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:~/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:~/Veil-Evasion# ./setup.sh //安装漫长

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