

四、 体验 NewBluePill

首先介绍下我的平台，在整个项目中我用了两台计算机

PC1（调试机）：Intel Core 2 6300, 1G RAM, XP SP2(X32)+windbg+WDK6001.18001

PC2（运行机）：Intel Core 2 6300, 1G RAM, Windows Server 2008 Beta 1(X64),NewBluePill
（以下简称 nbp）只能运行于这台机器上。

1) 编译 NewBluePill

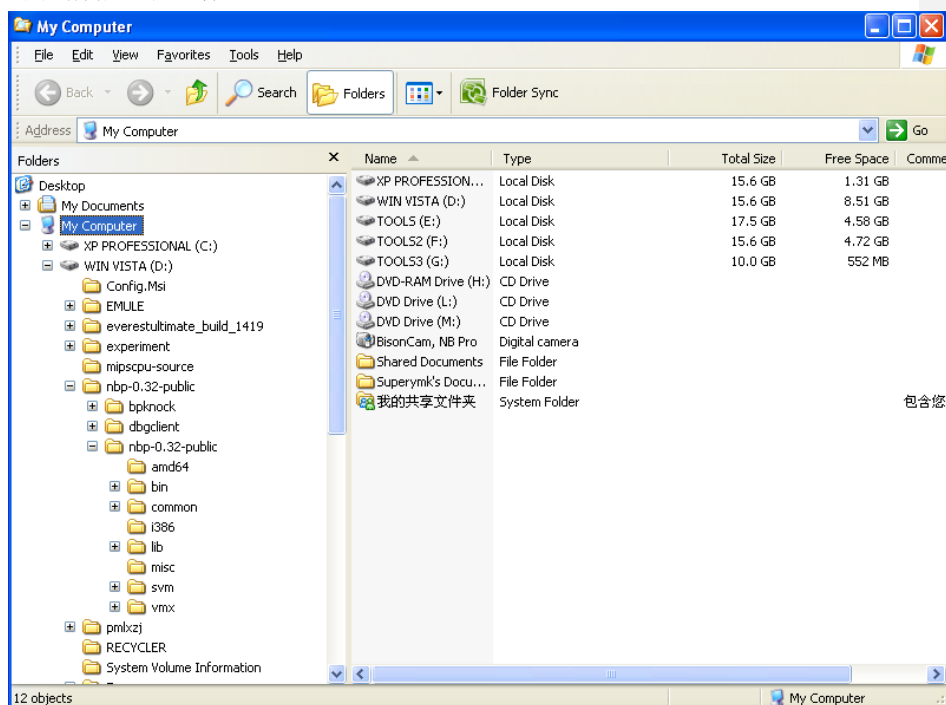
了解了以上那么多，是不是很想亲自动手尝试下呢？不过先别急，还是先把工具准备好再说。

工具一共有下面几个：

1. Windbg
2. DebugView 到 <http://download.sysinternals.com/Files/DebugView.zip> 下载
3. InstDrv 到 <http://dl2.csdn.net/fd.php?i=23314208212665&s=0affa2ecb56fc0dcc14cff07345a388e> 下载
4. Windows Driver Kits (WDK 6001.18001)

总体来说编译 NewBluePill 的过程很简单。

步骤 1. 首先确保手上有 nbp-0.32-public.zip 这个代码。没有的可以去 <http://www.bluepillproject.org/> 上去下载，然后解压缩到一个根目录，在这里我们假设是 D 盘。目录结构应该是这样的：

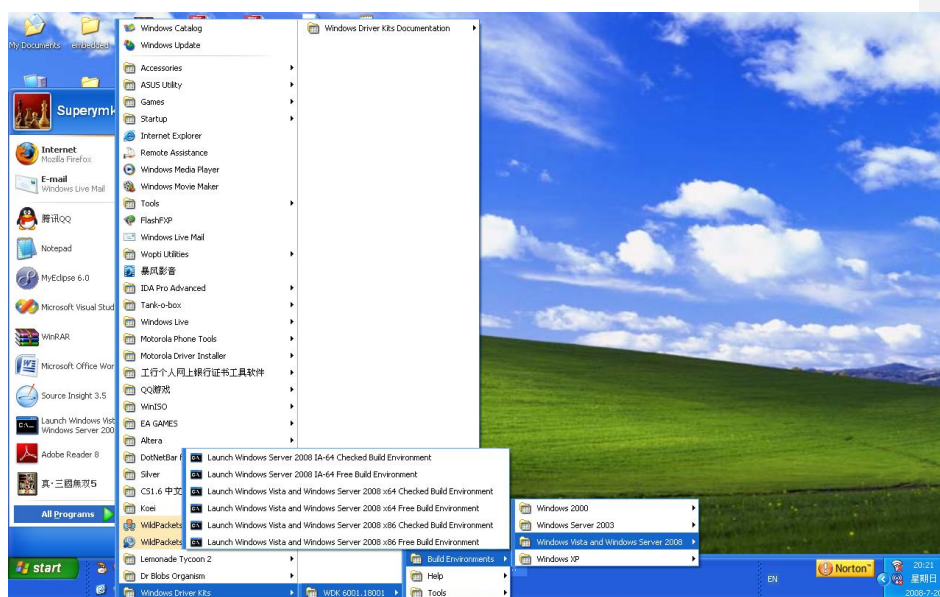


步骤 2. 然后为了后面的调试过程中可以下断点（切记做这一步只是为了以后能够调试，

并且只能运行在操作系统的 debug 模式下, 如果只是想直接观看效果, 可以跳过这一步), 修改下 common 目录下的 newbp.c 文件, 在 DriverEntry 方法的一开始添加 CmDebugBreak() 方法调用, 修改后的代码如下:

```
NTSTATUS DriverEntry (
    PDRIVER_OBJECT DriverObject,
    PUNICODE_STRING RegistryPath
)
{
    NTSTATUS Status;
    CmDebugBreak();
#ifdef USE_COM_PRINTS
    PioInit ((PUCHAR) COM_PORT_ADDRESS);
#endif
    ComInit ();
    .....
}
```

步骤 3. 然后打开 Launch Windows Vista and Windows Server 2008 x64 Checked Build Environment 编译环境:



步骤 4. 在该编译环境中执行 nbp-0.32-public\nbp-0.32-public\build_code.cmd, 如果编译成功则会出现以下窗口:

```

1>Compiling - vmx\vmxdebug.c
2>Building Library - lib\amd64\svm.lib
1>Building Library - lib\amd64\vmx.lib
1>BUILD: Compiling and Linking d:\nbp-0.32-public\nbp-0.32-public\common directory
1>Assembling - amd64\msr.asm
1>Assembling - amd64\svm-asm.asm
1>Assembling - amd64\vmx-asm.asm
1>Assembling - amd64\common-asm.asm
1>Assembling - amd64\regs.asm
1>Assembling - amd64\cpuid.asm
1>Assembling - amd64\instubs.asm
1>Compiling - common\newbp.c
1>Compiling - common\hvm.c
1>Compiling - common\portio.c
1>Compiling - common\comprint.c
1>Compiling - common\hypercalls.c
1>Compiling - common\traps.c
1>Warnings in directory d:\nbp-0.32-public\nbp-0.32-public\common
1>d:\nbp-0.32-public\nbp-0.32-public\common\traps.c : warning C4819: The file contains a character that cannot be represented in the current code page (936). Save the file in Unicode format to prevent data loss
1>Compiling - common\interrupts.c
1>Compiling - common\common.c
1>Compiling - common\paging.c
1>Compiling - common\snprintf.c
1>Compiling - common\chicken.c
1>Compiling - common\dbgclient.c
1>Linking Executable - bin\amd64\newbp.sys
BUILD: Finish time: Sun Jul 20 20:22:39 2008
BUILD: Done

30 files compiled - 2 Warnings
2 libraries built
1 executable built

D:\nbp-0.32-public\nbp-0.32-public>ctags -R
'ctags' is not recognized as an internal or external command,
operable program or batch file.

D:\nbp-0.32-public\nbp-0.32-public>

```

如果看到这个提示，恭喜你，编译成功了！

2) 演示 NewBluePill

运行 nbp 就有一定要求了，首先要求必须运行在支持虚拟技术（HVM）的 CPU 上，并且推荐在 64 位或者支持虚拟 64 位技术的 CPU 上运行，原因是虽然 nbp 程序中附带了支持 32 位 CPU 的代码，但是有几个函数在编译时（Vista x86 Checked Mode）会出问题，而且有几个函数是未实现的，所以还是在 x64 上去跑吧。

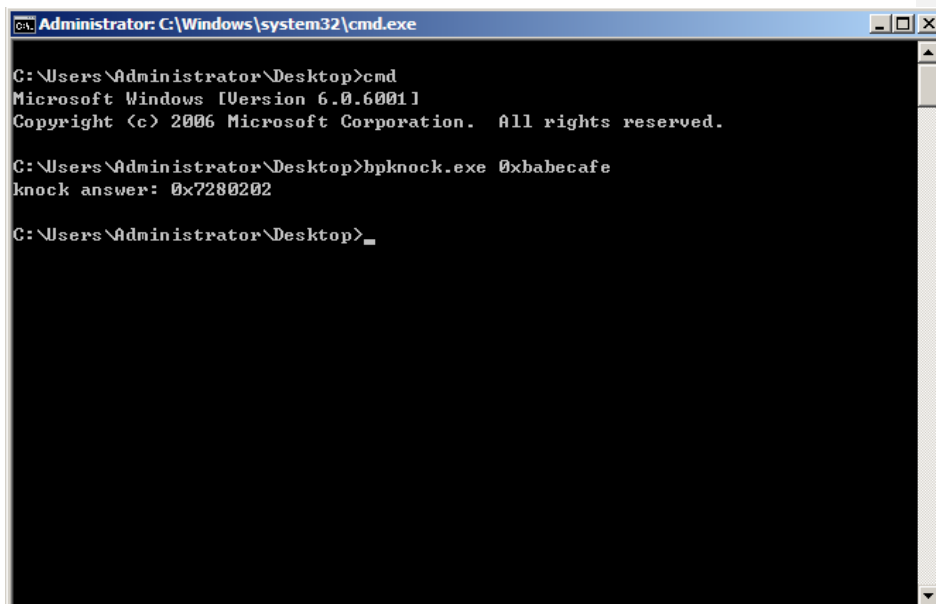
下面是详细步骤：

步骤 1：参考 Debugging Windows Vista（文章来源：http://www.microsoft.com/whdc/driver/tips/debug_vista.mspx）修改启动项和调试项（这一步只需做这一次就可以）

步骤 2：重启计算机，可以看到启动项中多了一个 DebugEntry [debugger enabled]项，选中它按 F8，然后选择 Disable Driver Signature Enforcement(切记一定要用这个模式启动，否则不能加载未签名的驱动程序)

步骤 3：去 nbp-0.32-public 主目录及其子目录内找到下面几个编译生成的二进制文件：bpknock.exe, dbgclient.sys, newbp.sys

步骤 4: 运行下 bpknock 0xbabecafe 看下没运行 nbp 的输出结果。



```
C:\Users\Administrator\Desktop>cmd
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>bpknock.exe 0xbabecafe
knock answer: 0x7280202

C:\Users\Administrator\Desktop>
```

步骤 5: 打开 DebugView, 在 DebugView 中的 Capture 菜单中选中下列项:

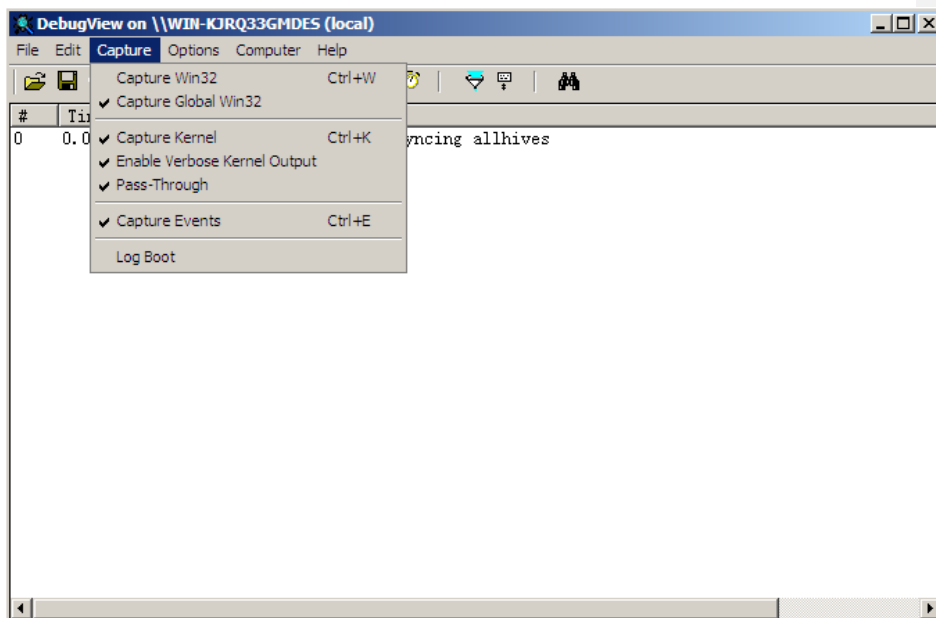
Capture Global Win32

Capture Kernel

Enable Verbose Kernel Output(这个一定要选中)

Pass-Through

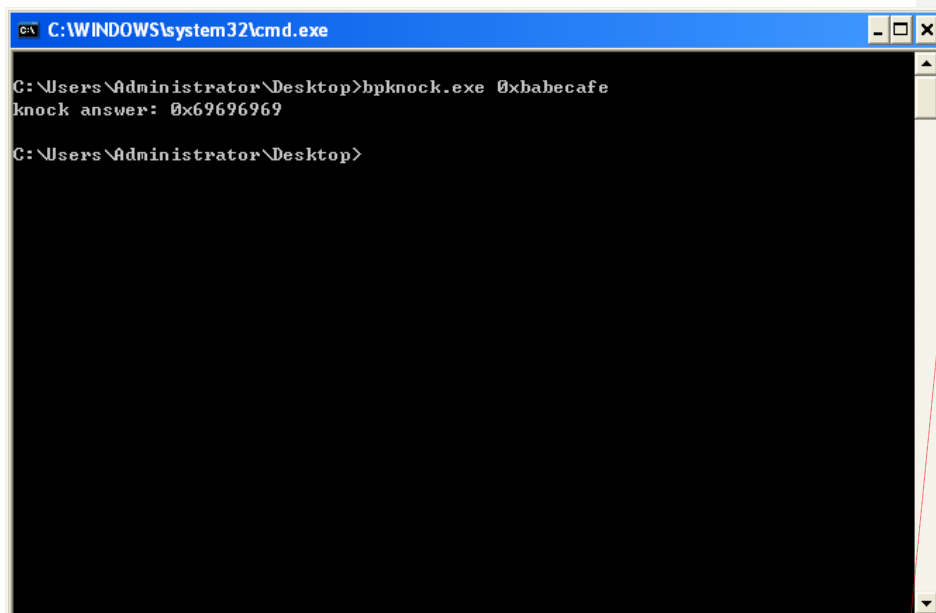
Capture Events



然后打开 InstDrv, 先安装并启动 dbgclient.sys 驱动, 再安装并启动 newbp.sys 驱动

步骤 6: 再运行下 `bpknock 0xbabecafe` 看下运行了 `nbp` 的输出结果。

注: 如果死机了那么可以把编译过程中的第 2 步去掉, 不过这样就不能调试 `nbp` 了。¹



```
C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator\Desktop>bpknock.exe 0xbabecafe
knock answer: 0x69696969
C:\Users\Administrator\Desktop>
```

批注 [S2]: 以后再把这个换成 win2k8 下面的

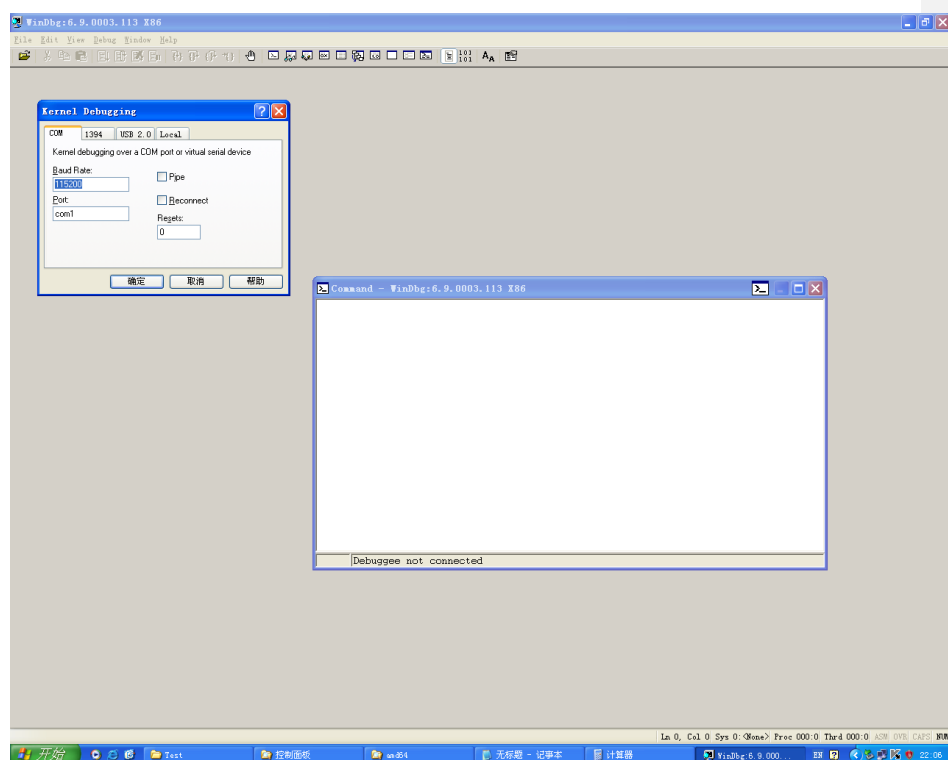
3) 调试 NewBluePill

调试 `nbp` 需要用到 WinDbg, 主要过程如下:

步骤 1: 设置 `_NT_SYMBOL_PATH` 环境变量, 指向 `newbp.pdb` 所在的目录, 用于链接符号表。

步骤 2: 启动 WinDbg, 单击 File 菜单选择 Kernel Debugging, 在弹出的对话框输入 Baud Rate 为 115200, Port 用 com1。这是由于刚才在演示过程的第一步我们用的是默认配置, 如果调试端口发生相应改变, 这里也要改。

¹ 死机的原因是插入的 `CmDebugBreak()` 函数实际上是一个 `int 3` 调用, 在非调试模式的 Windows 下, 这时这个中断的处理程序未注册, 因此执行 `int 3` 指令会死机



步骤 3: 调试机上加载 `dbgclient.sys` 和 `newbp.sys` 两个驱动，开始调试。

如果出现 `symbol` 不能被加载的情况可以试试 WinDbg 中的 `.reload` 命令，如果不行可以试试用 `.sympath` 在 WinDbg 运行时设定 `symbol` 路径，然后 `.reload` 重新加载符号表。
成功情况下的截图：

