 经常有人问我这个问题“ 怎样进入内网 ”，怎么回答呢，归纳起来就是一句话“ 突破网关，利用端口重定向进入内网 ”。 首选要突破网关（GetWay），这很容易理解，因为一个内网要访问internet总是必然通过网关接入的，至于怎样突破网关，这和进入不是网关的服务器没有什么两样，就不说了。 突破网关以后，我们的目标就是通过网关（IP为202.98.*.*）上网的192.168.21.75.以后的方法就是在网关力端口重定向，建立包转发。端口重定向分两种（local和remote），但是我们要进而内网，显然不能用local方式的重定向，local方式的重定向主要用来绕过_blank">防火墙（关于这个问题我将在随后单独写一篇文章来讨论怎样用端口重定向绕过_blank">防火墙）。 一、利用Fpipe建立端口重定向。 Fpipe是个非常有趣的东东。为了证明Fpipe的端口重定向功能，我们来做这样的试验。 首先在自己的机器上运行Fpipe，如下： E：toolFPip>fpipe -l 80 -s 90 -r 80 202.98.177.162 FPipe v2.1 - TCP/UDP port redirector. Copyright 2000 （c） by Foundstone， Inc. http://www.foundstone.com //解释一下这个命令 fpipe -l 80 -s 90 -r 80 202.98.177.162 将到本机80端口的连接通过90端口连接到202.98.177.162的80端口。 一下是详细语法： FPipe [-hv ？ ] [-brs ] IP - ？/-h - shows this help text -c - maximum number of allowed simultaneous connections. Default is 32 #连接的最大数目，默认是32 -l - listening port number #要监听的TCP端口号 -r - remote TCP port number #要

定向到的IP主机的端口号 -s - outbound connection source port number #从哪个端口发出重定向信息 -v - verbose mode #详细显示过程 在上面的过程中，我们在自己的机器上建立了端口重定向：将到本机80端口的连接通过90端口连接到202.98.177.162的80端口 然后我们在浏览器中输入：http://127.0.0.1，结果发现昆明高新区的网页打了，这说明我们的重定向成功。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com