1. Record Nr. UNINA9910781946803321

Autore	Eagle Chris
Titolo	The IDA pro book [[electronic resource]] : the unofficial guide to the world's most popular disassembler / / Chris Eagle
Pubbl/distr/stampa	San Francisco, : No Starch Press, 2011
ISBN	1-59327-395-9
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (954 p.)
Disciplina	004.2/4 004.24 005.14
Soggetti	Disassemblers (Computer programs) Debugging in computer science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	The IDA Pro Book; PRAISE FOR THE FIRST EDITION OF THE IDA PRO BOOK; Acknowledgments; Introduction; I. Introduction to IDA; 1. Introduction to Disassembly; Disassembly Theory; The What of Disassembly; The Why of Disassembly; Malware Analysis; Vulnerability Analysis; Software Interoperability; Compiler Validation; Debugging Displays; The How of Disassembly; A Basic Disassembly Algorithm; Linear Sweep Disassembly; Recursive Descent Disassembly; Sequential Flow Instructions; Conditional Branching Instructions; Unconditional Branching Instructions; Function Call Instructions; Return Instructions Summary2. Reversing and Disassembly Tools; Classification Tools; file; PE Tools; PEiD; Summary Tools; nm; ldd; objdump; otool; dumpbin; c++filt; Deep Inspection Tools; strings; Disassemblers; Summary; 3. IDA Pro Background; Hex-Rays' Stance on Piracy; Obtaining IDA Pro; IDA Versions; IDA Licenses; Purchasing IDA; Upgrading IDA; IDA Support Resources; Your IDA Installation; Windows Installation; OS X and Linux Installation; IDA and SELinux; 32-bit vs. 64-bit IDA; The IDA Directory Layout; Thoughts on IDA's User Interface; Summary; II. Basic IDA Usage; 4. Getting Started with IDA; Launching IDA IDA File LoadingUsing the Binary File Loader; IDA Database Files; IDA Database Creation; Closing IDA Databases; Reopening a Database; Introduction to the IDA Desktop; Desktop Behavior During Initial

Analysis; IDA Desktop Tips and Tricks; Reporting Bugs; Summary; 5. IDA Data Displays; The Principal IDA Displays; The Disassembly Window; IDA Graph View; IDA Text View; The Functions Window; The Output Window; Secondary IDA Displays; The Hex View Window; The Exports Window; The Imports Window; The Structures Window; The Enums Window; Tertiary IDA Displays; The Strings Window; The Names Window
The Segments WindowThe Signatures Window; The Type Libraries Window; The Function Calls Window; The Problems Window; Summary; 6. Disassembly Navigation; Basic IDA Navigation; Double-Click Navigation; Jump to Address; Navigation History; Stack Frames; Calling Conventions; The C Calling Convention; The Standard Calling Convention; The fastcall Convention for x86; C++ Calling Conventions; Other Calling Conventions; Local Variable Layout; Stack Frame Examples; IDA Stack Views; Searching the Database; Text Searches; Binary Searches; Summary; 7. Disassembly Manipulation; Names and Naming
Parameters and Local VariablesNamed Locations; Register Names; Commenting in IDA; Regular Comments; Repeatable Comments; Anterior and Posterior Lines; Function Comments; Basic Code Transformations; Code Display Options; Formatting Instruction Operands; Manipulating Functions; Creating New Functions; Deleting Functions; Function Chunks; Function Attributes; Stack Pointer Adjustments; Converting Data to Code (and Vice Versa); Basic Data Transformations; Specifying Data Sizes; Working with Strings; Specifying Arrays; Summary; 8. Datatypes and Data Structures; Recognizing Data Structure Use
Array Member Access

Sommario/riassunto

IDA Pro is a commercial disassembler and debugger used by reverse engineers to dissect compiled computer programs, and is the industry standard tool for analysis of hostile code. The IDA Pro Book provides a comprehensive, top-down overview of IDA Pro and its use for reverse engineering software. Author Chris Eagle, a recognized expert in the field, takes readers from the basics of disassembly theory to the complexities of using IDA Pro in real-world situations. Topics are introduced in the order most frequently encountered, allowing experienced users to easily jump in at the most appropriate p