使用反向连接突破Tcp_Ip限制的过程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/294/2021_2022__E4_BD_BF_E7_94_A8_E5_8F_8D_E5_c67_294539.htm 大家在搞unicode的时候有没有发现有时会tftp失败，说是对方主机强制关闭了一个远程连接，这种情况一般是对方管理员作了tcp/ip限制或者安了防火墙的缘故，我昨天经过试验，找到了一种突破这种限制的方法 工具：snake的idq溢出（要00016版的） nc.exe(必备） 过程： 1、如果你有自己的ip,就在cmd窗口里切换到nc的目录，输入 nc -l -p 813 这条命令的意思是打开813端口接收连接，端口可以自己改，不过下面的813也要改成你改的端口 2、在idq溢出程序里选那个溢出成功后主动连接到 ip填自己的，端口是813 3、如果cmd窗口里出现了对方的目录，那你就成功了 把idq溢出程序里的绑定命令改成cmd.exe，再溢出一次就可以了 4、这样，你就轻松得到了对方主机的system权限。 5、这样的机子一般有一定的背景，安个arpsniffer，接着开始渗透攻击，看看能不能控制内网。（我昨天搞的那台英国的内网实在是不小，哈哈）。渗透攻击下次再说吧 因为unicode的主机最多也就是sp2，所以尽管溢出，溢出程序可以支持到sp2,不过不排除对方删除isapi映射的可能性 