Introduction to Windbg – Modes Of Operation

By Anand George

Modes

- User mode live debugging
  - starting with debugger
  - attaching a debugger.
- Live Kernel mode debugging (most powerful mode. Other modes are more of less subset of this)
  - Need 2 machines.
  - Target can be a Virtual machine.
- Dump analysis
  - user dump
  - complete dump /kernel dump
- Open a binary.
- 32 bit
- 64 bit
- wow64 modes. User Mode / kernel mode.

Demo

How debugger does all these magic ?

Working of a Debugger

- Handle certain interrupts which are normally ignored or suppressed by the OS (e.g.: trap flag)
- Take control of some of the interrupt handlers once KD is attached and broken.
- Read / write access to memory and CPU registers of the program/os which is being debugged.
- Advanced hardware assistance (debug registers in X86) for some special functionalities like break on access etc.
- User mode debugger works slightly different but similar principle.
- Dumps are read like a file and debugger is as good as a notepad in that case. Reading a file, process and display output based on that. Dump analysis is a "one instance" special case of live debugging.
- Compiler, linker, loader or OS in general work together with debugger to get the debugging experience right.
- We will discuss some of the working and internals of basic debugging operation like breakpoint, attaching (user mode) and other operations of debugger in better detail in later presentations.
- Debugger has a core engine which does more of the above mentioned operations to which lot of UI and extensions attached.

Summary

- Modes
- Working

Thank you