

## <<IDA Pro代码破解揭秘>>

### 图书基本信息

书名：<<IDA Pro代码破解揭秘>>

13位ISBN编号：9787115234162

10位ISBN编号：7115234167

出版时间：2010年8月

出版时间：人民邮电出版社

作者：(美)Dan Kaminsky,Justin Ferguson

页数：257

译者：看雪论坛翻译小组

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<IDA Pro代码破解揭秘>>

### 前言

翻译很苦，作为翻译了三本书的人，我深有感触；但组织者更难，我是第一次体会。其中的酸甜苦辣不说也罢。

这本书能和大家见面，我作为组织者首先要感谢全心参与的四位译者，他们是余洋、任晓枫、崔孝晨和李军。

四位译者虽然专业不同，翻译技能的熟练度不一样，但都一样认真，一样按要求细心修订。

我想，所有的荣耀归于他们；如果有责难，就冲我来吧，我作为组织者，责无旁贷。

在四位译者中，我最欣赏的是第7章和第8章的译者崔孝晨。

他的行文很流畅，翻译也很到位，最后才了解他原来翻译过《Windows取证分析》。

当然，最令我钦佩的是他的一颗爱心，他主动提出要把稿费捐给地震灾区。

其次，要感谢看雪为这些志同道合的朋友提供了一个自由交流的空间，接下来，要感谢北京图灵文化发展有限公司的各位编辑，在与他们打交道的过程中，虽然一些细节有待商榷，但他们认真负责的态度深深感染了我，我想凭此一条，其他的就已不重要了，我还要借此机会向我的妻子表示感谢，虽然此次组织活动纯属业余活动，但她仍给予我一如既往的支持，理解万岁。

最后，请允许我向论坛上各位等待此书的朋友表示歉意，你们的支持是动力，也是鞭策。

thinkSJ, colboy、Anplando, bwin, fool, shellwolf, yingyue, terren, batter, dance, brodbus? combojlang、lixianhuei、wzinooo、鹅蛋壳、太难了、zapline、jordanpz、Second、icetowater、magicfx、iawen、wtxpwh、KENW、安摧、不尽湘江、seagull、googleman、克里克里、duanzhu、chinazgj、xuheping、cbarme、jwtkc、lovesuae、hcaihao、riusksk、adomore，感谢你们。

## <<IDA Pro代码破解揭秘>>

### 内容概要

本书阐述了IDA Pro逆向工程代码破解的精髓，细致而全面地讲述了如何利用IDA Pro挖掘并分析软件中的漏洞。

同时也展示了如何对病毒、蠕虫和木马程序的源代码进行分析，从而达到破解的目的。

本书注重实践，有大量图示和示例代码供参考使用，可读性和可操作性极强。

本书适合从事逆向工程和计算机安全工作的程序员阅读。

## <<IDA Pro代码破解揭秘>>

### 作者简介

Dan Kaminsky, IOActive公司的渗透测试主管。

Dan自1999年起(在去Cisco及Avaya上班前)在安全圈内就非常活跃。

使他广为人知的是他在黑帽子大会上一系列的“Black Ops”演讲，此外，他还是唯一一位出席并在每届微软内部训练活动“Blue Hat”上发言的人。

Dan致力于设计层面的

## &lt;&lt;IDA Pro代码破解揭秘&gt;&gt;

## 书籍目录

第1章 引言 1.1 代码调试器概述 1.2 小结第2章 汇编及逆向工程基础 2.1 引言 2.2 汇编语言及IA-32处理器 2.3 栈、堆及二进制可执行文件中的其他区段 2.4 最新的IA-32指令集及参考资料 2.5 小结第3章 可移植可执行文件格式和可执行链接格式 3.1 引言 3.2 可移植可执行文件格式 3.3 可执行链接格式 3.4 小结第4章 实战1 4.1 引言 4.2 跟踪执行流 4.3 快速跟踪并找出解决方案 4.4 常见问题第5章 调试 5.1 引言 5.2 调试的基础知识 5.2.1 断点 5.2.2 单步 5.2.3 监视 5.2.4 异常 5.2.5 跟踪 5.3 使用IDA Pro进行调试 5.4 调试技术在逆向工程中的应用 5.5 堆和栈的访问和修改 5.6 其他调试器 5.6.1 Windbg 5.6.2 Ollydbg 5.6.3 immdbg 5.6.4 PaiMei/PyDbg 5.6.5 GDB 5.7 小结第6章 反逆向技术 6.1 引言 6.2 调试 6.3 举例阐述 6.4 混淆技术 6.5 小结第7章 实战2 7.1 协议问题 7.2 协议结构 7.2.1 分帧与重组 7.2.2 自相似性 7.2.3 Hit Marking 7.2.4 Hitlist示例第8章 高级攻略 8.1 引言 8.2 逆向分析恶意软件第9章 IDA脚本编写和插件 9.1 引言 9.2 IDA脚本编写基础 9.3 IDC语法 9.3.1 输出 9.3.2 变量 9.3.3 条件 9.3.4 循环 9.3.5 函数 9.3.6 全局变量 9.4 简单脚本示例 9.5 编写IDC脚本 9.5.1 用IDC解决问题 9.5.2 新的IDC调试器功能 9.5.3 有用的IDC函数 9.6 IDA插件基础 9.6.1 模块/插件资源 9.6.2 IDA Pro SDK介绍 9.7 插件语法 9.8 设置开发环境 9.9 简单插件示例 9.9.1 Hello World插件 9.9.2 find memcpy插件 9.10 间接调用插件 9.10.1 收集数据 9.10.2 用户接口 9.10.3 实现回调 9.10.4 显示结果 9.11 插件开发和调试策略 9.11.1 创建一个新的IDA开发目录 9.11.2 编辑配置文件 9.12 加载器 9.13 处理器模块 9.14 第三方脚本插件 9.14.1 IDAPython 9.14.2 IDARub 9.15 常见问题

## <<IDA Pro代码破解揭秘>>

### 媒体关注与评论

“多年来我曾遇到许多高级的逆向工程问题，而它已在我的参考资料中占有一席之地。其中有些从前我没有意识到的有趣话题，它们使我获益匪浅。

” ——读者评论

## <<IDA Pro代码破解揭秘>>

### 编辑推荐

如果你想掌握IDA Pro，如果你想掌握逆向工程编码的科学和艺术，如果你想进行更高效的安全研究和软件调试，《IDA Pro代码破解揭秘》正适合你！

《IDA Pro代码破解揭秘》是安全领域内的权威著作，也是少有的一本面向逆向工程编码的书籍！书中阐述了IDA Pro逆向工程代码破解的精髓，细致而全面地讲述了利用IDA Pro挖掘并分析软件中的漏洞、逆向工程恶意代码、使用IDC脚本语言自动执行各项任务，指导读者在理解PE文件和ELF文件的基础上分析逆向工程的基本组件，使用IDA Pro调试软件和修改堆和栈的数据，利用反逆向功能终止他人对应用的逆向，还介绍了如何跟踪执行流、确定协议结构、分析协议中是否仍有未文档化的消息，以及如何编写IDC脚本和插件来自动执行复杂任务等内容。

《IDA Pro代码破解揭秘》注重实践，提供了大量图示和示例代码供大家参考使用，可读性和可操作性极强。

**安全编程修炼之道！**

看雪学院等著名安全论坛强烈推荐，安全专家兼IOActive公司渗透测试总监Dan Kaminsky经典力作。

<<IDA Pro代码破解揭秘>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>