windows10内核驱动运行与调试(环境搭建)

作者: Delort

1.win10禁止驱动程序强制签名

开始菜单->设置->更新和安全->恢复->高级启动(立即重启)->疑难解答->启动设置->重启。

启动选项选择禁用驱动程序强制签名



2.SC

管理员权限运行cmd。

2.1注册驱动

备注:

=号后面有空格

demand代表手动启动。

2.2启动服务

sc start xxxxx

3.3停止驱动服务

sc stop xxxxx

3.4删除驱动服务

sc delete xxxxx

3.驱动调试环境设置

有俩种方法:

- 1. VS+VM
- 2. Windbg+VM

清单:

- 调试机器 windows10
- 调试机ip 192.168.50.227
- 虚拟机 vmware15 pro
- 被调试机 windows10
- 被调试机ip 192.168.198.129

3.1VS+VM

1.管理员运行cmd 执行 bcdedit /debug on 把被调试机器设置为调试模式。

```
C:\Windows\system32>bcdedit /debug on
操作成功完成。
C:\Windows\system32>_
```

2.输入 bcdedit /dbgsettings net hostip:192.168.50.227 port:50000

```
C:\Windows\system32>bcdedit /dbgsettings net hostip:192.168.50.227 port:50000
Key=1r5tk1bj49x5z.1g9n1r90gmc1v.3sbzu4gqueot2.1fnvch6kmekdf
C:\Windows\system32>_
```

获得key:

Key=1r5tk1bj49x5z.1g9n1r90gmclv.3sbzu4gqueot2.1fnvch6kmekdf

3.设置VS2019

备注:

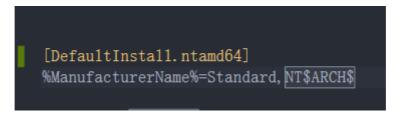
如果编译缺缓解库,找到对应的安装即可:

MSVC v142 – VS 2019 C++ ARM64 Spectre 缓解库(v14.21)
MSVC v142 – VS 2019 C++ ARM64 Spectre 缓解库(v14.22)
MSVC v142 - VS 2019 C++ ARM64 生成工具(v14.21)
MSVC v142 - VS 2019 C++ ARM64 生成工具(v14.22)
MSVC v142 - VS 2019 C++ ARM64 生成工具(v14.23)
MSVC v142 – VS 2019 C++ x64/x86 Spectre - 缓解库(v14.22)
✓ MSVC v142 – VS 2019 C++ x64/x86 Spectre - 缓解库(v14.26)
MSVC v142 - VS 2019 C++ x64/x86 生成工具(v14.21)
MSVC v142 - VS 2019 C++ x64/x86 生成工具(v14.25)
✓ MSVC v142 – VS 2019 C++ x64/x86 生成工具(v14.26)
Python 2 32-bit (2.7.16)
Puthon 2.64-hit /2.7.16\

如果编译报错error 1297: Device driver does not install on any devices, use primitive driver if this is intended.:

我刚学,但是看官方文档猜测做如下操作即可:

将[Manufacturer]替换为[DefaultInstall.ntamd64]



正文:

		State of the last										
(N)	工具(T)	扩展(X)	窗口(W)	帮助(H)	搜索 (Ctrl+Q)		م	MyDi	river1			
Debu	igging Toc	Driv	Driver		Test			A	Conf	igure Devices		- 5
	30 0	白 管理	管理扩展(M) 自定义菜单(C)	% ■	Launch Static	Driver Verifier		-	New	Test Group		
		自定			Create Driver	Verification Log						
				Ť (,	War Credit Biller	remedaen zeg						riverEntry(F
. h>		00.70.00										
			Driver0	bject)				27	Test	Group Explore		
bje ⊥ <i>("</i>	ct != N		1 d Dood	Ob i	iert Address:	N-" DIMOT	TONIII		verOl			
	Daws IDE	iver un	Toad. Dri	ver un	iedi Address:	MD . FUNCI	TONW	Dri	veru	o rect.)		
•												
,	isplay name											
_	√spiay name √yVM	s:										
	letwork hos	t name:										
b [1	92.168.198.	129										
f	Provisioning	g Options										
 Provision device and choose debugger settings Installs and configures components on the target to allow deploying drivers and running tests from Visual Studio. The specified debug settings also be set on the target, and the connection validated. 												g settings will
Í			re debugger ttings in Visua		ot provision connect to the targ	et, but does no va	lidation o	r provis	ioning.			
<u>S</u>	how help											

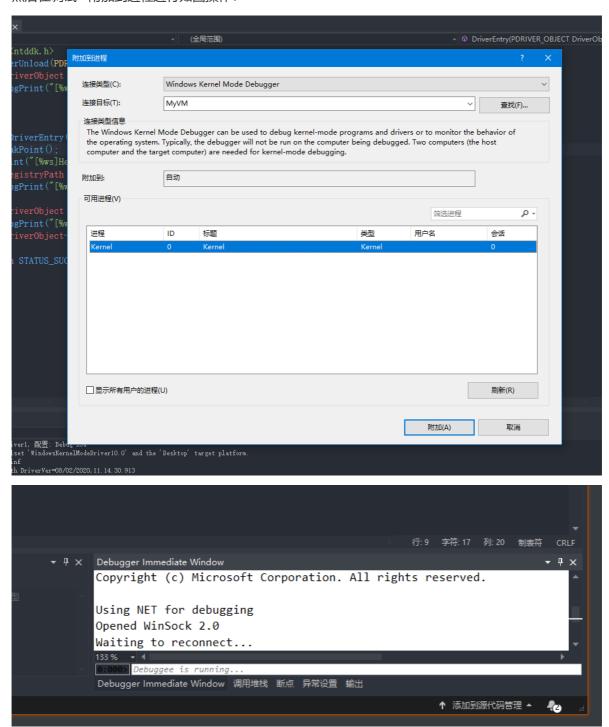
之后

portnumber写你开的端口号。

key写之前生成的。

点击完成即可。

然后在调试->附加到进程进行如图操作:



之后重启被调试机器。



之后把生成的.sys文件移动在虚拟机里面,然后进行SC操作。

注意: 使用powershell会报错

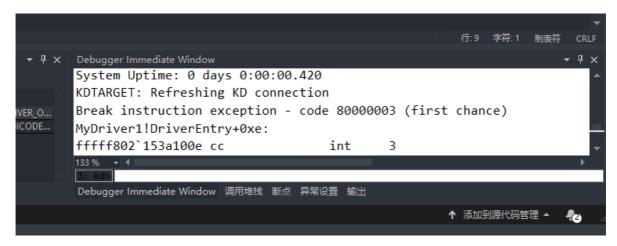
```
PS C:\MyDriver\) sc create MyDriverl binPath= "C:\MyDriver\MyDriverl.sys" type= kernel start= demand Set-Content: 技术到接受实际参数 "binPath=" 的位置形式参数。 所任位置 f:1 字符: 1 ** sc.create MyDriverl binPath= "C:\MyDriver\MyDriverl.sys" type= kernel ... ** + CategoryInfo : InvalidArgument: (:) [Set-Content], ParameterBindingException + FullyqualifiedErrorId: PositionalParameterNotFound, Microsoft. PowerShell. Commands, SetContentCommand PS C:\MyDriver\)

Microsoft Windows [Mpath 10.0.18363.592]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Windows\system32>sc create MyDriverl binPath= "C:\MyDriver\MyDriverl.sys" type= kernel start= demand [SC] CreateService 成功

C:\Windows\system32>
```

成功:



3.2Windbg

1.被调试机cmd管理员权限执行:

- bcdedit /debug on
- bcdedit /dbgsettings serial baudrate:115200 debugport:2

2.关闭系统,增加串口设备:



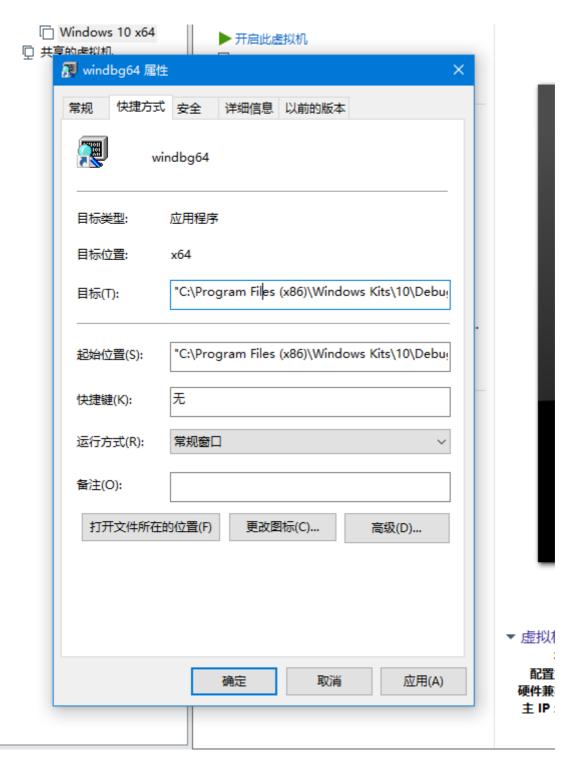
3.设置windbg

将windbg发送到桌面快捷方式

设置目标:

增加 b -k com:pipe,port=\\.\pipe\com_2,resets=0

我的设置: "C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\windbg.exe" -b -k com:pipe,port=\\.\pipe\com_2,resets=0



4.打开虚拟机,打开windbg

