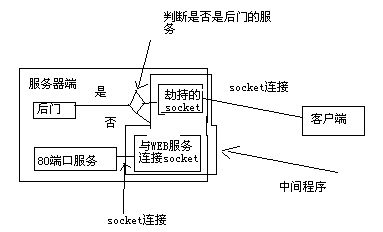
端口复用在黑客后门程序中十分重要,当你侵入一台服务器时,这台服务器如果安装了防火墙,则使用一般的后门程序时,后门程序使用的是防火墙禁止的端口,则可以通过复用防火墙允许的端口来与后门程序进行数据交流,比如一个服务器有WEB服务,我们可以通过复用80端口.

原理图如下:

[](http://img.bimg.126.net/photo/-2ZN2GAlEjNCpVj7GNyQyg==/4570872146805495959.jpg)

        复制端口的原理是用在服务器安装一个中间程序,在客户端发送数据给端口前劫获这个数据,判断这个是不是HACKER发来的数据,如果是把它发给后门程序,如果不是则转发给端口程序,返回信息再发给客户端.所以中间程序即是一个服务端程序(监听连接)也是一个客户端程序(发送给端口程序).要复用端口,必须使中间程序的监听SOCKET用setsockopt()函数设置.