专注APT攻击与防御
https://micropoor.blogspot.com/

项目地址：https://github.com/Veil-Framework/Veil-Evasion

Veil-Evasion是与Metasploit生成相兼容的Payload的一款辅助框架，并可以绕过大多数的杀软。

Veil-Evasion并没有集成在kali，配置sources.list，可直接apt-get。

```
root@John:~/Deskto# cat /etc/apt/sources.list
#中科大
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
#阿里云
#deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
#deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
#清华大学
#deb http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free
#deb-src https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free
#浙大
#deb http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free
#deb-src http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free
#东软大学
#deb http://mirrors.neusoft.edu.cn/kali kali-rolling/main non-free contrib
#deb-src http://mirrors.neusoft.edu.cn/kali kali-rolling/main non-free contrib
#官方源
deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib
#重庆大学
#deb http://http.kali.org/kali kali-rolling main non-free contrib
#deb-src http://http.kali.org/kali kali-rolling main non-free contrib
```

```
root@John:~# cat /etc/apt/sources.list
#中科大
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
#阿里云
#deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
#deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
#清华大学
#deb http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free
#deb-src https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free
#浙大
#deb http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free
#deb-src http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free
#东软大学
#deb http://mirrors.neusoft.edu.cn/kali kali-rolling/main non-free contrib
#deb-src http://mirrors.neusoft.edu.cn/kali kali-rolling/main non-free contrib
#官方源
deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib
#重庆大学
#deb http://http.kali.org/kali kali-rolling main non-free contrib
#deb-src http://http.kali.org/kali kali-rolling main non-free contrib
root@John:~#
```

root@John:~/Desktop# apt-get install veil-evasion

由于在实验中本机已经安装，所以我们在虚拟机中使用git方式来下载和安装。（以便截图）

ps:本次kali下截图使用scrot

root@John:~/Deskto# apt-get install scrot

root@John:~/Deskto# scrot -s　　//即可

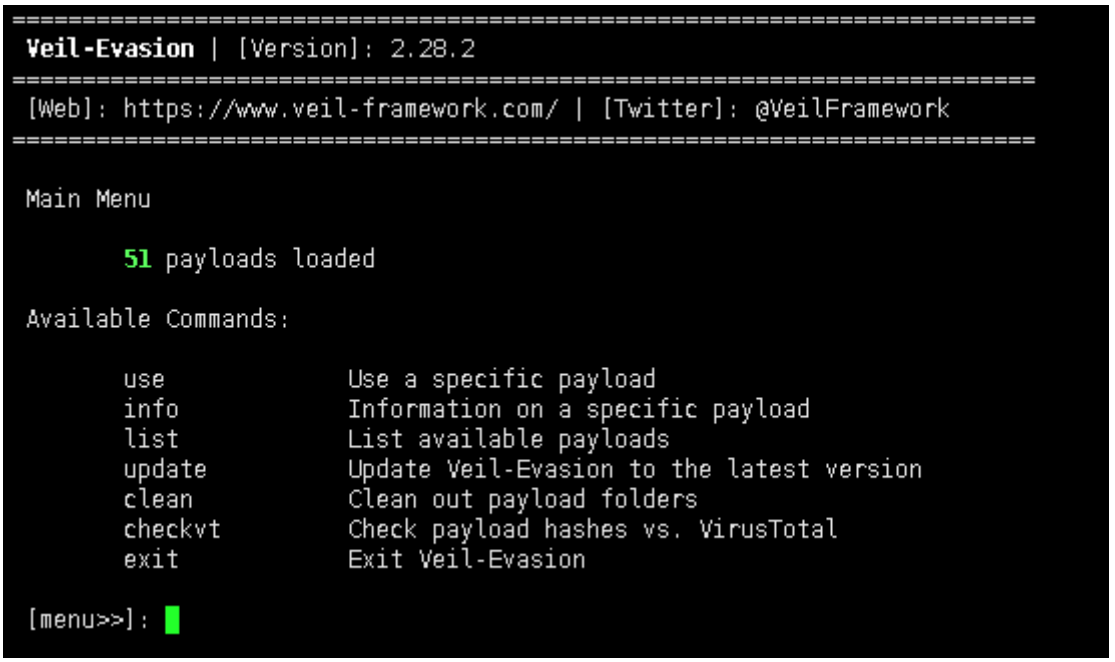
root@John:~/Deskto# git clone https://github.com/Veil-Framework/Veil-Evasion.git

```
root@John:~# 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 | 143.00 KiB/s, done.
Resolving deltas: 100% (2137/2137), done.
root@John:~#
```

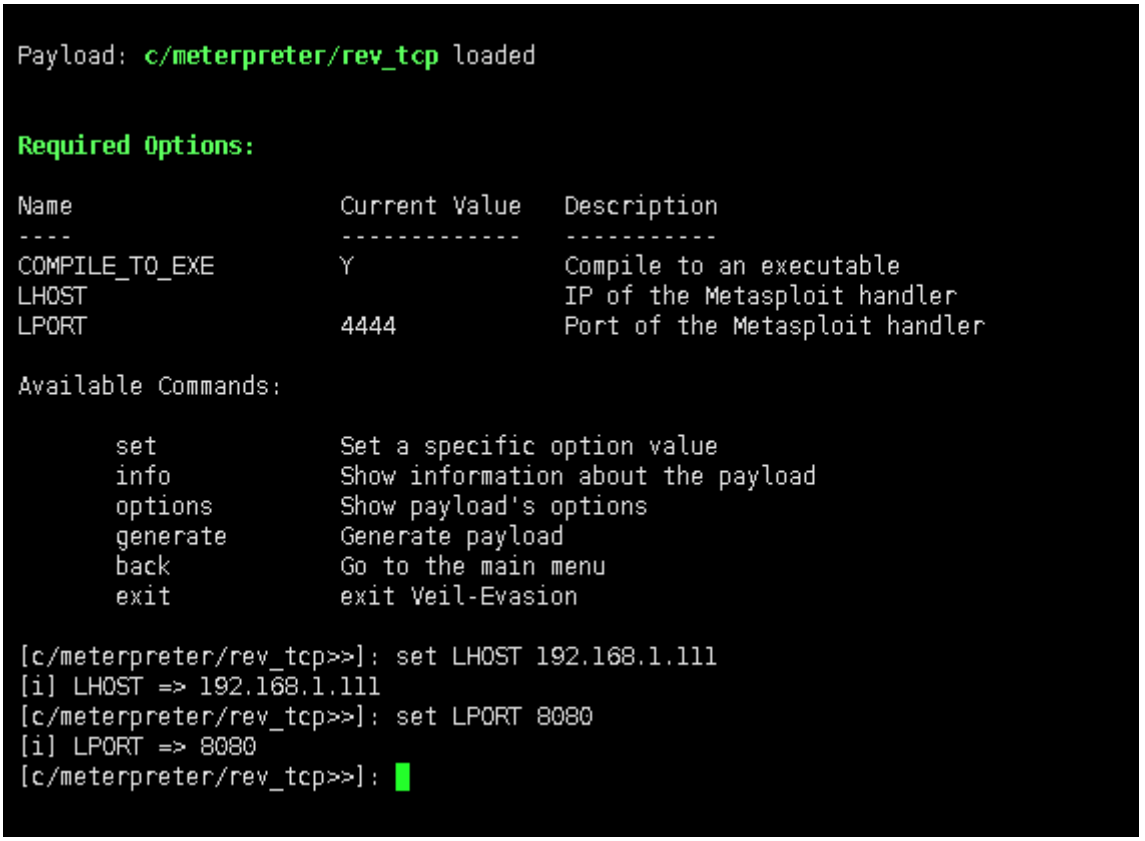
root@John:~/Veil-Evasion# ./setup.sh　//安装漫长

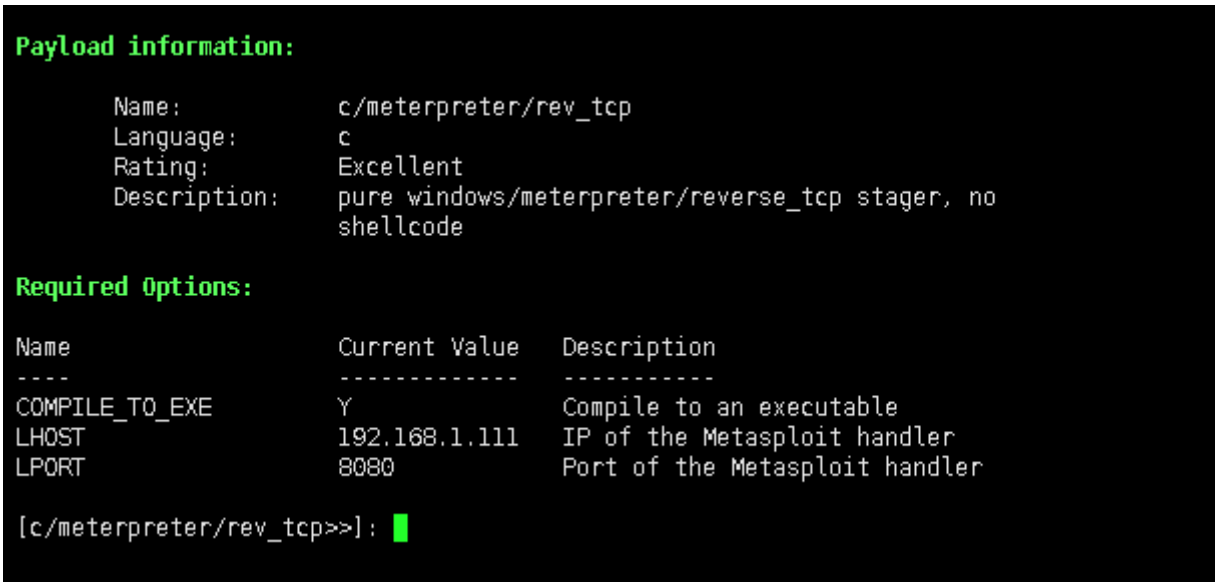
```
root@John:~/Veil-Evasion/setup# ./setup.sh
 ================================================================================
=
             Veil-Evasion (Setup Script) | [Updated]: 2016-09-09
 ================================================================================
=
  [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ================================================================================
=

 [I] Kali Linux "2017.1" x86_64 detected...

 [?] Are you sure you wish to install Veil-Evasion?

     Continue with installation? ([y]/[s]ilent/[N]o): y

 [*] Initializing package installation

 [*] Adding x86 architecture to x86_64 system for Wine
```

```
Setting up libpangoft2-1.0-0:i386 (1.40.12-1) ...
Setting up libxcb-sync1:i386 (1.12-1) ...
Setting up libsndfile1:i386 (1.0.28-4) ...
Setting up i965-va-driver:amd64 (2.0.0+dfsg1-1) ...
Setting up i965-va-driver:i386 (2.0.0+dfsg1-1) ...
Setting up python-gdal (2.2.2+dfsg-1) ...
Setting up libqgis-core2.14.20 (2.14.20+dfsg-1) ...
Setting up libldap-2.4-2:amd64 (2.4.45+dfsg-1) ...
Setting up libldap-2.4-2:i386 (2.4.45+dfsg-1) ...
Setting up libswscale4:amd64 (7:3.4-3) ...
Setting up mesa-va-drivers:amd64 (17.2.5-1) ...
Setting up mesa-va-drivers:i386 (17.2.5-1) ...
Setting up libpostproc54:amd64 (7:3.4-3) ...
Setting up libxcomposite1:i386 (1:0.4.4-2) ...
Setting up libxcb-shm0:i386 (1.12-1) ...
Setting up libxrender1:i386 (1:0.9.10-1) ...
Setting up libqgis-gui2.14.20 (2.14.20+dfsg-1) ...
Setting up libavahi-client3:amd64 (0.7-3) ...
Setting up libavahi-client3:i386 (0.7-3) ...
Setting up libkrb5-3:amd64 (1.15.2-2) ...
Setting up libkrb5-3:i386 (1.15.2-2) ...
Setting up libegl-mesa0:amd64 (17.2.5-1) ...
Setting up libwine:amd64 (2.0.3-1) ...
Setting up gdal-bin (2.2.2+dfsg-1) ...
Setting up libglx-mesa0:amd64 (17.2.5-1) ...
Setting up pulseaudio (11.1-1) ...
Installing new version of config file /etc/pulse/daemon.conf ...
Installing new version of config file /etc/xdg/autostart/pulseaudio.desktop ...
Setting up libgstreamer-plugins-base1.0-0:i386 (1.12.3-1) ...
Setting up libpango1.0-0:amd64 (1.40.12-1) ...
Setting up librsvg2-2:amd64 (2.40.18-2) ...
Setting up libavresample3:amd64 (7:3.4-3) ...
```



以c/meterpreter/rev_tcp为例：





ps:Veil-Evasion不在更新，新版本项目地址：https://github.com/Veil-Framework/Veil

附录：

[*] 可支持生成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

21) perl/shellcode_inject/flat

22) powershell/meterpreter/rev_http
23) powershell/meterpreter/rev_https
24) powershell/meterpreter/rev_tcp
25) powershell/shellcode_inject/download_virtual
26) powershell/shellcode_inject/download_virtual_https
27) powershell/shellcode_inject/psexec_virtual
28) powershell/shellcode_inject/virtual

29) python/meterpreter/bind_tcp
30) python/meterpreter/rev_http
31) python/meterpreter/rev_http_contained
32) python/meterpreter/rev_https
33) python/meterpreter/rev_https_contained
34) python/meterpreter/rev_tcp
35) python/shellcode_inject/aes_encrypt
36) python/shellcode_inject/aes_encrypt_HTTPKEY_Request
37) python/shellcode_inject/arc_encrypt
38) python/shellcode_inject/base64_substitution
39) python/shellcode_inject/des_encrypt

40) python/shellcode_inject/download_inject
41) python/shellcode_inject/flat
42) python/shellcode_inject/letter_substitution
43) python/shellcode_inject/pidinject
44) python/shellcode_inject/stallion

45) ruby/meterpreter/rev_http
46) ruby/meterpreter/rev_http_contained
47) ruby/meterpreter/rev_https
48) ruby/meterpreter/rev_https_contained
49) ruby/meterpreter/rev_tcp
50) ruby/shellcode_inject/base64
51) ruby/shellcode_inject/flat

- Micropoor