Broadview
www.broadview.com.cn

no starch press

Python黑帽子

黑客与渗透测试编程之道

Black Hat Python

Python Programming for Hackers and Pentesters

【美】Justin Seitz 著

孙松柏 李聪 润秋 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

Python黑帽子

黑客与渗透测试编程之道

Black Hat Python

Python Programming for Hackers and Pentesters

【美】Justin Seitz 著

孙松柏 李聪 润秋 译

電子工業出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

本书是畅销书《Python 灰帽子——黑客与逆向工程师的 Python 编程之道》的姊妹篇，那本书一面市便占据计算机安全类书籍的头把交椅。本书由 Immunity 公司的高级安全研究员 Justin Seitz 精心撰写。作者根据自己在安全界，特别是渗透测试领域的几十年经验，向读者介绍了 Python 如何被用在黑客和渗透测试的各个领域，从基本的网络扫描到数据包捕获，从 Web 爬虫到编写 Burp 扩展工具，从编写木马到权限提升等。作者在本书中的很多实例都非常具有创新和启发意义，如 HTTP 数据中的图片检测、基于 GitHub 命令进行控制的模块化木马、浏览器的中间人攻击技术、利用 COM 组件自动化技术窃取数据、通过进程监视和代码插入实现权限提升、通过向虚拟机内存快照中插入 shellcode 实现木马驻留和权限提升等。通过对这些技术的学习，读者不仅能掌握各种 Python 库的应用和编程技术，还能拓宽视野，培养和锻炼自己的黑客思维。读者在阅读本书时也完全感觉不到其他一些技术书籍常见的枯燥和乏味。

本书适合有一定编程基础的安全爱好者、计算机从业人员阅读，特别是对正在学习计算机安全专业，立志从事计算机安全行业，成为渗透测试人员的人来说，这本书更是不可多得的参考。

版权贸易合同登记号　图字：01-2015-3483

图书在版编目（CIP）数据

Python 黑帽子：黑客与渗透测试编程之道 /（美）塞茨（Seitz,J.）著；孙松柏，李聪，润秋译. —北京：电子工业出版社，2015.8
书名原文: Black Hat Python: Python Programming for Hackers and Pentesters
ISBN 978-7-121-26683-6

Ⅰ. ①P… Ⅱ. ①塞… ②孙… ③李… ④润… 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（2015）第 164267 号

策划编辑：张春雨
责任编辑：郑柳洁
印　　刷：北京天宇星印刷厂
装　　订：三河市华成印务有限公司
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：12.75　　字数：220 千字
版　　次：2015 年 8 月第 1 版
印　　次：2015 年 10 月第 3 次印刷
定　　价：55.00 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到 dbqq@phei.com.cn。
服务热线：（010）88258888。

致 帕特

尽管我们从未谋面，我永远感谢您那个有趣的家庭里每一位成员带给我的快乐。

加拿大癌症协会

www.cancer.ca

关于作者

Justin Seitz 是 Immunity[1]公司的高级安全研究员，他在该公司的主要工作是寻找软件漏洞、开展逆向工程、撰写攻击代码，以及使用 Python 编程。同时，他还是畅销书《Python 灰帽子——黑客与逆向工程师的 Python 编程之道》（*Gray Hat Python*）的作者，该书是第一本讲授如何使用 Python 进行安全分析的书籍。

关于技术编辑

Dan Frisch 在信息安全界有超过十年的工作经验。目前，他是加拿大一家律师事务所的高级安全分析师，在此之前，他曾作为顾问，为北美地区的金融和科技公司进行安全评估。他沉迷于黑客技术并且拥有跆拳道黑带三段的身份，你可以认为 Dan 就是黑客帝国中人物的现实版。

从早期的 Commodore 个人电子处理器和 VIC-20 机器时代开始，计算机技术就已经成为 Cliff Janzen 的一个固定伙伴（从某种程度上来说，Cliff 痴迷于技术）。在 IT 运维界混迹了十年后，Cliff 发现了他的职业热情所在，于 2008 年转行到信息安全领域。在过去的几年里，Cliff 非常开心地作为一名安全顾问服务于各个公司，无论是做安全策略评估还是做渗透测试，他为能够将自己的职业生涯和兴趣所在相结合感到非常幸运。

1. Immunity 是一家专注于计算机安全漏洞的公司，它的主打产品 Immunity Canvas 是与 Core Imapct 和 Metsaploit 齐名的三大渗透攻击测试平台之一。Immunity Canvas 全部使用 Pyhton 语言开发。
——译者注

译 者 序

毫无疑问，在脚本语言的世界里，Python 已经变得足够强大且流行。这不仅是因为 Python 简练的语法风格和非常高的开发效率，还由于 Python 拥有最活跃的开发社区和数量庞大的第三方库。用 Python 编写的代码短小而精干，越来越多的技术人员开始使用 Python 作为第一语言进行编程。

在渗透测试的过程中，我们可能面对非常复杂的网络环境，其中任何一个环节都可能是我们的突破点。这不仅要求我们全面掌握各种系统和环境的薄弱环节，然后使用工具或者编程进行测试，而且要求我们有快速处理和灵活应变的能力。特别是在分秒必争的 CTF 竞赛中，快速编码的能力显得尤为重要。使用 Python 能很好地满足这些要求。

本书是畅销书 *Gray Hat Python*（《Python 灰帽子——黑客与逆向工程师的 Python 编程之道》）的姊妹篇。在那本书中，作者介绍了 Python 在逆向工程和漏洞挖掘方面的强大功能；而在本书中，作者介绍了 Python 如何被用在黑客和渗透测试的各个领域，从基本的网络扫描到数据包捕获，从 Web 爬虫到编写 Burp 扩展工具，从编写木马到权限提升等。作者是一位经验非常丰富的安全工作人员，他结合自己在工作中经常碰到的问题、经常需要使用的工具等，运用大量的实例向我们展示如何轻松地使用 Python 迅速、高效地编写符合我们要求的工具。除了一些基本的 Python 编程技能，如使用 Socket 编写客户端与服务端、使用原始套接字和 Scapy 库进行嗅探，作者在本书中的很多实例都非常具有创新和启发意义。例如，HTTP 数据中的图片检测，基于 GitHub 进行命令和控制的模块化木马，浏览器的中间人攻击技术，利用 COM 组件自动化技术窃取数据，通过进程监视和代码插入实现权限提升，通过向虚拟机内存快照中插入 shellcode 实现木马驻留和权限提升等。通过阅读本书，读者不仅能学到各种 Python 库的应用和编程技术，还能拓宽视野，培养和锻炼自己的黑客思维，这使得读者在阅读本书的过程中不会感觉如阅读普通技术书籍那样的枯燥和乏味。

同时，作者在大部分实例的讲解过程中，指明了工具需要进一步拓展和完善的地方，并将这些工作布置为家庭作业。我建议读者按照作者的要求修改和完善这些工具，因为这个过程不仅能获得对已学知识的巩固和提升，还能获得满满的成就感！

在网络安全领域，我们通常将只懂得使用已有工具的黑客称为“脚本小子”。现在，有了本书，稍加学习和运用，你就能编写出功能足够强大的工具。赶紧行动起来，摆脱这个带有歧视性质的称呼吧！

本书的翻译分工如下：孙松柏翻译前言、第 1 章、第 2 章、第 5 章和第 6 章；李聪翻译第 3 章、第 4 章、第 7 章和第 8 章；　　翻译第 9 章、第 10 章和第 11 章。第 1 章、第 2 章、第 6 章、第 9 章和第 10 章由李聪负责审阅，第 3 章、第 4 章和第 11 章由孙松柏负责审阅，　　审阅第 5 章、第 7 章、第 8 章。本书的翻译工作由孙松柏负责组织和统筹。

由于水平有限，翻译中难免出现一些错漏和表达不准确的地方，恳请读者批评指正。

李聪

2015 年 5 月于广东

推荐序一

感谢孙松柏邀请我提前阅读此书，这本书读起来很顺畅，覆盖了黑客或渗透师常用的很多技巧。这本书的特点是，剖析技巧的本质，然后用 Python 的内置模块或优秀的第三方模块来实现之。

Python 是一门非常酷的主流语言，拥有优美的编码风格、顽强的社区与海量优质的模块，如果我们看到一段代码写得很好，我们会说："Pythonic！"这本书用 Python 来打造渗透过程中用到的各类技巧与工具，也不得不说："Pythonic！"。

从这本书里可以看出作者丰富的渗透经验与 Python 经验，感谢作者能把自己的经验如此清晰地分享出来，也感谢出版社能将这本书引入国内。

这本书的发行，会让更多人投身进 Python 黑客领域，不再是只用他人工具的"脚本小子"，而是在必要时刻，能用 Python 打造属于自己的利用工具。

Python 有句格言是"人生苦短，快学 Python"。是的，人生苦短，如果你立志成为一名真正的黑客，Python 值得你掌握，这本书是一个非常好的切入点。

余弦，知道创宇技术副总裁

推荐序二

曾经去高校　讲，被同学们问得最多的问题就是，如何成为一名黑客。成为一名　　的黑客高手，也是我们这批追求安全技术的人的　想。

那么，如何成为高手呢？两个秘　：持之以　和动手实践。

我记得刚刚接触计算机那会　，机缘巧合之下买到本安全技术杂志月　，但是由于水平所限，每篇技术文章都看不懂。不过我每期都买来看，大　持续了半年，慢慢地发现能够看懂了，后来甚至还可以在杂志上发表文章发布黑客工具了。就这样　持着，最终　进了安全行业。

古人说“　上得来终觉浅，绝知此事要　行”，意思就是要多实践，要想成为黑客高手的另一个秘　就是要多实战。实战中一定会涉及开发自己的工具或者优化别人的代码，所以就要求我们必须精通一门甚至多门脚本语言。Python就是这样一门强大的语言，很多知名的黑客工具、安全系统框架都是由Python开发的。比如功能强大的Fuzzing框架Sulley、交互式数据包处理程序Scapy都是Python开发的，基于这些框架可以扩展出自己的工具（多学一些总是好的，我们在这里也不用争论是Python好还是Perl好这样的问题）。

就我个人的经验来看，与实战结合是快速学习相关能力的最佳路径。这本《Python黑帽子：黑客与渗透测试编程之道》就是从实战出发，基于实际攻防场景讲解代码思路，是能够让读者快速了解和上手Python及黑客攻防实战的一本书，所以特别推荐给大家。

知易行难，大家在读书的同时不要忘记实践：先　懂原理，再根据实际需求写出一个强大的Python工具。

——腾讯安全中心副总监 胡珀（lake2）

推荐序三

Python 是网络安全领域的编程利器，在分秒必争的 CTF 赛场中拥有绝对的统治位置，在学术型白帽研究团队和业界安全研究团队中也已经成为第一编程语言。本书作者在畅销书《Python 灰帽子——黑客与逆向工程师的 Python 编程之道》之后，再次强力推出姊妹篇《Python 黑帽子：黑客与渗透测试编程之道》，以其在网络安全领域，特别是漏洞研究与渗透测试方向上　　十数年的经验积累，献上了又一本经典的 Python 黑客养成手册。作为与三位译者曾经　师　友的合作伙伴，我非常高兴地看到他们能够以精准的翻译、专业的表达将这本书原　原味地带给国内的读者们。

诸葛建伟
清华大学副研究员
蓝莲花战队联合创始人及领队
XCTF 联赛联合发起人及执行组织者

推荐序四

我们一直认为，一个合格的安全从业者必须具有自己动手编写工具和代码的意愿和能力。在这个安全攻防和业务一样日趋大数据化、对抗激烈化又隐蔽化的年代，攻防双方都必须能有快速实现或验证自己想法的能力，选择并学习使用一个好的工具会起到事半功倍的效果。

Python 则是目前最适合这种需求的语言，平缓的学习曲线、胶水语言的灵活性和丰富的支持库使其天然成为了攻防双方均可使用及快速迭代的利器，几乎可以覆盖安全测试的方方面面。在我求学时，使用 scapy（本书中作了详细介绍）和 PyQt 库编写了 Wifi 嗅探工具 WifiMonster，参加的 CTF 比赛中，基本所有的 exploit 也都是基于 Python 的 pwntools 和 zio 库编写；在 Keen，我们的很多 fuzzer 和静态分析器也都是用 Python 编写的。

但令人遗憾的是，目前高校计算机和信息安全专业很少有将 Python 及其在安全领域方面的应用列入培养计划的，也缺乏相关书籍供从业人员学习。本书弥补了这个空白：本书作者从逆向和漏洞分析挖掘的角度编写了《Python 灰帽子——黑客与逆向工程师的 Python 编辑之道》后，又从渗透测试和嗅探、取证的角度编写了本书，介绍了 Python 在这些方面的应用和相关库的使用。本书译者也都在安全领域具有丰富经验，并翻译过多本安全技术书籍，保证了本书的翻译质量。

相信读者们会从本书中受益良多。

何淇丹（a.k.a Flanker，Keen Team 高级研究员）

2015 年 7 月于上海

推荐序五

在接触信息安全之前我就已经将 Python 作为我最常用的语言了，它能满足我日常工作的所有需求。因为对 Python 已经有了一定了解，在我接触信息安全以后，它也使我在信息安全领域的探索进行得很顺利。

老牌大黑客查理·米勒说的没错："脚本小子和职业黑客的区别是黑客会多编写自己的工具而少用别人开发的工具。"我从事 Web 渗透相关工作、参加 CTF 竞赛的时候，基本都在使用自己写的 Python 脚本来实现自己的目的：扫描收集目标信息，测试大量已知漏洞是否存在，对 SQL 注入、XSS 攻击点的自动发现，对攻击进行抓取、截获、重放，在比赛中大量部署后门进行控制。

Python 中有大量的第三方库可以让你从无关的工作中脱身而出，专心去实现你所需要的功能（有时你甚至会发现有人已经把你所需要的功能很好地实现了），令人不被杂乱的事务所困扰。在 Web 渗透这种重视效率的工作中，在 Python 的帮助下快速地把自己的需求变成能运行的程序，实在是令人兴奋的一件事。

作者在本书中所给出的大量的样例和方向，足以让那些想利用 Python 使自己的 Web 渗透水平迅速提高的人们得到很大的帮助。但请记住，一定要动手。只有动手实践，才能真正体会到本书的精华所在。

Hacking the planet by Python!

陈宇森

北京长亭科技有限公司联合创始人，蓝莲花战队核心成员，BlackHat 2015 讲者

2015 年 7 月 1 日

推荐序六

编程语言的选择问题更像是一场信仰之战，尽管如此，Python 在信息安全界依旧是一门具有统治地位的语言。基于 Python 的工具，包括各种各样的模糊测试工具、代理工具，甚至包括偶尔出现的攻击代码。渗透攻击平台，如 CANVAS 也是用 Python 编写的，还有其他的工具，例如 PyEmu 和 Sulley 等。

我所写的每一个模糊测试工具或攻击代码都使用了 Python 语言。事实上，Chris Valasek 和我在最近对汽车黑客行为的研究过程中，还使用 Python 编写了一个库，将局域网控制器（CAN）的信息注入汽车网络中，实现对智能行车电脑的破解。

如果你对信息安全项目中的查漏补缺感兴趣的话，那么 Python 是一门非常值得学习的语言，因为 Python 中有大量的逆向工程和攻击代码库供你使用。现在，如果 Metasploit 的开发者能够顿悟，并且把开发语言从 Ruby 转到 Python 上，那么两大渗透测试平台阵营应该能够统一了。

在这本新书中，Justin 使用了大量的篇幅讨论具有进取精神的年轻黑客们应该如何迅速成长。他将在书中实际演练如何读取和生成网络数据包，如何在网络中进行嗅探，当然还包括 Web 应用审计和攻击方面的技术。在这之后，他将重点讨论如何编写代码针对 Windows 系统进行攻击。总而言之，《Python 黑帽子：黑客与渗透测试编程之道》是一本非常有趣的书。当然，这本书不能让你成为一个像我一样的超级大黑客，但至少可以为你指引一条正确的道路。记住，脚本小子和职业黑客的区别是编写自己的工具，少用别人开发的工具。

查理·米勒

圣路易斯，密苏里州

2014 年 9 月

前　言

Python 黑客，你可以用这个词来形容我。在 Immunity 公司，我非常幸运，能和一群真正懂得使用和编写 Python 的人一起工作。然而我不是他们中的一员。我将大量的时间用在渗透测试的工作中，这需要使用 Python 在短时间开发出工具，我们关注的是工具是否能正常执行和得到结果（而不关心这个工具是否好看、是否做过优化，甚至是否稳定）。通过本书你将看到我的编程方式，我感觉这种方式在某种程度上让我成为了一名优秀的渗透测试人员。我希望这种编程的哲学理念和风格也可以帮助你。

在阅读本书的过程中，你会了解到我不会对单一话题做深入的探讨，这是本书的一个特点。我想让读者浅尝辄止，并保留一定的兴趣，这样读者就可以获得基础知识。在此基础上，我通过每章的习题把我的一些想法留给读者，这样有助于读者独自思考并选择自己的方向。我鼓励读者朋友们实现这些想法，并非常乐意读者在实现一个具体项目、完成自己的工具或者家庭作业后给我反馈。

和其他技术书籍一样，读者对 Python 掌握程度的不同（或者对信息安全的理解不同）会使他们对本书有不同的体验。一些读者可能只会找出几个自己感兴趣的章节并进行深入学习，另一些读者可能会逐篇阅读。我的建议是，如果你是一个初级或中级的 Python 程序员，你可以按顺序通读本书，你将在本书的阅读过程中学到 Python 的精华部分。

简要介绍一下，我将在第 2 章介绍网络方面的基础知识，在第 3 章主要介绍原始套接字，在第 4 章介绍如何使用 Scapy 开发有趣的网络工具。本书的剩余部分将介绍如何攻击 Web 应用程序，具体来说，我们将在第 5 章介绍常用工具，在第 6 章介绍流行的 Web 应用渗透工具（Burp Suite）。从这里开始，我们将花大量的篇幅讨论木马，在第 7 章中讨论 GitHub 的命令与控制，在第 10 章

中讨论 Windows 权限提升的技巧。在最后一章中讨论使用 Volatility 自动检测攻击内存的取证技术。

我尽量保持全书样本代码的简短性和针对性，对代码注释也是如此。如果你是一个学习 Python 的新手，我建议你动手实践每一行代码以加强记忆。书中所有的源代码可以通过 *http://nostarch.com/blackhatpython/*链接下载。

现在让我们开始吧！

致　谢

感谢我的家庭——我美丽的妻子 Clare，我的 5 个孩子 Emily、Carter、Cohen、Brady 和 Mason，感谢他们在我写书的一年半期间给予我的鼓励和宽容。我的兄弟、姐妹、父母和 Paulette 同样在写书期间持续鼓励我，我爱你们。

致 Immunity 的所有同人（如果有足够的空间，我愿意在这里列出你们所有人的名字）：感谢你们每天对我的宽容，你们是一群了不起的工作伙伴。致 No Starch 出版社的 Tyler、Bill、Serena 和 Leigh，感谢你们对本书所做的辛勤工作，你们所有的建议我都接受并表示感谢。

感谢本书的技术编辑 Dan Frisch 和 Cliff Janzen。他们敲击并审阅了每一行代码，编写了支持代码，编辑和校验了书中代码的格式，并在本书出版的整个过程中对我给予了大力支持。任何撰写信息安全书籍的人都应该与他们合作，他们是值得称赞的合作伙伴。

感谢那些与我分享饮料、欢笑和聊天的死党们，感谢你们接受我在写书过程中对你们的发泄。

目　录