Basic commands for Windbg – breakpoints Part 3 - bu

By Anand George

Breakpoints

- F9
- bp
- bm
- bu
- ba
- bd*
- bl*
- be
- .bpcmds

bu - Unresolved

- Break point before a binary is loaded.
- We cannot use BP as we don't have the function address as binary is not yet load in the memory.
- More rigorous demo when we discuss drivers and dlls.
- Very frequently used to break in to the DriverEntry of a kernel driver which is yet to be loaded.
- Alternative for bu would be break on load event (we are yet to see) and then a bp.

Three primary differences between **bp** breakpoints and **bu** breakpoints

- A **bp** breakpoint location is always converted to an address. If a module change moves the code at which a **bp** breakpoint was set, the breakpoint remains at the same address. On the other hand, a **bu** breakpoint remains associated with the symbolic value (typically a symbol plus an offset) that was used, and it tracks this symbolic location even if its address changes.
- If a **bp** breakpoint address is found in a loaded module, and if that module is later unloaded, the breakpoint is removed from the breakpoint list. On the other hand, **bu** breakpoints persist after repeated unloads and loads.
- Breakpoints that you set with **bp** are not saved in WinDbg workspaces. Breakpoints that are set with **bu** are saved in workspaces.

Demo

Summary

- bu

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

Thank you