

Forum:[Hack Forums](#)

Thread: [\[TuT\] How to symlink on a linux server \[TuT\] \[Website hacking !!\]](#)

-ThatGuy- - August 29, 2011, 6:45 am

How to symlink ? (TUTORIAL)

Written by -ThatGuy- for begginer webhackers.

NOTE : I do not take any responsibility for your actions. This was written for educational purposes only ! Also sorry for my bad english !

Hello HackForums.

Today i'll try to help begginer webhackers by teaching them a method called symlink.

What is symlink ?

Symlink is a method used by hackers to read files from other users on a linux server, only by using a php-shell.

So what do we require to start the tutorial :

Requirements :

- a phpshell uploaded in a linux server (Safe MODE = OFF)
- a target site
- basic phpshell & linux knowledge
- a brain !

Let's start by the tutorial.

Where to get a target, if you only have a phpshell uploaded in a linux server that has some sites ?

It's easy , first get the IP of the server.

Then go to [bing.com](#) and search like that :

Code ip:xx.xxx.xxx.xxx vbulletinxxx replace with the ip adress of the server , and 'vbulletin', you can change to a name of a forum software or a CMS you wish as a target. But for this example i'll take vBulletin.

OK , now we got the target site , let's suppose that its domain name is mytarget.com and it uses vBulletin forum software.

Now starts the real hacking !

Go to your phpshell , and in the 'Execute command' field , execute there that command :

Code `ls -la /etc/valiases/mytarget.com` By executing this command , i'll get the name of the user (on the linux server) that keeps the website mytarget.com.

It should return with a result similar to that :

```
>>>>>>-rw-r--r-- 1 target mail 28 May 28 2011 /etc/valiases/mytarget.com
```

The red colored piece is the user of mytarget.com on the server.

So in our case the username is 'target'

Many of us know that the configuration file of vBulletin script ,can be found in /includes/config.php. This is the file we need to read in our case , in order to get access at our target site.

How can we read that file ?

Simple , execute that command on the shell :

Code `ln -s /home/target/public_html/includes/config.php symlink.txt`As you can see, we're writting the content of config.php , into symlink.txt file.

After you execute the command , you will se a new file called symlink.txt.

Open it and w00t !! You successfully read the configuration file (symlinked).

Now , just get an MySQL connector script coded in PHP , and login with the details you get from configuration file of your target. Then at the admin table, get the admin's hash and crack it , or better , change the admin's email you yours , and then do a forgot password at mytarget.com And then you successfully will get full access in your target site !

That was all ,very easy if you practice many times. Maybe soon i will make a video tutorial if you still didn't understand , just request the video tut in the comments , and i will try ASAP to make it for you !

Thanks for reading , -ThatGuy- !

Thegame - August 29, 2011, 8:28 am

how to symlink a windows server ?

if have knowledge of that do post it here ;-)

daxx - March 27, 2012, 7:48 am

Thanks for the tut! Simple and effective.

Just hacked a forum with it :D

Uiqueblhats - April 3, 2012, 5:00 am

okkk! bookmarked it thx

and its oosom