<<IDA Pro权威指南>>

图书基本信息

书名：<<IDA Pro权威指南>>

13位ISBN编号：9787115222633

10位ISBN编号：7115222630

出版时间：2010-3

出版时间：人民邮电出版社

作者：Chris Eagle

页数：445

译者：石华耀,段桂菊

前言

这些年来，人们曾无数次地问我一个问题：究竟应该如何开始逆向工程？
当然，回答这个问题并不容易，因为每个人的具体情况都不一样。
一些人希望阅读一本有关这个主题的好书，另一些人宁愿参加培训，还有人却愿意坐下来自学必要的技能。
我应该属于最后一类，在逆向工程方面，我主要靠自学，尽管我在计算机工程和计算机科学方面接受了良好的正规教育。
接受正规教育通常是达到某种目的（如取得学位）的途径，不过更多的是为我研究某个我更感兴趣的、非专业的领域而服务。
如果想进入逆向工程领域，需要特别强调的是，你必须培养熟练的编程技能。
你最好是爱上代码，甚至是吃饭、睡觉、呼吸都离不开代码。
如果你害怕编程，那么逆向工程可能不适合你。
就我而言，编程和逆向工程就像做《纽约时报》上的填字游戏一样——解决特别困难的问题总是会有所回报。
我撰写本书的目的，是帮助其他人学习使用IDA和培养对逆向工程的兴趣。
我想通过本书为读者提供一些更加具体的内容，而不是让大家花几个小时听我漫谈IDA和各种逆向工程问题。
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、希望深入学习的用户可以从第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并加载二进制文件；第5章到第7章介绍IDA的主要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的高级用法及其自带的一些工具。
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。
IDA是一款即装即用的强大工具，可扩展是它的一个最大的优点，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，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的用法，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），以此结束这一部分的讨论。
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，以及调试器与反汇编器的集成；第26章则讨论IDA的远程调试功能。
本书在很大程度上以IDA 5.2为介绍对象，这主要是因为5.2版与5.1版和5.0版有许多相似之处。
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 4.9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）；其他情况下，单独一个IDC函数可能等同于几个SDK函数调用。
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。

<<IDA Pro权威指南>>

内容概要

本书一共分为六个部分，以反汇编与逆向工程的基本信息和IDA Pro的背景知识开篇，为读者奠定基础，紧接着循序渐进地讲解IDA Pro的基本使用、高级使用、扩展功能和它在安全领域的实际应用，最后介绍IDA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。

本书适合IT领域的所有安全工作者阅读。

作者简介

Chris EagIe，美国海军研究生院计算机系副主任、高级讲师，著有Gray，4at Hacking，在多种全球性安全会议中发表过演讲。

<<IDA Pro权威指南>>

书籍目录

第一部分　IDA简介　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　第二部分　IDA基本用法　第4章　IDA入门　　第5章　IDA数据显示窗口　　第6章　反汇编导航　　第7章　反汇编操作　第8章　数据类型与数据结构　　第9章　交叉引用与绘图功能　　第10章　IDA的多种面孔　第三部分　IDA高级应用　第11章　定制IDA　　第12章　使用FLIRT签名来识别库　　第13章　扩展IDA的知识　　第14章　修补二进制文件及其他IDA限制　第四部分　扩展IDA的功能　第15章　编写IDC脚本　　第16章　IDA软件开发工具包　　第17章　IDA插件体系结构　第18章　二进制文件与IDA加载器模块　　第19章　IDA处理器模块　第五部分　实际应用　第20章　编译器变体　　第21章　模糊代码分析　　第22章　漏洞分析　　第23章　实用IDA插件　第六部分　IDA调试器　第24章　IDA调试器　　第25章　反汇编器/调试器集成　　第26章　Linux、OS X平台的IDA和远程调试　附录A　使用IDA 4.9免费版　附录B　IDC/SDK交叉引用　附录C　IDA 5.3的新功能

章节摘录

插图：拿到一本专门介绍IDAPro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。
口第一代语言。
这些语言是最低级的语言，一般由0和l或某些简写编码（如十六进制码）组成。
只有像Skape这样的超人才能读懂它们。
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。
口第二代语言。
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。

媒体关注与评论

“它是迄今为止最全面、最准确、最棒的IDA Pro图书。”
——Pierre Vandevenne，DataRescue公司的所有人和CEO“我家里有好几本IDA Pro方面的图书，但当我遇到Chris Eagle的这本佳作时，如获至宝，其他所有书都可以抛弃了。”
——Amazon读者评论

<<IDA Pro权威指南>>

编辑推荐

《IDA Pro权威指南》：IDA Pro发行者亲自作序推荐，Amazon全五星畅销图书，引领你步入IDA Pro和逆向工程的殿堂。

版权说明