小白复现HOW TO EXPLOIT ETERNALBLUE & DOUBLEPULSAR TO GET AN EMPIRE/METERPRETER SESSION ON WINDOWS 7/2008

Paper原文下载：https://www.exploit-db.com/docs/41896.pdf

本人没有任何信息安全基础，学过C语言，计算机专业知识仅停留在考研一年后的水平上。本文只是完全复现paper里面的过程，算是增加一些自己对这方面的了解，之后会对这里面涉及到的内容进行进一步的学习，但是本文内只是复现的内容，你也可以把它看做一个对paper的简单翻译，加上一下我自己的理解。

1. 在虚拟机上安装kali、windows xp、windows 7，在windows xp上面安装python、pyWin32、notepad++。

目标机器：Windows 7(cn\_windows\_7\_ultimate\_with\_sp1\_x64\_dvd\_u\_677408.iso)

攻击机器：

Windows XP (zh-hans\_windows\_xp\_professional\_with\_service\_pack\_3\_x86\_cd\_vl\_x14-74070.iso)

安装python 2.6(注意添加环境变量), PyWin32 v2.12(下载地址见原paper)

下载shadowbroker的github项目(https://github.com/misterch0c/shadowbroker)。需要里面的FUZZBUNCH

Kali(kali-linux-2016.2-amd64.iso)

安装Empile (metasploit不需要安装)

|  |
| --- |
| 虚拟机中三个机器IP地址的设置：  ①编辑->虚拟网络编辑器：添加网络，类型选择桥接模式，桥接到你的外部主机网络所用网卡上。可以在这里看  C:\Users\zeonyu\AppData\Roaming\Tencent\Users\348300328\QQ\WinTemp\RichOle\V2@V)5U9~VC~93C1LXI(IEQ.png  ②虚拟机设置中，网络适配器选择 自定义(VMnet0)  这时打开系统应该就已经有一个自动分配的IP地址了，可以在cmd中使用ipconfig查看。可能有些教程里面写要自己设置IP、DNS、网关…我没这么做有两点原因：一个是我用的校园网，有好多机子的IP地址和我在同一个局域网，自己设置你也不知道是不是占用了其他人机子的IP；二是没有必要，这里只需要拥有同一个网段的IP地址就可以了。如果把系统的防火墙关掉，这时候是可以ping通的。（我在攻击的时候win7的防火墙也是关着的，不知道对攻击有没有影响，有没有童鞋试过开着防火墙攻击？） |

最终三台机器的IP：

Windows 7: 172.31.74.114

Windows XP: 172.31.74.116

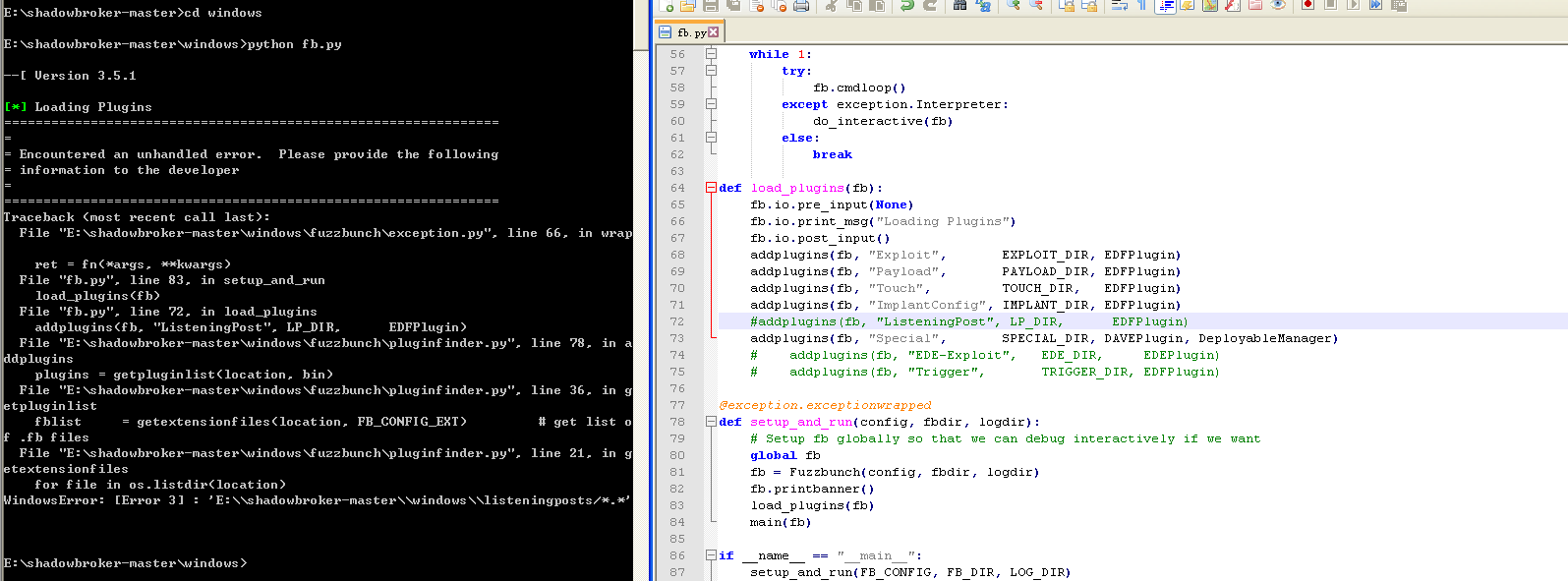
KALI: 172.31.74.117

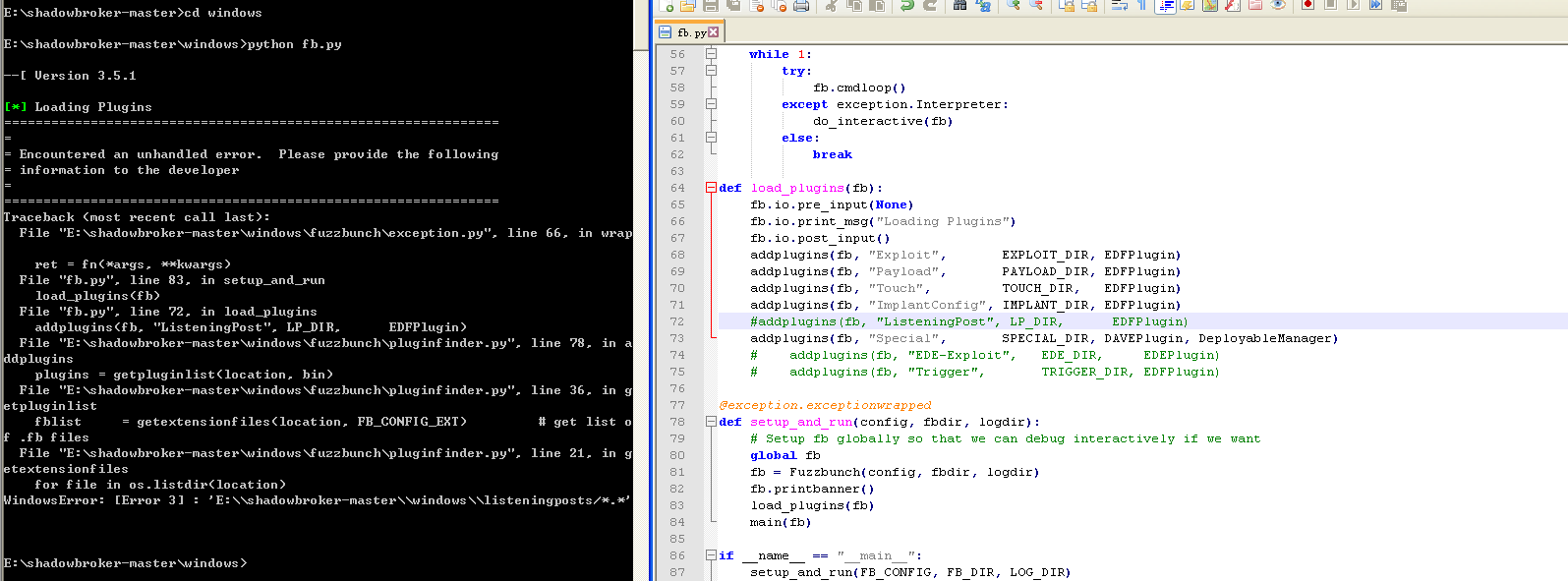
1. 配置FuzzBunch 并使用EternalBlue攻击Win7

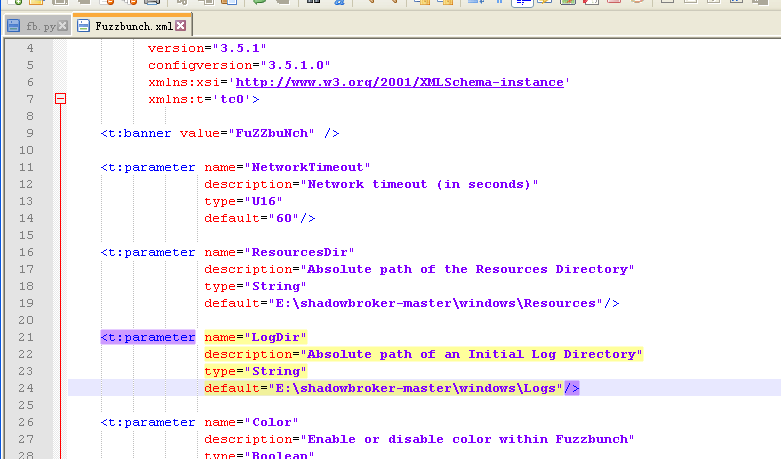
这里你应该已经下载好了shadowbroker(并且解压了。。。)。打开cmd.exe进入到对应的文件夹里，我的是”E:\shadowbroker-master\windows”。

|  |
| --- |
| 这里我遇到的问题是怎么进入E盘((⊙﹏⊙)b)，因为我之前用的一直是PowerShell，只要cd就可以，原来在cmd是要输入”E:”(不加双引号)。 |

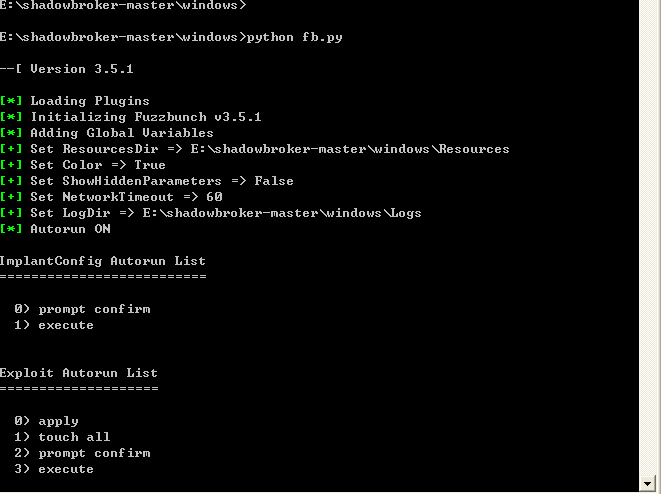
现在运行python fb.py，报错，按照paper中修改。

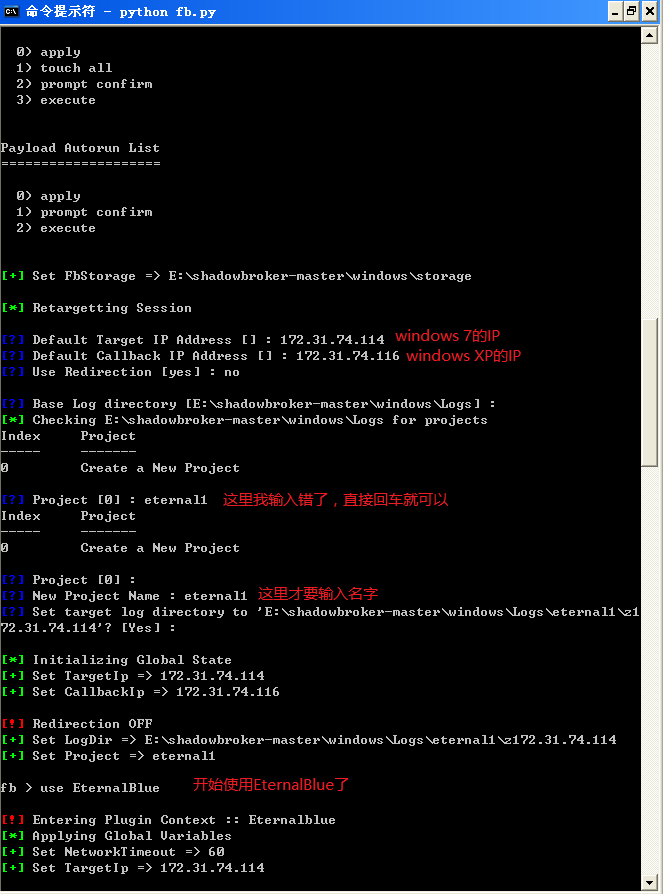




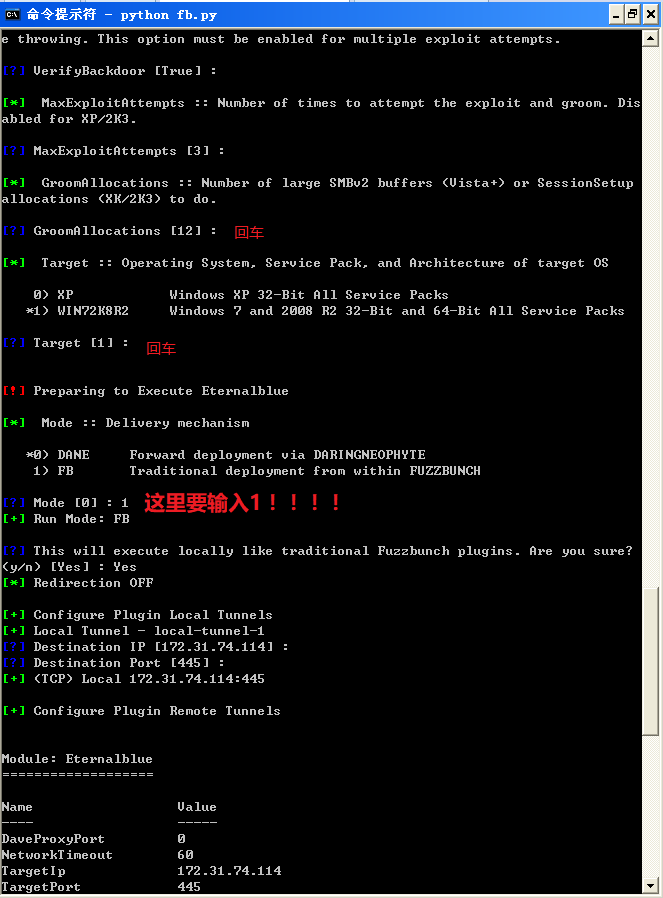


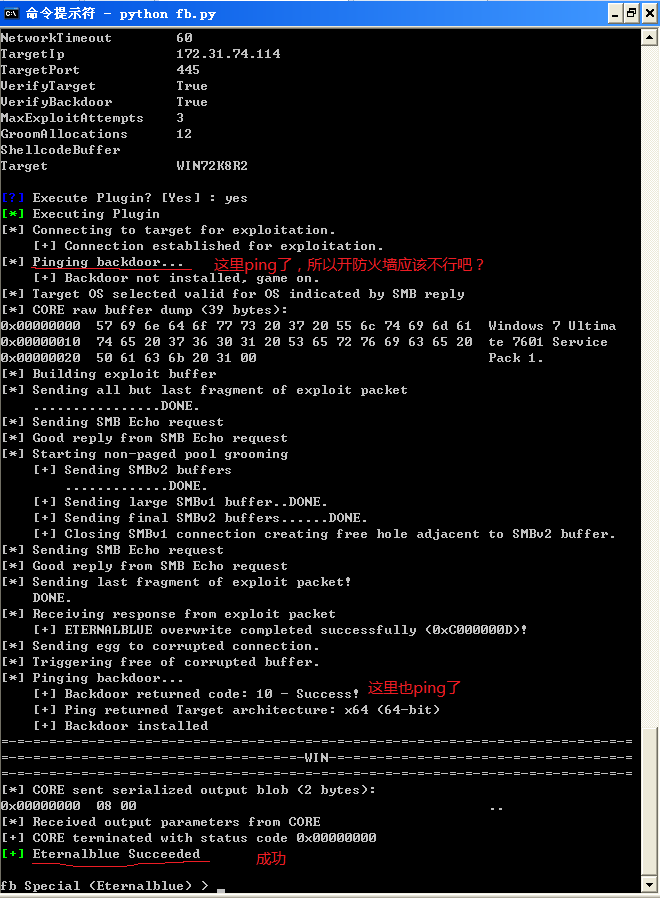
重新运行python fb.py，成功，下面是一系列的截图：







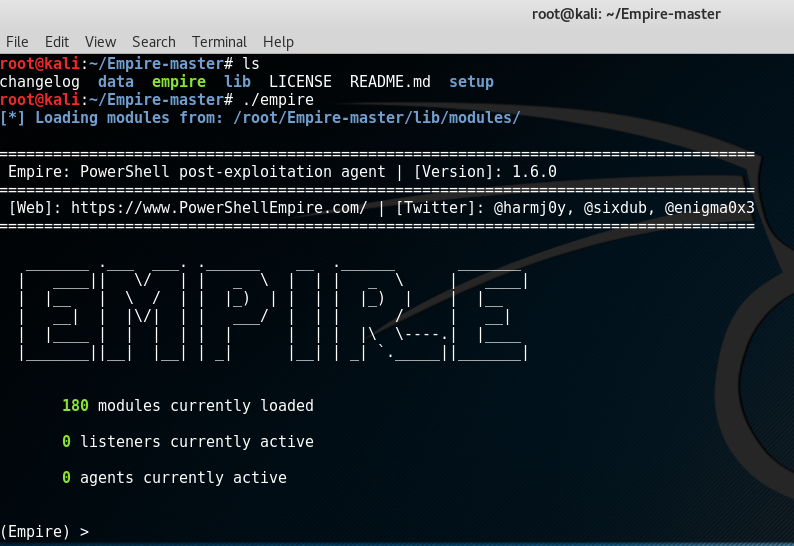




1. 制作 恶意DLL(payload)

这个DLL接下来会用DOUBLEPULSAR远程注入到已经被ETERNALBLUE感染的目标机器Win7中。

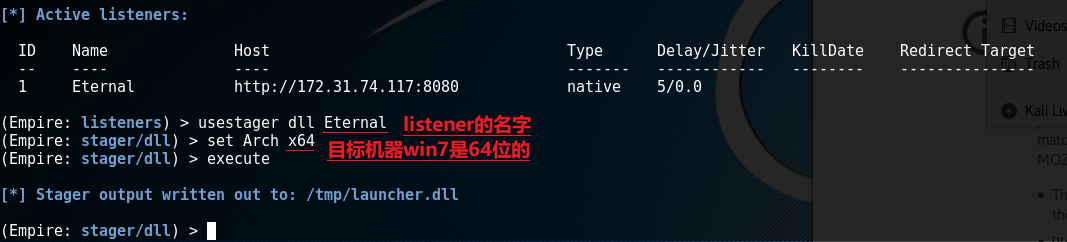
在kali里面装Empire，步骤按照Empire的github页面里面的介绍。



设置一个listener，这样当dll被注入后，这里可以建立一个反向连接。



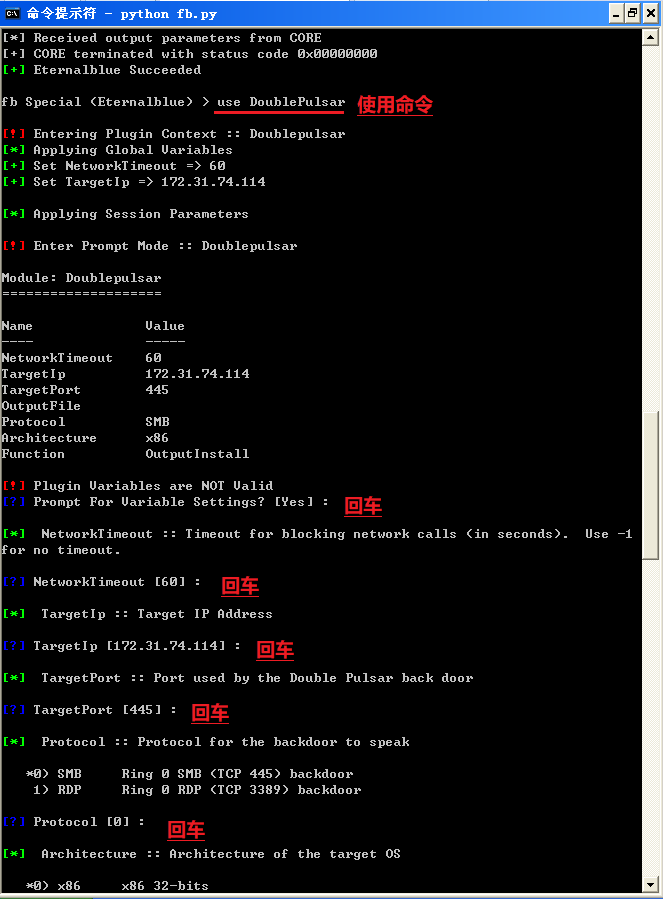
接下来生成dll，Empire的手册里也有相关说明(http://www.powershellempire.com/?page\_id=135)



生成的dll文件在/tmp/launcher.dll，复制改文件到windows XP中。我放在了E:\shadowbroker-master\windows\launcher.dll(这个路径后面要用到)

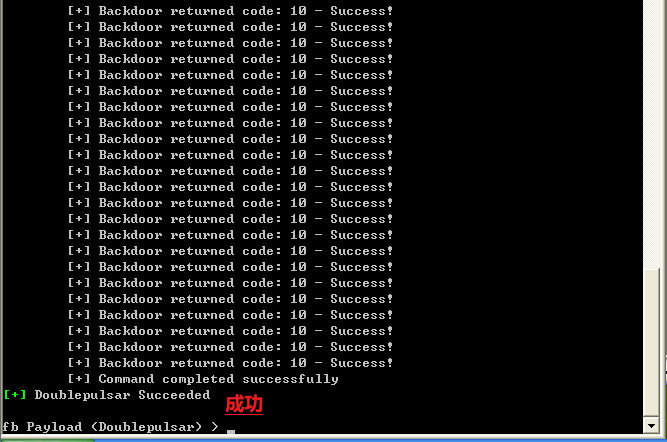
1. 用DoublePulsar把恶意DLL注射到目标机器中

回到windows XP，使用命令use DoublePulsar

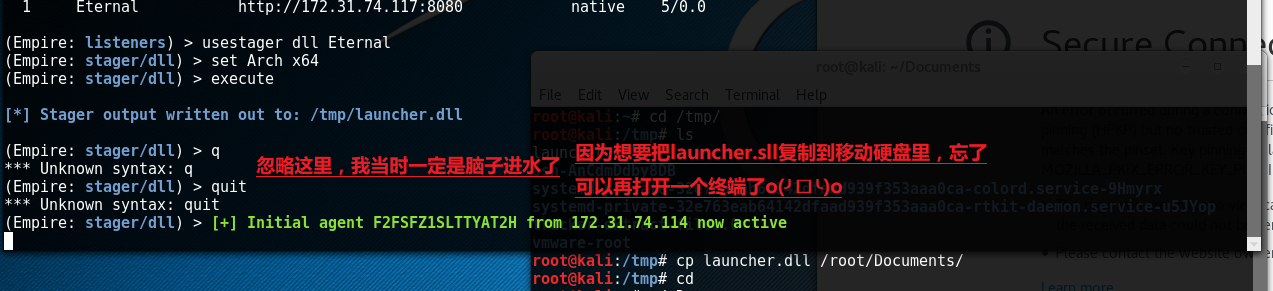


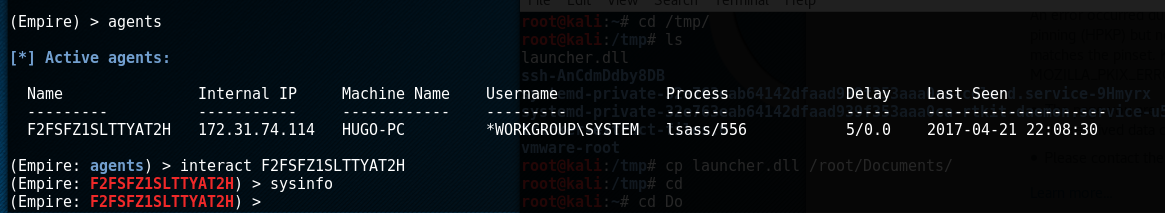






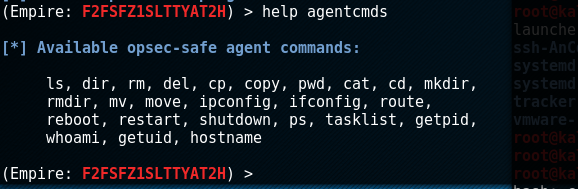
1. 这个时候kali那里告诉listener建立了反向连接。



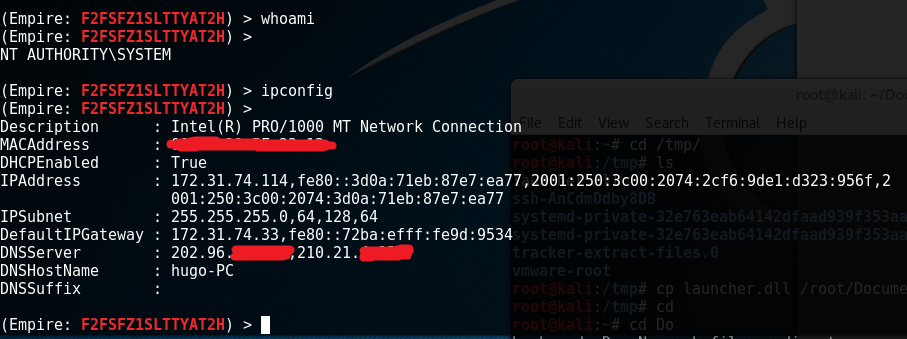


这里我输入之后没有输出我还以为出了什么问题，后来发现只是反应有点慢，等着吧…还在等…我觉得可能是我的虚拟机设置有些问题？？

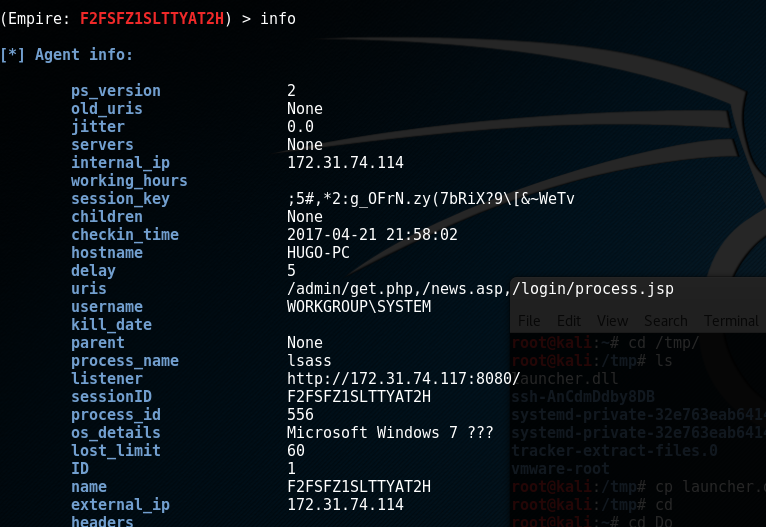
可以支持的命令，没有sysinfo?：



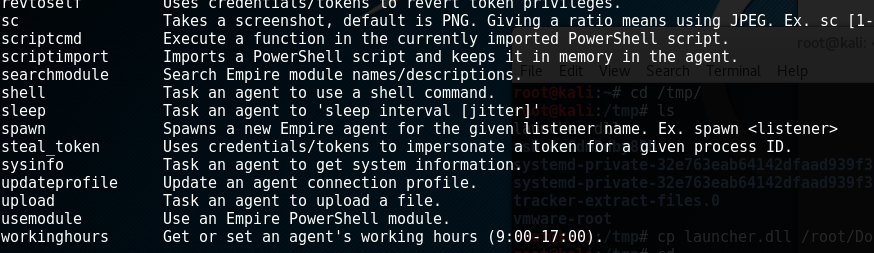
其他命令没有问题。



可以使用info命令



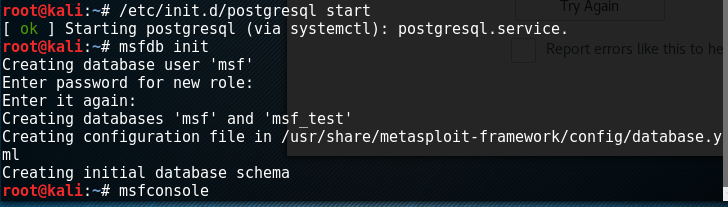
但是help里面有sysinfo命令，说明是可以使用的

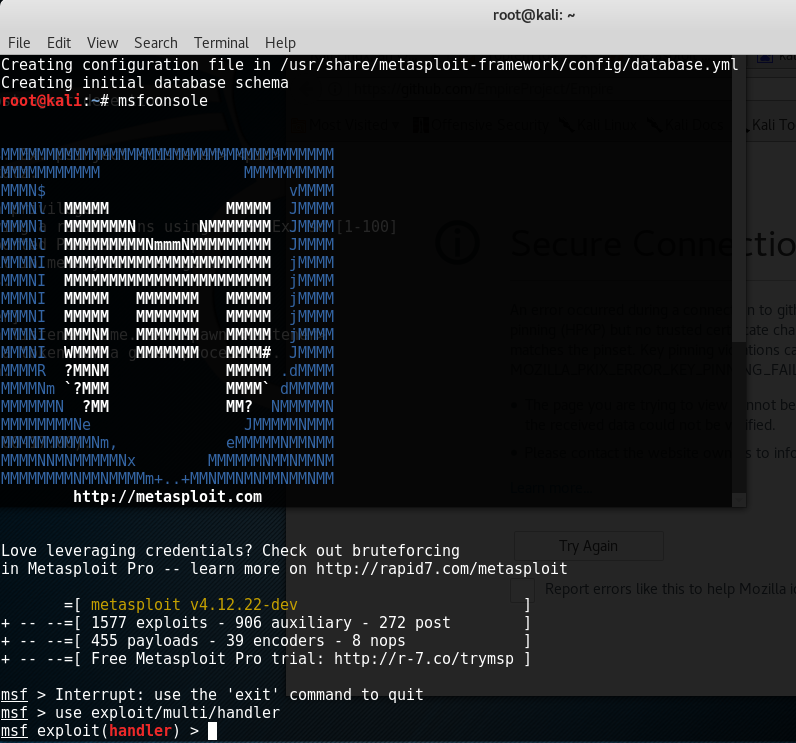


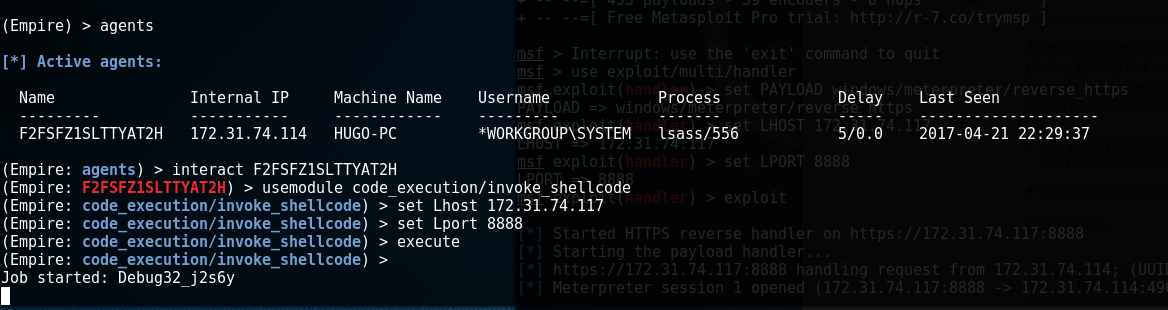
可能真的都需要等很长时间？不清楚了。

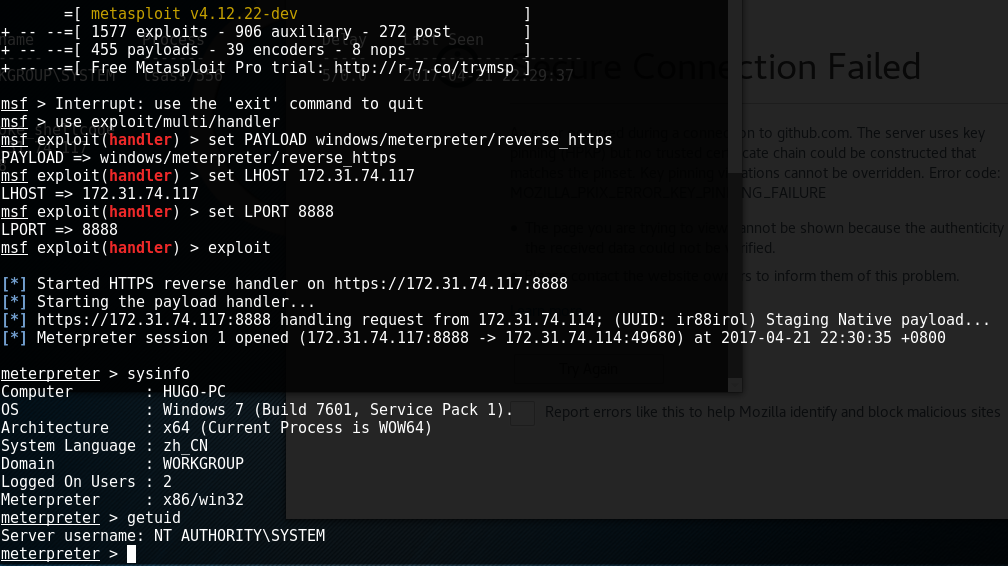
1. 现在试一下最后一个功能Migrating to Meterpreter

启用msf









在这里运行sysinfo可以，o(╯□╰)o