\*\*\*The following instructions were kindly written by Victor Westbrook of Offensive Logic and serves as the working configuration on Mac OSX running Fusion, and Linux. This came to be during the initial beta run of SEC760 in October, 2013 in Baltimore. Jamie Baxter also helped to determine the proper configuration that worked on the systems. Your experience with the below configuration may vary.\*\*\*

In order to get things running on your VMWARE Fusion installation, you will need to add the following lines to the .vmx file of your installation. You will first need to locate your Vmware Image’s file locations and then locate the .vmx file for that installation. If it seems like you have one big file for your installation, open a terminal shell and traverse to the same location of your image and you will notice that the file is indeed a directory. Enter the directory and simply open the .vmx file with your favorite editor. If you currently have a serial port configured on your system, you may see a mention of Serial0 or such in the .vmx file. For the serial number you are about to place in the configuration file, simply increment the digit by 1 from the existing serial interface (i.e. Serial0 already exists, add Serial1). Below are the configurations on two working systems with Fusion, both target (server) and debugging (client).

**System with IDA/Windbg Running on it:**

serial1.present = "TRUE"

serial1.fileType = "pipe"

serial1.yieldOnMsrRead = "FALSE"

serial1.startConnected = "TRUE"

serial1.fileName = "/tmp/com2"

serial1.tryNorxloss = "FALSE"

serial1.pipe.endPoint = "client"

**Target System:**

serial1.present = "TRUE"

serial1.fileType = "pipe"

serial1.yieldOnMsrRead = "FALSE"

serial1.startConnected = "TRUE"

serial1.fileName = "/tmp/com2"

serial1.pipe.endPoint = "server"

serial1.tryNoRxLoss = "FALSE"

After the .vmx files contain the above additions, I simply added “com2” to under port in windbg (under File -> Kernel Debug) to get the kernel debug working as shown in the following screenshot:

