Kernel Debugging with VMplayer and Windbg

By Anand George

Steps

SourceLens

sourcelens.com.au/Training
sourcelens.com.au/Mentoring
sourcelens.com.au/Consult

1. Download and install free vmplayer from vmware.

2. Install the target Windows OS in the vmplayer.

3. Add virtual serial port in VM player.

4. Make the other end (host end)of virtual serial port as named pipe.

5. Boot the VM and Enable debugging inside the VM from msconfig.

6. Start windbg kernel debugging such that it will wait for connection on the named pipe. (Make sure that you have the latest version of debugger)

7. Restart the VM.

Demo

SourceLens
sourcelens.com.au/Training
sourcelens.com.au/Mentoring
sourcelens.com.au/Consult
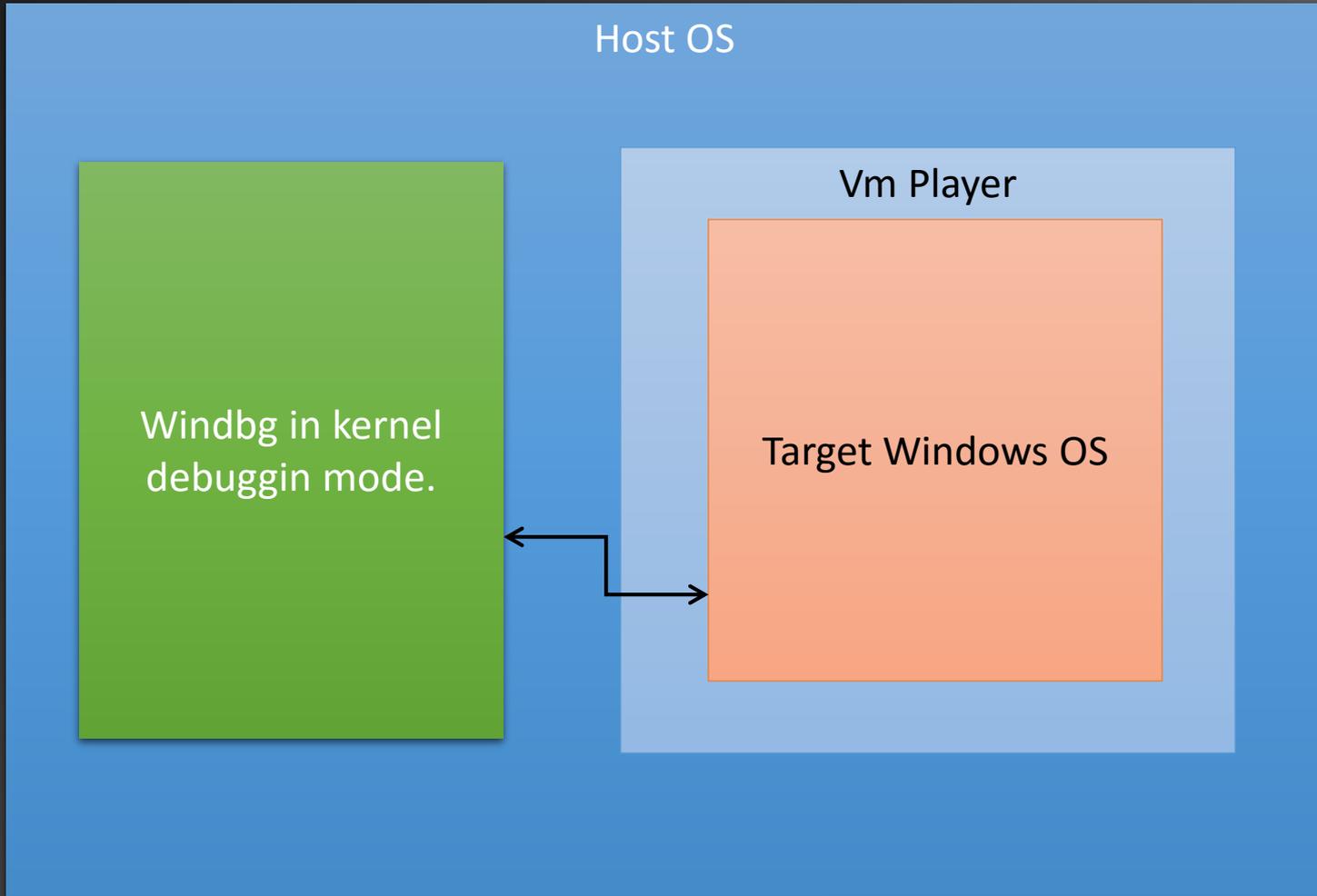
Summary

- Make sure all your tools are latest.
- Normally very straight forward if you following the steps correct.
- Similar steps you can find for other VM infra structure like hyper v, Vm ware work station etc.

SourceLens

sourcelens.com.au/Training
sourcelens.com.au/Mentoring
sourcelens.com.au/Consult

Thank you