Broadview
www.broadview.com.cn

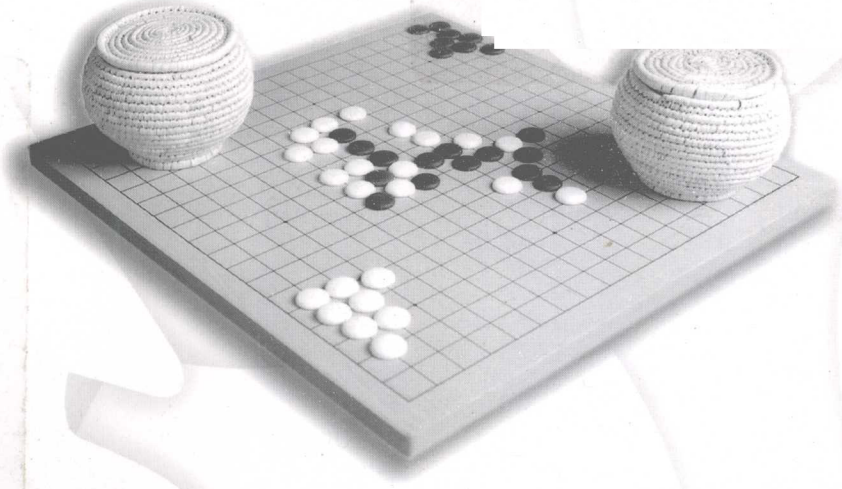
“十一五”国家重点图书出版规划项目

安全技术大系

Hacker Disassembling Uncovered，Second Edition

黑客反汇编揭秘（第二版）

【俄】Kris Kaspersky 著　　谭明金 等译



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“十一五”国家重点图书出版规划项目

Hacker Disassembling Uncovered，Second Edition

黑客反汇编揭秘（第二版）

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

很多人认为，黑客行为（Hacking）是不道德的，而本书作者 Kris Kaspersky 认为，这有失公允。黑客行为其实是天性不安分的人的一种本能，此类人天生就爱破解谜题，并乐此不疲。他们与那些以牟利或伤害他人为目标的“黑客”们，根本就是两码事。所以，本书既不是一本破解代码的技术手册，也不是一本关于反黑客的防护手册，本书可以看做是一位喜欢刨根问底的自由主义者的学习笔记。你可以跟随他的脚步，考察 Intel 编译器，洞悉商业程序的保护机制，学习使用反汇编器与调试器。在第二版中，添加了一些新内容，比如克服反调试技术、探查经过打包、加密、异化或者混淆的代码等。

如果你也和作者一样，想探究清楚那些商业软件浩瀚的代码中都有些什么，不妨读一读本书。

Hacker Disassembling Uncovered, Second Edition ISBN: 978-1-931769-64-8

版权贸易合同登记号　图字：01-2009-0638

图书在版编目（CIP）数据

黑客反汇编揭秘：第二版 /（俄罗斯）卡巴斯基著；谭明金等译. —北京：电子工业出版社，2010.6
（安全技术大系）
书名原文：Hacker Disassembling Uncovered, Second Edition
ISBN 978-7-121-10627-9

Ⅰ. ①黑…　Ⅱ. ①卡… ②谭…　Ⅲ. ①计算机网络－安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 056108 号

责任编辑：许　艳
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：28.75　字数：658 千字
印　　次：2010 年 6 月第 1 次印刷
定　　价：65.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

前　言

打我还是一个懵懂无知的孩子时起，计算机一直是让我捉摸不透的“冤家”。现在，我专攻逆向工程（反汇编）技术问题，致力于发现现有保护机制中存在的软肋（漏洞），并开发自己的保护系统。写这本书的原始冲动，最初源于我那颗对计算机“打破砂锅问到底”的天生好奇心，以及那种希望用一根撬棍或者一把榔头就能破解点什么的异想天开。当然，“撬棍”或者“榔头”纯属“幽它一默”而已。要是不经过这样的“绞尽脑汁”，哪里能够透彻理解计算机是怎么一回事呢？如果说黑客就是那些对宇宙万物百思不得其解而仍乐此不疲的人，那么我就是一名黑客。

黑码（hacking，“黑”在此转义为动词——译者注）是许多天性不安分的人的一种本能举动。他们沿着一条荆棘之路，尽力理解周围事物的本质，毅然决然地要搞点儿破坏。放眼四顾，核物理学家在裂变原子，化学分析师将大分子分离成许多小分子，数学家在积极地使用分解方法。但是，他们没有一个受到责难。令人感到奇怪的是，试图对软件做出些类似事情的代码挖掘人员，却经常受到非议。谴责他们公平吗？一般意义上的黑码和特定意义上的反汇编行为，都是非法的吗？

黑码不能与破坏主义相提并论。黑码是好奇秉性的一种自然流露，是对理解周围世界的渴望。经过反汇编得到的代码清单、机器命令以及使人想起早期 MS-DOS 的 SoftICE 黑色屏幕——所有这一切都令人感兴趣并心弛神往。在它们之中埋藏着隐匿机制与保护代码的整个世界。这个世界在地图上找不到，它只存在于打印输出的代码片断中，存在于在最令人感兴趣的位置自动开启的技术手册之中，存在于在显示器前度过的无数个不眠之夜之中。

黑客与保护机制开发人员之间不仅是对手，而且是伙伴。要是你认为黑客利用了程序员在建立高品质保护机制方面的无能，他们是寄生虫的话，那你就必须意识到，程序员也是寄生虫，因为他们同样利用了用户在编程方面的无能。

黑码与编程具有许多共同之处。创建高品质的可靠保护机制，离不开底层编程技能，离不开与操作系统、驱动程序及设备打交道的能力，也离不开关于现代处理器的体系结构、特定编译器的典

型代码生成细节，以及所用库文件的“生物学”等多种知识。处于这个层次的编程与黑码之间的细微差别显得如此微不足道，我甚至懒得去在它们之间画一条分界线。

要开发保护机制，程序员必须至少具备关于黑客所用的工作方法与技术工具等方面的一般知识。掌握不亚于对手的这十八般技术兵器，那就再好不过了。实践经验（这里指在破解程序方面的经验）十分可贵，因为这会促使程序员去仔细研究对手的战略与战术，从而能够构造出一个最优的防御组织。经验会促使程序员觉察并巩固最可能遭受黑客攻击的目标，将自己的精力最大限度地集中在这些目标之上。这意味着，保护机制的开发人员要参透黑客心理，并且应该开始像黑客一样思考问题。

由此可见，掌握信息防护技术就意味着掌握破解了技术。要是不知道保护机制是如何被破解的，不了解保护机制的薄弱环节，以及不清楚黑客所用的兵器库，那就无法创建出价廉易行的强大保护机制。完全不从保护角度考虑问题的安全类书籍，与那些只能写入信息的存储设备差不多——没有什么实际用途。

本书既不是一本关于破解代码的技术手册，也不是一本关于反黑客的防护手册。相关书籍已经多得可以信手拈来。相反，本书要展示的是一位代码挖掘人员的“旅行笔记”。通过本书，你可以考察 Intel 的编译器，洞悉商业程序的保护机制，并学习反汇编器与调试器的工作原理，以及如何像专家一样使用它们。如果你没有因此而畏缩，没有合起本书将其丢至一旁，相信你一定会获悉许多价值不菲的新知识。

第二版的新内容

起初，这本书是打算写给专业人士看的。不过，在第一版出版以后，我收到许多读者的评论，褒奖与批评兼而有之。很自然，每位读者都希望有一本在内容安排上对于他来说是最方便的书。只是，要用一本书来满足各种读者群的希望与兴趣是不可能的（特别是用一本并不打算装做什么都有的书，更难做到这一点）。我以黑客新手作为本书最主要和最应感激的读者对象。如果本书能帮助他们克服主要的心理障碍——一种在计算机面前很无助的感觉，我会很高兴。

专业人士不需要这样的书。他们大多数人告诉我，整个第一版书中零星地散落着那么十几页纸的内容令人感兴趣，因而他们只对全书进行了走马观花式的审阅。例如，其中就有这样一条意见：“虽然素材不错，但对我来说缺乏实际的深度。”许多专业读者责备我写了一本以 Windows 为中心的书。这样一些评论有助于我更好地理解我的角色和使命。

着手写本书的第二版时，我仔细分析了所有批评意见，并将这些评论作为写书时的参考。本书第二版增补了很多实用的反汇编技巧。书中所提供的素材描述了在开始反汇编时什么是必须要做的，从何处入手分析特定的语言结构，怎样避免在数兆字节的反汇编代码中迷失方向，以及如何避免落入错综复杂的陷阱之中。本书的新章节中考虑了内存转储探查、合法软件保护机制与恶意程序。素材也经过修订，考虑了新理念与现代的发展趋势，关注的重点放在一些重要主题之上，诸如克服反调试技术，探查经过打包、加密、异化或者混淆的代码等。该修订版还更正了第一版中出现的错误，并补充了遗漏部分。

本书结构

第二版的内容共分为四篇：第一篇，“黑客工具介绍”；第二篇，“基本黑客技术”；第三篇，“高级反汇编技术”；第四篇，“实用代码探查技术”。

本书包含如下 21 章。

- 第 1 章简要概述了最流行的 Windows 黑客工具，包括调试器、反汇编器、反编译器、十六进制编辑器、解包器与转储器等。此外，本章还开出了一个必读的图书清单，它们能帮你获取进入黑客领域所需的最基本的知识。
- 第 2 章描述可以用的 UNIX 与 Linux 黑客工具。
- 第 3 章集中介绍一个通俗而令人感兴趣的主题——调试器与仿真器的仿真，这为代码挖掘人员提供了几乎无限的可能性。除了描述最流行的仿真器及其应用领域外，本章还比较分析了现有仿真器，并介绍了这个领域的最新技术进展。
- 第 4 章偏重概述现有汇编器及其优势与不足。这个主题特别重要，因为一个没有掌握汇编语言的黑客还算不上一位真正的黑客。仅仅具备高级编程语言的知识，怎么可以随心所欲地反汇编软件呢？本章特别重点介绍了如何选取汇编语言编译器的问题，这不仅对于黑客新手至关重要，而且对于专业程序员意义重大。
- 第 5 章作为第二篇的开篇，概述了保护机制及其优缺点，以及现有保护机制最常见的实现错误。此外，本章还为保护机制开发人员推荐了一些方法，这有助于在提升保护强度的同时，不会为合法用户带来不便。
- 第 6 章介绍了黑客用于破解保护机制的基本技巧。本章演示了使用十六进制编辑器、API 窥探器与反汇编器（以 IDA Pro 为例）的基本方法，同时给出了简单的黑码实例用以说明。
- 第 7 章介绍了应用程序调试技术。虽然本书重点讨论反汇编，但对整个程序的反汇编清单进行分析时效率通常很低。调试器是最流行的黑客工具，它们经常与反汇编器一起使用。本章演示了使用调试器高效定位保护机制的技巧，并给出具体的实例。
- 第 8 章在逻辑上是前一章的延续，内容是在 UNIX 与 Linux 环境下展开调试的特殊之处。本章讨论了使用 UNIX 世界中最强大的调试器之一——GDB 的一些高效方法。对调试不带有符号信息的二进制文件给予了特别的关注。
- 第 9 章讨论了内核调试技术这个主题，具体以 Linice 为例。Linice 是一个特别适合于破解带保护机制的应用程序的调试器。
- 第 10 章作为第二篇的总结，涵盖了高级调试内容，为你开始进行正式的代码探查做准备。本章使你熟悉各种不同的黑客诡计，以便能够实施效率更高的黑码操作。这些技术包括如何使用断点、将 SoftICE 用做日志记录器、组合使用调试器与反汇编器，以及在大型程序中快速定位保护机制等。
- 第 11 章偏重于介绍 32 位 PE 文件的反汇编。本章描述 PE 文件的结构，讨论在这种文件中插入外码的各种技巧。该主题对于理解本书提供的其他素材是特别重要的，因为代码插入技术在蠕虫、病毒、外壳程序以及保护机制中被广泛采用。

- 第 12 章讨论反汇编 ELF 文件的问题，涵盖了向 ELF 文件插入外码的各种技术，并提供反汇编的实例。
- 第 13 章以 AMD 64 芯片体系结构为例，讨论反汇编 64 位可执行文件的问题。
- 第 14 章描述反汇编操作系统内核的技术，集中介绍 Linux 内核实例。本章演示了如何探查内核的技术，给出的素材以简单的内核篡改为例。
- 第 15 章涉及高级补丁技术，包括在线补丁的秘密与技巧，以及窃取技术。补丁技术以 Windows NT/2000/XP 内核修订版为例进行演示。本章涵盖的其他重要主题还包括使用公开与未公开的功能和函数来删除针对在线补丁的内核保护装置，特别关注了如何克服由拙劣的内核补丁所引起的后果，包括使用 SoftICE 来克服 BSOD（蓝屏死机）。
- 第 16 章作为第三篇的最后一章，对各种不同格式文件的反汇编事宜进行了总结。与前面介绍反汇编 32 位与 64 位的 PE 文件和 ELF 文件的章节不同，本章以 PDF 文件为例演示了反汇编其他格式文件的技术。
- 第 17 章演示了在 Windows 世界中反调试技术以及窃取技术的使用。本章的补充材料是关于在 UNIX 与 Linux 中使用这些技术的，在本书的网站下载资源包中提供。
- 第 18 章讨论在 Windows 平台下探查经过打包的保护程序的问题。以打包形式发布的程序数量与日俱增。打包器的主要目的是使代码分析复杂化，因此，打包器迅速演化成保护器。这是一把双刃剑，它在用于保护合法用户利益的同时，也被黑客们充分利用：蠕虫程序、病毒与特洛伊木马都活跃地使用打包器与保护器来保护自己，躲开反病毒程序的检测。
- 第 19 章专门讨论如何消除代码混淆的主题。代码混淆是一套使软件代码分析复杂化的技术和方法。这种武器是由黑客发明的，目前还没有什么技术来反制它。但是，有人已经开始研究这样的技术了。
- 第 20 章是关于剔除 UNIX 与 Linux 平台下的打包器、保护器与干扰器的。当前，UNIX 中的这种保护机制仅仅适合用做 crackme 例子，黑客把它们用做训练素材。这是因为绝大多数 UNIX 程序是以源代码形式发布的开源项目。不过，UNIX 商业产品的数量正在增长，而黑客已经准备好与这一真正的对手放手一搏。
- 第 21 章讨论针对蠕虫程序、病毒与其他恶意软件进行审计、监测与反汇编的重要主题。说这个主题特别重要，是因为反病毒软件（即使用了所有可用的更新版本）也不是总能正确地识别恶意软件。有经验的黑客倾其心智使选取调试器（通常是 SoftICE 或者其他更好的调试器），并结合其他工具，不管恶意代码隐藏在何处，都将它揪出来而使之无处容身。

网站资源

要开发保护机制，程序员必须知道对手使用的工作方法和技术工具。具备破解程序的实践经验是十分必要的，因为它让程序员细致地了解攻击方的战略战术，从而组织起最优的防御机制。这意味着，保护机制开发人员必须研究黑客心理并像黑客那样思考问题。

在网站 www.broadview.com.cn 上提供了书中的补充素材资源包。资源包根目录下的 MISCELLANEOUS 文件夹中，含有由作者编写的各种各样的 crackme 例子、工具和实用软件。你

可以免费使用这些源代码。

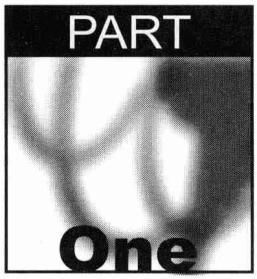
每章的素材按文件夹进行分组，文件夹根据相应的章序号进行编号。每章包含如下一些内容：

- LISTINGS——具有这个名称的文件夹含有全部代码清单的各种版本，以及在本书中提供的十六进制转储内容，同时给出了 FileListxx.txt 文件，其中有它们的详细描述。
- IMAGES——相关章的图解。
- SRC——本书提到的实例的源代码和编译结果。你可以根据需要免费使用这些源代码。
- SUPPLEMENTARY——本书前一版的片断和作者所写的其他一些文章，推荐给你作为补充阅读材料。

目　录

第一篇　黑客工具介绍

第二篇 基本黑客技术



第一篇 黑客工具介绍

CHAPTER 1

第 1 章　携黑客工具启程

黑客事务是门外汉无法插足的领域。立志成为黑客军团的一员，首先必须学习 C/C++编程语言，掌握汇编语言，理解现代微处理器的工作原理以及 Windows 和 UNIX 操作系统的体系结构，学习如何快速反汇编机器代码，等等。换句话说，通往黑客军团营地的是一条丛林密布的漫漫长路，逻辑陷阱、比特尖楔与圈套遍布其间，要是没有向导引路，几乎是难以逾越的。不过书是最好的老师，你需要找很多书来看，本书也包括在内。我推荐一个相关的书、手册与其他参考文献的清单，放在本书的网站资源中，目录为\PART_01\CH01\SUPPLEMENTARY。其中列出了一些必读书目和可以得到的最佳资源。

现在，就该为自己收集必需的黑客装备了！黑客，其实也是辛勤劳作的代名词，他们一直在用脑子和双手埋头苦编代码。不过，专用程序使新手在进行黑客操作时保持清晰的思路，从而由代码苦力迈出了第一步。问题在于，这类程序如此众多，任何初次访问黑客网站的新手不可避免地会迷失方向。通常，新手无法确定自己需要什么以及什么对自己没有用处。本章简要给出黑客软件的概况，可以大致满足各位黑客的需要。

1.1　调试器

无论在何时何地，SoftICE 作为 Windows 平台事实上的调试标准，都算得上是最好的调试工具，当然也堪当任何黑客的首选。几代黑客人都是这么认为的，也是这么选择的。SoftICE 是一种具有高级命令接口的交互式工具（如图 1.1 所示）。它在易学和好用两方面进行了平衡。换句话说，阅读 SoftICE 手册很有必要，因为 SoftICE 没有向用户提供任何 Turbo Debugger 样式的直观菜单。

SoftICE 起初是由 NuMega 创建的，但是后来卖给了 Compuware。Compuware 将 SoftICE 作为庞大的 DriverStudio 构架的一部分进行部署。遗憾的是，2006 年 4 月 3 日，该公司宣布，由于“一系列技术、商业与市场因素”，公司已经停止对这个成为绝版的软件项目提供支持。然而，对于黑客来说，这不是一个令人满意的理由。

本产品的最后一版 DriverStudio 3.2，支持全部 Windows 操作系统版本系列（直到 Windows Server 2003）与 AMD x86-64 体系。这意味着，SoftICE 在未来大约 5 年左右的时间里还能用于调

试，5 年以后，黑客们就不得不发明点别的什么了。

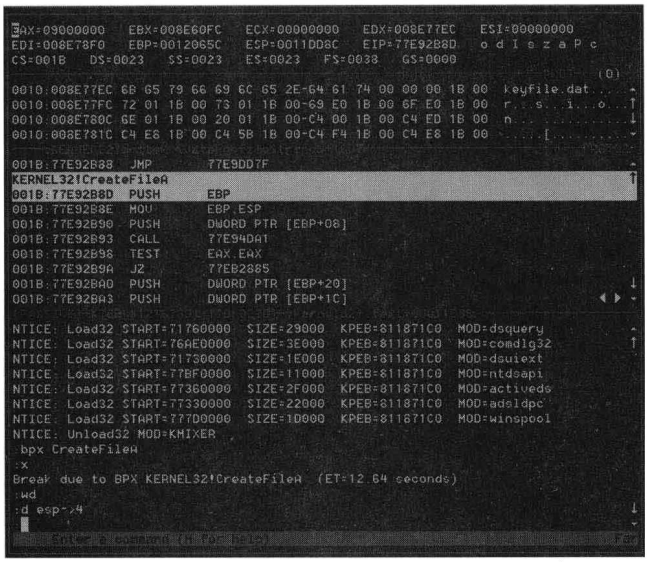


图 1.1　SoftICE 是面向专业人士的调试器

在 e-Donkey 或者任何其他黑客网站（例如，**http://www.woodmann.com/crackz/Tools.htm**）上，你都可以找到 SoftICE。随 SoftICE 一起，还应同时安装 IceExt（**http://sourceforge.net/projects/iceext**）——SoftICE 的一个非官方扩展软件，它可以隐藏起调试器使之在大多数保护机制的视野里消失，还可以保存内存转储（如图 1.2 所示），挂起线程以及执行许多其他操作。

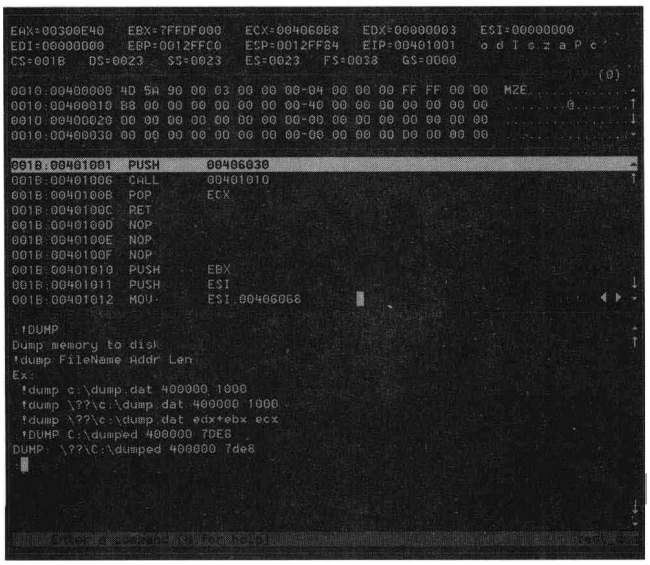


图 1.2　使用 IceExt 保存转储内容

如果 IceExt 不能成功启动，请在注册表中找到注册关键字 HKLM\SYSTEM\CurrentControlSet\Services\NTice 下的 KDHeapSize 与 KDStackSize DWORD 设置项，并将它们分别设置为 KDHeapSize (DWORD):0x8000 与 KDStackSize(DWORD) :0x8000。

IceDump（**http://programmerstools.org/system/files?file=icedump6.026.zip**）是 SoftICE 的另一个非官方扩展软件，它可以执行许多有用的操作，是对 IceExt 功能的合理补充（如图 1.3 所示）。

图 1.3 使用 IceDump 保存转储

顺便提一下，SoftICE 在 VMware 虚拟机上的运行效果不错。要让 SoftICE 在 VMware 虚拟机上运行，只要在 VMX-file 文件中加入如下两行就行了：paevm=TRUE 与 processor1.use=FALSE。有报道说，在多处理器配置和超线程处理器平台上运行 SoftICE 会出现一些问题。这样的问题可以通过在 boot.ini 文件中加入/ONECPU 选项来消除。

除 SoftICE 以外，还有其他一些调试器可用。其中，免费的 Olly 调试器或者 OllyDbg（**http://www.ollydbg.de**）特别值得一提（如图 1.4 所示）。

OllyDbg 是一个便捷的面向黑客的应用程序级调试器。它支持插件机制，因为这个原因，黑客们共同开发了许多优良的扩展件与添加件，使 OllyDbg 在保护机制的视野中隐匿行迹，自动确定打包程序的原始入口位置，简化保护机制的消除过程，等等。

可以在 **http://www.openrce.org** 上找到大量的 OllyDbg 插件集。

Syser（**http://www.sysersoft.com**）是最新的（在许多方面仍然是实验性的）内核调试器。这是由中国的开发人员发布的，并且在迅速发展之中（如图 1.5 所示）。