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，另外一个用途是可以用来分析 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

参数配置： 使用命名管道 ->

\\.\pipe\com\_1

CPU -> 确定

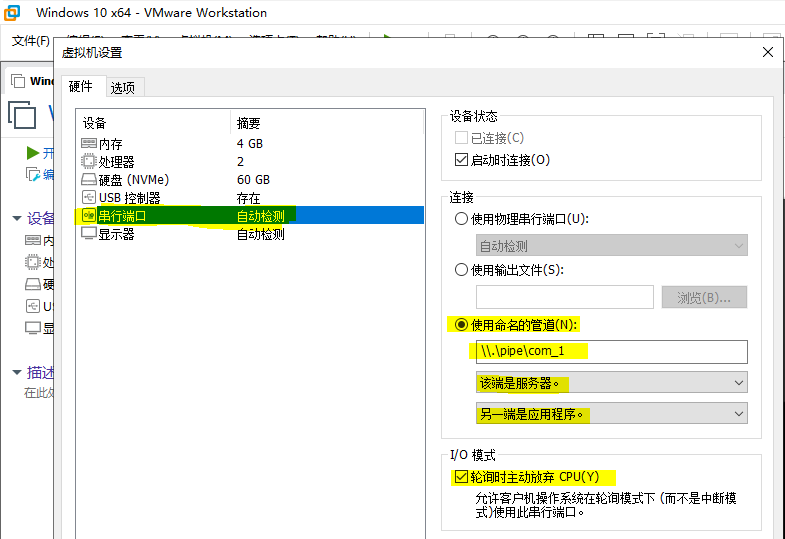
-> 完成

-> ->

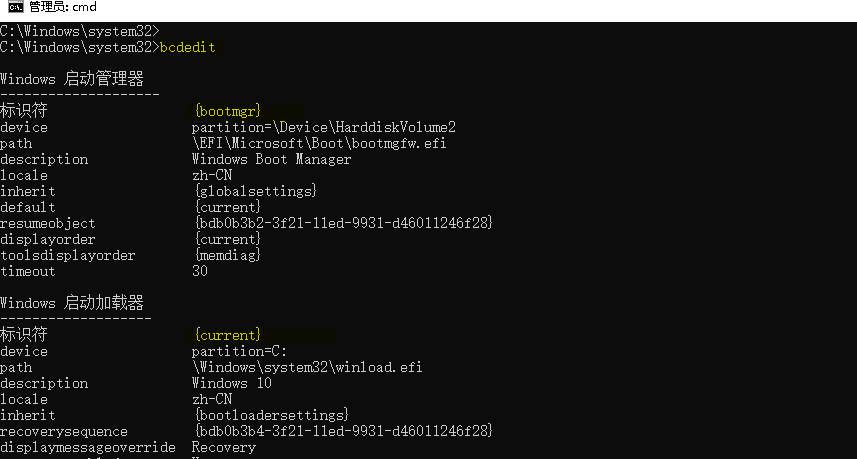
串行端口

该端是服务器，另一端是应用程序

轮询时主动放弃



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，则只会有 {current} 启动项以及一个 {bootmgr} 项。



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

动方式为Legacy

// 修改启

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"

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

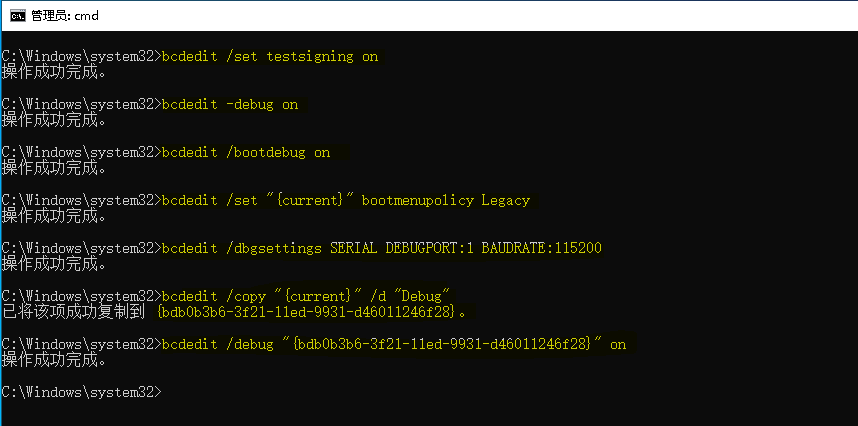
开关

// 将当前

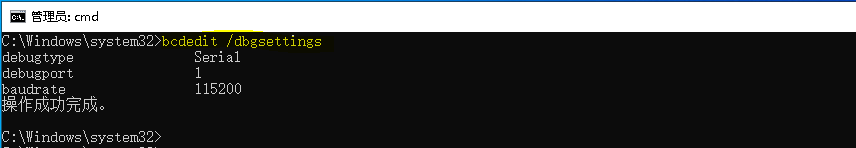
// 打开调试

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。



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。



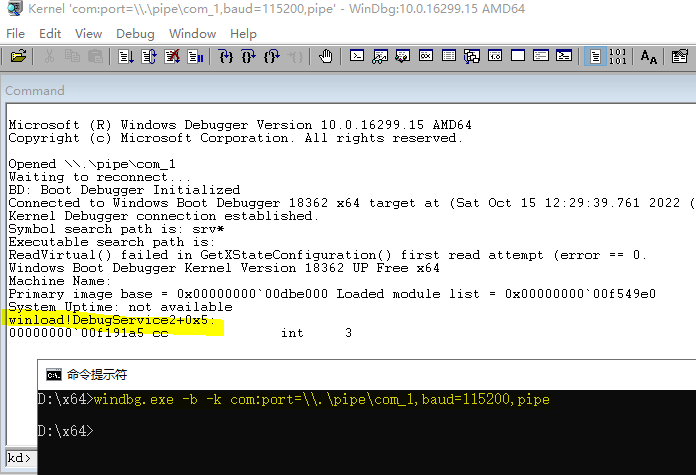
4.配置完成后，重新启动系统，在开机的时候选择 Windows10 [启用调试程序] 则系统会黑屏，说明已经正常进入调试模式了。



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 如下图

windbg.exe -b -k com:port=\\.\pipe\com\_1,baud=115200,pipe



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。

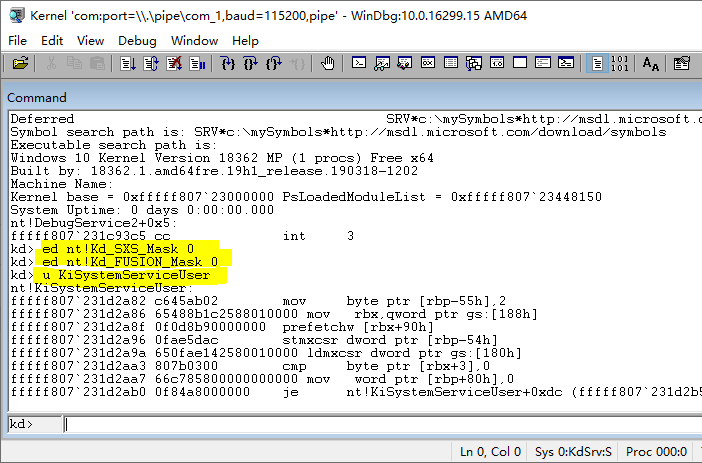


kd> .sympath SRV c:\mySymbols <http://msdl.microsoft.com/download/symbols> kd> .reload

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。



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。

