

Forum:[Hack Forums](#)

Thread: [\[TUT\]-Symlink-\[/TUT\]\[Pics\]\[Noob-Friendly\]](#)

BeggFoMercy - April 16, 2012, 6:57 am

Hey HF , Today ill be showing u how to symlink a hacked web site/server

WhySymlinking ?

Some times, After hacking a web site , We find that the kernel of the server is 2011,2012 , So its gonna be hard or impossible to exploit/root it and gain the other web sites hosted on that server , So Our PlanB Is to symlink it - Gain access to all web sites on that server without gaining root access..

Requirements:

- 1-Hacked (web site - shell -)
- 2-Some scripts will be posted at the end of the Tutorial
- 3-A hacker's brain

First step" Uploading Tools":

First of all we will need to make a new folder on a hacked web server To start symlinking in a clean Enviroment ;)

Now after entering our Folder name And click forward , We will see a new folder made , Now we will head up to open it and upload:

- 1-.htaccess - Lists the folder as List
 - 2- Perl Script , That will config the /etc/passwd/ Into the web sites configuration
 - 3-Mysql Connector - Connects to the Mysql DB on the localhost.
- Just like that

Now we will need to chmod Our Perl Script To "0755" So we can view/edit/rename it Other wise we will be forbidden

Just click on the

Code `-rw-r--r--`At the same line of allsoft.pl

Then chmod to 0755 As in the pic

Now lets click on the Sec.Info For the /etc/passwd/ Infoz

Now for the view of the /etc/passwd/ We click on View Beside it

Now copy all the Daemons And head over to ur pl script Like that

And then it will look like that

Paste the codes u got from /etc/passwd viewing And Click Get Config

It will start loading then It will tell you Done!

Now this is the most loved part ever Viewing the gathered sites on the directory

Now head over to ur directory that contains the .htaccess

Example:

Code `www.site.com/logs/testfolder/`The testfolder Should be the folder that contains our scripts including .htaccess

It will load for some secs , Then it will open like a list

The shaded things are The web sites configuration

Now open a specific one ... Open ur mysql.php Connector that is uploaded on the same folde

Connect to the mysql / Shell it

I will not be showing u how to do that because most of u Know how to do it

<https://hackforums.net/showthread.php?tid=2404357>

This is just for joomla provided sites , Ill be making another tutorial about how to shell wordpress Sites...

Shout outs :

1-Inj3ctors

2-INTRA

3-Zer0Freak

4-HaxOr <3

5-joomlafkr

Etc..

Download scripts: [Click me](#)

End of the Tutorial ;)

-BeggFoMercy

Sw1x - April 16, 2012, 7:00 am

Thank you for this, I was wondering when I would see when you make a tutorial. :)

Thanks this will be useful.

VipVince - April 16, 2012, 7:03 am

Nice tutorial man. Good to read about something not as frequently discussed on here.

BeggFoMercy - April 16, 2012, 7:04 am

(Apr 16, 2012 07:03 AM)VipVince Wrote: [\[CITE\]](#) Nice tutorial man. Good to read about something not as frequently discussed on here.Thanks for the feed back brothaz , And yea that made me make the tutorial ...

joomlafkr - April 16, 2012, 7:27 am

Good writeup BeggforMercy !

Now they don't have any excuse to not to symlink the whole server :p

I have a remark : sometimes your perl file won't be able to find config files ,some of them are hidden...!

the trick is to symlink to index.php,read the source code and follow the calls to other php files !

BeggFoMercy - April 16, 2012, 7:29 am

(Apr 16, 2012 07:27 AM)joomlafkr Wrote: [\[CITE\]](#) Good writeup BeggforMercy !

Now they don't have any excuse to not to symlink the whole server :p

I have a remark : sometimes your perl file won't be able to find config files ,some of them are hidden...!

the trick is to symlink to index.php,read the source code and follow the calls to other php files !

Yea i know that Thanks for the remark bruh , Forgot ur name though bruh mb ;D

-zerocool - April 16, 2012, 7:33 am

nice one BeggFoMercy . .

Keep it up .

Bacardi - April 16, 2012, 7:44 am

Really nice tutorial. I tried it out right away and worked like a charm!

HeXagone - April 16, 2012, 7:50 am

Nice tutorial always happy to see lot of files :)

BeggFoMercy - April 16, 2012, 8:13 am

Thanks for the feed back brutharz, That really made my day ;)

Error667 - April 16, 2012, 8:53 am

Seems to be an HQ tutorial, thanks to share on HF.

BeggFoMercy - April 16, 2012, 10:40 am

Thanks for the feed back bruthah..xD

Delphi - April 16, 2012, 11:50 am

Thank you for this bro. Nice tutorial!

mObile - April 16, 2012, 12:11 pm

Fuckin-A Bro! Nice tutorial and very easy to understand. ? Unfortunately only a handful of us here know this method. ? Maybe with this tutorial it will inspire more people to symlink while they have a website shelled. You'd be surprised how many high traffic websites that may be hosted on that server. ?

BeggFoMercy - April 16, 2012, 3:02 pm

Thanks for the feed back bruthah ;) , And Yea im really surprised , Worth 10k web sites + :D

Vivek_s - April 18, 2012, 2:23 am

thanks man

Very Nice post..

353535353535

kilus - April 20, 2012, 12:33 pm

What shell are you using?

Maybe I can get it?

BeggFoMercy - April 20, 2012, 12:39 pm

Its Just a normal WSo 2.3 shell , Google it

kilus - April 20, 2012, 2:24 pm

(Apr 20, 2012 12:39 PM)BeggFoMercy Wrote: [\[CITE\]](#) Its Just a normal WSo 2.3 shell , Google it
Thanks!

Really nice shell :)

Edit, 35 characters...

noober1001 - April 25, 2012, 1:59 pm

Thanks for sharing this.
It works really good.

einbrettholz - May 1, 2012, 10:40 am

I love how all the symlinking magic becomes clearer and clearer through all the attention it gets here on the forum recently.

I wonder what other magic lies beyond :)

BeggFoMercy - May 2, 2012, 7:38 am

(Apr 25, 2012 01:59 PM)noober1001 Wrote: [\[CITE\]](#) Thanks for sharing this.

It works really good. Thanks for the feed back bruthah

UltraCyber - May 2, 2012, 9:15 am

Weird, it's not working for me, I am doing that and the folder load normal but when I am going to the shell and to the folder that has it all, there are all the txt files but the user permission is still root/root u--.

Can someone help me?

Regards,
Ultracyber

HeXagone - May 2, 2012, 9:21 am

i can help you pm me the details :)

torque59 - May 3, 2012, 4:06 am

Excellent tutorial man

Keep up the good Work

?Victory - May 15, 2012, 11:10 am

You know what ... I didnt knew it before !

gj man keep up the good work ^.^

Would be happier if I found myself in shout outs xD

gave me an error : Fatal error: Allowed memory size of 67108864 bytes exhausted (tried to allocate 71 bytes) in /home/amrit476/public_html/images/upload/scroll/404.php on line 615

Bacardi - May 16, 2012, 6:09 am

I'm having a small problem.

When I the tools says done and I go to the directory, it's empty.

It just shows these 3 files:

allsoft.pl
mysql.php
tar.tmp

And when I go and check the dir in my shell it won't open.

Like so:

<https://i.imgur.com/Wipxo.png>

Any idea on whats happening?

ProfessorGreen z - May 16, 2012, 6:17 am

Awesome tutorial HQ post thank you for the contribution bro.

Grey-Tech - June 1, 2012, 4:13 pm

(May 2, 2012 09:15 AM)UltraCyber Wrote: [\[CITE\]](#) Weird, it's not working for me, I am doing that and the folder load normal but when I am going to the shell and to the folder that has it all, there are all the txt files but the user permission is still root/root u--.

Can someone help me?

Regards,
Ultracyber

OP: Nice tutorial, I really liked it. So far it hasn't worked for me though, but I won't give up just yet. :)

I've had the same problem, anyone know what gives?

BeggFoMercy - June 1, 2012, 5:21 pm

(May 16, 2012 06:09 AM)Bacardi Wrote: [\[CITE\]](#) I'm having a small problem.

When I the tools says done and I go to the directory, it's empty.

It just shows these 3 files:

allsoft.pl
mysql.php
tar.tmp

And when I go and check the dir in my shell it won't open.

Like so:

<https://i.imgur.com/Wipxo.png>

Any idea on whats happening? Sorry for the delay ,I have been through this alot ,
Either httpd.config , Is blocking ur entire request Or You can only read the .txt web sites When ur root ..?

?mnipotent - June 1, 2012, 6:01 pm

Thanks for the great tutorial. This will come in handy soon. Good work!

ibaijc - June 18, 2012, 6:15 am

Oh god... You should have said that this is only for joomla sites at the beginning of the TUT not at the end... But nice tutorial anyway!

BeggFoMercy - June 19, 2012, 6:05 pm

Who said this is only for the joomla sites ? Sym linking can be done with every single web server!
Doesnt depend on what type is it !

12345xmen - July 26, 2012, 1:33 pm

not wrking when i try sym.php then i get access in all symlink dir but when i go this method

get tar.tmp dnt knw where is error ..

ny solution for this !

frankie777 - November 22, 2012, 7:35 am

Great tutorial. Please can someone tell me where to find the Sec.Info so I can proceed? Huge

thanks in advance

Methanol - *November 22, 2012, 8:24 am*

Great tutorial right here, I'm a newbie but I understood this right away, thanks. :)

drukoZ - *November 22, 2012, 9:50 am*

i did so and for some reason the text files seem to be forbidden can anyone help me?

Sh4dowH4cking - *November 22, 2012, 11:20 am*

Thank you! Going to try out this later:)