Reverse Engineering Training – 15 Module Curriculum

Hands-on reverse engineering curriculum covering Windows, Linux, Android binaries, malware analysis, and real-world reversing techniques.

Module 1: Reverse Engineering Fundamentals

- What is reverse engineering
- Legal and ethical considerations
- Static vs dynamic analysis
- Use-cases: malware, software analysis

Module 2: Computing & OS Internals Refresher

- Process memory basics
- Executable loading
- User mode vs kernel mode
- Syscalls overview

Module 3: Assembly Language Basics

- x86 / x64 architecture
- Registers and stack
- Control flow instructions
- Calling conventions

Module 4: Executable File Formats

- PE file structure (Windows)
- ELF file structure (Linux)
- Sections and headers
- Imports and exports

Module 5: Static Analysis Fundamentals

- Disassembly concepts
- Strings and symbols
- Control flow graphs
- Code navigation techniques

Module 6: Dynamic Analysis Fundamentals

- Debugging basics
- Breakpoints and stepping
- Memory inspection
- API monitoring

Module 7: Windows Reverse Engineering

- Windows APIs
- Debugging Windows binaries
- Anti-debug techniques
- Patching basics

Module 8: Linux Reverse Engineering

- ELF debugging
- LD_PRELOAD abuse
- Syscall tracing
- Binary patching

Module 9: Android Reverse Engineering – Basics

- APK structure
- DEX and Smali
- Static APK analysis
- Manifest analysis

Module 10: Android Reverse Engineering – Advanced

- Dynamic analysis with instrumentation
- Runtime hooking concepts
- SSL pinning analysis
- Native library reversing

Module 11: Obfuscation & Packing

- Common obfuscation techniques
- Packers and protectors
- Unpacking basics
- Anti-analysis bypass

Module 12: Malware Analysis Fundamentals

- Malware types
- Behavioral analysis
- IOC extraction
- Sandboxing basics

Module 13: Advanced Malware Reverse Engineering

- C2 analysis
- Persistence mechanisms
- Anti-VM and evasion
- Decrypting configurations

Module 14: Automation & Scripting for RE

- Scripting concepts
- Automating analysis
- Binary diffing
- YARA rule basics

Module 15: Capstone & Real-World Case Studies

- Reverse engineer a protected binary
- Analyze a real malware sample
- Prepare professional RE report