

# **Examcollection**

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



<http://www.ipass4sure.com>

# GPEN

## GIAC

*Certified Penetration Tester*

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

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

### GIAC GPEN Exam Features

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

# **DEMO EXAM**

For Full Version visit

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

<b>Exam Name:</b>	<b>GIAC Certified Penetration Tester</b>		
<b>Exam Type:</b>	<b>GIAC</b>	<b>Exam Code:</b>	<b>GPEN</b>
<b>Certification:</b>	<b>GIAC Information Security</b>	<b>Total Questions:</b>	<b>384</b>

**Question: 1**

You execute the following netcat command:

```
c:\target\nc -l -p 53 -d -e cmd.exe
```

What action do you want to perform by issuing the above command?

- A. Capture data on port 53 and performing banner grabbing.
- B. Listen the incoming traffic on port 53 and execute the remote shell.
- C. Listen the incoming data and performing port scanning.
- D. Capture data on port 53 and delete the remote shell.

**Answer: B**

**Question: 2**

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. Windows
- D. Knoppix

**Answer: C**

**Question: 3**

You work as a professional Ethical Hacker. You are assigned a project to perform blackhat testing on [www.we-are-secure.com](http://www.we-are-secure.com). You visit the office of [we-are-secure.com](http://www.we-are-secure.com) as an air-condition mechanic. You claim that someone from the office called you saying that there is some fault in the air-conditioner of the server room. After some inquiries/arguments, the Security Administrator allows you to repair the air-conditioner of the server room.

When you get into the room, you found the server is Linux-based. You press the reboot button of the server after inserting knoppix Live CD in the CD drive of the server. Now, the server promptly boots backup into Knoppix. You mount the root partition of the server after replacing the root password in the `/etc/shadow` file with a known password hash and salt. Further, you copy the netcat tool on the server and install its startup files to create a reverse tunnel and move a shell to a remote server whenever the server is restarted. You simply restart the server, pull out the Knoppix Live CD from the server, and inform that the air-conditioner is working properly.

After completing this attack process, you create a security auditing report in which you mention various threats such as social engineering threat, boot from Live CD, etc. and suggest the countermeasures to stop booting from the external media and retrieving sensitive data. Which of the following steps have you suggested to stop booting from the external media and retrieving sensitive data with regard to the above scenario?

Each correct answer represents a complete solution. Choose two.

- A. Encrypting disk partitions
- B. Using password protected hard drives
- C. Placing BIOS password
- D. Setting only the root level access for sensitive data

**Answer: A,B**

**Question: 4**

Which of the following statements are true about KisMAC?

Exam Name:	GIAC Certified Penetration Tester		
Exam Type:	GIAC	Exam Code:	GPEN
Certification:	GIAC Information Security	Total Questions:	384

- A. Data generated by KisMAC can also be saved in pcap format.
- B. It cracks WEP and WPA keys by Rainbow attack or by dictionary attack.
- C. It scans for networks passively on supported cards.
- D. It is a wireless network discovery tool for Mac OS X.

**Answer: A,C,D**

**Question: 5**

A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department. What security risk does this present?

- A. An unauthorized WAP is one way for hackers to get into a network.
- B. It is likely to increase network traffic and slow down network performance.
- C. This circumvents network intrusion detection.
- D. None, adding a wireless access point is a common task and not a security risk.

**Answer: A**

**Question: 6**

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

**Answer: B**

**Question: 7**

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

- A. SSIDs are case insensitive text strings and have a maximum length of 64 characters.
- B. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.
- C. SSID is used to identify a wireless network.
- D. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

**Answer: B,C,D**

**Question: 8**

Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails. Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

- A. /log/var/logd
- B. /var/log/logmail
- C. /log/var/maillog
- D. /var/log/maillog

Exam Name:	GIAC Certified Penetration Tester		
Exam Type:	GIAC	Exam Code:	GPEN
Certification:	GIAC Information Security	Total Questions:	384

**Answer: D**

**Question: 9**

You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

- A. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start
- B. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
- C. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
- D. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

**Answer: D**

**Question: 10**

Which of the following are the scanning methods used in penetration testing?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Vulnerability
- B. Port
- C. Network
- D. Services

**Answer: A,B,C**

**Question: 11**

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person. What type of attack is this?

- A. Session Hijacking
- B. PDA Hijacking
- C. Privilege Escalation
- D. Bluesnarfing

**Answer: D**

**Question: 12**

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

- A. TCP FTP proxy scanning
- B. Eavesdropping
- C. Web ripping
- D. Fingerprinting

**Answer: C**

**Question: 13**

Which of the following statements is true about the Digest Authentication scheme?



## 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](#)

