

Examcollection

<http://www.ipass4sure.com/examcollection.htm>



<http://www.ipass4sure.com>

GCIH

GIAC

Certified Incident Handler

<http://www.ipass4sure.com/exams.asp?examcode=GCIH>

The GCIH practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The GCIH Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The GCIH exam is very challenging, but with our GCIH questions and answers practice exam, you can feel confident in obtaining your success on the GCIH exam on your FIRST TRY!

GIAC GCIH Exam Features

- Detailed questions and answers for GCIH exam
- Try a demo before buying any GIAC exam
- GCIH questions and answers, updated regularly
- Verified GCIH answers by Experts and bear almost 100% accuracy
- GCIH tested and verified before publishing
- GCIH examcollection vce questions with exhibits
- GCIH same questions as real exam with multiple choice options

Acquiring GIAC certifications are becoming a huge task in the field of I.T. More over these exams like GCIH exam are now continuously updating and accepting this challenge is itself a task. This GCIH test is an important part of GIAC certifications. We have the resources to prepare you for this. The GCIH exam is essential and core part of GIAC certifications and once you clear the exam you will be able to solve the real life problems yourself. Want to take advantage of the Real GCIH Test and save time and money while developing your skills to pass your GIAC GCIH Exam? Let us help you climb that ladder of success and pass your GCIH now!

DEMO EXAM

For Full Version visit

<http://www.ipass4sure.com/allexams.asp>

Exam Name:	GIAC Certified Incident Handler		
Exam Type:	GIAC	Exam Code:	GCIH
Certification:	GIAC Information Security	Total Questions:	328

Question: 1

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions: Remove the network cable wires. Isolate the system on a separate VLAN Use a firewall or access lists to prevent communication into or out of the system. Change DNS entries to direct traffic away from compromised system which of the following steps of the incident handling process includes the above actions?

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

Answer: B

Question: 2

Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd. Which of the following is the mostly likely the cause of the problem?

- A. Computer is infected with the stealth kernel level rootkit.
- B. Computer is infected with stealth virus.
- C. Computer is infected with the Stealth Trojan Virus.
- D. Computer is infected with the Self-Replication Worm.

Answer: A

Question: 3

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

- A. Denial of Service attack
- B. Replay attack
- C. Teardrop attack
- D. Land attack

Answer: A

Question: 4

Which of the following types of attack can guess a hashed password?

- A. Brute force attack
- B. Evasion attack
- C. Denial of Service attack
- D. Teardrop attack

Answer: A

Exam Name:	GIAC Certified Incident Handler		
Exam Type:	GIAC	Exam Code:	GCIH
Certification:	GIAC Information Security	Total Questions:	328

Question: 5

In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536bytes to the target system?

- A. Ping of death
- B. Jolt
- C. Fraggle
- D. Teardrop

Answer: A

Question: 6

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop. Which of the following attacks has been occurred on the wireless network of Adam?

- A. NAT spoofing
- B. DNS cache poisoning
- C. MAC spoofing
- D. ARP spoofing

Answer: C

Question: 7

Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

- A. Demon dialing
- B. Warkitting
- C. War driving
- D. Wardialing

Answer: D

Question: 8

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

- A. Gathering private and public IP addresses
- B. Collecting employees information
- C. Banner grabbing
- D. Performing Neotracerouting

Answer: D

Question: 9

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

Exam Name:	GIAC Certified Incident Handler		
Exam Type:	GIAC	Exam Code:	GCIH
Certification:	GIAC Information Security	Total Questions:	328

- A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
- 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 allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
- D. tcp wrapper protects a Linux server from IP address spoofing.

Answer: A,B,C

Question: 10

Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

- A. Evasion attack
- B. Denial-of-Service (DoS) attack
- C. Ping of death attack
- D. Buffer overflow attack

Answer: D

Question: 11

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

- A. IIS buffer overflow
- B. NetBIOS NULL session
- C. SNMP enumeration
- D. DNS zone transfer

Answer: A

Question: 12

Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?

- A. Non persistent
- B. Document Object Model (DOM)
- C. SAX
- D. Persistent

Answer: D

Question: 13

Which of the following applications is an example of a data-sending Trojan?

- A. SubSeven
- B. Senna Spy Generator
- C. Firekiller 2000
- D. eBlaster



Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of **Professional & Certified Experts** available via support.
- Free **90 days** updates to match real exam scenarios.
- **Instant Download Access!** No Setup required.
- Price as low as **\$19**, which is 80% more **cost effective** than others.
- **Verified answers** researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (**Android, iPhone, iPod, iPad**)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- **Guaranteed Success.**
- **Fast**, helpful support **24x7**.



View list of All certification exams offered;
<http://www.ipass4sure.com/all exams.asp>

View list of All Study Guides (SG);
<http://www.ipass4sure.com/study-guides.asp>

View list of All Audio Exams (AE);
<http://www.ipass4sure.com/audio-exams.asp>

Download Any Certification Exam DEMO.
<http://www.ipass4sure.com/samples.asp>

To purchase Full version of exam click below;
<http://www.ipass4sure.com/all exams.asp>

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list [Here](#)

