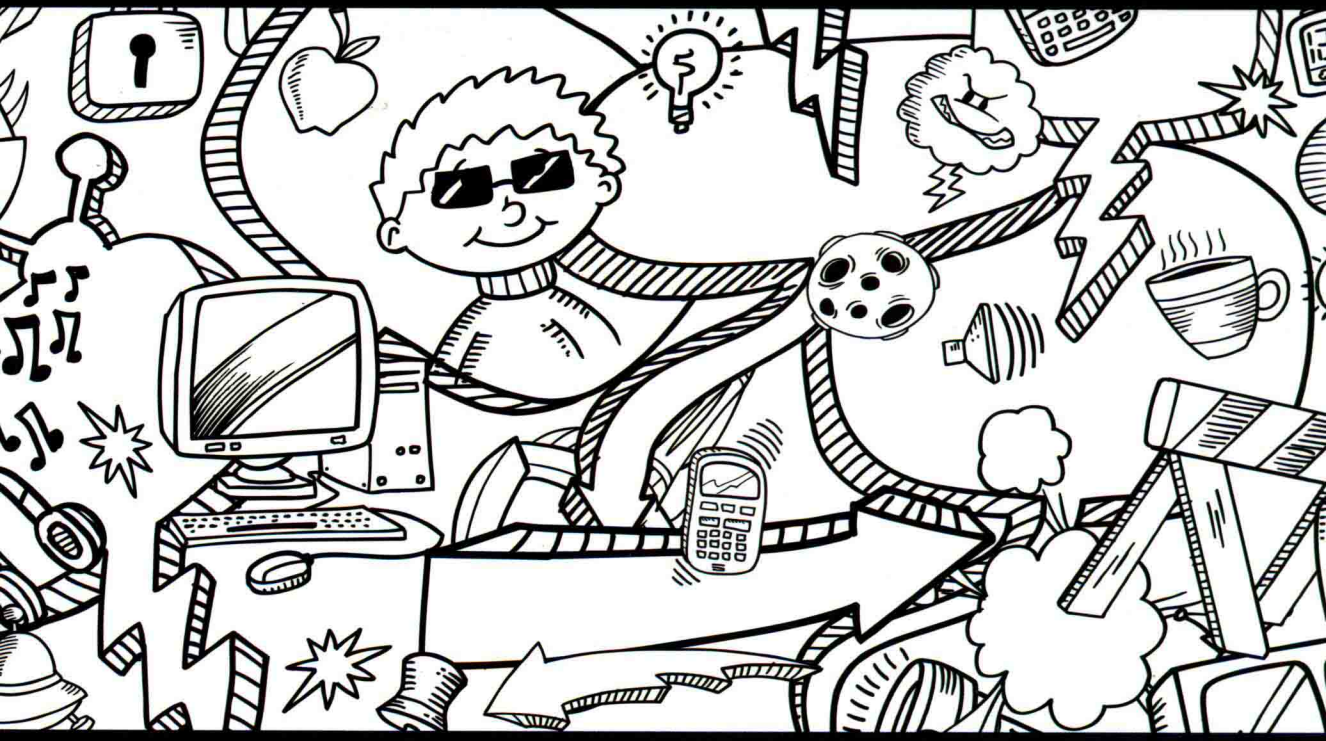
ELSEVIER 安全技术大系

Broadview
www.broadview.com.cn

深入热点实例分析，熟练编写Python代码，全面晋级为安全技术达人！

Python绝技

运用Python成为顶级黑客



Violent Python

A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers

[美] TJ.O'Connor 著

崔孝晨 武晓音 等译

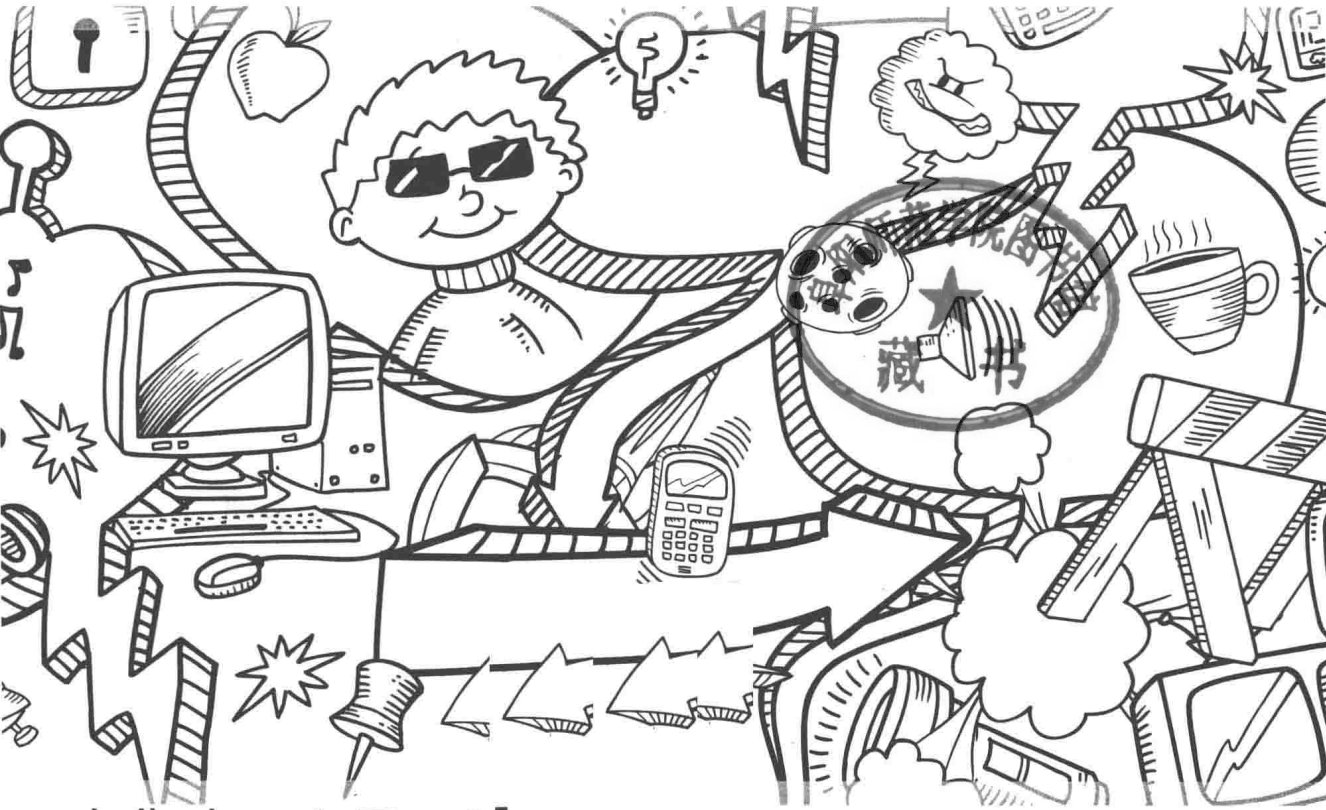
中国工信出版集团

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

安全技术大系

Python绝技

运用Python成为顶级黑客



Violent **Python**

A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers

[美] TJ.O'Connor 著

崔孝晨 武晓音 等译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

Python 是一门常用的编程语言，它不仅上手容易，而且还拥有丰富的支持库。对经常需要针对自己所处的特定场景编写专用工具的黑客、计算机犯罪调查人员、渗透测试师和安全工程师来说，Python 的这些特点可以帮助他们又快又好地完成这一任务，以极少的代码量实现所需的功能。本书结合具体的场景和真实的案例，详述了 Python 在渗透测试、电子取证、网络流量分析、无线安全、网站中信息的自动抓取、病毒免杀等领域内所发挥的巨大作用。

本书适合计算机安全管理人员、计算机犯罪调查和电子取证人员、渗透测试人员，以及所有对计算机安全感兴趣的爱好者阅读。同时也可供计算机、信息安全及相关专业的本/专科院校师生学习参考。

Violent Python: A Cookbook for Hackers, Forensic Analysts,Penetration Testers and Security Engineers
TJ. O'Connor
ISBN: 978-1597499576
Copyright © 2013 by Elsevier Inc. All rights reserved.
Authorized Simplified Chinese translation edition published by the Proprietor.
Copyright © 2015 by Elsevier (Singapore) Pte Ltd. All rights reserved.
Published in China by PHEI under special arrangement with Elsevier (Singapore)Pte Ltd.. This edition is authorized for sale in the mainland of China only, excluding Hong Kong, Macau SAR and Taiwan. Unauthorized export of this edition isa violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由 Elsevier (Singapore) Pte Ltd.授予电子工业出版社在中国大陆地区（不包括香港、澳门特别行政区以及台湾地区）出版与发行。未经许可之出口，视为违反著作权法，将受法律之制裁。本书封底贴有 Elsevier 防伪标签，无标签者不得销售。
版权贸易合同登记号　图字：01-2013-4712

图书在版编目（CIP）数据

Python 绝技：运用 Python 成为顶级黑客 /（美）奥科罗（Connor,T.）著；崔孝晨等译. —北京：电子工业出版社，2016.1
（安全技术大系）
书名原文：Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
ISBN 978-7-121-27713-9

Ⅰ. ①P… Ⅱ. ①奥… ②崔… Ⅲ. ①软件工具－程序设计 Ⅳ. ①TP311.56

中国版本图书馆 CIP 数据核字(2015)第 285621 号

策划编辑：刘　皎
责任编辑：李利健
印　　刷：三河市鑫金马印装有限公司
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：16.5　字数：325 千字
版　　次：2016 年 1 月第 1 版
印　　次：2016 年 6 月第 5 次印刷
定　　价：79.00 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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819　faq@phei.com.cn。

序一

在我从事信息安全技术研究学习的近 20 年间，带领过不少安全团队，发现编程能力是真正黑客和“脚本小子”的本质区别，在安全研究人员和希望成长为黑客高手的技术爱好者们的成长过程中一直面临着一个编程语言的选择问题，但是 Python 在黑客领域拥有着霸主的地位。在 XCon 召开的这 15 年中，Python 被越来越多地应用，越来越多的优秀黑客工具和安全工具都是用 Python 开发的，Python 已经发展成为和 C/C++一样作为黑客必备的技能之一。

Python 是一门非常优秀的主流编程语言，拥有用户友好的语法和大量的第三方模块。它提供了一个更好的支撑平台，能明显平缓大多数程序员初学攻击技术时的学习曲线。这本书涵盖了黑客、渗透测试人员、取证分析师和安全工程师需要具备的很多技巧。

Python 是一门优秀的黑客编程语言，复杂度低、效率高，入门门槛低，尽管已经有了很多攻击工具，但 Python 为编写你自己的攻击工具提供了一个极好的开发平台，仍然对解决某些特定条件下那些已有工具无法处理的问题。这本书的特点是剖析技巧的本质，使用 Python 内置模块和优秀的第三方模块来完成，并通过众多实例引领读者更好地体会理解 Python 的技巧和用法。

本人与本书译者相识相交多年，亦师亦友。我们经常在一起讨论交流技术，探讨发展，对译者的技术水平和经验能力是非常认可与钦佩的，也多次邀请他来 XCon 和 XKungfoo 进行演讲并分享技术，每每演讲都是博得广大技术高手的赞扬与认可。从此书中可以看出，作者在攻防、取证和编程多反面的深厚功底，也可以看出译者在这方面的超强能力和丰富经验。这本书包含渗透测试、Web 分析、网络分析、取证分析，以及利用无线设备等方面的 Python 攻击利用方法，并且书中采用的实例都会深入浅出地讲解说明 Python 该如何帮助你实现各种攻击的方法。不管你是刚开始学习 Python 程序的小白，还是一个具有丰富经验的渗透攻击高手，这本书都会给你非常大的帮助，引领你成为顶级的黑客高手。

在我创办的“神话——信息安全人才颠覆行动”中，Python 是我们的必修课之一。本书将会是我们“神话行动”学员学习的专业书籍之一。

王英键（呆神）

XCon 创始人，神话行动创始人，XFocus 创始人之一

试读结束：需要全本请在线购买： www.ertongbook.com

序二

作为一名安全研究从业人员，在日常工作中经常需要编写代码来解决一些简单的自动化文本处理、验证自己的某些推测、编写一套工具等。回眸大学时代，那时候不明白脚本语言的强大性，遇到任何问题一概用 C 语言来解决。久而久之，发现自己的研究进度总是比别人慢，有时候一些非常简单的字符串处理排版问题，用 C 语言一写就是几个小时，而用脚本几分钟就能搞定。在这之后，我逐渐开始改用 VBScript 作为我主要的脚本编写语言，并且在很长一段时间里满足了我绝大多数的需求。某天，当我接到一个应急响应任务，在 Linux 上做一些日志搜集分析时，已经理解脚本语言强大的快速开发能力的我，只能用非常愚蠢的办法——将日志复制到 Windows 上再处理，而就在那时，我已经感到，熟悉一门更加强大、跨平台的脚本语言迫在眉睫。自那之后，我逐渐接触了 Perl，并且能够通过 Perl 来满足一些日常的需要。可是，Perl 代码的可读性总是让我在看别人代码的时候显得毫无效率，在朋友的推荐下，我最终选择了 Python。

Python 是一门非常容易上手的脚本语言，相比 Perl 语言，我几乎是在完全不懂 Python 语法的情况下读懂了网上一些简单的 Python 代码，在简单的语法学习之后，便可以事半功倍地满足日常需要。Python 对于白帽黑客来说，也是必须掌握的一门脚本语言。相比其他脚本语言来说，其丰富的库几乎可以覆盖安全研究的方方面面，例如：强大的 Scapy 库可以很方便地实现跨平台的网络嗅探、网络发包等需求；文档分析工具 PyPDF 提供了强大的 PDF 格式解析功能，这些功能对 PDF 格式的 Fuzz 测试、PDF 0day 的分析，甚至 PDF Exploit 的编写都起了极大的帮助。这样的例子还举不胜举，在我参加的两届 Pwn2Own 黑客大赛的准备过程中，我几乎天天和 Python 打交道。例如，在使用 IDA 分析一个 OS X 的服务时，编写一个 IDA Python 脚本可以将一些没有符号的接口提取出来进行测试，对函数进行 Pattern 筛选，找出可疑函数进行进一步代码审计；在 Exploit Safari 中，堆布局是非常关键的一环，lldb 提供的 Python 接口可以很方便地对 WebKit 对象进行分析，对每个 WebKit 对象大小以及快速发现对象的可利用特性，对最终编写出完整的攻击代码起了决定性的作用。

虽然 Python 脚本上手容易，要迅速掌握其丰富的安全工具库并熟练运用绝非易事。我刚接触 Python 语言时，很多朋友就对我说过：Python 是一门非常适合白帽黑客学习的语言，然而我却在很长一段时间里一知半解，用了几年时间理解了这句话的含义。多而杂的工具库需要时间和经验的积累，才能慢慢“吃透”和掌握。市面上的 Python 入门书籍虽然非常多，但真正从安全从业者角度深入浅出介绍的书籍几乎没有。本书的出现无疑给安全从业者带来了福音，对 Python 初学者来说，第 1 章内容可以使其迅速掌握 Python 语言。而之后的几章几乎涵盖了安全研究的每个方面，并且配以近几年比较热门的案例（例如：LOIC、Conficker 等），无论你是进行漏洞研究还是取证分析、渗透测试、DDoS 对抗、反病毒等，都可以从本书中学到有用的知识和技能，使自己在学习过程中少走弯路，在工作中事半功倍。更加难得的是，负责本书翻译工作的崔孝晨老师是一位具有极其丰富数字取证从业经验的安全界专家，并且他曾经翻译过多本安全技术书籍，只有像他这样国内顶级安全从业者并且具备丰富翻译经验的专家，才能将这样一本好书的精髓以中文的方式原原本本地还原在读者面前，而读者也可以从字里行间体会到他“功力”的深厚。

相信读者会从本书中受益良多。

陈良

KeenTeam 高级研究员

译者序

Python 是一门非常常用的编程语言，除应用在科学计算、大数据处理等人们熟知的领域外，在计算机安全领域中使用也非常广泛。这是因为对黑客、软件逆向工程师、电子取证人员来说，Python 与 C/C++语法上的相似性使它上手十分容易。

本人大约在 2008 年通过 IDAPython 接触到了 Python 语言。相对于 IDA 自带的 IDC 脚本来说，IDAPython 的功能非常强大，可以很方便地搞定用 IDC 完成起来很麻烦的一些工作；而相对于用 C/C++开发 IDA 插件，IDAPython 使用非常灵活，要写的代码量也少了很多，当时感觉真是“出门在外、居家旅行、杀人越货之必备良药”。当时，Immunity Debugger 等各种常用工具也都支持 Python 脚本，甚至出现了纯用 Python 打造的计算机内存取证分析工具——Volatility。

2010 年，我应丁赟卿之邀，成为他翻译的大作《Python 灰帽子：黑客与逆向工程师的 Python 编程之道》一书的技术审校，审校的过程也使我对 Python 在安全领域所能发挥的作用有了更深刻的理解。但美中不足的是，该书仅仅介绍了在一些调试器、反汇编器等安全专用工具中 Python 的使用方法，甚至可以说它只是对一些专用的 Python 库的介绍。当然，这些很重要，但除此之外，Python 的强大功能应该能在更多的场景下发挥作用。

应该说这本 *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers*（《Python 绝技：运用 Python 成为顶级黑客》）确实是填补了这方面的空白：书中结合具体的场景，甚至是真实的案例，详述了 Python 在渗透测试、电子取证、网络流量分析、无线安全、网站中信息的自动抓取、病毒免杀等领域内的用途。每一章都针对一个专门的领域，完全用 Python 完整实现了非常实用的功能，而且代码量非常少。

本书在国外 Amazon 网站上的评价也非常高——76 个用户评价，得分 4 星半，是很高的分数。

本书由上海公安高等专科学校基础教研部的教师教官翻译完成，全书共 7 章，分工安排如下：

第 1、2 章由武晓音翻译，第 3 章由崔孝晨翻译，第 4 章由吴杰丽翻译，第 5 章由孙蓓翻译，第 6 章由王宏翻译，第 7 章由龚济悦翻译。全书由崔孝晨统一审校。

本书中文版的面世要感谢博文视点的各位编辑老师，特别是李利健、刘皎老师，感谢你们对我的一贯支持和耐心指导，使我从中获益良多！同时也要感谢你们为本书的出版所花费的大量时间！

由于翻译时间仓促，书中的错误在所难免，敬请读者不吝指正。

崔孝晨

2015 年 10 月

致谢

军事用语中，“观察你的六点钟方向”意思是说要你注意后方。当小队长在观察十二点钟方向的情况时，小队中至少应该有一名队员转向后方，观察六点钟方向有无小队长无法观测到的敌情。当我第一次去找出版本书的指导老师时，他就告诫我：在我的队友专注于观察我的六点钟方向时，我能做的唯一一件事就是：也好好地看着他的六点钟方向。我当时略加思索，付出这么大的努力对我这一生会有什么回报？三秒钟之后，我意识到：他们都是很棒的。

感谢我的技术编辑——Mark Baggett，你兢兢业业的技术校订保证了这本书的质量。感谢 Reeves 博士、Freeh 博士、Jacoby 博士和 Blair 博士——感谢你们对一个年轻急躁的军官的多年栽培，把我变成了这么一名能写出一本书的非传统学者。感谢 Fanelli 博士，感谢您教导我：神明变化之才，必出于规矩方圆之手，踏实打好基础，别老想着不走寻常路。感谢 Conti 博士，感谢您总是及时地引导我大胆采取行动。感谢我的同窗校友，特别是“忍者”社团的 Alan、Alex、Arod、Chris、Christina、Duncan、Gremlin、Jim、James、Kevin、Rob、Steven、Sal 和 Topher——你们的创新不断地激发着我的灵感。

感谢 Rob Frost，你写的“网络侦查”那一章比我写的强太多了！感谢 Matt、Ryan、Kirk、Mark、Bryan 和 Bill，感谢你们理解我之前为什么整晚不睡觉，眼瞅着时针从 1 走到 12。感谢我深爱的妻子，我调皮的儿子和我的忍者公主——感谢你们在我写本书的过程中，给我无条件的爱、理解和支持。感谢我的父母——感谢你们对我价值观的教育。最后还要感谢 Cook 博士——上战车，兄弟！

参编作者——Robert Frost

2011 年 Robert Frost 毕业于美国军事学院，随后成为一名陆军通信兵。他以优异的成绩获得了计算机科学的理学学士学位，其毕业论文主要关注于开源信息的收集。在 2011 年度电子防御练习赛中，由于他规避规则的能力，Rob 个人被公认为国家锦标赛团队中最优秀的两名成员之一。Rob 也参加并赢得了多次电子安全竞赛。

试读结束：需要全本请在线购买： www.ertongbook.com

技术编辑——Mark Baggett

Mark Baggett 是 SANS 的认证讲师，担任了 SANS 的渗透测试课程体系中多门课程的授课任务。Mark 是提供应急响应和渗透测试服务的深度防御公司的首席顾问和创始人。目前他是 SANS 防御部门的技术指导教师，专注于把 SANS 的资源实际应用于提升军事能力的方向。

Mark 在跨国公司和财富 1000 强企业中拥有多个信息安全职位。他曾经是一名软件开发者、网络和系统工程师、安全管理员和 CISO（首席信息安全官）。作为一名首席信息安全官，Mark 对信息安全策略的制定、遵守情况、应急事件的响应，以及其他信息安全操作负责。Mark 掌握当前在销售、实现和支持信息安全时，信息安全专家所面临挑战的第一手资料。Mark 也是信息安全社区中的一名活跃成员，是 Greater Augusta ISSA 的创始人兼总裁。他拥有包括 SANS 声誉卓著的 GSE 在内的多张认证证书。Mark 的个人博客中对多个安全主题均有涉猎，其地址为：http://www.pauldotcom.com。

前言

Python 是黑客的语言，具有低复杂度、高效率和几乎无限多的第三方库，入门门槛低，拥有这一切的 Python 为你编写自己的攻击工具提供了一个极好的开发平台。如果你使用的是 Mac OS X 或 Linux，那么还有个额外的优势——它已经在系统中预装好了。尽管已经有了很多攻击工具，但学习 Python 仍有助于你应付那些现有工具无法对付的困难情况。

目标读者

尽管每个人的基础不尽相同，但无论你是一个有意学习如何编写 Python 程序的菜鸟，还是一个想学习怎样把自己的技术运用在渗透测试中的编程老手。这本书都适合你。

本书组织结构

在写本书的过程中，我们确实是想把它写成一本以 Python 黑暗面案例构成的暗黑秘籍。接下来的内容中提供了渗透测试、Web 分析、网络分析、取证分析，以及利用无线设备等方面的 Python 操作清单。我希望这些例子能够激发起读者编写自己的 Python 脚本的热情。

第1章：入门

如果你之前没有 Python 编程经验，第 1 章将提供关于这一语言、变量、数据类型、函数、迭代、语句块和如何使用模块等背景信息，并通过编写一些简单的程序系统地学习它们。如果你已经能够完全驾驭 Python 编程语言，则完全可以跳过本章。在第 1 章之后的各章之间几乎都是独立的，你完全可以根据自己的喜好决定阅读的顺序。

第2章：用Python进行渗透测试

第 2 章中介绍使用 Python 编程语言在渗透测试中进行脚本化攻击的思想。本章中的例子包括编写一个端口扫描器，构建一个 SSH 僵尸网络，通过 FTP 进行“批量入侵”（mass-compromising），重新写一个“Conficker”病毒，以及编写一段漏洞利用代码（exploit）。

第3章：用Python进行取证调查

第 3 章介绍用 Python 进行电子取证。本章中的例子包括确定计算机的地理位置信息、恢复被删除的数据、从 Windows 注册表中提取键值。检查文档和图片中的元数据，以及检查应用程序和移动设备备份文件中记录的信息。

第4章：用Python进行网络流量分析

第 4 章介绍使用 Python 分析网络流量。本章涉及的脚本有：从抓包文件中 IP 地址对应的地理位置，调查流行的 DDoS 工具包、发现诱骗扫描（decoy scan），分析僵尸网络的流量及挫败入侵检查系统。

第5章：用Python进行无线网络攻击

本章的例子展示了如何嗅探和解析无线流量、编写无线键盘记录器、识别隐藏的无线网络、远程控制无人驾驶飞行器（Unmanned Aerial Vehicles，UAV）、识别出正在被使用的恶意无线工具包、追踪蓝牙设备，以及编写蓝牙漏洞的利用代码。

第6章：用Python刺探网络

第 6 章演示了使用 Python 刺探网络获取信息的技术。本章的例子包括通过 Python 匿名浏览网络、利用开发 API 工作、在流行的社交网站上收集信息以及生成钓鱼邮件。

第7章：用Python实现免杀

在最后一章，也就是第 7 章中，我们要编写一段能逃避杀毒软件检测的恶意软件。另外，我们还要写一个脚本把我们的恶意软件上传到一个在线病毒扫描器上，验证它是否真能做到免杀。

本书的Web站点

本书涉及的所有代码都被放在了本书的 Web 站点上。读者可以在阅读本书时访问 http://www.elsevierdirect.com/companion.jsp?ISBN=9781597499576 下载代码、分析样本，以及进行网络抓包文件。

目录

试读结束：需要全本请在线购买： www.ertongbook.com