IDA 6.1 调试驱动

By obaby

火星信息安全研究院 http://www.h4ck.org.cn

今天在测试的时候发现 IDA 5.5 可以启动 windbg 调试器，而 IDA 6.0 却无法启动 windbg 调试器。大体看了一下可能是由于搜索路径造成的，重新将 windbg 安装到 program files 下之后问题就结局了。

网上也有关于用 IDA 调试驱动的文章，这里只是再整理一下，用 IDA 载入驱动分析完成之后选择调试器为 Windbg debugger，如图 1 所示：

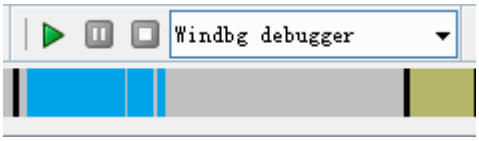

图 1

然后执行菜单中的 Debugger->Debugger options 打开如图 2 所示的设置窗口。

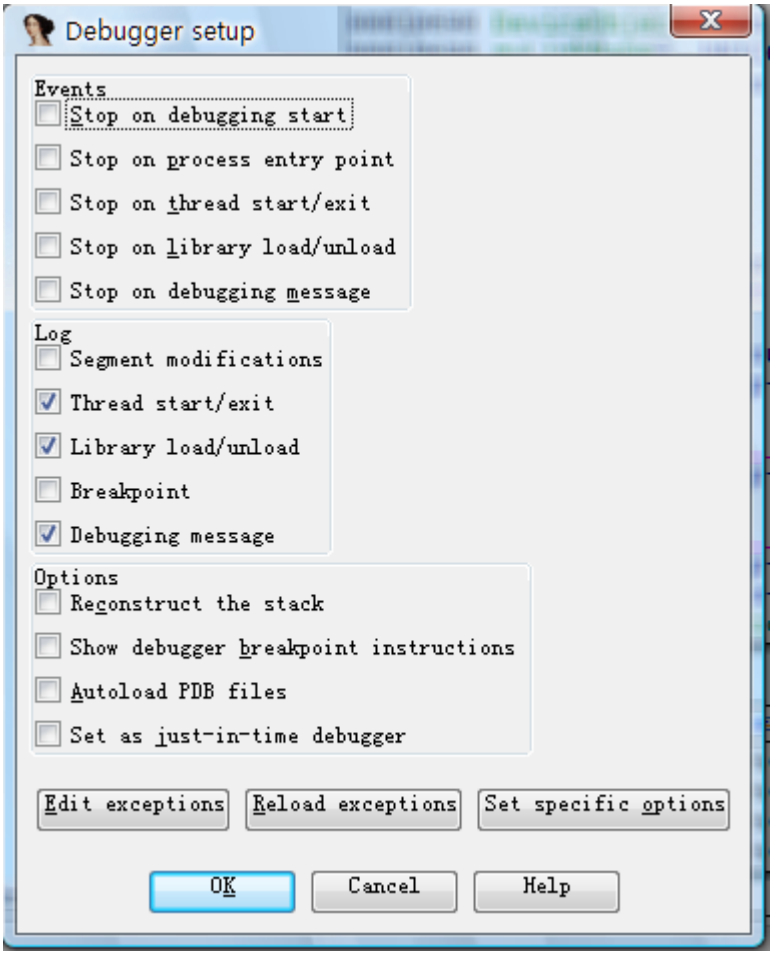

图 2

点击 Set specific options 打开特殊选项窗口，如图 3 所示：

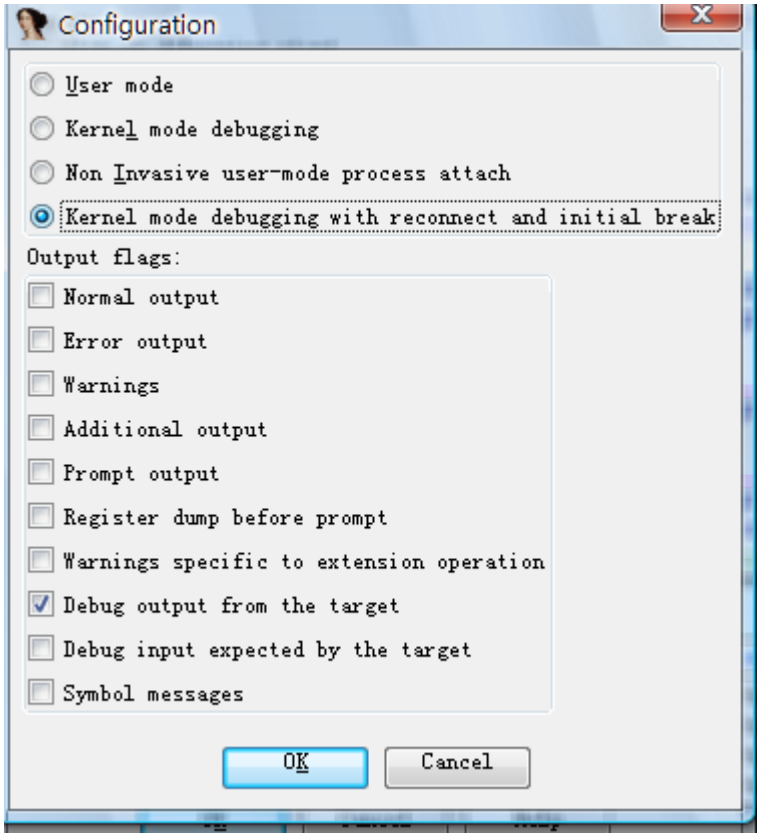

图 3

将最上方的默认 user mode 修改为 Kernel mode debugging 或者 kernel mode debugging with reconnect and initial break，至于两个选项的区别读者可以自行测试一下，这里就不说废话了，按照字面意思理解即可。设置完成后关闭设置窗口，然后执行菜单中的 Debugger->Process options 打开进程选项设置窗口，在 Connet string 中输入要连接的字符串，也就是 com 接口的名称，这里是 com:port=\\.\pipe\com_1,baud=115200,pipe，如图 4 所示。

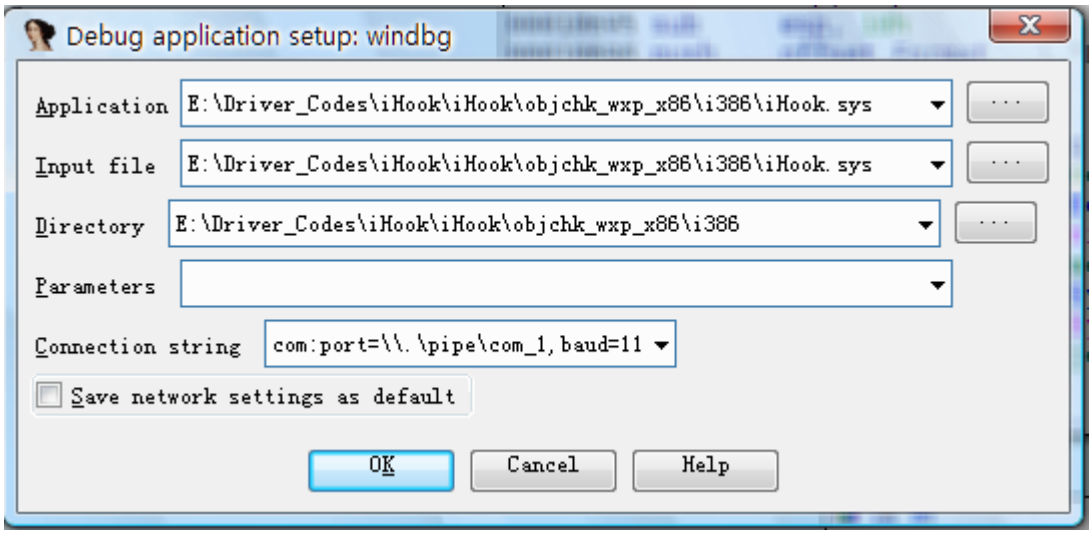

图 4

设置完成后关闭设置窗口，执行菜单中的 Debugger->Attach Process，打开进程附加窗口，如图 05 所示。

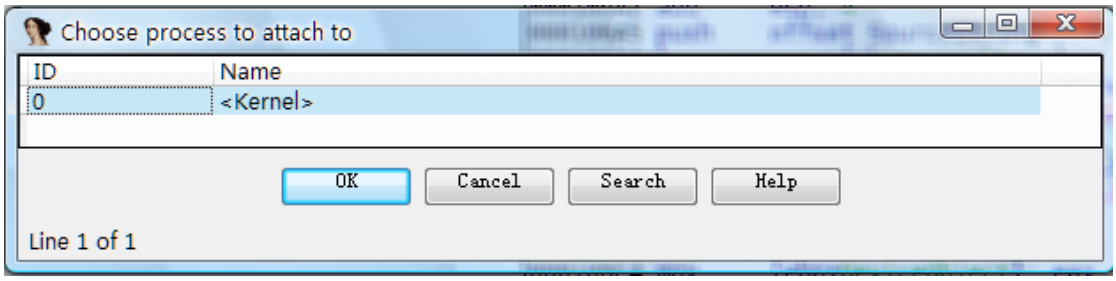

图 5

附加之后等待符号库加载完就可以进行调试了。调试器挂在之后如果没有意外会中断在第一个 int3 断点，如图 6 所示。

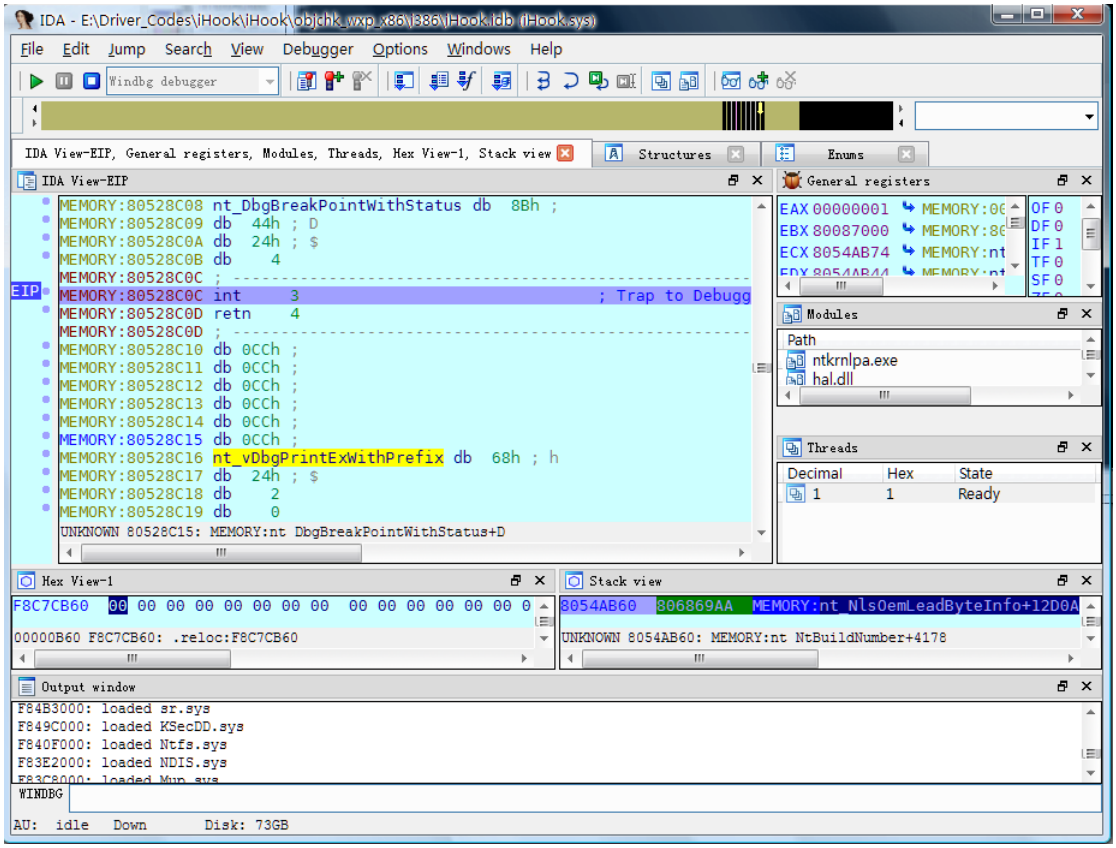

图 6

现在就可以对驱动进行设置断点和调试了，效果如图 7 所示：

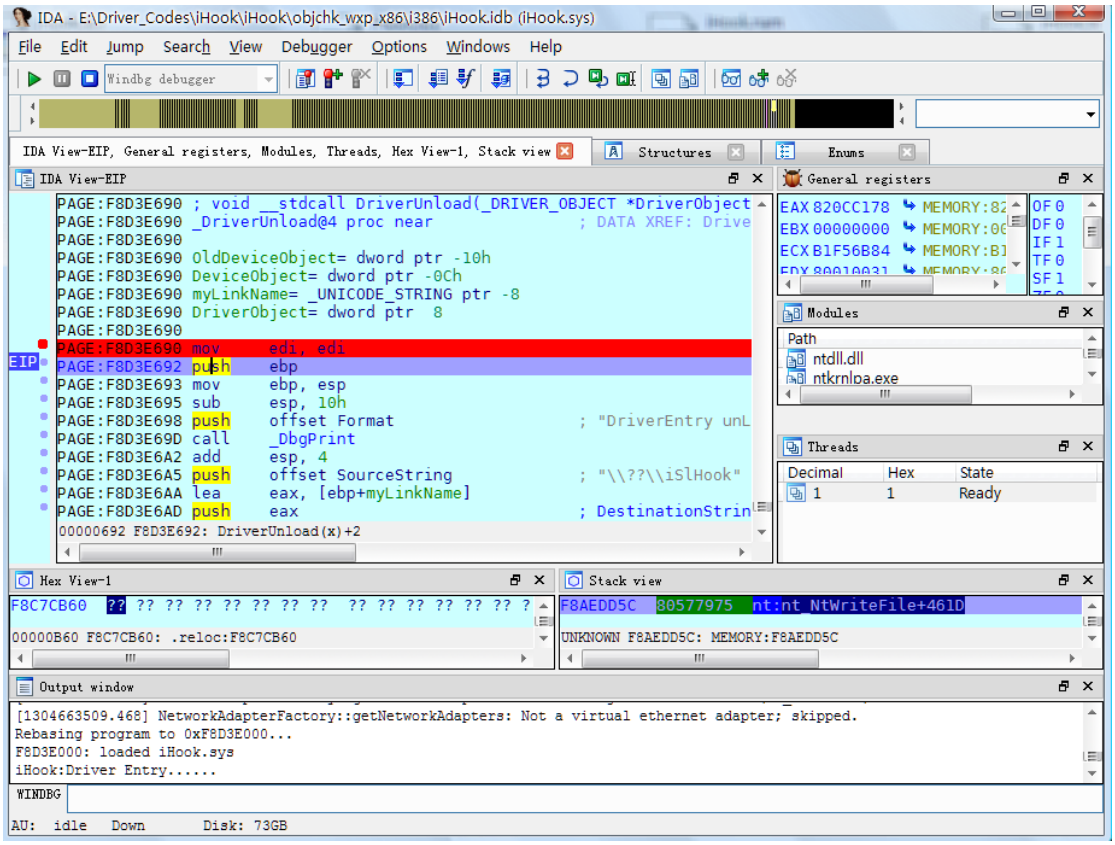

图 7

在调试之前为了使程序的断点能够中断需要修正 Process options 选项中的部分参数，如图 8 所示。

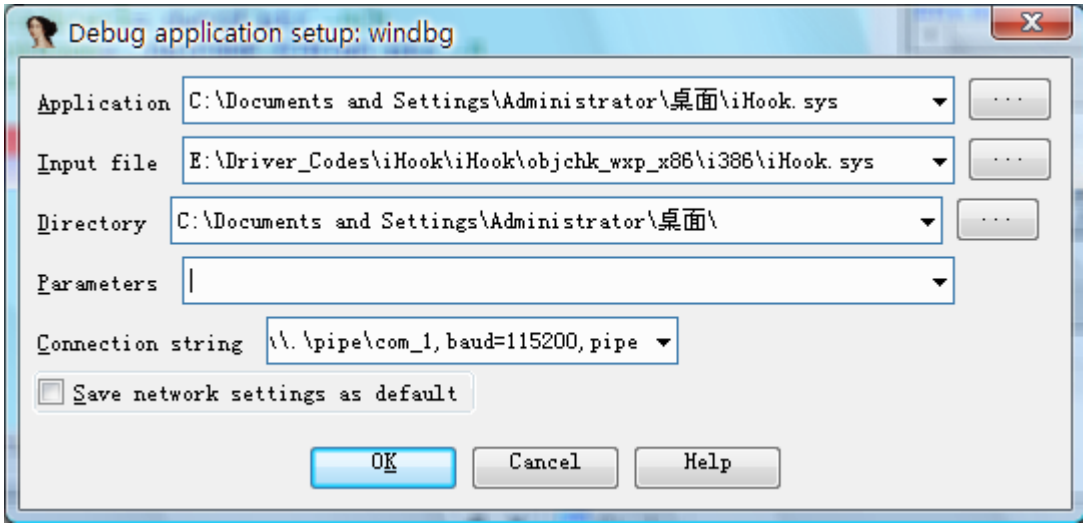

图 8

需要将 Application 修改为程序在远程目标机器上的路径，另外 Directory 同样需要修改为远程系统的目录。否则在调试的过程中如果设置断点将会询问本地文件与远程文件是否一样，并且设置的断点将无法触发。

如果使用 IDA 5.5 设置方法是类似的，与上一篇文章《IDA 调试内核》http://www.h4ck.org.cn/2011/05/kernel-debugging-with-ida-pro/ 不同的是本文的调试没有使用第三方的工具，并且实现方法也比较简单。如果调试没有源码的驱动用 IDA 应该会更直观

一些吧，如果有源码的话还是使用 Windbg 更好一些。

注意：

需要注意的是前提已经配置好了 Windbg 的远程调试，否则使用 IDA 是无法连接虚拟机进行调试的，设置方法可以参考下面的连接：

Windows 7：http://www.h4ck.org.cn/2010/11/win7-remote-debug-via-windbg/

Windows XP：http://www.h4ck.org.cn/2009/09/driverdevelop1/