PACKT PUBLISHING

BackTrack 5 Cookbook

中文版

渗透测试实用技巧荟萃

BackTrack 5 Cookbook

[美] Pritchett Willie
[墨] David De Smet 著
Archer 译

人民邮电出版社
POSTS & TELECOM PRESS

BackTrack 5 Cookbook
中文版 渗透测试实用技巧荟萃

[美] Pritchett Willie
[墨] David De Smet 著
Archer 译

人民邮电出版社
北京

图书在版编目（CIP）数据

BackTrack 5 Cookbook中文版 : 渗透测试实用技巧荟萃 / (美) 威利 (Willie,P.), (墨西哥) 斯梅特 (Smet,D.D.) 著 ; 阿彻译. -- 北京 : 人民邮电出版社, 2014.5
ISBN 978-7-115-34867-8

Ⅰ. ①B… Ⅱ. ①威… ②斯… ③阿… Ⅲ. ①Linux操作系统－安全技术 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2014)第042555号

版权声明

◆ 著 [美] Pritchett Willie [墨]David De Smet
译 Archer
责任编辑 傅道坤
责任印制 彭志环 杨林杰

◆ 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
北京天宇星印刷厂印刷

◆ 开本：800×1000 1/16
印张：16.25
字数：317 千字 2014 年 5 月第 1 版
印数：1- 3 000 册 2014 年 5 月北京第 1 次印刷

著作权合同登记号 图字：01-2013-7462 号

定价：49.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

BackTrack 是一个基于 Linux 的渗透测试和安全审计平台，旨在帮助网络安全人员对网络黑客行为进行评估，如今被世界各地的安全社区和安全人员所使用。

本书分为 10 章，以示例方式讲解了 BackTack 中很多流行工具的使用方法，其内容涵盖了 BackTrack 的安装和配置、BackTrack 的调整、信息采集、漏洞识别、漏洞利用、提权、无线网络分析、VoIP、密码破解、电子取证等内容。

本书讲解详细，示例丰富，无论你是经验丰富的渗透测试老手，还是打算紧跟时代潮流，希望掌握 BackTack 5 中常用软件使用方法的新手，都会从本书中获益匪浅。

译者序

与人民邮电出版社合作翻译本书是我的荣幸，但是翻译这样一本安全题材的图书，也是我的隐忧。同是一种载体和同一种技术，铀可以成为洁净能源的来源，也可以变成毁灭文化的武器。计算机信息安全技术也面临同样的问题。距 20 世纪 PC 病毒问世尚不足 30 年，当下各国在探讨计算机信息安全事件时已经是谈虎色变。

请问尊敬的读者：您是否为保护绝大多数人的福祉而学习计算机安全技术呢？每一个“是”的回答，都会令我感到这近百小时的翻译和排版工作是值得的！

如果您有机会看到英文原书，将会发现作者就有这样的忧虑。例如原文有“URL 伪造和渗透”的标题，而正文却是现在看到的简单得多的“掌握 Arpspoof”——这一部分并不是我们刻意做了修改，而是作者因为害怕被滥用而进行了删减，只是标题没有更正过来。现在高校间计算机安全技术竞赛经常会涉及无线网络部分，我仅仅针对无线网络部分的“彩蛋”进行了标注。其实其他地方也偶尔能见到这种人为的纰漏，不过并不影响阅读；尤其是在互联网的帮助下，在略微理解作者意图后，“彩蛋”都不影响您进行相应的练习和使用。

君子有所为有所不为，知其可为而为之，知其不可为而不为。与作者一样，希望您能将相应的技术用于正确的行为上。同时，希望您有意愿加入我们的非商业活动中来，在学术研究、促进行业进步的公益舞台上展示您独到的风采！

Archer

idf.cn 与 cisrg.org 联合创始人

关于作者

Willie Pritchett，MBA，一名在 IT 领域有 20 余年的行业经验、热衷于信息安全的编程老手。他目前是 Mega Input Data Services 公司的总经理。Mega Input Data Services 公司不仅专注于安全和数据驱动的应用程序的开发，并且提供人力资源服务；是一家提供全方位服务的数据库管理公司。Willie 本人与国家和地方政府机构都有着融洽的合作关系，他为很多发展中的小型企业提供过技术服务。

Willie 持有众多行业认证，同时也在诸多领域进行培训，其中耳熟能详的培训项目有道德骇客与渗透测试（ethical hacking and penetration testing）。

我要感谢我的太太 Shavon，她在我著书的时候一直陪在我身边，支持我继续努力下去。感谢我的孩子 Sierra 和 Josiah，他们使我懂得珍惜宝贵的时间。感谢我的父母 Willie 和 Sarah，谢谢你们教给我职业的道德和人生核心的价值观，这些知识带领我挺过人生最难熬的日子。同时特别感谢我现在所有的同事、业内同仁和商业伙伴。他们在我选择了 IT 职业生涯时给予了我相应的机会，所以我的成绩就是你们的成绩。保护了众多的企业、并且帮助了他们发展——所有我所作的事情，也可归功于你们当初给我的机会和赏识。最后感谢所有的评审和技术顾问。他们在整个创作期间毫无保留地将独到见解与我分享。

David De Smet 自 2007 年起在软件行业工作。他是 iSoftDev 公司的 CEO 和创始人，担负着公司的很多事务。咨询、顾客需求分析、软件设计、软件编程、软件测试、软件维护、数据库开发、网页设计，这些工作仅是他职责中的一部分。

他在软件研发方面注入了无数的时间与热情，同时他也对黑客技术与网络安全持有浓厚的兴趣，并且为不少公司提供了网络安全评估的服务。

请允许我感谢 Usha Iyer 给我机会参加本书的著作。我也要感谢项目协调人 Sai Gamare 和本书的整个创作团队。感谢我的家人特别是女友 Paola Janahaní 给予我的支持和鼓励，最重要的是在我通宵达旦撰写本书时给予的耐心。

关于审稿人

Daniel W. Dieterle 在 IT 行业有 20 年以上的经验。他为从小型到大型的各类公司企业均提供过各种各样的技术指导。实际上 Daniel 非常享受信息安全领域的工作，他在各大期刊上发表过大量关于计算机安全的文章，并维护着一个名为“用数码武装计算机安全”（Cyber Arms Computer Security）的博客，其地址为 `cyberarms.wordpress.com`。

Daniel 是 Packt Publishing 出版社的老朋友了，他担任过 *BackTrack 5 Wireless Penetration Testing Beginner's Guide* 一书的技术审稿人，同时还是 *Hakin9 IT Security Magazine*、*eForensics Magazine*、*The Exploit Magazine*、*PenTest Magazine* 和 *Software Developer's Journal* 等期刊的技术审稿人。

感谢我美丽的夫人和女儿，谢谢她们在我参与本书审阅时给予的支持。

Abhinav Singh 来自印度，是一位年轻有为的信息安全专家。他在黑客技术和网络安全方面一直情有独钟，以至于最终选择做这行的全职工作。Packt Publishing 出版过的 *Metasploit Penetration Testing Cookbook*（该书中文版《Metasploit 渗透测试手册》由人民邮电出版社出版）就出自他的笔下。那本书介绍了渗透测试领域使用得最广泛的框架程序——Metasploit。

读者常常可以在门户网站和技术杂志上见到 Abhinav 著作的节选。在 SecurityXploded（安全大爆炸）社区中他也颇有名气。读者可以通过 `abhinavbom@gmail.com` 和 Twitter 账户 `@abhinavbom` 找到他。

感谢我的祖父母和他们的祝福，感谢父母给予的支持和姐姐对我的关照。

Filip Waeytens 在安全领域成名已经超过 12 年之久。从接触这个行业至今，他分别以安全工程师、安全经理、测试工程师的角色，从事各类大中行企业的跨国项目。

Filip 安全评估服务的客户群体颇为广泛，他的客户遍布银行、电信、工业生产环境、SCADA 和政府各个领域。他也为 Linux BackTrack 项目编写了许多安全工具，并且擅长渗透方面的培训。

音乐、电影和各种各样的放松活动是他的爱好。目前他与太太、两个女儿还有 4 只宠物小鸡定居在比利时。他特意向中文读者留言，读者可通过访问他的网站 http://www.wsec.be 与其进行沟通。

特别向 Muts、Max 和 MjM 致敬！他们是 BackTrack 的先驱。

前言

BackTrack 是为渗透测试而研发的 Linux 平台上的军火库，是辅助安全行业专业人士进行安全评估的一个平台，一种纯粹为渗透而产生的原生环境。BackTrack 基于 Debian GNU/Linux 受权发行，主要应用于信息领域的法证调查和渗透测试。Backtrack 这个名字由一种应用于渗透测试的算法 backtracking 而得来。

本书将介绍很多流行工具的操作方法，相信读者可以从中学会渗透测试的基础知识：信息收集、漏洞的识别与利用、提权，以及隐匿踪迹。

本书将从安装 BackTrack 5、设置虚拟测试环境着手介绍相关知识。在此之后，我们逐一涉及渗透测试的基本原则，例如信息收集、漏洞识别和利用。在读者熟悉这些之后，本书将开始讲解提权、无线网络分析、VoIP、破解密码和法证调查。

本书适合信息安全专业人士和希望入门的读者阅读。本书不仅提供了详细的介绍，并且列举了很多具体的操作范例，供您快速掌握 BackTrack 5 和渗透测试的相关领域知识。

希望您能够喜欢这本书！

本书内容

第 1 章，安装、运行 BackTrack，描述如何在测试环境中安装 BackTrack，以及如何配置 BackTrack，使其适用于您的网络。

第 2 章，调整 BackTrack，讲解安装常见的显卡、无线网卡安装和配置驱动程序的方法。

第 3 章，信息采集，介绍采集信息阶段需要用到的工具，例如 Maltego 和 Nmap。

第 4 章，漏洞识别，介绍 Nessus 和 OpenVAS 漏洞扫描工具的使用方法。

第 5 章，漏洞利用，通过对常用服务进行攻击来讲解 Metasploit 的使用方法。

第 6 章，提权，讲解很多工具（例如 Ettercap、SET 和 Meterpreter）的使用方法。

第 7 章，无线网络分析，讲解如何使用不同的工具评估无线网络安全。

第 8 章，VoIP，讲解各种用于攻击无线电话及 VoIP 系统的工具。

第 9 章，密码破解，讲解密码哈希和用户账户的破解方法。

第 10 章，电子取证，介绍用来恢复数据和加密的工具。

学习本书的先决条件

如果您需要使用书中的方法进行实践，您需要有一台计算机，而且它具有足够大的内存和硬盘空间，还要具有强大的处理能力，这样才能运行虚拟化的测试环境。本书提到的很多工具都需要同时运行多台虚拟机。第 1 章介绍的虚拟化工具可以在绝大多数的操作系统上运行。

本书读者对象

如果你打算紧跟潮流，希望掌握 BackTrack 5 中常见软件的使用方法，亦或是渗透测试经验丰富，本书都值得你一读。本书讨论的练习和实践，仅能用于符合道德和法律的用途。针对计算机网络的攻击或信息收集，应当获得相关机构或个人的完全同意。未经许可的操作，将会触犯法律，可能引起诉讼或者带来牢狱之灾。

免责声明：对于滥用本书知识而进行不道德实践的个人及行为，以及可能产生的法律后果，我们不负任何责任。因为同样的法律问题，我们强烈建议您参考本书设置测试环境的章节，建立自己的测试环境。

本书体例

警告或重要的提示会使用这种格式。

目录