GCIA

GIAC

Certified Intrusion Analyst Practice Test

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=GCIA

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your GCIA exam in first attempt, but also you can get a high score to acquire GIAC certification.

If you use pass4sureofficial GCIA Certification questions and answers, you will experience actual GCIA exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our GIAC exam prep covers over 95% of the questions and answers that may be appeared in your GCIA exam. Every point from pass4sure GCIA PDF, GCIA review will help you take GIAC GCIA exam much easier and become GIAC certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial GIAC GCIA course:

** Up-to-Date GIAC GCIA questions taken from the real exam.*
** 100% correct GIAC GCIA answers you simply can't find in other GCIA courses.*
** All of our tests are easy to download. Your file will be saved as a GCIA PDF.*
** GIAC GCIA brain dump free content featuring the real GCIA test questions.*

GIAC GCIA certification exam is of core importance both in your Professional life and GIAC certification path. With GIAC certification you can get a good job easily in the market and get on your path for success. Professionals who passed GIAC GCIA exam training are an absolute favorite in the industry. You will pass GIAC GCIA certification test and career opportunities will be open for you.

Exam Name:	GCIA – GIAC Certified Intrusion Analyst Practice Test		
Exam Type:	GIAC	Exam Code:	GCIA
Certification:	GIAC Information Security	Total Questions:	508

Question: 1
Andrew works as a System Administrator for NetPerfect Inc. All client computers on the network run on Mac OS X. The Sales Manager of the company complains that his MacBook is not able to boot. Andrew wants to check the booting process. He suspects that an error persists in the bootloader of Mac OS X. Which of the following is the default bootloader on Mac OS X that he should use to resolve the issue?

A. LILO
B. BootX
C. NT Loader
D. GRUB

Answer: B

Question: 2
Sasha wants to add an entry to your DNS database for your mail server. Which of the following types of resource records will she use to accomplish this?

A. ANAME
B. SOA
C. MX
D. CNAME

Answer: C

Question: 3
John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Dictionary attack
B. Hybrid attack
C. Brute Force attack
D. Rule based attack

Answer: A,B,C

Question: 4
Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Tunneling proxy server
B. Reverse proxy server
C. Anonymous proxy server
D. Intercepting proxy server

Answer: D

Question: 5
Which of the following statements about a *host-based intrusion prevention system (HIPS)* are true? Each correct answer represents a complete solution. Choose two.

A. It can detect events scattered over the network.
B. It can handle encrypted and unencrypted traffic equally.
C. It cannot detect events scattered over the network.
D. It is a technique that allows multiple computers to share one or more IP addresses.

Answer: B,C

Question: 6
Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed? Each correct answer represents a complete solution. Choose all that apply.

A. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.
B. Attacker can gain access to the Web server in a DMZ and exploit the database.
C. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.
D. Attacker can exploit any protocol used to go into the internal network or intranet of the company

Answer: A,B,D

Question: 7
Which of the following is known as a message digest?

A. Hash function
B. Hashing algorithm
C. Spider
D. Message authentication code

Answer: A

Question: 8
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. Document Object Model (DOM)
B. Non persistent
C. SAX
D. Persistent

Answer: D

Question: 9
Peter works as a Technical Representative in a *CSIRT* for Secure net Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, interne t Traces.
B. Volatile data, file slack, file system, registry, memory dumps, system state backup, interne t Traces.

C. Volatile data file slack, internet traces, registry, memory dumps, system state backup, file System.
D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory Dumps.

Answer: B

Question: 10
You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Enable verbose logging on the firewall
B. Install a network-based IDS
C. Install a DMZ firewall
D. Install a host-based IDS

Answer: B

Question: 11
Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task? Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files
B. EDB and STM database files
C. Temporary files
D. cookie files

Answer: A,B,C

Question: 12
This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows: It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. It is commonly used for the following purposes:

A. War driving
B. Detecting unauthorized access points
C. Detecting causes of interference on a WLAN
D. WEP ICV error tracking
E. Making Graphs and Alarms on 802.11 Data, including Signal Strength

Answer: D

Question: 13
SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol? Each correct answer represents a complete solution. Choose all that apply.

A. Blowfish
B. IDEA
C. DES
D. RC4

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.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	SNIA