

TURING

图灵程序设计丛书



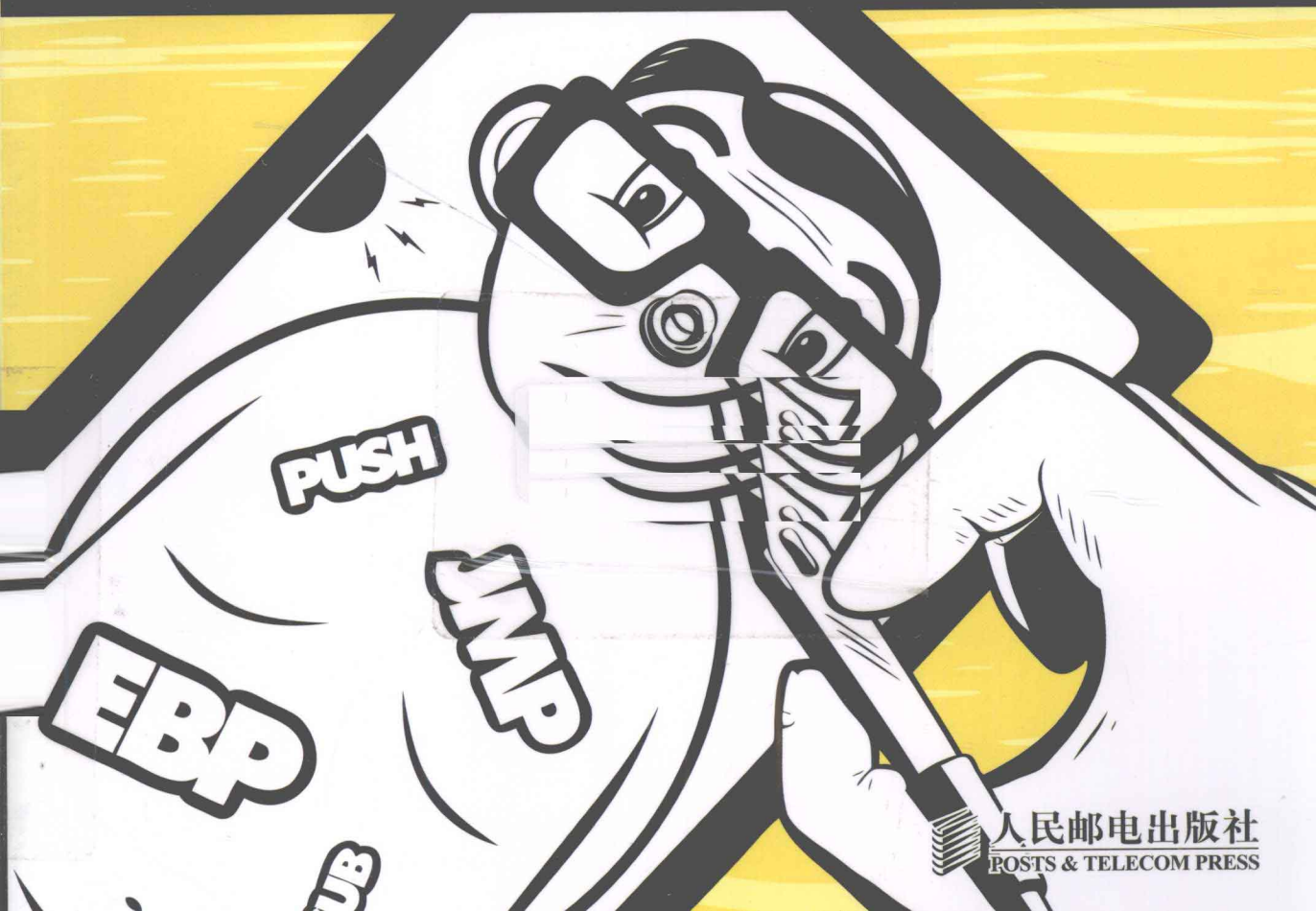
The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler **Second Edition**

IDA Pro权威指南

(第2版)

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
POSTS & TELECOM PRESS

TURING

图灵程序设计丛书

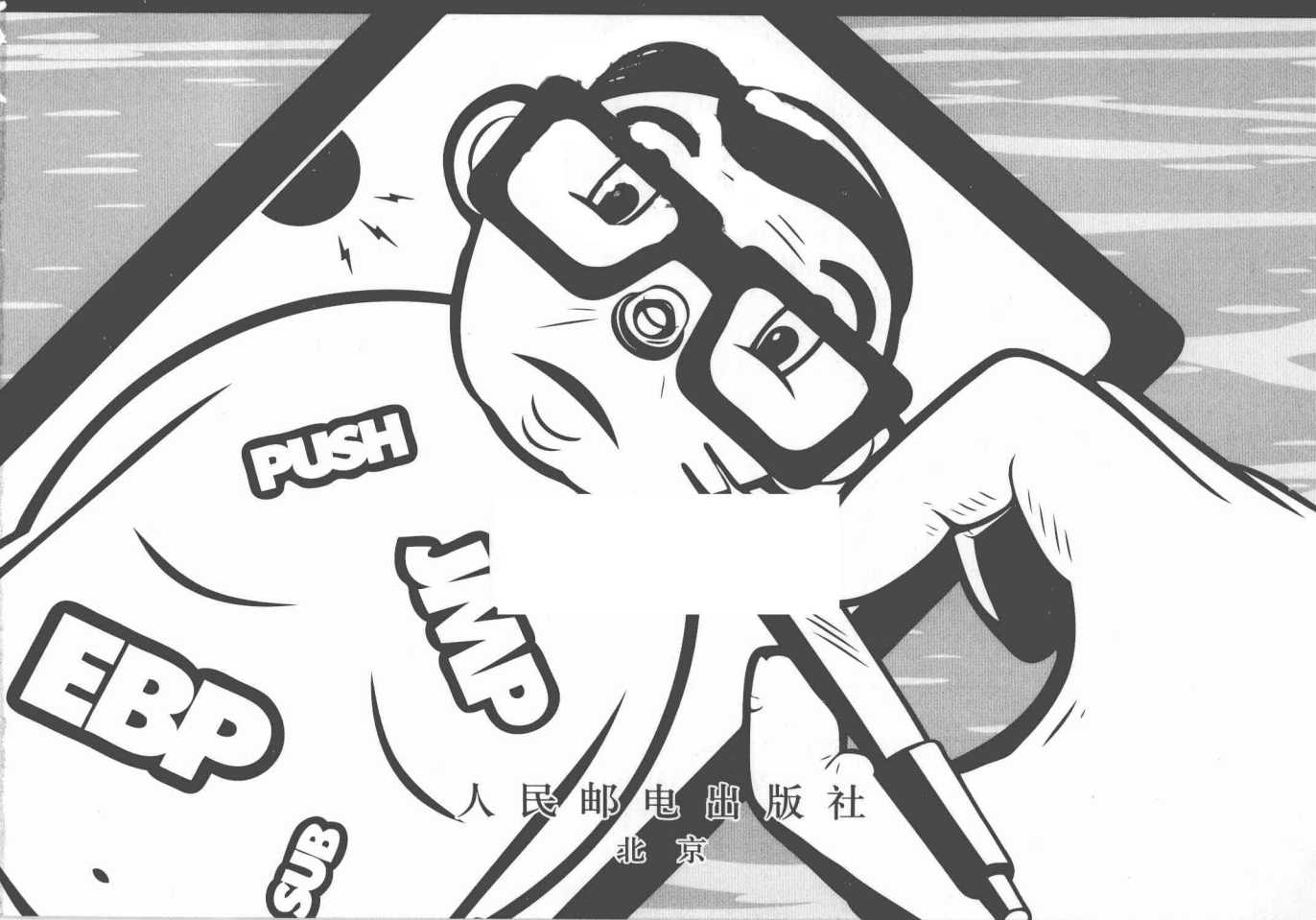
The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler Second Edition

IDA Pro权威指南

(第2版)

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
北京

图书在版编目 (CIP) 数据

IDA Pro权威指南 / (美) 伊格尔 (Eagle, C.) 著 ; 石华耀, 段桂菊译. -- 2版. -- 北京 : 人民邮电出版社, 2012.2

(图灵程序设计丛书)

书名原文: The IDA Pro Book : The Unofficial Guide to the World's Most Popular Disassembler
Second Edition

ISBN 978-7-115-27368-0

I. ①I… II. ①伊… ②石… ③段… III. ①反汇编程序 IV. ①TP313

中国版本图书馆CIP数据核字(2012)第004334号

内 容 提 要

本书共分为六部分, 首先介绍了反汇编与逆向工程的基本信息和 IDA Pro 的背景知识, 接着讨论了 IDA Pro 的基本用法和高级用法, 然后讲解了其高扩展性及其在安全领域的实际应用, 最后介绍了 IDA 的内置调试器 (包括 Bochs 调试器), 一方面让用户对 IDA Pro 有全面深入的了解, 另一方面让读者掌握 IDA Pro 在现实中的应用。相比上一版, 这一版以 IDA6.0 为基础, 介绍了它的新的、基于 Qt 的图形用户界面, 以及 IDAPython 插件。

本书适合 IT 领域的所有安全工作者阅读。

图灵程序设计丛书

IDA Pro权威指南 (第2版)

-
- ◆ 著 [美] Chris Eagle
 - 译 石华耀 段桂菊
 - 责任编辑 王军花
 - 执行编辑 丁晓昀
 - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
 - 邮编 100061 电子邮件 315@ptpress.com.cn
 - 网址 <http://www.ptpress.com.cn>
 - 北京鑫正大印刷有限公司印刷
 - ◆ 开本: 800×1000 1/16
 - 印张: 31.75
 - 字数: 750千字 2012年2月第2版
 - 印数: 4 801—7 800册 2012年2月北京第1次印刷

著作权合同登记号 图字: 01-2011-7808号

ISBN 978-7-115-27368-0

定价: 89.00元

读者服务热线: (010)51095186转604 印装质量热线: (010)67129223

反盗版热线: (010)67171154

版 权 声 明

Copyright © 2011 by Chris Eagle. Title of English-language original: *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, Second Edition* ISBN 978-1-59327-289-0, published by No Starch Press. Simplified Chinese-language edition copyright © 2012 by Posts and Telecom Press. All rights reserved.

本书中文简体字版由No Starch Press授权人民邮电出版社独家出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

版权所有，侵权必究。

谨以此书献给我的母亲。

对上一版的赞誉

“我衷心地向所有IDA Pro用户推荐《IDA Pro权威指南》一书。”

——Ilfak Guilfanov, IDA Pro的开发者

“本书内容精练而且结构合理……包括逐步深入的示例以及IDA各个方面所必需的详细信息，是你学习IDA的最佳选择。”

——Cody Pierce, TippingPoint DVLabs

“Chris Eagle无疑是一名杰出的教育工作者，因为他能够使深奥晦涩的技术材料变得简单易懂，并且总是能够提供适当的示例。”

——Dino Dai Zovi, Trail of Bits博客

“本书不仅能够帮助你全面了解IDA Pro，而且能够帮助你了解整个PE流程。”

——Ryan Linn, *The Ethical Hacker Network*

“本书内容翔实，信息全面！”

——Eric Hulse, Carnal0wnage博客

“迄今为止最全面、最准确、最优秀的IDA Pro著作。”

——Pierre Vandevenne, DataRescue SA股东兼CEO

“无论是IDA Pro的初学者还是经验丰富的使用者，我强烈建议你们阅读本书。”

——Dustin D. Trammell, 安全研究员

“我强烈建议大家购买本书。它结构合理，而且据我所知，它比任何其他文档（包括IDA Pro手册）都更加全面。”

——Sebastian Porst, 微软高级软件安全工程师

“无论是处理严重的运行时缺陷，还是由内而外地检查应用程序的安全，IDA Pro都是你的首选工具，而本书则是你尽快学习IDA Pro的指南。”

——Joe Stagner, 微软程序经理

致 谢

和第1版一样，我想感谢家人在我撰写本书时给予我的支持。我对他们的忍耐和宽容深表感谢。

我还要感谢那些推动第1版取得成功的人们，特别是广大的读者们，希望我的著作能够为他们学习逆向工程提供帮助。没有他们的支持和建议，我不可能撰写第2版。

我要再次感谢技术编辑Tim Vidas，感谢他努力工作，还要感谢他的妻子Sheila对我们工作的支持。

我还要感谢Hex-Rays的开发人员，不仅感谢他们开发出优秀的产品，而且谢谢他们容忍我那“漏洞百出”的报告，事实证明，其中许多报告都是错误警报。感谢Ilfak投入大量时间，感谢Elias、Igor和Daniel提供的深刻见解。正是因为他们的努力，才使IDA成为我最喜爱的软件。

最后，我要感谢Alison Law及No Starch出版社的所有工作人员，他们的辛苦劳动使得本书得以顺利出版。

前言

撰写一本关于IDA Pro的书是一个充满挑战的任务。事实上，IDA是一款非常复杂的软件，它的功能特别强大，要在一本书中详细介绍所有这些功能，几乎是一项无法完成的任务。而且，IDA一直在不断推出新版本，因此，任何介绍IDA的图书在出版时都会落后一两个版本。在本书第1版即将出版时，IDA发布了版本5.3，但自本书第1版出版以来，IDA已发布了7个新版本（包括版本5.3）。IDA 6.0采用了一个新的、基于Qt^①的图形用户界面，这促使我对本书进行更新，以介绍许多第1版并未介绍的功能。当然，和往常一样，IDA的另一个版本（6.1）也即将发布，^②这确实让人非常兴奋。

我撰写这一版的目的是帮助更多用户了解IDA，并培养他们对逆向工程的兴趣（如果可能）。对于希望进入逆向工程领域的读者，我希望向你们强调掌握熟练的编程技巧的重要性。理想情况下，你们应热爱编程，甚至要时时刻刻都想着编程。如果你对编程感到畏惧，那么逆向工程可能并不适合你。你可能会认为，逆向工程根本不需要编程，因为这只需要分解其他人的程序，但如果无法开发出能帮助你自动完成各种任务的脚本和插件，你永远也不可能成为真正高效的逆向工程人员。对我而言，编程和逆向工程就像是《纽约时报》周日版的纵横字谜游戏，对此我乐在其中。

为保持一致性，这个版本保留了第1版的总体结构，并且更为详细地阐述了部分章节，同时增加了一些新内容。阅读本书的方式多种多样。对逆向工程知之甚少的用户可以从第1章和第2章开始，了解有关逆向工程和反汇编器的一些信息；对IDA了解不多、希望深入学习的读者可以从第3章开始，这一章主要介绍IDA的基本布局；第4章则描述如何启动IDA并加载文件进行分析；第5章到第7章介绍IDA的用户界面窗口和基本功能。

对IDA有一定了解的读者可以从第8章开始阅读，这一章讨论如何使用IDA处理复杂的数据结构，包括C++类；而第9章则介绍IDA交叉引用，它是IDA基于图形的显示（也在第9章介绍）的基础；第10章说明如何在非Windows平台上（Linux或OS X）运行IDA。

更加高级的IDA用户可能会发现，第11章到第14章是不错的起点，主要介绍IDA的高级用法及其配套工具。第11章简要说明IDA的一些配置选项；第12章描述IDA的FLIRT/FLAIR技术和相关工具，我们利用它们开发签名，并利用这些签名将库代码与应用程序代码区分开来；第13章讨论IDA类型库及如何扩展类型库；而第14章则回答一些常见的问题，说明IDA是否可用于修补二进制文件。

① Qt是诺基亚开发的一个跨平台的C++图形用户界面应用程序框架。——译者注

② 2011年4月发布了IDA 6.1，2011年10月发布了IDA 6.2。——编者注

IDA是一款即装即用的强大工具，可扩展性是它最大的优点之一，这些年来，用户利用这一优点让IDA完成了一些非常有趣的任务。IDA的可扩展性在第15章到第19章讨论。第15章介绍IDA的脚本功能（新增了IDAPython），并系统讨论IDA的SDK（软件开发工具包）提供的编程API；第16章全面介绍SDK；而第17章到第19章则讨论插件、文件加载器和处理器模块。

介绍完IDA的全部功能后，第20章至第23章转而讨论IDA在逆向工程方面更加实际用法，分析各种编译器的区别（第20章），介绍如何使用IDA分析恶意软件中常见的模糊代码（第21章），以及如何利用IDA发现和分析漏洞（第22章）。第23章则介绍这些年来发布的一些有用的IDA扩展（插件）。

最后，第24章至第26章介绍IDA的内置调试器。第24章首先介绍调试器的基本功能；第25章讨论使用调试器分析模糊代码遇到的一些挑战，其中包括处理可能出现的反调试功能所带来的挑战；第26章则讨论IDA的远程调试功能，以及使用Bochs模拟器作为集成的调试平台，以此结束本书的讨论。

写作本书时，IDA的最新版本为6.1，本书在很大程度上以IDA 6.1为介绍对象。Hex-Rays公司非常慷慨，为用户提供了一个免费版本。IDA免费版是IDA 5.0的一个删减了部分功能的版本。本书讨论的大部分IDA功能也适用于免费版本，附录A简要介绍了用户在使用免费版本时可能遇到的一些不同之处。

首先学习IDA脚本功能，然后逐步学习如何创建编译插件，这似乎是一个自然的发展过程。因此，我们在附录B中全面介绍了每一个IDC函数及其对应的SDK操作。有时候，你可以在IDC函数与SDK函数之间建立起一一对应的关系（尽管这些函数的名称并不相同）；而有时候，实现单独一个IDC函数可能需要调用几个SDK函数。附录B回答了这个问题：“我知道如何用IDC完成某个任务，但是，如何使用插件完成这个任务呢？”附录B中的信息通过逆向工程IDA内核获得，根据IDA的非传统许可协议，这样做完全合法。

在整本书中，我都尽量使用较短的代码说明问题。绝大多数的示例代码，以及许多用于生成示例的二进制文件，都可以在本书的官方网站上找到，其地址为<http://www.idabook.com/>。在那里，你还可以找到本书并未包含的一些示例，以及本书所使用的所有参考文献（如脚注中引用的URL的最新链接）。

目 录

第一部分 IDA 简介

第 1 章 反汇编简介	2
1.1 反汇编理论	2
1.2 何为反汇编	3
1.3 为何反汇编	3
1.3.1 分析恶意软件	4
1.3.2 漏洞分析	4
1.3.3 软件互操作性	4
1.3.4 编译器验证	4
1.3.5 显示调试信息	5
1.4 如何反汇编	5
1.4.1 基本的反汇编算法	5
1.4.2 线性扫描反汇编	6
1.4.3 递归下降反汇编	7
1.5 小结	10
第 2 章 逆向与反汇编工具	11
2.1 分类工具	11
2.1.1 file	11
2.1.2 PE Tools	13
2.1.3 PEiD	14
2.2 摘要工具	14
2.2.1 nm	15
2.2.2 ldd	16
2.2.3 objdump	18
2.2.4 otool	18
2.2.5 dumpbin	19
2.2.6 c++filt	19
2.3 深度检测工具	20

2.3.1 strings	20
2.3.2 反汇编器	22
2.4 小结	23
第 3 章 IDA Pro 背景知识	24
3.1 Hex-Rays 公司的反盗版策略	24
3.2 获取 IDA Pro	25
3.2.1 IDA 版本	25
3.2.2 IDA 许可证	25
3.2.3 购买 IDA	26
3.2.4 升级 IDA	26
3.3 IDA 支持资源	26
3.4 安装 IDA	27
3.4.1 Windows 安装	28
3.4.2 OS X 和 Linux 安装	28
3.4.3 IDA 与 SELinux	29
3.4.4 32 位 IDA 与 64 位 IDA	29
3.4.5 IDA 目录的结构	30
3.5 IDA 用户界面	30
3.6 小结	31

第二部分 IDA 基本用法

第 4 章 IDA 入门	34
4.1 启动 IDA	34
4.1.1 IDA 文件加载	35
4.1.2 使用二进制文件加载器	37
4.2 IDA 数据库文件	38
4.2.1 创建 IDA 数据库	39
4.2.2 关闭 IDA 数据库	40
4.2.3 重新打开数据库	41

4.3 IDA 桌面简介	42	6.3.2 二进制搜索	77
4.4 初始分析时的桌面行为	44	6.4 小结	78
4.5 IDA 桌面提示和技巧	45	第 7 章 反汇编操作	79
4.6 报告 bug	45	7.1 名称与命名	79
4.7 小结	46	7.1.1 参数和局部变量	79
第 5 章 IDA 数据显示窗口	47	7.1.2 已命名的位置	80
5.1 IDA 主要的数据显示窗口	47	7.1.3 寄存器名称	82
5.1.1 反汇编窗口	47	7.2 IDA 中的注释	82
5.1.2 函数窗口	52	7.2.1 常规注释	83
5.1.3 输出窗口	52	7.2.2 可重复注释	84
5.2 次要的 IDA 显示窗口	52	7.2.3 在前注释和在后注释	84
5.2.1 十六进制窗口	52	7.2.4 函数注释	84
5.2.2 导出窗口	53	7.3 基本代码转换	85
5.2.3 导入窗口	54	7.3.1 代码显示选项	85
5.2.4 结构体窗口	54	7.3.2 格式化指令操作数	87
5.2.5 枚举窗口	55	7.3.3 操纵函数	88
5.3 其他 IDA 显示窗口	55	7.3.4 数据与代码互相转换	93
5.3.1 Strings 窗口	55	7.4 基本数据转换	94
5.3.2 Names 窗口	57	7.4.1 指定数据大小	94
5.3.3 段窗口	58	7.4.2 处理字符串	95
5.3.4 签名窗口	58	7.4.3 指定数组	97
5.3.5 类型库窗口	59	7.5 小结	99
5.3.6 函数调用窗口	59	第 8 章 数据类型与数据结构	100
5.3.7 问题窗口	60	8.1 识别数据结构的用法	102
5.4 小结	61	8.1.1 数组成员访问	102
第 6 章 反汇编导航	62	8.1.2 结构体成员访问	107
6.1 基本 IDA 导航	62	8.2 创建 IDA 结构体	112
6.1.1 双击导航	62	8.2.1 创建一个新的结构体 (或联合)	112
6.1.2 跳转到地址	64	8.2.2 编辑结构体成员	113
6.1.3 导航历史记录	64	8.2.3 用栈帧作为专用结构体	115
6.2 栈帧	65	8.3 使用结构体模板	115
6.2.1 调用约定	66	8.4 导入新的结构体	118
6.2.2 局部变量布局	69	8.4.1 解析 C 结构体声明	118
6.2.3 栈帧示例	70	8.4.2 解析 C 头文件	119
6.2.4 IDA 栈视图	73	8.5 使用标准结构体	120
6.3 搜索数据库	77	8.6 IDA TIL 文件	123
6.3.1 文本搜索	77		

8.6.1 加载新的 TIL 文件	123	11.2 其他 IDA 配置选项	164
8.6.2 共享 TIL 文件	123	11.2.1 IDA 颜色	165
8.7 C++逆向工程基础	124	11.2.2 定制 IDA 工具栏	165
8.7.1 this 指针	124	11.3 小结	167
8.7.2 虚函数和虚表	125	第 12 章 使用 FLIRT 签名来识别库	168
8.7.3 对象生命周期	128	12.1 快速库识别和鉴定技术	168
8.7.4 名称改编	129	12.2 应用 FLIRT 签名	169
8.7.5 运行时类型识别	130	12.3 创建 FLIRT 签名文件	172
8.7.6 继承关系	131	12.3.1 创建签名概述	172
8.7.7 C++逆向工程参考文献	132	12.3.2 识别和获取静态库	173
8.8 小结	132	12.3.3 创建模式文件	174
第 9 章 交叉引用与绘图功能	133	12.3.4 创建签名文件	175
9.1 交叉引用	133	12.3.5 启动签名	178
9.1.1 代码交叉引用	134	12.4 小结	178
9.1.2 数据交叉引用	136	第 13 章 扩展 IDA 的知识	179
9.1.3 交叉引用列表	138	13.1 扩充函数信息	179
9.1.4 函数调用	139	13.1.1 IDS 文件	181
9.2 IDA 绘图	140	13.1.2 创建 IDS 文件	182
9.2.1 IDA 外部 (第三方) 图形	140	13.2 使用 loadint 扩充预定义注释	184
9.2.2 IDA 的集成绘图视图	147	13.3 小结	185
9.3 小结	149	第 14 章 修补二进制文件及其他 IDA 限制	186
第 10 章 IDA 的多种面孔	150	14.1 隐藏的补丁程序菜单	186
10.1 控制台模式 IDA	150	14.1.1 更改数据库字节	187
10.1.1 控制台模式的共同特性	150	14.1.2 更改数据库中的字	187
10.1.2 Windows 控制台	151	14.1.3 使用汇编对话框	188
10.1.3 Linux 控制台	152	14.2 IDA 输出文件与补丁生成	189
10.1.4 OS X 控制台	154	14.2.1 IDA 生成的 MAP 文件	189
10.2 使用 IDA 的批量模式	156	14.2.2 IDA 生成的 ASM 文件	190
10.3 小结	157	14.2.3 IDA 生成的 INC 文件	191
第三部分 IDA 高级应用		14.2.4 IDA 生成的 LST 文件	191
第 11 章 定制 IDA	160	14.2.5 IDA 生成的 EXE 文件	191
11.1 配置文件	160	14.2.6 IDA 生成的 DIF 文件	191
11.1.1 主配置文件: ida.cfg	160	14.2.7 IDA 生成的 HTML 文件	192
11.1.2 GUI 配置文件: idagui.cfg	161	14.3 小结	192
11.1.3 控制台配置文件: idatui.cfg	163		

第四部分 扩展 IDA 的功能

第 15 章 编写 IDA 脚本	194
15.1 执行脚本的基础知识	194
15.2 IDC 语言	196
15.2.1 IDC 变量	196
15.2.2 IDC 表达式	197
15.2.3 IDC 语句	197
15.2.4 IDC 函数	198
15.2.5 IDC 对象	200
15.2.6 IDC 程序	200
15.2.7 IDC 错误处理	201
15.2.8 IDC 永久数据存储	202
15.3 关联 IDC 脚本与热键	203
15.4 有用的 IDC 函数	204
15.4.1 读取和修改数据的函数	204
15.4.2 用户交互函数	205
15.4.3 字符串操纵函数	206
15.4.4 文件输入/输出函数	206
15.4.5 操纵数据库名称	207
15.4.6 处理函数的函数	207
15.4.7 代码交叉引用函数	208
15.4.8 数据交叉引用函数	209
15.4.9 数据库操纵函数	209
15.4.10 数据库搜索函数	210
15.4.11 反汇编行组件	210
15.5 IDC 脚本示例	211
15.5.1 枚举函数	211
15.5.2 枚举指令	212
15.5.3 枚举交叉引用	212
15.5.4 枚举导出的函数	214
15.5.5 查找和标记函数参数	215
15.5.6 模拟汇编语言行为	217
15.6 IDAPython	219
15.7 IDAPython 脚本示例	220
15.7.1 枚举函数	220
15.7.2 枚举指令	221
15.7.3 枚举交叉引用	222

15.7.4 枚举导出的函数	222
15.8 小结	223

第 16 章 IDA 软件开发工具包	224
16.1 SDK 简介	225
16.1.1 安装 SDK	225
16.1.2 SDK 的布局	225
16.1.3 配置构建环境	226
16.2 IDA 应用编程接口	227
16.2.1 头文件概述	228
16.2.2 网络节点	230
16.2.3 有用的 SDK 数据类型	237
16.2.4 常用的 SDK 函数	238
16.2.5 IDA API 迭代技巧	242
16.3 小结	246
第 17 章 IDA 插件体系结构	247
17.1 编写插件	247
17.1.1 插件生命周期	249
17.1.2 插件初始化	250
17.1.3 事件通知	251
17.1.4 插件执行	252
17.2 构建插件	254
17.3 插件安装	258
17.4 插件配置	259
17.5 扩展 IDC	259
17.6 插件用户界面选项	262
17.6.1 使用 SDK 的“选择器”对话框	262
17.6.2 使用 SDK 创建自定义表单	265
17.6.3 仅用于 Windows 的用户界面生成技巧	269
17.6.4 使用 Qt 生成用户界面	269
17.7 脚本化插件	271
17.8 小结	272

第 18 章 二进制文件与 IDA 加载器模块	273
18.1 未知文件分析	274
18.2 手动加载一个 Windows PE 文件	275
18.3 IDA 加载器模块	281

24.3.1 断点.....	417	25.5 处理异常.....	449
24.3.2 跟踪.....	420	25.6 小结.....	454
24.3.3 栈跟踪.....	422		
24.3.4 监视.....	423	第 26 章 其他调试功能.....	455
24.4 调试器任务自动化.....	423	26.1 使用 IDA 进行远程调试.....	455
24.4.1 为调试器操作编写脚本.....	424	26.1.1 使用 Hex-Rays 调试服务器.....	455
24.4.2 使用 IDA 插件实现调试器 操作自动化.....	428	26.1.2 连接到远程进程.....	458
24.5 小结.....	430	26.1.3 远程调试期间的异常处理.....	458
		26.1.4 在远程调试过程中使用脚本 和插件.....	458
第 25 章 反汇编器/调试器集成.....	431	26.2 使用 Bochs 进行调试.....	459
25.1 背景知识.....	431	26.2.1 Bochs IDB 模式.....	459
25.2 IDA 数据库与 IDA 调试器.....	432	26.2.2 Bochs PE 模式.....	460
25.3 调试模糊代码.....	434	26.2.3 Bochs 磁盘映像模式.....	461
25.3.1 启动进程.....	435	26.3 Appcall.....	461
25.3.2 简单的解密和解压循环.....	436	26.4 小结.....	463
25.3.3 导入表重建.....	439		
25.3.4 隐藏调试器.....	443	附录 A 使用 IDA 免费版本 5.0.....	464
25.4 IDAStealth.....	448	附录 B IDC/SDK 交叉引用.....	466

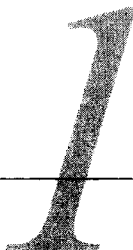
Part 1

第一部分

IDA 简介

本 部 分 内 容

- 第1章 反汇编简介
- 第2章 逆向与反汇编工具
- 第3章 IDA Pro背景知识



拿到一本专门介绍 IDA Pro 的书，你很可能急切地想知道书里会讲些什么。很明显，本书以 IDA 为中心，但我并不希望读者将其作为 IDA Pro 用户手册。相反，本书旨在将 IDA 作为推动逆向工程技术讨论的工具。你会发现，在分析各种软件（包括易受攻击的应用程序和恶意软件）时，这些技术非常有用。在适当的时候，我将提供在使用 IDA 时需要遵循的详细步骤，好让你执行与你手头的任务有关的特殊操作。因此，我将简略地介绍 IDA 的功能，包括最初分析文件时需要执行的基本任务，最后讨论 IDA 的高级用法和定制功能（用来解决更具挑战性的逆向工程问题）。我不会介绍 IDA 的所有功能。但是，你将发现，在应对逆向工程挑战时，本书介绍的功能极其有用，这也使得 IDA 成为你工具箱中最强大的武器。

在详细介绍 IDA 之前，了解反汇编过程的一些基础知识，以及其他一些对编译代码进行逆向工程的可用工具，会有一定好处。虽然这些工具的功能都不如 IDA 全面，但它们具备 IDA 的一部分功能，有助于我们了解 IDA 的某些功能。本章的剩余部分主要介绍反汇编过程。

1.1 反汇编理论

任何学过编程语言的人都知道，编程语言分为好几代，下面为那些上课不认真的读者简要总结一下。

- ❑ **第一代语言。**这些语言是最低级的语言，一般由 0 和 1 或某些简写编码（如十六进制码）组成。只有二进制超人才能读懂它们。由于数据和指令看起来都差不多，人们往往很难将它们区分开来，因此这种语言很容易造成混淆。第一代语言也称为机器语言，有时也叫做字节码，而机器语言程序常被称为二进制文件。
- ❑ **第二代语言。**第二代语言也叫汇编语言，它只是一种脱离了机器语言的表查找方式。通常，汇编语言会将具体的位模式或操作码，与短小且易于记忆的字符序列（即助记符）对应起来。有时候，这些助记符确实有助于程序员记住与它们有关的指令。汇编器是程序员用来将汇编语言程序转换成能够执行的机器语言的工具。
- ❑ **第三代语言。**这些语言引入了关键字和结构（它们是程序的构建块），因而其表达能力更接近于自然语言。通常，第三代语言不依赖于任何平台。但是，由于用第三代语言编写的程序使用了特定于操作系统的独特功能，它们便具有了平台依赖性。常见的第三代语