<<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

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、goooglеman、克里克里、duanzhu、chinazgj、xuheping、cbarme、jwtck、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。

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

<<IDA Pro代码破解揭秘>>

书籍目录

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

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发和软件调试，《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。

版权说明