Reverse Engineering 10 hours of content | 100 hours of practice | Final Project

1. Fundamentals of Assembly Development

- Introduction to processor operations
- Introduction to memory operations
- Introduction to memory registers
- Setting up the work environment
  - Tools: GDB, IDA, Ghidra
- Functions of memory registers
  - EAX, EBX, ECX, EDX
  - ESI, EDI, ESP, EBP, EIP
- EFLAGS register
  - OF, SF, ZF, CF
  - DF, IF, TF, AF, PF
- Writing a first assembly program (NASM)
- Compilation and execution
- Working with System Calls
- Defining groups with EQU
  - Working with sections: Text, Data, Rdata, BSS
- Memory zones: initialized vs. uninitialized
- Non-returning and returning operations (REP)
- REP repeating operations
- Working with text strings
- MOVS, LODS, STOS
- CMPS, SCAS
- Development of 2 basic programs
- Proper work with GDB
- Practice labs

2. Development and Debugging Using GDB

- Working with memory and registers using LEA
- Basic arithmetic operations:
  - INC, DEC, DIV
  - MUL, ADD, SUB
- Debugging exercises using GDB
- Navigating code with GDB
- Memory debugging with GDB
- Comparisons using CMP and TSET
- Conditions and jump flags using JMP
- Detailed explanation of each EFLAGS flag
- GDB debugging with EFLAGS
- Working with numbers in ASCII and BCD formats
- Debugging a multi-function program
- Debugging a program that receives input from the user
- Debugging a program that returns values to the user
- Program development, debugging, and documentation

3. Advanced Reverse Engineering

- Functions and the Call instruction
- Creating and analyzing the Frame Stack
- Working with memory
- EBP, ESP, RET
- Push & Pop
- Calling Convention
- Extern procedures
- Advanced debugging with GDB
- Reverse engineering exercise of 20 labs using GDB
- Advanced work with Time Travel in GDB
- Creating a Keygen using GDB and binary patching
- Fast code analysis
- Working with IDA
- Static code analysis with IDA
- Reverse engineering using IDA
- Correct integration between GDB and IDA
- Advanced debugging techniques
- Final project