**基于ring0层的端口复用**

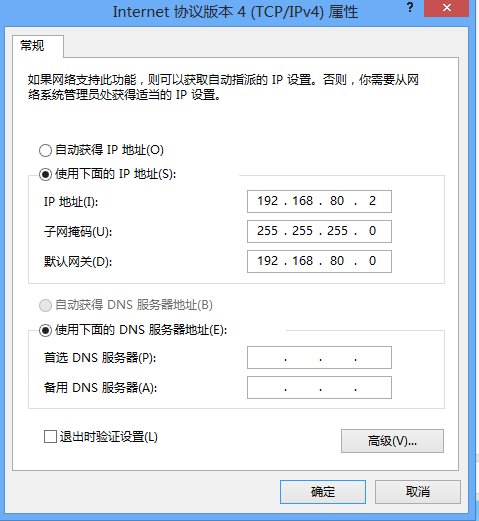
原理：

Ring3层中，服务器再启动时会调用socket的listen函数持续监听是否有客户端与主机进行连接，在监听到链接信号以后，会调用accept函数接收套接字并返回数据（包含端口信息）。在ring0层中，调用listen后服务器会调用TDI\_EVENT\_CONNECT注册回调函数。一旦监听到，便会调用回调函数，并在回调函数中组建TDI\_ACCEPT消息并继续往底层发送，在完成函数取得远程机器的套接字返回到ring3层。所以如果在注册TDI\_EVENT\_CONNECT函数时对该函数进行hook并且在调用过原函数以后获取该套接字，便可以利用这个端口进行数据的传输。

实验环境：

虚拟机（主机）：windows 8.1 x64 有appache服务器 连接方式使用host-only模式

Ip地址：192.168.80.2



客户端：windows 8 x64

Ip地址：192.168.80.3

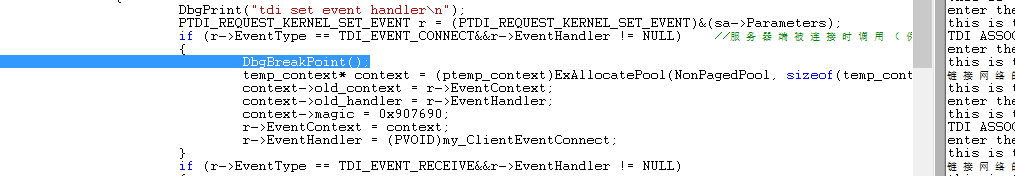


Demo程序：

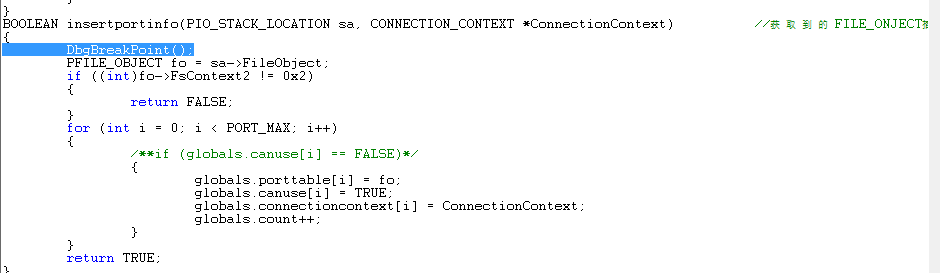
1. TDI底层驱动，负责对回调函数进行hook，收到的端口对象进行拦截并存储，和组包发送数据。
2. 客户端连接，负责连接到服务器，接收服务器返回的数据
3. 服务器返回数据，打开TDI的控制设备，利用已经拦截并保存的端口组建包并发出去。

使用方法：

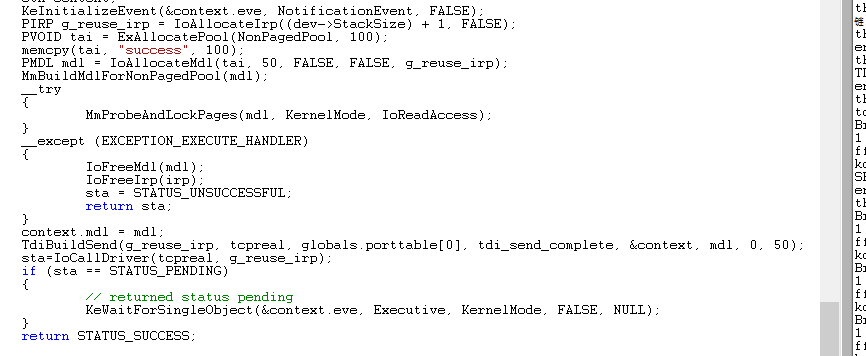
1.安装TDI驱动，并打开appache,程序对注册回调函数进行hook



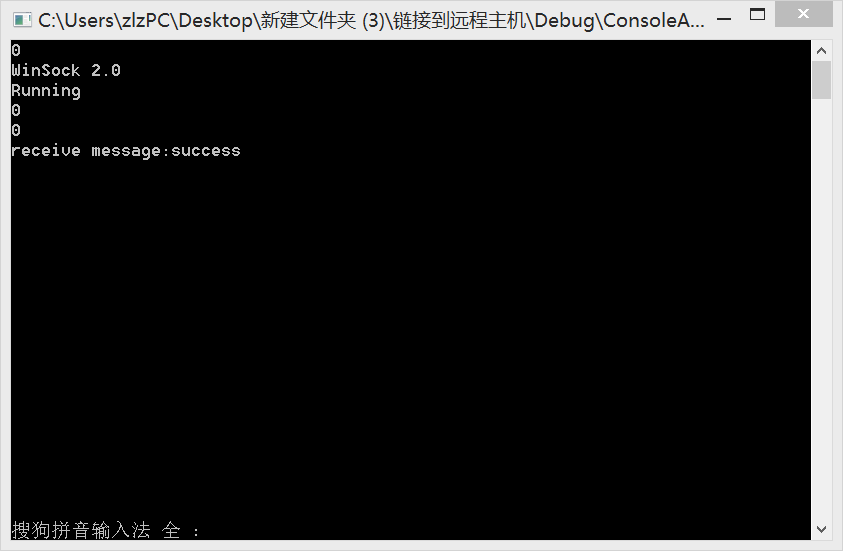
2.在客户端上运行链接到主机程序，调用hook函数，并在完成原回调函数后对acceptirp（端口以及远程主机信息）进行保存



3.运行服务器返回数据，服务器端会根据已经保存好的链接端口，向客户端发送数据（success！）。



4.客户端接收服务器发送的数据并显示



存在的问题：

1. 必须在加载驱动以后加载appache才有效果
2. 在服务器返回数据时如果关机会因为pending没有取消产生蓝屏（DRIVER\_UNLOADED\_WITHOUT\_CANCELLING\_PENDING\_OPERATIONS）