

# **Examcollection**

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



<http://www.ipass4sure.com>

# GCFA

## GIAC

*GIAC Certified Forensics Analyst*

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

The GCFA 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 GCFA Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The GCFA exam is very challenging, but with our GCFA questions and answers practice exam, you can feel confident in obtaining your success on the GCFA exam on your FIRST TRY!

### GIAC GCFA Exam Features

- Detailed questions and answers for GCFA exam
- Try a demo before buying any GIAC exam
- GCFA questions and answers, updated regularly
- Verified GCFA answers by Experts and bear almost 100% accuracy
- GCFA tested and verified before publishing
- GCFA examcollection vce questions with exhibits
- GCFA 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 GCFA exam are now continuously updating and accepting this challenge is itself a task. This GCFA test is an important part of GIAC certifications. We have the resources to prepare you for this. The GCFA 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 GCFA Test and save time and money while developing your skills to pass your GIAC GCFA Exam? Let us help you climb that ladder of success and pass your GCFA now!

# **DEMO EXAM**

For Full Version visit

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

**QUESTION: 1**

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

**Answer: C**

**QUESTION: 2**

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

- A. Trademark law
- B. Cyber law
- C. Copyright law
- D. Espionage law

**Answer: A**

**QUESTION: 3**

You work as a Network Administrator for Perfect Solutions Inc. You install Windows 98 on a computer. By default, which of the following folders does Windows 98 setup use to keep the registry tools?

- A. \$SYSTEMROOT\$REGISTRY

- B. \$SYSTEMROOT\$WINDOWS
- C. \$SYSTEMROOT\$WINDOWSREGISTRY
- D. \$SYSTEMROOT\$WINDOWSSYSTEM32

**Answer:** B

**QUESTION:** 4

Which of the following tools can be used to perform tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing?

- A. John the Ripper
- B. L0phtcrack
- C. Obiwan
- D. Cain

**Answer:** D

**QUESTION:** 5

Which of the following type of file systems is not supported by Linux kernel?

- A. vFAT
- B. NTFS
- C. HFS
- D. FAT32

**Answer:** D

**QUESTION:** 6

Which of the following modules of OS X kernel (XNU) provides the primary system program interface?

- A. BSD
- B. LIBKERN
- C. I/O Toolkit
- D. Mach

**Answer: A**

**QUESTION: 7**

You work as a Network Administrator for Blue Bell Inc. You want to install Windows XP Professional on your computer, which already has Windows Me installed. You want to configure your computer to dual boot between Windows Me and Windows XP Professional. You have a single 40GB hard disk. Which of the following file systems will you choose to dual-boot between the two operating systems?

- A. NTFS
- B. FAT32
- C. CDFS
- D. FAT

**Answer: B**

**QUESTION: 8**

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He receives the following e-mail:

Hi!e Disney fans,  
And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an email tracking program that tracks everyone to whom this message is forwarded to. It does this through a unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 11,000 people, 1,380 of the people on the list will receive \$5,000, and the rest will receive a free trip for two to Disney World for one week, being the summer of 1999 at our expense. Enjoy.  
Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 11,000 people.  
Your friends,  
Walt Disney Jr., Disney, Bill Gates  
& The Microsoft Development Team.

The e-mail that John has received is an example of \_\_\_\_\_.

- A. Virus hoaxes
- B. Spambots
- C. Social engineering attacks
- D. Chain letters

**Answer: D**

**QUESTION: 9**

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

- A. Wiretap Act
- B. Computer Fraud and Abuse Act
- C. Economic Espionage Act of 1996
- D. Electronic Communications Privacy Act of 1986

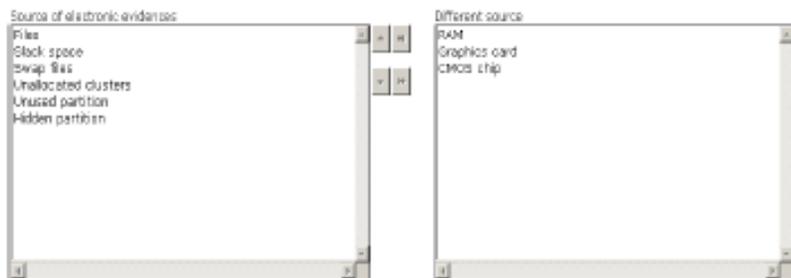
**Answer:** D

**QUESTION:** 10

Choose the appropriate source of electronic evidences.



**Answer:** A



**QUESTION:** 11

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

- A. Solaris
- B. Red Hat
- C. Knoppix
- D. Windows

**Answer:** D

**QUESTION:** 12

Which of the following encryption methods uses AES technology?

- A. Dynamic WEP
- B. Static WEP
- C. TKIP
- D. CCMP

**Answer:** D

**QUESTION:** 13

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e-mailing company's secrets to an opponent?

- A. Electronic surveillance
- B. Civil investigation
- C. Physical surveillance
- D. Criminal investigation

**Answer:** A

**QUESTION:** 14

Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?



## 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](#)

