# 渗透神器Empire

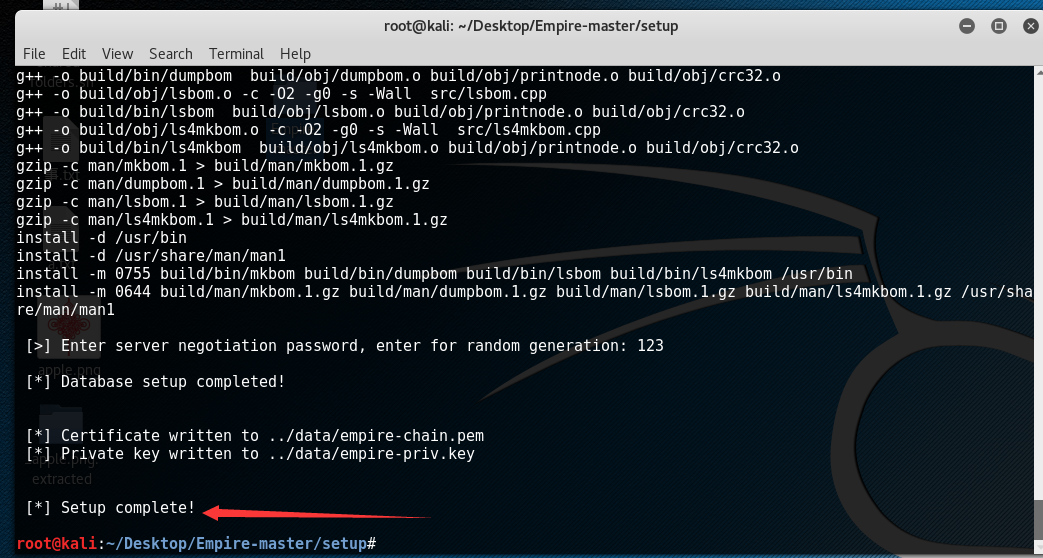
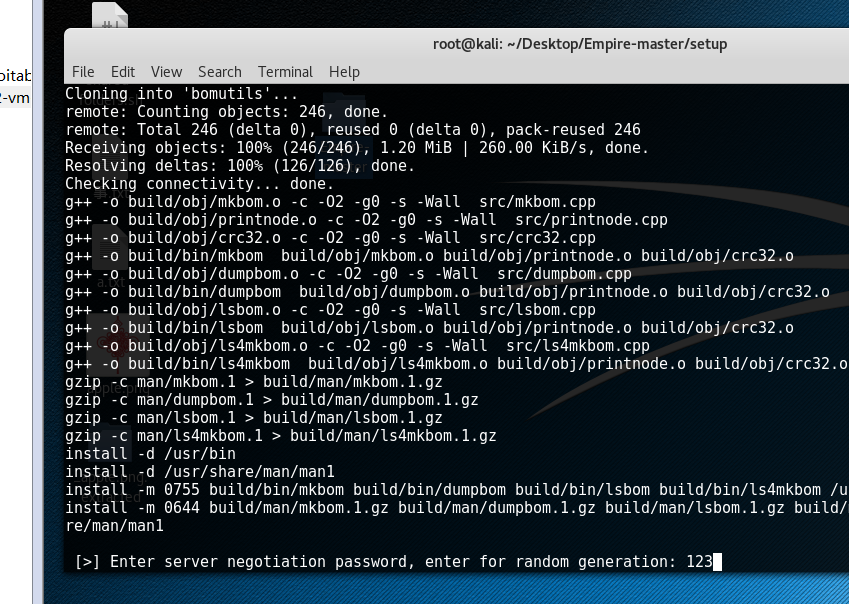
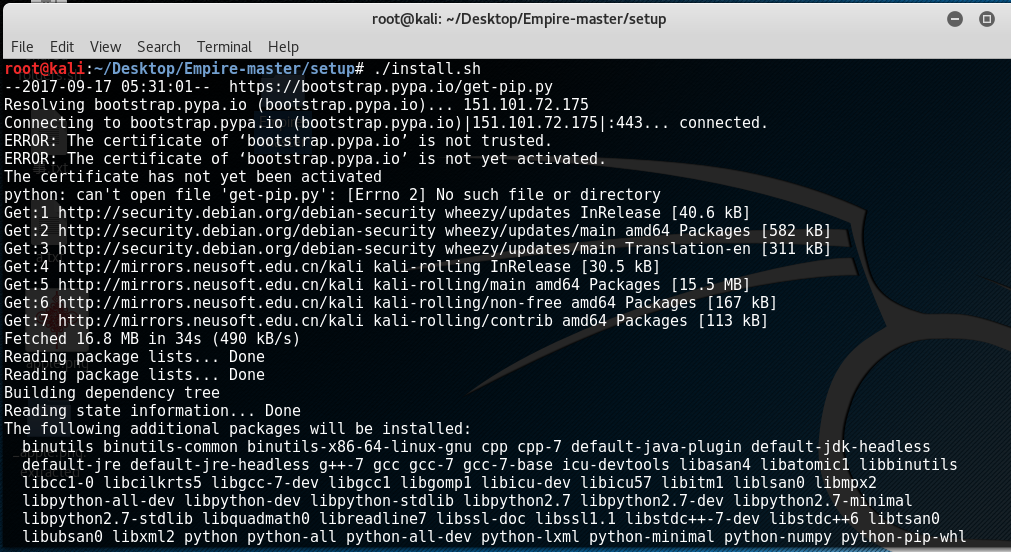
## 0x00 安装

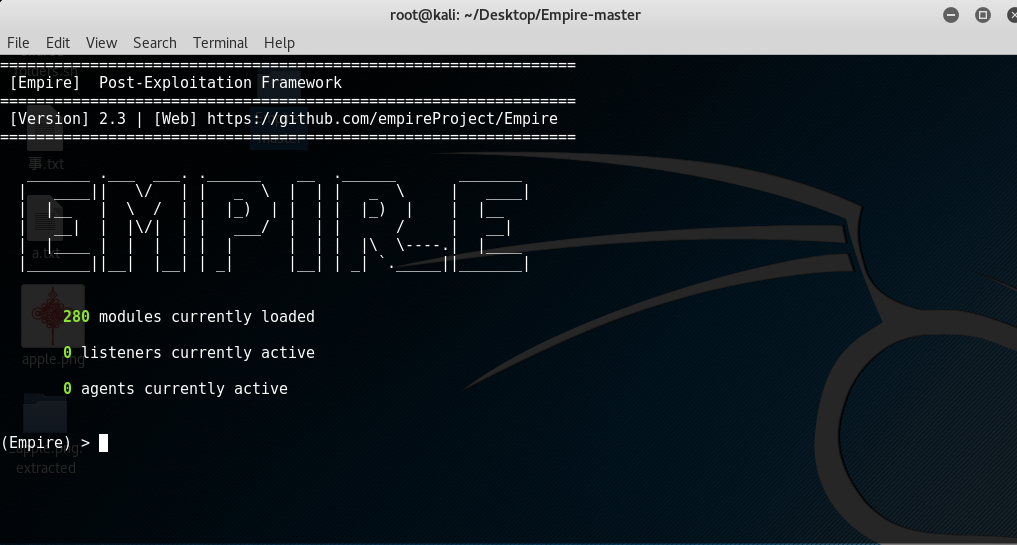
下载地址：Github:https://github.com/EmpireProject/Empire

不喜欢用命令的同学可以去安装一个GUI界面的，也是国外大牛用php写的一个web界面

GUI版本下载地址：Github:https://github.com/interference-security/empire-web

github上克隆回来运行./install.sh，傻瓜式安装，只需要输入一个预设的密码就可以了，其他会自动安装。





## 0x01 监听

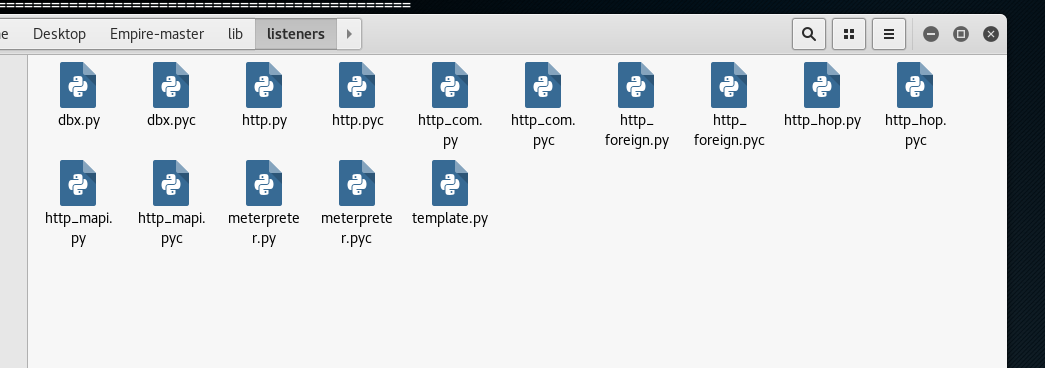
首先要设定监听模块，跟Metaploit创建一个监听载荷一个意思

在命令行里输入Listener就可以进入监听

第一次进入会显示如下

C:\Users\ASUS\AppData\Roaming\Tencent\Users\354050819\QQ\WinTemp\RichOle\GHA6]MC8Y_UZ6PF_%I`%(NX.png

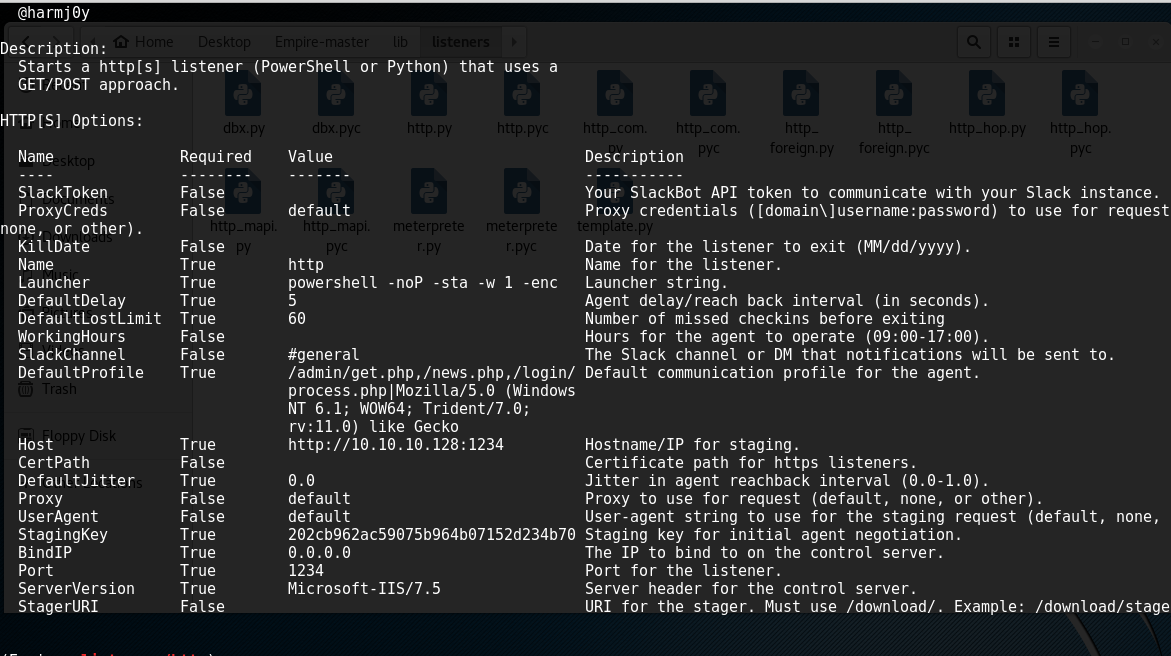
一共有以下那么多监听模块



最常用的监听模块为http

命令：uselistener http进入监听模块

命令：info 查看当前的信息



一般只需要设置Host，与metasploit的设置方法相同，设置好之后命令execute启动监听

## 0x02 攻击

攻击有两种方式：

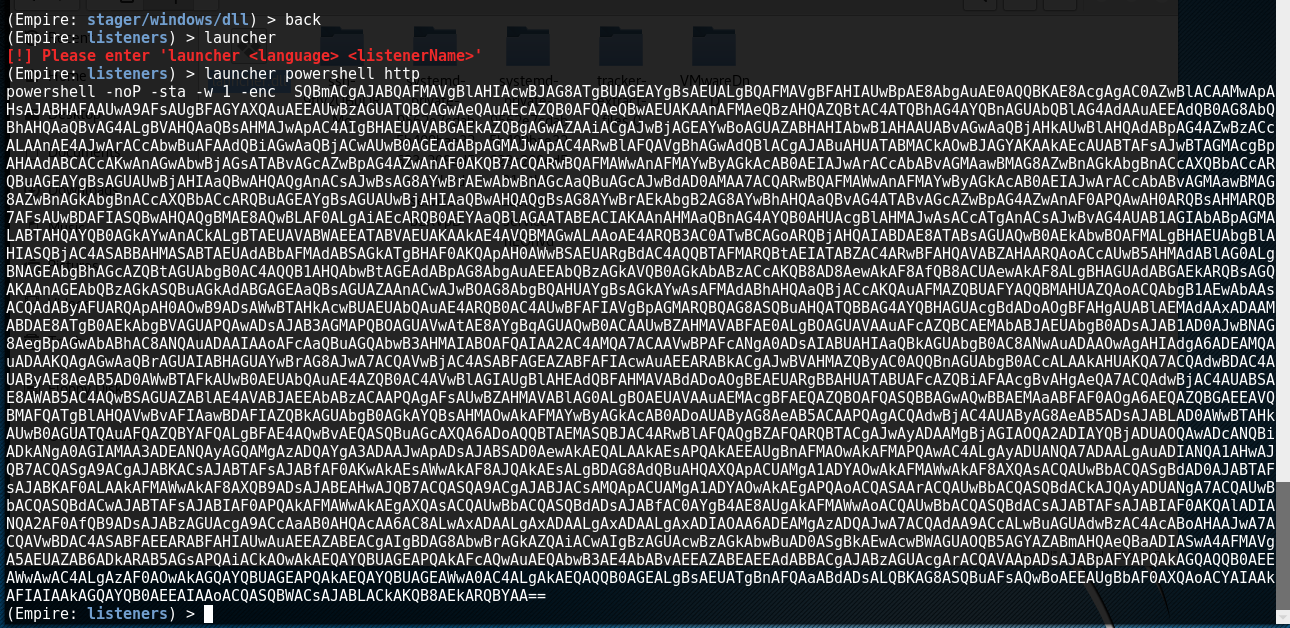
1. 直接生成powershell命令，当执行这命令的时候会给我们回弹一个shell
2. 可以生成14种类型的木马

### 一、直接生成powershell命令

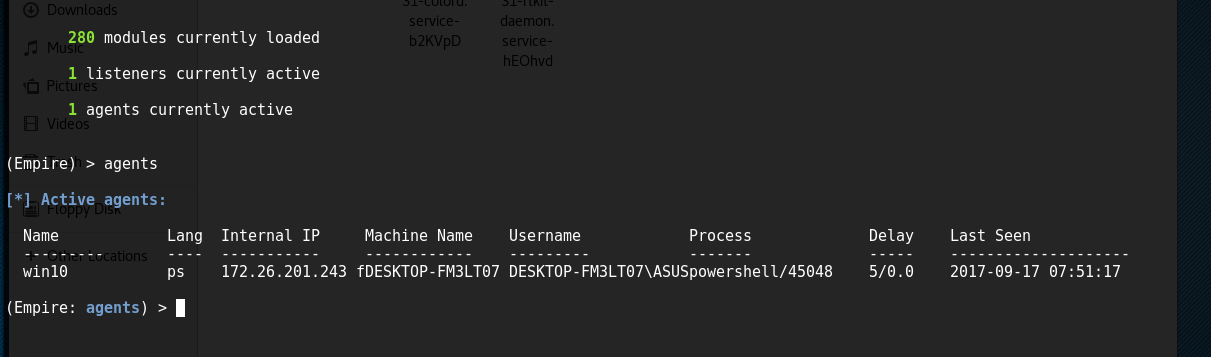
在listener监听模块输入命令 launcher powershell http

将一大段代码传到靶机的powershell下执行

当执行这命令的时候会给我们回弹一个shell



当我们执行后，命令行窗口一闪而过，接不到图，但是在我本机下已经反弹了一个会话



查看会话列表 命令：agents

命令：Interact <Name>进入会话

命令：help 查看可操作选项（有很多内设的命令）

注意：在这里输入的命令如果不是这里面的命令的话，命令会被解析为windows命令执行，并给我们回显，但是这里要注意了，你每写完一道命令敲下回车以后，不要感觉是没有回显，要稍等一下才会回显出来

命令事例：

1.download、upload选项可用于上传下载文件

2.Rename可将当前的会话重命名方便后续操作

3.Shell命令可用于执行cmd的命令 eg：shell dir

4.sc命令截图

5.Pypassuac <监听模块> 用于提权

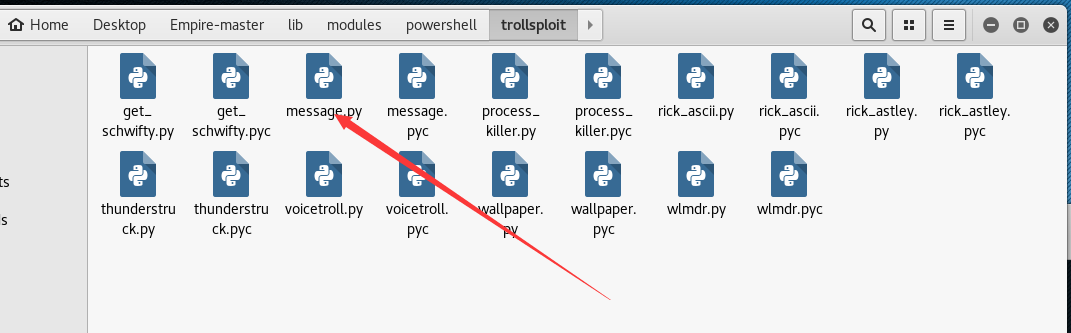
![C:\Users\ASUS\AppData\Roaming\Tencent\Users\354050819\QQ\WinTemp\RichOle\JYOR[7X%9OD](2D7Q]E~8L7.png](data:image/png;base64,)

6.mimikatz 用于获取靶机的密码（需要提权之后才能使用）

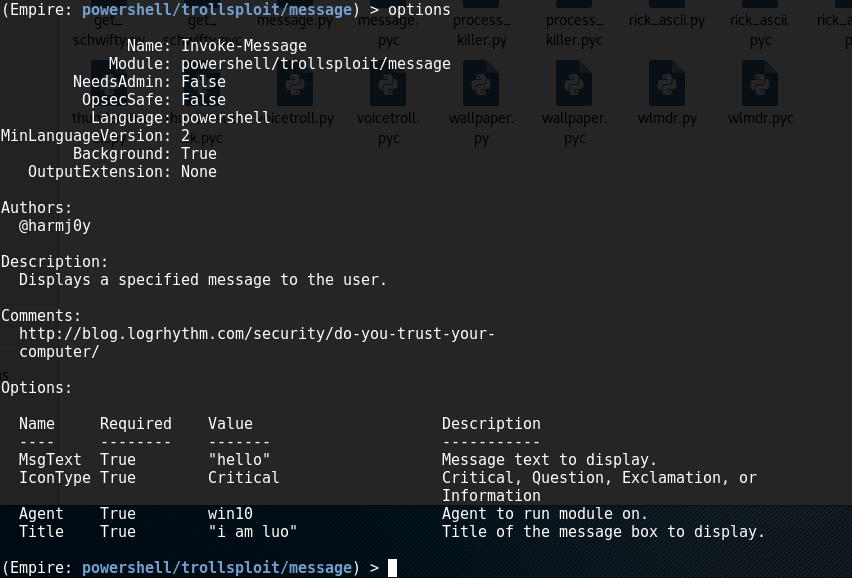
7.最强大的命令为usemodule 可用各种模块



（1）用message模块可在靶机上弹出一个窗口

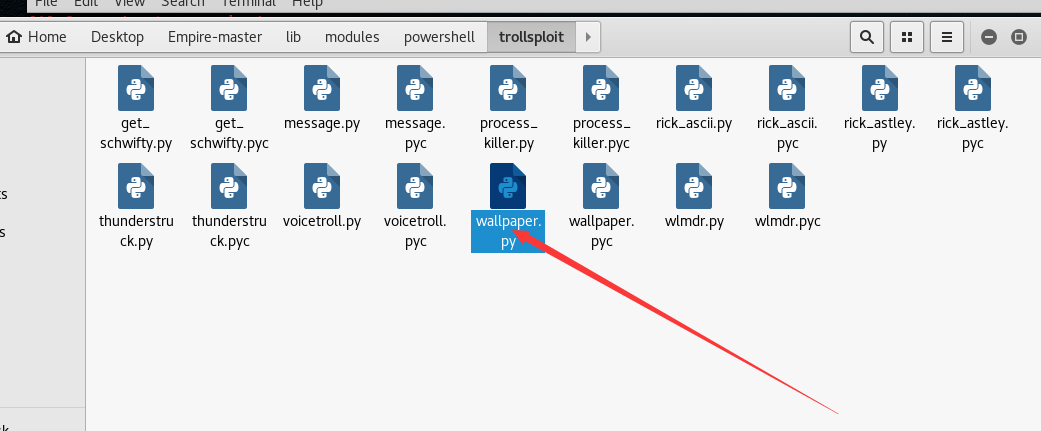


里面的description部分是对该模块功能的介绍

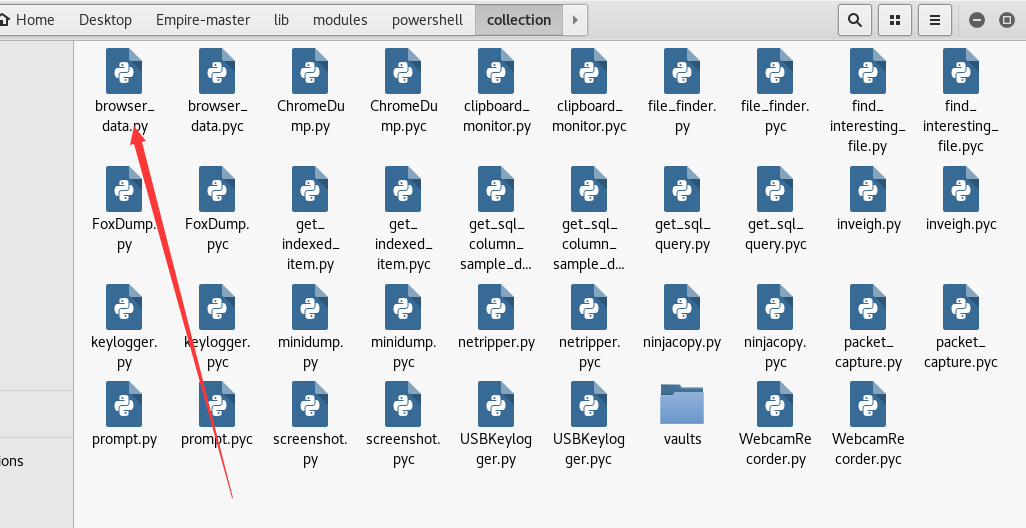


设置完之后命令：execute执行

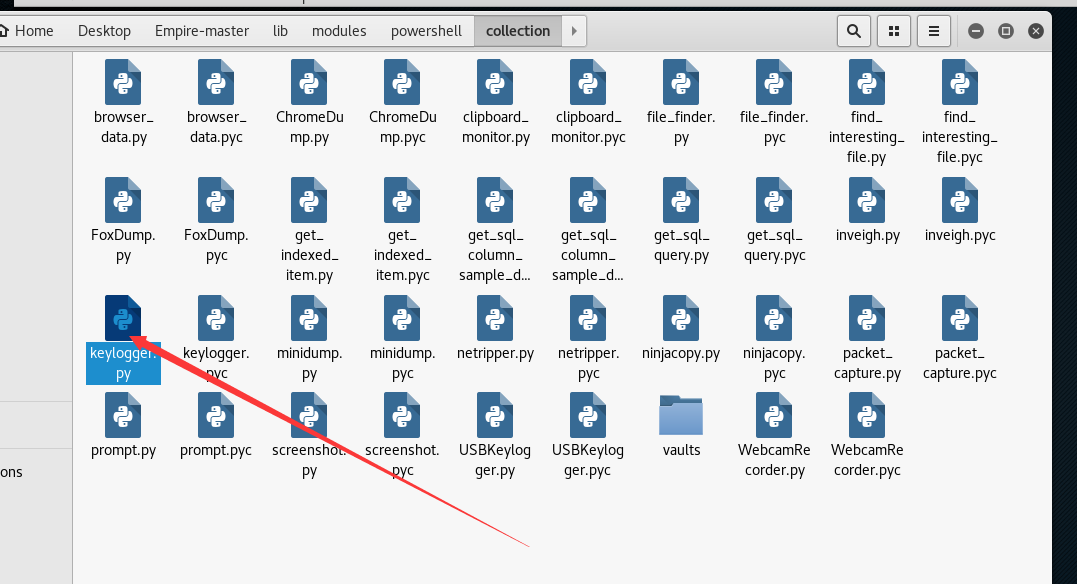
（2）Wallpaper模块用于更改靶机的桌面背景



（3）browser\_data模块用于获取靶机浏览器信息



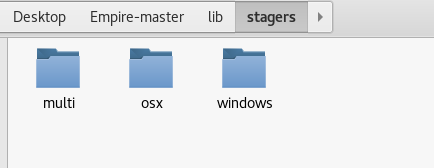
（4）keylogger键盘记录器

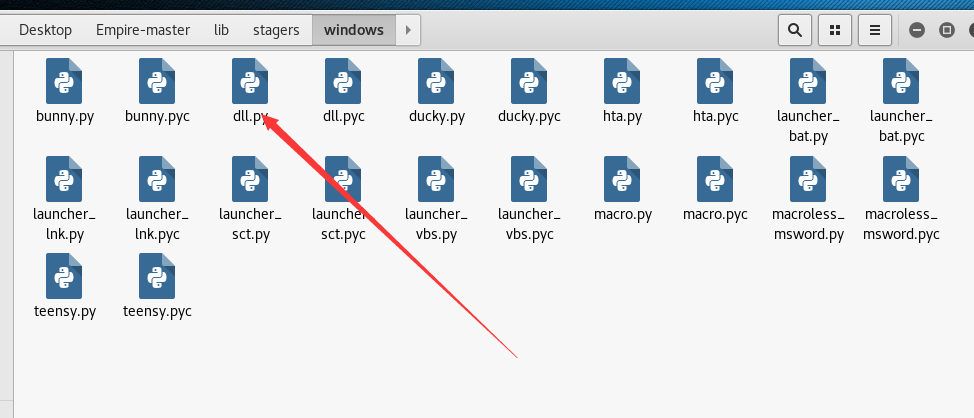


### 二、生成木马

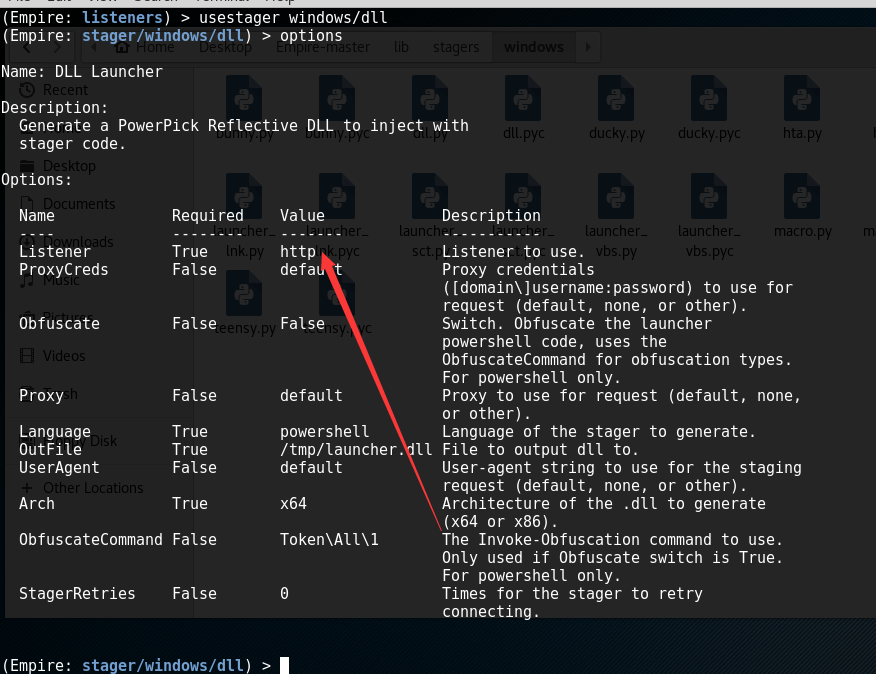
命令：usestageter <模块名称>

一共有三种不同类型的木马



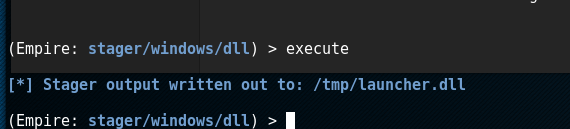
这里选择windows下常用的dll木马

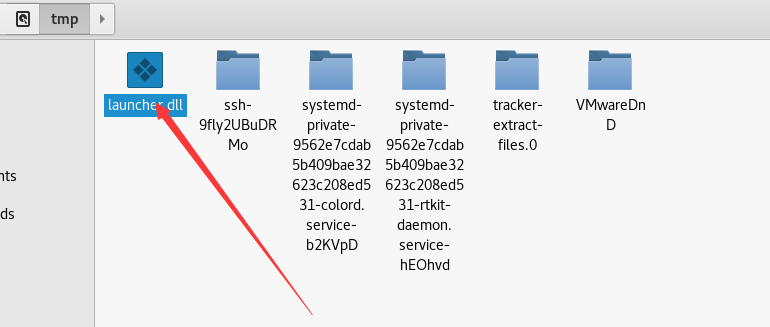
操作跟metasploit的相同，这里只需要设置监听为刚刚启动的监听程序



然后命令：execute生成恶意程序

会返回生成的文件路径





这时这需要上传到靶机运行即可

参考文章：<http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/3311.html>

<http://www.freebuf.com/articles/web/76892.html>