How to set up Windbg Kernel Debugging between two Windows VM's in VMware fusion

1. Start VMware Fusion, make sure you have a **TARGET VM** (to be debugged) and a **DEBUGGER VM** ready.
   - A. I used a Windows 10 64-bit VM as my **TARGET VM**, and a Windows 10-32 bit VM as my **DEBUGGER VM**.

II. Configurations in the **TARGET VM**:

- A. start powershell as Administrator
  1. Use the BCDedit tool to configure the VM properly.
     - a) For reference: https://msdn.microsoft.com/en-us/library/windows/hardware/ff542187(v=vs.85).aspx
  2. **BCDedit /dbgsettings** will list the current settings
     - **(1) BCDedit /dbgsettings SERIAL DEBUGPORT:2 BAUDRATE:115200**
  3. Turn Debugging on with: **BCDedit /debug on**

III. Shutdown the **TARGET VM** and configure VMware Fusion

- A. Edit **TARGET VM**'s .vmx file
  1. **cd ~/Documents/Virtual Machines.localized/[TARGET VM**]
  2. **sudo nano [TARGET VM].vmx**
  3. Add this code (if these settings already exist in the file, ensure they are set correctly):
     - a) serial1.present = "TRUE"
     - b) serial1.fileType = "pipe"
     - c) serial1.fileName = "/private/tmp/serial"
     - d) serial1.tryNoRxLoss = "FALSE"
     - e) serial1.pipe.endPoint = "server"
- B. Edit **Debugger VM**'s .vmx file
  1. **cd ~/Documents/Virtual Machines.localized/[TARGET VM**]
  2. **sudo nano [TARGET VM].vmx**
  3. Add this code (if these settings already exist in the file, ensure they are set correctly):
     - a) serial1.present = “TRUE"cd ../
     - b) serial1.fileType = "pipe"
     - c) serial1.fileName = "/private/tmp/serial"

d) serial1.tryNoRxLoss = "FALSE"

e) serial1.pipe.endPoint = "client"

C. Configure a **SHARED FOLDER** (YOU WILL NEED TO DO THIS FOR BOTH VM’s)

1. Open VMware Fusion. Open the Virtual Machine Library.

a) In the left pane, select the **TARGET VM**.

b) From the menu bar, click "Virtual Machine ", Settings.

c) In the "System Settings" section, click Sharing.

d) In the "Shared Folders" box, on the left side, click the + sign.

e) Accept the default folder and click the Add button

2. **sudo nano [TARGET VM].vmx** again

a) change the hostpath for your new shared directory to “/private/tmp”

IV. Install Windbg on the **DEBUGGER VM** and load the symbols

A. Download Debugging Tools for Windows from Microsoft

B. To set up the debugger symbols:

1. Make a new folder “C:\symbols”

2. Control Panel -> edit environment variables

3. Symbol: “_NT_SYMBOL_PATH”

4. value: “symsrv*symsrv.dll*c:\symbols*http://msdl.microsoft.com/download/symbols”

V. DEBUGGING

A. Start your **DEBUGGING VM** and boot up WinDbg

1. File -> Kernel Debug

2. MAKE SURE THE PORT IS **com2**

3. click OK

B. Start the **TARGET VM** in debug mode

C. ???

D. PROFIT!