

# EC0-350

## ECCouncil

### *Ethical Hacking and Countermeasures*

Visit: <http://www.pass4sureofficial.com/exams.asp?examcode=EC0-350>

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your EC0-350 exam in first attempt, but also you can get a high score to acquire ECCouncil certification.

If you use pass4sureofficial EC0-350 Certification questions and answers, you will experience actual EC0-350 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ECCouncil exam prep covers over 95% of the questions and answers that may be appeared in your EC0-350 exam. Every point from pass4sure EC0-350 PDF, EC0-350 review will help you take ECCouncil EC0-350 exam much easier and become ECCouncil certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial ECCouncil EC0-350 course:

- \* Up-to-Date ECCouncil EC0-350 questions taken from the real exam.
- \* 100% correct ECCouncil EC0-350 answers you simply can't find in other EC0-350 courses.
- \* All of our tests are easy to download. Your file will be saved as a EC0-350 PDF.
- \* ECCouncil EC0-350 brain dump free content featuring the real EC0-350 test questions.

ECCouncil EC0-350 certification exam is of core importance both in your Professional life and ECCouncil certification path. With ECCouncil certification you can get a good job easily in the market and get on your path for success. Professionals who passed ECCouncil EC0-350 exam training are an absolute favorite in the industry. You will pass ECCouncil EC0-350 certification test and career opportunities will be open for you.



**QUESTION: 1**

Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

- A. Gif-It-Up
- B. Image Hide
- C. NiceText
- D. Snow

**Answer: D**

**Explanation:**

The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

**QUESTION: 2**

In the context of Trojans, what is the definition of a Wrapper?

- A. A tool used to encapsulate packets within a new header and footer
- B. An encryption tool to protect the Trojan
- C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan
- D. A tool used to bind the Trojan with a legitimate file

**Answer: D**

**Explanation:**

These wrappers allow an attacker to take any executable back-door program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code.

**QUESTION: 3**

When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

- A. nfscopy
- B. macof
- C. filesnarf
- D. webspay

**Answer:** C

**Explanation:**

Filesnarf - sniff files from NFS traffic

**OPTIONS**

-i interface

Specify the interface to listen on.

-v "Versus" mode. Invert the sense of matching, to select non-matching files.

pattern

Specify regular expression for filename matching.

expression

Specify a tcpdump(8) filter expression to select traffic to sniff. SEE ALSO Dsniff, nfsd

**QUESTION:** 4

What type of port scan is shown below?

Scan directed at open port:

ClientServer

192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23

192.5.2.92:4079 <----NO RESPONSE-----192.5.2.110:23

Scan directed at closed port:

ClientServer

192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23

192.5.2.92:4079<-----RST/ACK-----192.5.2.110:23

- A. Windows Scan
- B. Idle Scan
- C. SYN Stealth Scan
- D. XMAS Scan

**Answer:** D

**Explanation:**

An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

**QUESTION:** 5



- B. The buffer overflow attack has been neutralized by the IDS
- C. The attacker is creating a directory on the compromised machine
- D. The attacker is attempting an exploit that launches a command-line shell

**Answer:** D

**Explanation:**

This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of /bin/sh into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the "payload" that launches the command shell.

**QUESTION: 7**

Bill has started to notice some slowness on his network when trying to update his company's website and while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that cannot access the company website and cannot purchase anything online. Bill logs on to a couple of his routers and notices that the logs show network traffic is at an all time high. He also notices that almost all the traffic is originating from a specific address. Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that the IP is coming from Panama. Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service attack. Now Bill needs to find out more about the originating IP address. What Internet registry should Bill look in to find the IP address?

- A. RIPE LACNIC
- B. APNIC
- C. ARIN
- D. LACNIC

**Answer:** D

**Explanation:**

LACNIC is the Latin American and Caribbean Internet Addresses Registry that administers IP addresses, autonomous system numbers, reverse DNS, and other network resources for that region.

**QUESTION: 8**

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

## 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	

