DAY 1

Why Reverse Engineering?

Knowing our Tools of Trade

- Getting comfortable with IDA Disassembler
  - Practical walkthrough
  - Understanding & learning to use
- Getting comfortable with WinDbg.
  - Practical walkthrough
  - Understanding & learning to use
- Setting up and understanding Visual Studio
  - Load projects
  - View disassembly
  - Source level debugging
  - Understanding various windows of VS

Journey to understand

- Flashback
  - Conversion
  - Sizes of data types
  - Understanding ENDIANNESS
- Registers
  - Checking CPUID
  - Listing existing Registers
  - RFLAGS
  - Register Conventions
- Instructions
- Understanding Stack
  - PUSHing
  - POPing
  - PEEKing
- Control Flow
  - Conditional
  - Unconditional
- Booleans
  - INC
  - TEST
  - DEC
  - AND, OR, XOR, NOR
- Bit Shifting
  - SHL
  - SLR
  - CDQ
  - SAR
- Labels
- Calls

C and advanced x64 assembly

- Understanding calling functions
- Local variables
  - Singlelocalvariable
  - Arrays
  - Struct
- Parameters & functions
  - Calling conentions
  - Single and multiparameters
  - Subtopic 3
- Control Flow
  - IF..ELSE
  - GOTO
  - Switch
- Arithmetic(Multiply & Divide)

Practicals

- Locating control flow
- Locating subroutines
- Finding values in stack
- De-mystifying local variables
- Jumps
- Writing a program to print about yourself(Name, age, add 2 numbers) all in one using assembly