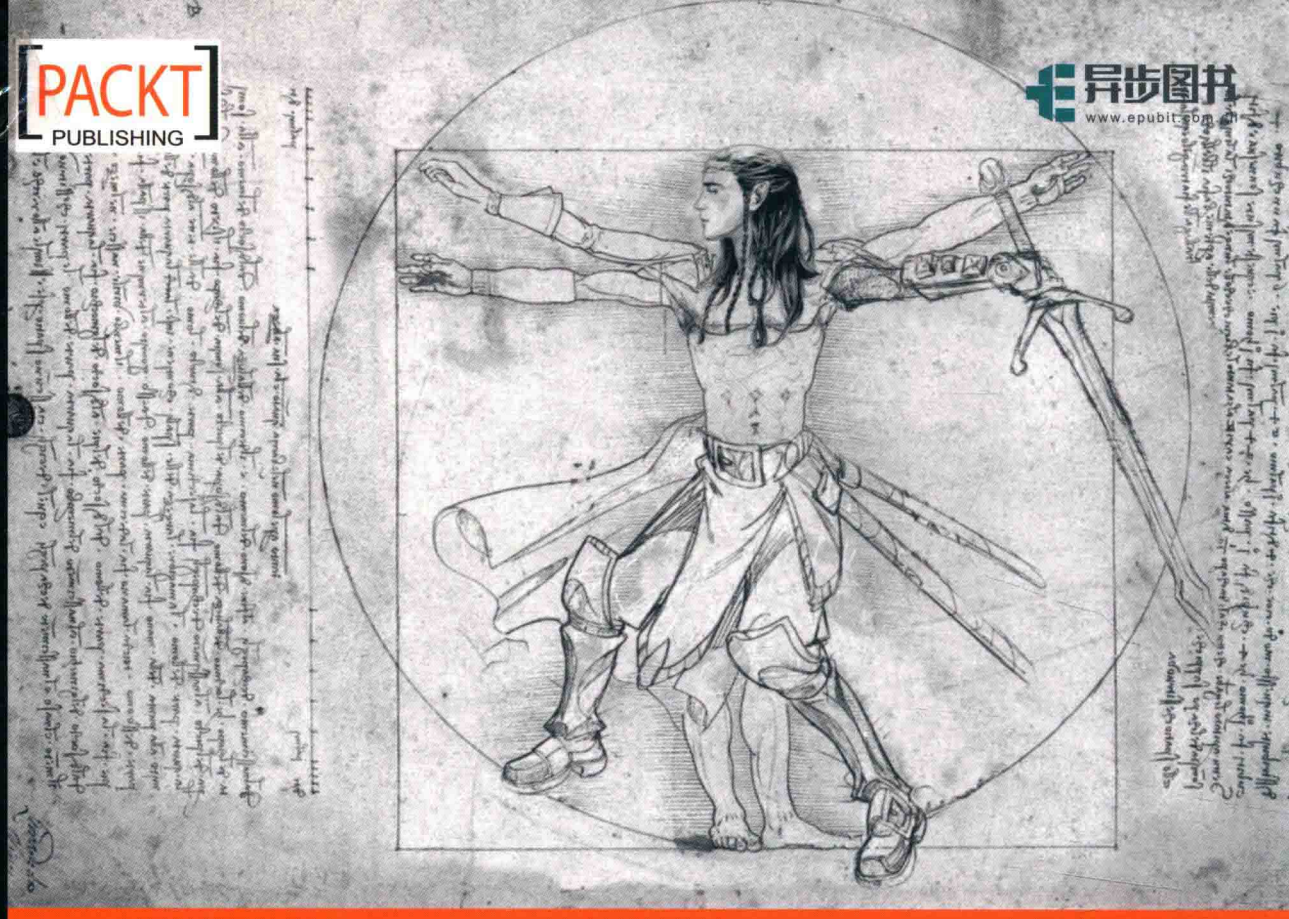


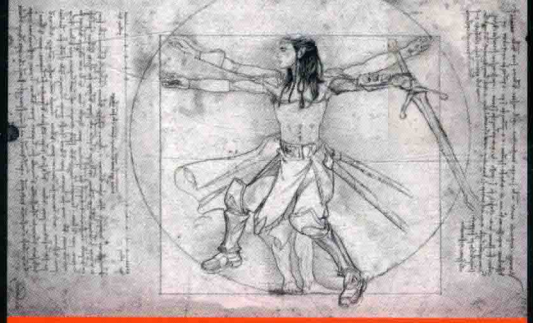
Linux二进制分析

Learning Linux Binary Analysis

[美] Ryan O'Neill 著
棣琦 译
Linux中国 审

中国工信出版集团
人民邮电出版社 POSTS & TELECOM PRESS

Linux二进制分析



本书首先讲解了UNIX/Linux中分析目标文件的实用工具和ELF二进制格式的相关内容，随后介绍了进程追踪、各种不同类型的Linux和UNIX病毒，以及如何使用ELF病毒技术进行处理。

本书的后半部分介绍了如何使用Kprobe工具进行内核破解、代码修补和调试，如何检测并处理内核模式的rootkit，以及如何分析静态代码；最后对复杂的用户级内存感染分析进行了相关讲解。

本书将带领读者探索甚至连一些专家都未曾接触的领域，正式进入计算机黑客世界。

本书读者对象

如果你是一名软件工程师或者逆向工程师，想要学习Linux二进制分析相关的内容，本书实为明智之选。本书提供了在安全、取证和杀毒领域中实施二进制分析的解决方案。本书也适合安全爱好者和系统工程师阅读。为了更好地理解本书内容，读者需要具备一定的C语言编程基础和Linux命令行知识。

本书内容：

- ELF二进制格式的内部工作原理；
- UNIX病毒感染和分析的相关技术；
- 二进制加固和软件防篡改技术；
- 修补可执行文件和进程内存；
- 绕过恶意软件中的反调试；
- 高级的二进制取证分析技术；
- 用C语言设计ELF相关的工具；
- 如何使用ptrace操作内存。

异步社区
人民邮电出版社
www.epubit.com.cn

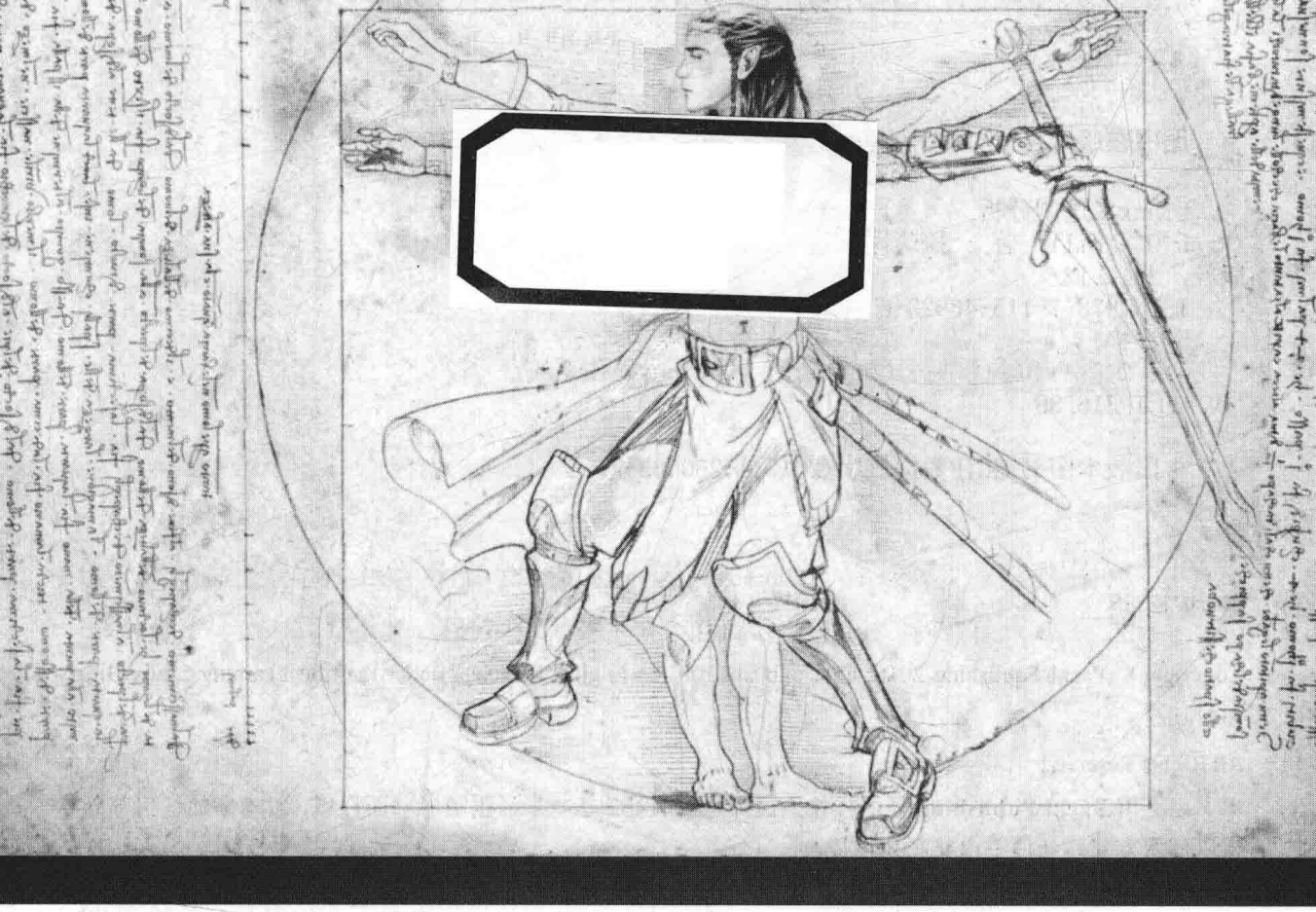
异步社区 www.epubit.com.cn
新浪微博 @人邮异步社区
投稿/反馈邮箱 contact@epubit.com.cn

美术编辑：董志桢

ISBN 978-7-115-46923-6

ISBN 978-7-115-46923-6
定价：59.00 元

分类建议：计算机／信息安全
人民邮电出版社网址：www.ptpress.com.cn



Linux二进制分析

[美] Ryan O'Neill 著
棣琦 译
Linux中国 审

人民邮电出版社
北京

图书在版编目（CIP）数据

Linux二进制分析 / (美) 瑞安·奥尼尔
(Ryan O'Neill) 著 ; 棣琦译. -- 北京 : 人民邮电出
版社, 2017.12
ISBN 978-7-115-46923-6

Ⅰ. ①L… Ⅱ. ①瑞… ②棣… Ⅲ. ①Linux操作系统
Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2017)第260033号

版权声明

◆ 著　[美] Ryan O'Neill
译　棣　琦
审　Linux 中国
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：17.5
字数：238 千字　2017 年 12 月第 1 版
印数：1 – 2 000 册　2017 年 12 月北京第 1 次印刷

著作权合同登记号　图字：01-2016-7606 号

定价：59.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

二进制分析属于信息安全业界逆向工程中的一种技术，通过利用可执行的机器代码（二进制）来分析应用程序的控制结构和运行方式，有助于信息安全从业人员更好地分析各种漏洞、病毒以及恶意软件，从而找到相应的解决方案。

本书是目前为止唯一一本剖析 Linux ELF 工作机制的图书，共分为 9 章，其内容涵盖了 Linux 环境和相关工具、ELF 二进制格式、Linux 进程追踪、ELF 病毒技术、Linux 二进制保护、Linux 中的 ELF 二进制取证分析、进程内存取证分析、扩展核心文件快照技术、Linux/proc/kcore 分析等。

本书适合具有一定的 Linux 操作知识，且了解 C 语言编程技巧的信息安全从业人员阅读。

译者序

译者棣琦（本名张萌萌），曾梦想成为一名高级口译，却阴差阳错成了一个爱写代码的程序员。在 IT 江湖升级打怪的过程中，为了不断提高自己的技能，看书是少不了的；而要想成为高级玩家，看英文书自然也是必须。一个很偶然的机会，我接触到了本书的英文版。第一遍翻看时略显吃力，毕竟书中讲述的许多概念都是作者的原创，网上几无相关资料。但是这些稀缺的内容对于深入理解二进制分析却非常重要，译者由此尝到了知识的甜头。本着“独乐乐不如众乐乐”和“知识分享”的目的，本书的翻译之路就这样顺理成章地开始了。

要想成为一名真正的黑客，不仅要会编写程序，还需要解析程序，对已有的二进制文件进行反编译，洞悉程序的工作原理。而本书完全是作者多年来在逆向工程领域的实战经验总结，其内容从 Linux 二进制格式的简单介绍到二进制逆向的细节，不一而足。书中还穿插了作者自己维护的许多项目或软件代码示例。相信通过本书的学习，读者完全可以掌握 Linux 二进制分析相关的一套完整的知识体系，为成长为一名高水平的黑客打下坚实的基础。考虑到本书并非针对零基础的读者编写，因此建议读者能够有一定的 C 语言和 Linux 基础，以便更好地理解领会书中精华。另外，任何 IT 技术的学习掌握，都离不开动手操作。读者要想叩开 Linux 二进制世界的大门，需要亲自动手实践书中示例，才能将书本知识转换为自身技能。

最后，不能免俗的是各种致谢（虽然俗，但诚意百分百）。感谢我的父母对我闯荡江湖的支持，感谢 Linux 中国创始人王兴宇的信赖，感谢语音识别

领域的技术大牛姚光超提出的宝贵建议，感谢我的朋友 Ray 对我的鼓励。当然，更要感谢各位读者的支持。

最后的最后，由于译者水平有限，外加本书作者在表达上多有晦涩之处，因此译文难免有纰漏，还望广大读者以及业内同行批评指正。

2017 年 9 月

北京

关于作者

Ryan O'Neill 是一名计算机安全研究员兼软件工程师，具有逆向工程、软件开发、安全防御和取证分析技术方面的背景。他是在计算机黑客亚文化的世界中成长起来的——那个由 EFnet、BBS 系统以及系统可执行栈上的远程缓冲区溢出组成的世界。他在年轻时就接触了系统安全、开发和病毒编写等领域。他对计算机黑客的极大热情如今已经演变成了对软件开发和专业安全研究的热爱。Ryan 在 DEFCON 和 RuxCon 等很多计算机安全会议上发表过演讲，还举办了一个为期两天的 ELF 二进制黑客研讨会。

他的职业生涯非常成功，曾就职于 Pikewerks、Leviathan 安全集团这样的大公司，最近在 Backtrace 担任软件工程师。

Ryan 还未出版过其他图书，不过他在 *Phrack* 和 *VXHeaven* 这样的在线期刊上发表的论文让他声名远扬。还有许多其他的作品可以从他的网站（`http://www.bitlackeys.org`）上找到。

致谢

首先，要向我的母亲 Michelle 致以真诚的感谢，我已经将对她的感谢表达在这本书里了。这一切都是从母亲为我买的第一台计算机开始的，随后是大量的图书，从 UNIX 编程，到内核内部原理，再到网络安全。在我生命中的某一刻，我以为会永远放弃计算机，但是大约过了 5 年之后，当我想要重新点燃激情时，却发现已经把书扔掉了。随后我发现母亲偷偷地把那些书帮我保存了起来，一直到我重新需要的那一天。感谢我的母亲，你是最美的，我爱你。

还要感谢我生命中最重要的一个女人，她是我的另一半，是我的孩子的母亲。毫无疑问，如果没有她，就不会有我今天生活和事业上的成就。人们常说，每一个成功男人的背后都有一个伟大的女人。这句古老的格言道出的的确是真理。感谢 Marilyn 给我带来了极大的喜悦，并进入了我的生活。我爱你。

我的父亲 Brian O'Neill 在我生活中给了我巨大的鼓舞，教会了我为人夫、为人父和为人友的许多东西。我爱我的父亲，我会一直珍惜我们之间哲学和精神层面的交流。

感谢 Michael 和 Jade，感谢你们如此独特和美好的灵魂。我爱你们。

最后，要感谢我的 3 个孩子：Mick、Jayden 和 Jolene。也许有一天你们会读到这本书，知道你们的父亲对计算机略知一二。我会永远把你们放在生活的首位。你们 3 个是令我惊奇的存在，为我的生活带来了更深刻的意义和爱。

Silvio Cesare 在计算机安全领域是一个传奇的名字，因为他在许多领域都

有高度创新和突破性的研究，从 ELF 病毒，到内核漏洞分析方面的突破。非常感谢 Silvio 的指导和友谊。我从你那里学到的东西要远远多于从我们行业其他人处所学的东西。

Baron Oldenburg 也对本书起了很大的推动作用。好多次由于时间和精力的原因我几乎要放弃了，幸好 Baron 帮我进行了初始的编辑和排版工作。这为本书的编写减轻了很大的负担，并最终促使本书问世。谢谢 Baron！你是我真正的朋友。

Lorne Schell 是一位真正的文艺复兴式的人物——软件工程师、音乐家、艺术家。本书的封面就是出自他的聪慧之手。Vitruvian（维特鲁威风格的）Elf 与本书的描述艺术性的重合是多么令人惊喜！非常感谢你的才华，以及为此付出的时间和精力。

Chad Thunberg 是我在 Leviathan 安全集团工作时的老板，他为我编写本书提供了所需要的资源和支持。非常感谢！

感谢 Efnet 网站所有在`#bitlackeys`上的朋友的友谊和支持！

关于审稿人

Lubomir Rintel 是一名系统程序员，生活在捷克的布尔诺市。他是一位全职的软件开发人员，目前致力于 Linux 网络工具的开发。除此之外，他还对许多项目做出过贡献，包括 Linux 内核和 Fedora 发行版。活跃在开源软件社区多年之后，他懂得一本好书涵盖的主题要比参考手册更加广泛。他相信本书就是这样，希望你也能够像他一样喜欢这本书。另外，他还喜欢食蚁兽。

截至 2015 年 11 月，**Kumar Sumeet** 在 IT 安全方面已经有 4 年多的研究经验了，在此期间，他开创了黑客和间谍工具的前沿。他拥有伦敦大学皇家霍洛威分校的信息安全硕士学位，最近的重点研究领域是检测网络异常和抵御威胁的机器学习技术。

Sumeet 目前是 Riversafe 公司的一名安全顾问。Riversafe 是伦敦的一家网络安全和 IT 数据管理咨询公司，专注于一些尖端的安全技术。该公司也是 2015 年在 EMEA 地区的 Splunk Professional Services 的合作伙伴。他们已经完成了涉及许多领域（包括电信、银行和金融市场、能源和航空局）的大型项目。

Sumeet 也是 *Penetration Testing Using Raspberry Pi*（Packt Publishing 出版）一书的技术审稿人。

有关他的项目和研究的更多详细信息，可以访问他的网站 `https://krsumeet.com`，或者扫描右侧的二维码。

你也可以通过电子邮件 `contact@krsumeet.com` 联系他。

Heron Yang 一直致力于创造人们真正想要的东西。他在高中时就建立了这样坚定的信仰。随后他在台湾交通大学和卡内基梅隆大学专注于计算机科学的研究。在过去几年，他专注于在人和满足用户需求之间建立联系，致力于开发初创企业创意原型、新应用或者网站、学习笔记、出书、写博客等。

感谢 Packt 给我这个机会参与本书的创作过程，并感谢 Judie Jose 在本书的创作过程中给我的很多帮助。此外，感谢我经历过的所有挑战，这让我成为一个更好的人。本书深入二进制逆向的诸多细节，对于那些关心底层机制的人来说会是很好的资料。大家可通过 heron.yang.tw@gmail.com 或者 http://heron.me 跟我打招呼或讨论图书内容。

前言

软件工程是创建能够在微处理器上存在、运行和发挥作用的造物行为。我们称这种造物为程序。逆向工程是发现程序如何运行和发挥作用的行为，进一步讲，就是使用反编译器和逆向工具进行组合，并依靠我们的专业技能来控制要进行反编译的目标程序，来理解、解析或者修改程序的行为。我们需要理解二进制格式、内存布局和给定处理器的指令集的复杂性，才能控制微处理器上某个程序的生命周期。逆向工程师是掌握了二进制领域相关知识的技术人员。本书将教会你成为一名 Linux 二进制黑客所需要的合理的课程、洞察力和相关任务。当一个人自称逆向工程师的时候，他自己其实已经超出了工程师的水平。一个真正的黑客不仅可以编写代码，还可以解析代码，反编译二进制文件和内存段，他追求的是修改软件程序的内部工作原理。这就是反编译工程师的动力。

从专业或者兴趣爱好的角度来看，我都会在计算机安全领域（无论是漏洞分析、恶意软件分析、防病毒软件、rootkit 检测，还是病毒设计）使用自己在逆向工程方面的技能。本书的大部分内容专注于计算机安全方面。我们会分析内存转储、进程镜像重建，并对二进制分析更深奥的领域进行探索，包括 Linux 病毒感染和二进制取证分析。我们将会解析被恶意软件感染的二进制文件，还会感染运行中的进程。本书旨在解释 Linux 逆向工程所必需的组件，因此我们会深入学习 ELF（可执行文件和链接格式）。ELF 是 Linux 中可执行文件、共享库、核心转储文件和目标文件的二进制格式。本书最重要的一个方面是针对 ELF 二进制格式的结构复杂性给出了深入的分析。ELF 节、

段、动态链接等这些概念都是非常重要的，也是逆向工程方面相关知识的比较有意思的分支。我们将会深入探索 ELF 二进制攻击，并了解如何将这些技能应用到更广泛的工作中。

本书的目标是让读者成为对 Linux 二进制攻防有扎实基础的少数人之一，这将会为打开创新性研究的大门提供一个非常广泛的主题，并将读者带领到 Linux 操作系统高级黑客技术的前沿。你将掌握 Linux 二进制修补、病毒工程化/分析、内核取证分析和 ELF 二进制格式这一套宝贵的知识体系。读者也会对程序执行和动态链接有更深入的了解，对二进制保护和调试的内部原理有更深入的理解。

我是一名计算机安全研究员、软件工程师，也是一名黑客。本书只是有组织地对我所做过的研究进行了文档性描述，也是对已经做出研究结果的一些基础知识的描述。

本书所涵盖的很多知识都无法在互联网上找到。本书试图将一些相关联的主题集中在一起，以便作为 Linux 二进制和内存攻击这一主题的入门手册和参考。虽然不是非常完善，不过也涵盖了入门需要的很多核心信息。

本书涵盖的内容

第 1 章，Linux 环境和相关工具，简要介绍了 Linux 环境和相关的工具，在整本书中都会用到。

第 2 章，ELF 二进制格式，帮助读者了解 ELF 二进制格式每个主要的组件，在 Linux 和大多数类 UNIX 系统上都会用到。

第 3 章，Linux 进程追踪，教会读者使用 ptrace 系统调用读写进程内存并注入代码。

第 4 章，ELF 病毒技术——Linux/UNIX 病毒，将会介绍 Linux 病毒的过去、现在和将来，以及病毒的工程化和围绕病毒进行的相关研究。

第 5 章，Linux 二进制保护，解释 ELF 二进制保护的基本原理。

第 6 章，Linux 下的 ELF 二进制取证分析，通过解析 ELF 目标文件来研究病毒、后门和可疑的代码注入。

第 7 章，进程内存取证分析，将会介绍如何解析进程的地址空间，以研究内存中的恶意软件、后门和可疑的代码注入。

第 8 章，ECFS——扩展核心文件快照技术，是对 ECFS 这一用于深入进程内存取证分析的新开源产品的介绍。

第 9 章，Linux /proc/kcore 分析，介绍了如何使用/proc/kcore 进行内存分析来检测 Linux 内核中的恶意软件。

阅读本书的先决条件

阅读本书的先决条件如下：假定读者具有 Linux 命令行相关的操作知识，对 C 语言编程技巧有一定的理解，对 x86 汇编语言知识有基本的掌握（不是必需，但会有很大的帮助）。有句话说得好：“如果你可以读懂汇编语言，那么一切都是开源的”。

本书读者对象

如果你是一名软件工程师或者逆向工程师，想学习 Linux 二进制分析相关的更多知识，本书将会为你提供在安全、取证分析和防病毒领域进行二进制分析所需要用到的一切知识。假如你是一位安全技术领域的爱好者或者是一名系统工程师，并且有 C 语言编程和 Linux 命令行相关的经验，这本书将非常适合你。

异步社区
人民邮电出版社
www.epubit.com.cn

欢迎来到异步社区！

异步社区的来历

异步社区（www.epubit.com.cn）是人民邮电出版社旗下IT专业图书旗舰社区，于2015年8月上线运营。

异步社区依托于人民邮电出版社20余年的IT专业优质出版资源和编辑策划团队，打造传统出版与电子出版和自出版结合、纸质书与电子书结合、传统印刷与POD按需印刷结合的出版平台，提供最新技术资讯，为作者和读者打造交流互动的平台。

社区里都有什么？

购买图书

我们出版的图书涵盖主流IT技术，在编程语言、Web技术、数据科学等领域有众多经典畅销图书。社区现已上线图书1000余种，电子书400多种，部分新书实现纸书、电子书同步出版。我们还会定期发布新书书讯。

下载资源

社区内提供随书附赠的资源，如书中的案例或程序源代码。

另外，社区还提供了大量的免费电子书，只要注册成为社区用户就可以免费下载。

与作译者互动

很多图书的作译者已经入驻社区，您可以关注他们，咨询技术问题；可以阅读不断更新的技术文章，听作译者和编辑畅聊好书背后有趣的故事；还可以参与社区的作者访谈栏目，向您关注的作者提出采访题目。

灵活优惠的购书

您可以方便地下单购买纸质图书或电子图书，纸质图书直接从人民邮电出版社书库发货，电子书提供多种阅读格式。

对于重磅新书，社区提供预售和新书首发服务，用户可以第一时间买到心仪的新书。

用户账户中的积分可以用于购书优惠。100积分=1元，购买图书时，在 0 使用积分 里填入可使用的积分数值，即可扣减相应金额。

特 别 优 惠

购买本书的读者专享异步社区购书优惠券。

使用方法：注册成为社区用户，在下单购书时输入 S4XC5 使用优惠码，然后点击“使用优惠码”，即可在原折扣基础上享受全单9折优惠。（订单满39元即可使用，本优惠券只可使用一次）

纸电图书组合购买

社区独家提供纸质图书和电子书组合购买方式，价格优惠，一次购买，多种阅读选择。

社区里还可以做什么？

提交勘误

您可以在图书页面下方提交勘误，每条勘误被确认后可以获得100积分。热心勘误的读者还有机会参与书稿的审校和翻译工作。

写作

社区提供基于Markdown的写作环境，喜欢写作的您可以在此一试身手，在社区里分享您的技术心得和读书体会，更可以体验自出版的乐趣，轻松实现出版的梦想。

如果成为社区认证作译者，还可以享受异步社区提供的作者专享特色服务。

会议活动早知道

您可以掌握IT圈的技术会议资讯，更有机会免费获赠大会门票。

加入异步

扫描任意二维码都能找到我们：

异步社区	微信服务号	微信订阅号	官方微博	QQ群：436746675

社区网址：www.epubit.com.cn

投稿 & 咨询：contact@epubit.com.cn