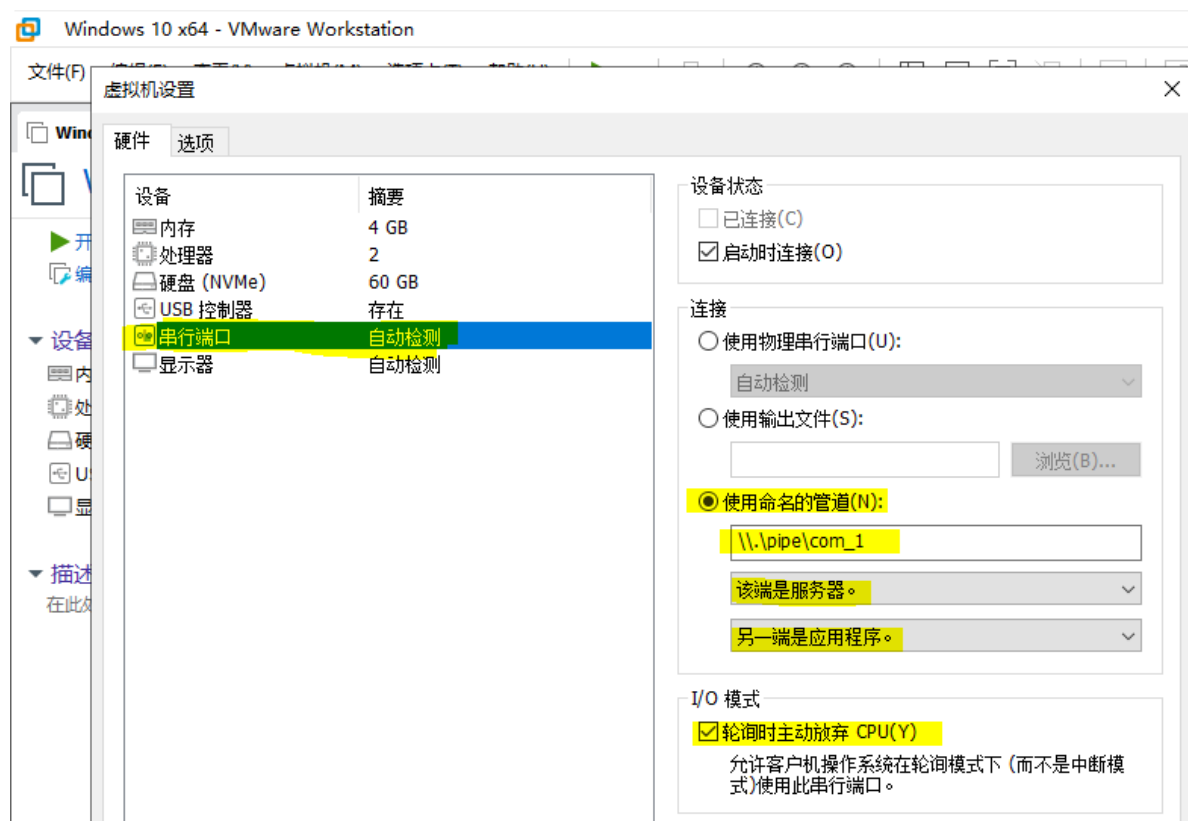


WinDBG 是在 windows 平台下，强大的用户态和内核态调试工具，相比较于 Visual Studio 它是一个轻量级的调试工具，所谓轻量级指的是它的安装文件大小较小，但是其调试功能却比VS更为强大，WinDBG由于是微软的产品所以能够调试 windows 系统的内核，另外一个用途是用来分析 dump 数据，本笔记用于记录如何开启 windows 系统内核调试功能，并使用 WinDBG 调试驱动。

1.首先需要安装 vmware 虚拟机，并自行安装好 windows 10 系统，虚拟机关闭状态下添加一个 管道虚拟串口，此处需要删除打印机，否则串口之间冲突。

操作步骤：编辑虚拟机设置 -> 添加 -> 串行端口 -> 完成

参数配置：使用命名管道 -> \\.\pipe\com_1 -> 该端是服务器，另一端是应用程序 -> 轮询时主动放弃 CPU -> 确定



2.开启虚拟机中的 windows 系统，然后以管理员身份运行CMD命令行，输入 bcdedit 命令，可以查看到系统的当前启动项，如果是新的系统，则只有 {current} 启动项以及一个 {bootmgr} 项。

```
管理员: cmd
C:\Windows\system32>
C:\Windows\system32>bcdedit

Windows 启动管理器
-----
标识符                {bootmgr}
device                partition=\Device\HarddiskVolume2
path                  \EFI\Microsoft\Boot\bootmgfw.efi
description            Windows Boot Manager
locale                zh-CN
inherit                {globalsettings}
default                {current}
resumeobject           {bdb0b3b2-3f21-11ed-9931-d46011246f28}
displayorder           {current}
toolsdisplayorder      {memdiag}
timeout                30

Windows 启动加载器
-----
标识符                {current}
device                partition=C:
path                  \Windows\system32\winload.efi
description            Windows 10
locale                zh-CN
inherit                {bootloadersettings}
recoverysequence       {bdb0b3b4-3f21-11ed-9931-d46011246f28}
displaymessageoverride Recovery
```

连续执行下方的三条命令，依次建立启动项，并激活调试模式。

```
C:\LyShark > bcdedit /set testsigning on
C:\LyShark > bcdedit -debug on
C:\LyShark > bcdedit /bootdebug on
C:\LyShark > bcdedit /set "{current}" bootmenupolicy Legacy // 修改启动方式为Legacy
C:\LyShark > bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200 // 设置串口1为调试端口波特率为115200
C:\LyShark > bcdedit /copy "{current}" /d "Debug" // 将当前配置复制到Debug启动配置
C:\LyShark > bcdedit /debug "{<新建的启动配置的标识符>}" on // 打开调试开关
```

一气呵成，但需要注意 {<新建的启动配置的标识符>} 需替换成 {bdb0b3b6-3f21-11ed-9931-d46011246f28} 标志，如下所示。

```
管理员: cmd
C:\Windows\system32>bcdedit /set testsigning on
操作成功完成。
C:\Windows\system32>bcdedit -debug on
操作成功完成。
C:\Windows\system32>bcdedit /bootdebug on
操作成功完成。
C:\Windows\system32>bcdedit /set "{current}" bootmenupolicy Legacy
操作成功完成。
C:\Windows\system32>bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200
操作成功完成。
C:\Windows\system32>bcdedit /copy "{current}" /d "Debug"
已将该项成功复制到 {bdb0b3b6-3f21-11ed-9931-d46011246f28}。
C:\Windows\system32>bcdedit /debug "{bdb0b3b6-3f21-11ed-9931-d46011246f28}" on
操作成功完成。
C:\Windows\system32>
```

3.最后查看一下当前调试配置选项，执行命令 `bcdedit /dbgsettings`，显示出使用的第一个串口，波特率为 115200bps，保持默认不需要修改。

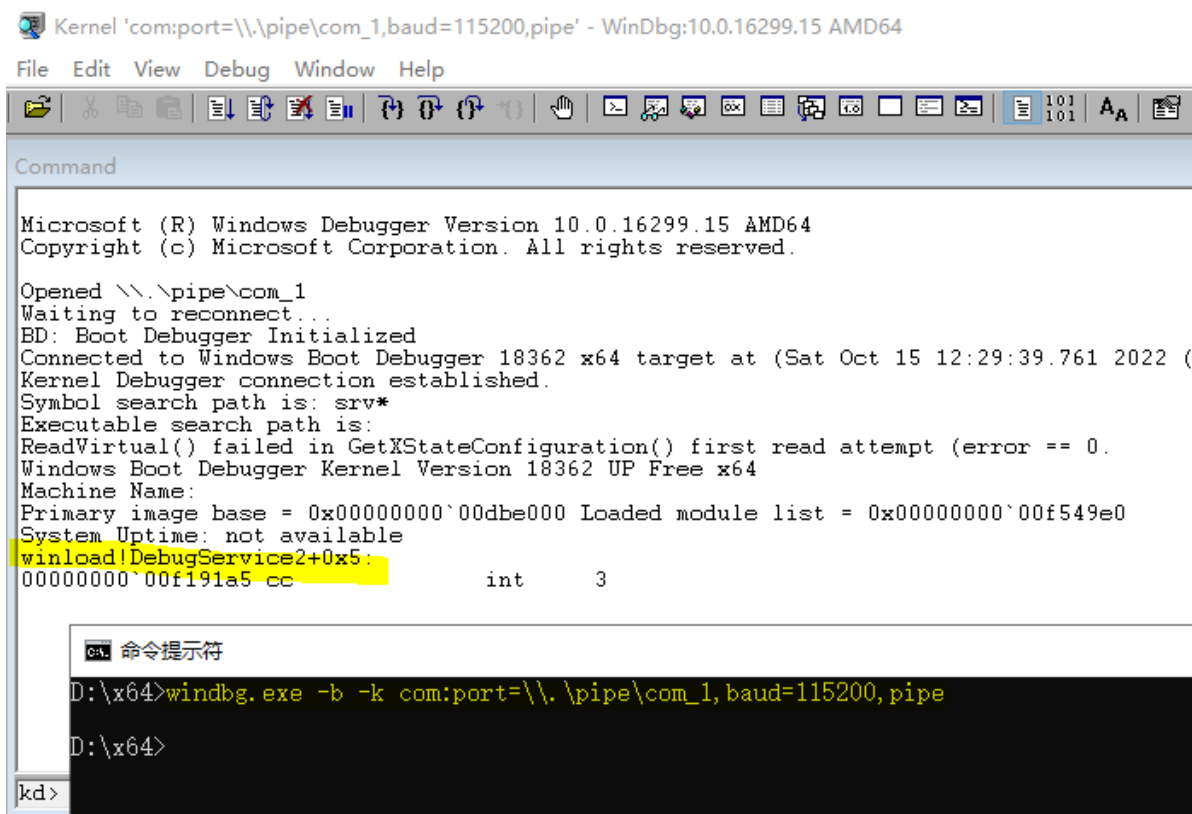
```
管理员: cmd
C:\Windows\system32>bcdedit /dbgsettings
debugtype Serial
debugport 1
baudrate 115200
操作成功完成。
C:\Windows\system32>
```

4.配置完成后,重新启动系统,在开机的时候选择 Windows10 [启用调试程序] 则系统会黑屏,说明已经正常进入调试模式了。



5.回到物理机上面,我们在命令行中切换到 WinDBG 的根目录下,并执行以下命令,即可连接虚拟机串口进行调试了。

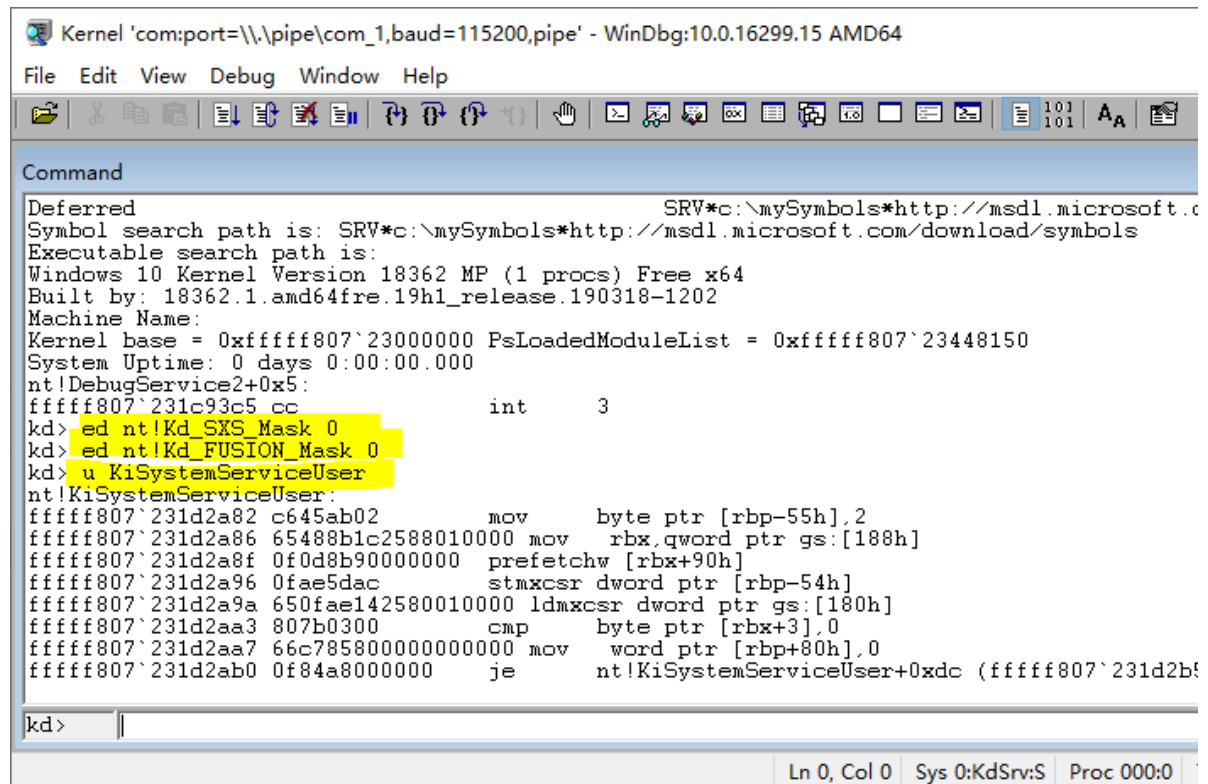
- 执行命令 `windbg.exe -b -k com:port=\\.\pipe\com_1,baud=115200,pipe` 如下图



6.至此我们还需要加载符号,在命令行下依次执行以下命令,配置好符号加载并启动系统。

```
kd> .sympath SRV*c:\mysymbols*http://msdl.microsoft.com/download/symbols
kd> .reload
kd> g
kd> g
kd> ed nt!Kd_SXS_Mask 0
kd> ed nt!Kd_FUSION_Mask 0
kd> u KiSystemServiceUser
```

这样即可完成配置操作。



The screenshot shows the WinDbg interface with the title bar 'Kernel 'com:port=\\.\pipe\com_1,baud=115200,pipe' - WinDbg:10.0.16299.15 AMD64'. The menu bar includes File, Edit, View, Debug, Window, and Help. The toolbar contains various icons for file operations, debugging, and viewing. The Command window shows the following text:

```
Deferred SRV*c:\mySymbols*http://msdl.microsoft.com/download/symbols
Symbol search path is: SRV*c:\mySymbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 18362 MP (1 procs) Free x64
Built by: 18362.1.amd64fre.19h1_release.190318-1202
Machine Name:
Kernel base = 0xfffff807`23000000 PsLoadedModuleList = 0xfffff807`23448150
System Uptime: 0 days 0:00:00.000
nt!DebugService2+0x5:
fffff807`231c93c5 cc int 3
kd> ed nt!Kd_SXS_Mask 0
kd> ed nt!Kd_FUSION_Mask 0
kd> u KiSystemServiceUser
nt!KiSystemServiceUser:
fffff807`231d2a82 c645ab02 mov byte ptr [rbp-55h],2
fffff807`231d2a86 65488b1c2588010000 mov rbx,qword ptr gs:[188h]
fffff807`231d2a8f 0f0d8b9000000000 prefetchw [rbx+90h]
fffff807`231d2a96 0fae5dac stmxcsr dword ptr [rbp-54h]
fffff807`231d2a9a 650fae142580010000 ldmxcsr dword ptr gs:[180h]
fffff807`231d2aa3 807b0300 cmp byte ptr [rbx+3],0
fffff807`231d2aa7 66c78580000000000000 mov word ptr [rbp+80h],0
fffff807`231d2ab0 0f84a8000000 je nt!KiSystemServiceUser+0xdc (fffff807`231d2b5)
```

The status bar at the bottom shows 'Ln 0, Col 0 Sys 0:KdSrv:S Proc 000:0'.

7.最后我们配置测试一下调试功能，首先编写以下代码，代码中使用 DbgBreakPoint() 设置断点，将会在入口处中断。

```
#include <ntifs.h>

NTSTATUS DriverDefaultHandle(PDEVICE_OBJECT pDevObj, PIRP pIrp)
{
    NTSTATUS status = STATUS_SUCCESS;
    pIrp->IoStatus.Status = status;
    pIrp->IoStatus.Information = 0;
    IoCompleteRequest(pIrp, IO_NO_INCREMENT);

    return status;
}

VOID UnDriver(PDRIVER_OBJECT driver)
{
    DbgPrint("驱动已卸载 \n");
}

// By: LyShark
NTSTATUS DriverEntry(IN PDRIVER_OBJECT Driver, PUNICODE_STRING RegistryPath)
{
    // 初始化默认派遣函数
    NTSTATUS status = STATUS_SUCCESS;
    Driver->DriverUnload = UnDriver;
    for (ULONG i = 0; i < IRP_MJ_MAXIMUM_FUNCTION; i++)
    {
        Driver->MajorFunction[i] = DriverDefaultHandle;
    }

    // 设置断点
```

```

DbgBreakPoint();
// KdBreakPoint();
// __debugbreak();

DbgPrint("驱动已加载 \n");
Driver->DriverUnload = UnDriver;
return STATUS_SUCCESS;
}

```

当 Windows 系统加载完成以后，拖入我们的驱动文件 WinDDK.sys，并通过驱动加载工具加载运行，此时 Windows 系统会卡死，回到 WinDBG 中发现已经可以进行调试了。

