DAY 3

Windows System Internals

- Understanding Windows Driver Module
- Exceptions
- WoW64 Subsytem
- Process, Jobs, Threads
- Mutexes
- Critical region
- Preemptive Process Planning
- Scheduling in OS

Getting started with the System Internals (Windows)

- Setting up WinDbg for Kernel Mode
- Execution Modes
- Privilege Rings
- Interrupts
- Paging
- Port I/O
- System Calls
- MSRs
- Registry
- Kernel Mode vS User Mode
- Key system components of Windows

Practicals

TBD