x64 Architecture & Programming

Course Summary Table

Duration:	3 Days (24 hours)
Target Audience:	Experienced developers/researchers, interested in digging deeper into the x64 (Intel/AMD) processors.
Objectives:	• Write x64 assembly confidently. • Understand the x64 architecture and modes of operation. • Interface x64 assembly with Windows programs. • Write shellcode.
Pre-Requisites:	• Basic understanding of Windows OS concepts such as processes, threads and virtual memory • Experience writing C code
Software/Hardware requirements:	• Windows 10 or 11 64 bit (any SKU, latest stable version) • Visual Studio 2022 (any SKU) + latest update • Windows 11 SDK (latest)

Instructor: **Pavel Yosifovich**

Abstract

x64 processors are the most used processors on which Windows systems run. Understanding how these processors work is essential when working closely with the OS, such as when debugging, reverse engineering, or researching.

This course describes the x64 architecture in detail, its registers, instruction set, modes of operations, and more. The participants will write stand alone assembly programs and modules that interface with C/C++ programs.

In addition, shellcode will be developed that can be injected into a target process to accomplish specific tasks.

Syllabus

- Module 1: Basic x64 Architecture
  - Quick historic overview
  - Data types
  - Registers
  - 64 vs. 32-bit
  - Hello Assembly!
  - Using Visual Studio and MASM
  - Calling Assembly from C/C++
  - The x64 Calling Convention
  - Summary

- Module 2: Assembly Programming I
    - Memory and Assembly
    - Addressing Modes
    - The Stack
    - MASM: variables, constants, structures
    - Strings
    - Arrays
    - Unions
    - Calling Windows APIs
    - Summary

- Module 3: Assembly Programming II
    - Procedures
    - Arithmetic Operations
    - String Instructions
    - Bits
    - SIMD
    - MASM Macros
    - RIP Relative Addressing

- Module 4: Advanced Architecture
    - CPUID
    - Real mode
    - Protected Mode
    - 64-bit modes
    - Other modes
    - Control Registers
    - Global Descriptor Table
    - Segments
    - Windows and Segments
    - Interrupt Dispatch Table
    - GDTR and IDTR
    - Paging

- Module 5: Miscellaneous Topics
    - Shellcode
    - Building shellcode
    - Injecting shellcode
    - System boot
    - BIOS
    - Writing a simple loader