

Reverse Engineering

Overview

In this 5 day hands-on course, you gain the necessary binary analysis skills to discover the true nature of any Windows binary.

Target Audience

Course Objectives

You will learn how to recognize the high level language constructs (such as branching statements, looping functions and network socket code) critical to performing a thorough and professional reverse engineering analysis of a binary. After learning these important introductory skills, you will advance to the analysis of:

- * Hostile Code & Malware, including: Worms, Viruses, Trojans, Rootkits and Bots.
- * Vulnerabilities in Binaries, including: Format string vulnerabilities, buffer overflow conditions, and the identification of flawed cryptographic schemes
- * Binary obfuscation schemes, used by: Hackers, Trojan writers and copy protection algorithms

Course Outline

Introduction to Reverse Engineering

Foundations of Reversing The Reversing Process Program Structure
Common Code Constructs
Identifying Variables & Lists
Low level data management - Stacks, Heaps and Data sections
Compiler representations Kernel vs. User memory Virtual Memory and Paging
Reversing threaded applications
Defining the Win32 API Win32 executable formats and image sections
Discovering undocumented APIs in ntdll.dll
Fundamentals of IDA Pro

Reverse Engineering

Reversing file formats
Reversing encrypted file formats
Understanding conditional branching statements
Virtual machines and bytecode System vs. Code Level reversing Identifying variables
Compilers and branch prediction
Memory management
Advanced uses of IDA Pro
Using Ollydbg for runtime analysis
Kernel mode debugging with SoftICE

[Register Online](#)

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Reverse Engineering - Malware

Using Ollydbg for runtime analysis of malware
Kernel mode debugging with SoftICE
Dumping executables from memory with Dumpbin
Obfuscation of file formats Understanding hashing functions Working with encrypted binaries Polymorphism
Metamorphism
Reversing UPX and other compression types
Reversing a Trojan backdoor
Understanding network communications

Reverse Engineering - Anti-reversing techniques

Basic anti-reversing strategies Symbol elimination IsDebuggerPresent API
Single Step Interrupt Detection
Softice Backdoor Exploits for IDA Pro IDA Pro obfuscation
Code flow transformations
Opaque Predicates Interleaving Code Restructuring Arrays Encoding variables
Recursive traversal disassemblers
Reversing .NET bytecode Legal issues and the DMCA CREA review

Binary Diffing & CREA Exam

Using IDA to diff binaries Manual patch investigation Manual patch diffing
Building fuzzers
Using pei-mei
Using other code coverage tools
Protocol reversing

Related Courses, Certifications, Exams

- Certified Reverse Engineering Analyst
- CREA