEW QUESTION # 93

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

```
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958
ms 13.416 ms 3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1) 16.743 ms
16.207 ms 4 ip68-100-0-137.
nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms 20.938 ms 5 68.1.1.4
(68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7 unknown.Level3.net (209.247.9.173) 14.227
ms 17.553 ms 15.415 ms "PassGuide" - 8 so-0-1-0.bbr1.
NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so-7-0-0.gar1. NewYork1.Level3.
net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms 10 so-4-0-0.edge1.NewYork1.Level3.
net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3- oc48.NewYork1.Level3.net (209.244.160.12) 21.411 ms
19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78)
21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms
23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms
33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms
49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.
NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6- 0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms
50.280 ms 53.647 ms 18 PassGuidegw1. customer.alter.net (65.195.239.14)
51.921 ms 51.571 ms 56.855 ms 19 www.PassGuide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms
20 www.PassGuide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
```

Which of the following is the most like cause of this issue?

- A. Intrusion Detection System
- B. An application firewall
- C. A stateful inspection firewall
- D. Network Intrusion system

Answer: C

NEW QUESTION # 94

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

- A. Netstat
- B. Tripwire
- C. SubSeven
- D. Fport

Answer: D

Explanation:
Section: Volume A
Explanation/Reference:

NEW QUESTION # 95

......

GCIH Vce Free: https://www.pass4test.com/GCIH.html

- Free PDF GIAC - Unparalleled Accurate GCIH Study Material □ Open ✔ www.practicevce.com □✔□ and search for ➠ GCIH □ to download exam materials for free □GCIH Passed
- Free PDF Quiz GCIH - Reliable Accurate GIAC Certified Incident Handler Study Material □ Immediately open ➽ www.pdfvce.com □ and search for □ GCIH □ to obtain a free download □Valid GCIH Exam Experience
- Exam GCIH Tutorial ⤵ GCIH Cert Guide □ GCIH Valid Test Format □ Open □ www.troytecdumps.com □ enter □ GCIH □ and obtain a free download □GCIH Valid Exam Blueprint
- Latest GCIH - Accurate GIAC Certified Incident Handler Study Material □ Download □ GCIH □ for free by simply entering ➥ www.pdfvce.com □ website !!GCIH Valid Test Format
- Marvelous Accurate GCIH Study Material - Guaranteed GIAC GCIH Exam Success with High Pass-Rate GCIH Vce Free □ Search for 【 GCIH 】 and easily obtain a free download on ➡ www.dumpsmaterials.com □□□ □Latest GCIH Test Practice
- GCIH Valid Exam Blueprint □ GCIH Pass4sure Exam Prep □ Latest GCIH Test Practice □ Download （ GCIH ） for free by simply entering （ www.pdfvce.com ） website □GCIH Valid Test Format
- Free PDF Quiz GCIH - Reliable Accurate GIAC Certified Incident Handler Study Material □ Simply search for “ GCIH ” for free download on [www.vce4dumps.com] □GCIH Learning Engine
- Pdfvce GIAC GCIH Dumps PDF Preparation Material is Available □ Search for ✔ GCIH □✔□ and download it for free on ➥ www.pdfvce.com □ website □GCIH Reliable Test Sample
- Latest GCIH Test Practice □ Exam GCIH Tutorial □ GCIH Dump File ➾ Open ⇛ www.pass4test.com ⇚ and search for [GCIH] to download exam materials for free □GCIH Reliable Test Sample
- Valid GCIH Exam Experience □ GCIH Valid Exam Blueprint □ Latest GCIH Test Practice □ Download “ GCIH ” for free by simply searching on { www.pdfvce.com } □GCIH Reliable Test Sample
- Latest GCIH - Accurate GIAC Certified Incident Handler Study Material □ ⇛ www.prep4away.com ⇚ is best website to obtain 《 GCIH 》 for free download □GCIH Pass4sure Exam Prep
- iachm.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, barisbarasho.com, 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

P.S. Free 2026 GIAC GCIH dumps are available on Google Drive shared by Pass4Test: https://drive.google.com/open?id=1HzvikjIHX2NmAdOqi2LkBu-b1jsgPD1F