安全技术经典译丛

灰帽黑客

正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术

(第 3 版)

Gray Hat Hacking:
The Ethical Hacker's Handbook, Third Edition

[美] Allen Harper, Shon Harris 等著

杨明军 韩智文 程文俊 译

专家级的系统攻击方法

最先进的渗透测试技术

最新安全漏洞和补救措施

恶意软件和rootkit的分析与捕获

缓冲区溢出、SQL注入、逆向工程

McGraw Hill Education

清华大学出版社

安全技术经典译丛

灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)

[美] Allen Harper
Shon Harris
等著
杨明军 韩智文 程文俊 译

清华大学出版社

北 京

Allen Harper, Shon Harris, et al.
Gray Hat Hacking: The Ethical Hacker's Handbook, Third Edition
EISBN：978-0-07-174255-9

北京市版权局著作权合同登记号　图字：01-2011-3514

图书在版编目(CIP)数据

灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第 3 版) / (美)哈珀(Harper, A.), (美)哈里斯(Harris, S.)等 著；杨明军，韩智文，程文俊 译. —北京：清华大学出版社，2012.11
(安全技术经典译丛)

ISBN 978-7-302-30150-9

书名原文：Gray Hat Hacking: The Ethical Hacker's Handbook, Third Edition

Ⅰ. ①灰… Ⅱ. ①哈… ②哈… ③杨… ④韩… ⑤程… 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(2012)第 222891 号

责任编辑：王　军　韩宏志
装帧设计：康　博
责任校对：蔡　娟
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：37.75　　**字　数**：895 千字
版　　次：2012 年 11 月第 1 版　　**印　次**：2012 年 11 月第1 次印刷
印　　数：1～3000
定　　价：79.80 元

产品编号：042870-01

译 者 序

当人类跨入网络信息时代，人们在享受信息技术带来的高效率的同时，也面临着更大的挑战：小到个人隐私信息，大到企业信息资产，再到国家信息安全，现代社会的方方面面都受到越来越多的网络威胁和攻击。2010 年伊朗核设施遭受 Stuxnet 蠕虫攻击，分析显示这次攻击针对的是该设施使用的西门子 SCADA 系统，最终导致浓缩铀离心机被病毒破坏。2011 年底 CSDN 用户数据库泄露事件导致众多中国互联网用户人人自危，因为泄露的用户数据中包含部分以明文方式保存的用户密码，而其中的相当一部分人在其他网站上也使用了同样的用户名和密码，从而可能导致泄露更多的数据。

不断出现的各类网络安全事件使得人们越来越重视网络信息安全的重要性。孙子说："知己知彼，百战不殆"。虽然没有绝对的安全，但如果能够做到知己知彼，了解敌方的攻击手段，包括如何利用漏洞(物理、信息系统)进入系统、如何展开攻击以及如何规避探测，那么对于防御战而言，即使不能百战百胜，也能做到及时发现漏洞，使损失最小化。

本书从渗透测试的角度来讨论网络攻防技术，在研究黑客攻击的策略、技能、工具和动机的同时，还探讨如何进行有效的防御。本书出自安全领域富有实战经验的专家之手，既包含广泛的、透彻的理论分析，又包括大量可操作性极高的实用范例。"魔高一尺，道高一丈"，安全领域的攻防技术日新月异。本书的作者来自安全一线战场，他们在本书中介绍了最新的黑客攻击技术和相应的防御手段，其中的大部分内容都是研究网络安全的不可多得的宝贵资料。

如果您是一位希望从事网络安全工作的新手，那么本书讨论的广泛主题能够让您对安全领域有一个综合性认识。而如果您是一名具有丰富实践经验的老兵，那么本书提供的最新攻防技术将会让您开阔视野，耳目一新。

本书主要由杨明军、韩智文、程文俊翻译。对于本书的翻译，我们力求做到语言平实无华、技术方面准确无误，希望能给读者带来轻松愉悦的阅读体验。

作者简介

Allen Harper，CISSP、PCI QSA，北卡罗莱纳州 N2NetSecurity, Inc.公司总裁和所有者。他曾在美国海军陆战队服役 20 年并在伊拉克“旅游”之后退役。此外，他还曾经担任美国财政部、国税局计算机安全应急响应中心(IRS CSIRC)的安全分析师。他经常在 Black Hat 和 Technot 等会议上发表演讲和授课。

Shon Harris，CISSP，Logical Security 总裁，作家、教育工作者和安全咨询师。曾经担任过美国空军信息战部队的工程师，并且出版过一些有关信息安全领域的不同学科的著作和论文。信息安全杂志(Information Security Magazine)曾经将她评为信息安全领域的 25 位最杰出的女性精英之一。

Jonathan Ness，CHFI，微软安全响应中心(MSRC)首席软件安全工程师。他和他的同事致力于确保微软的安全更新能够全面地修复已报告的漏洞。他还负责微软的应急响应流程的技术响应，致力于解决公开披露的针对微软软件的漏洞和攻击。他每月中有一个周末要担任预备役部队的安全工程师。

Chris Eagle 是位于美国加州蒙特利尔的海军研究生院计算机科学系的高级讲师。作为一位具有超过 25 年经验的计算机工程师和科学家，他的研究兴趣包括计算机网络攻防、计算机取证以及逆向工程和反逆向工程技术。他经常在 Black Hat 会议上发表演讲，并且特别钟爱 Defcon 的夺旗(capture the flag)比赛。

Gideon Lenkey，CISSP，Ra Security Systems, Inc.公司总裁和联合创始人，这是一家总部位于新泽西州的托管服务公司，他在那里专门负责测试企业 IT 基础设施的信息安全状况。他曾为 FBI 提供过高级培训，而且担任过 FBI 在新泽西州的 InfraGard 项目的负责人。他在多个场合中的杰出贡献得到了 FBI 主管 Robert Muller 的认可，而且经常为国内外政府机构提供咨询。他经常为 Internet Evolution 网站供稿，而且是东西方研究所网络安全计划的参与者。

Terron Williams，NSA IAM-IEM、CEH、CSSLP，Elster Electricity 资深测试工程师，主要关注智能网格安全。他曾经在 Nortel 担任安全测试工程师和 VoIP 系统集成工程师。还曾经在 Hakin9 IT Security Magazine 杂志编辑部工作，并在该杂志发表过多篇文章。他主要关注的是 VoIP、漏洞攻击研究、SCADA 安全以及新兴的智能网格技术。

免责声明：本书中发表的内容均属本书作者的个人观点，并不代表政府或微软公司的观点。

技术编辑简介

Michael Baucom 是北卡罗莱纳州 N2NetSecurity, Inc.公司的研发副总裁。他的软件工程师职业生涯长达 15 年，曾经编写过各种软件，既包括采用汇编语言编写的路由转发代码，也包括 Windows 应用程序和服务。除编写软件外，他还从事过安全咨询工作，包括培训、源代码审查以及渗透测试。

致　　谢

本书所有作者都非常感谢麦格劳希尔出版社的编辑们。尤其想要感谢 Joya Anthony，正是您让我们步入正轨，而且在整个过程中给予了我们巨大的帮助。您对这个项目所做的贡献非常显著。非常感谢。

Allen Harper：感谢爱妻 Corann 和女儿 Haley 与 Madison，感谢她们在本书写作期间所给予的支持和理解。我每天都深深地爱着你们。此外，我还想感谢教会成员给予的爱和支持。尤其是 Rob Martin 和 Ronnie Jones 已经成为真正的兄弟和知己。此外，我还想感谢在写作过程中提供帮助的其他黑客：Alex Sotirov、Mark Dowd、Alexey Sintsov、Shuichiro Suzuki、Peter Van Eeckhoutte、Stéfan Le Berre 和 Damien Cauquil。

Shon Harris：感谢其他作者和团队成员对这个项目所做的持续努力以及对整个行业所做的持续不断的贡献。我还想感谢狂热的 Fairbairn 姐妹 Kathy Conlon、Diane Marshall 和 Kristy Gorenz 对我和我的工作所给予的毕生支持。

Jonathan Ness：感谢爱妻 Jessica 忍受我花费大量时间写作本书以及从事其他工作。还要感谢 Didier Stevens 为第 15 章所提供的慷慨帮助(以及在 http://blog.didierstevens.com/programs/pdf-tools 提供免费的 PDF 分析工具)。还要十分感谢 Terry McCorkle 提供的专家指导和建议，这帮助我完成了现在的第 16 章的内容，Terry 真是一位救命的大好人！最后，我想向在职业生涯中曾经指导过自己的导师、老师、同事、牧师、家庭和朋友们表示感谢，他们为我的成功提供了莫大的帮助。

Chris Eagle：感谢 DDTEK 团队的所有核心成员。他们所做的艰苦卓绝的工作和所提供的技能令我惊叹不已。

Gideon Lenkey：感谢亲爱的家庭和朋友们对我的工作的支持。还想感谢所有 FBI 特工，包括在职的和退休的，他们让我不再感到无聊！

Terron Williams：感谢亲爱的妻子 Mekka 和继子 Christian Morris。你们是我生活的中心，感激我们一起分享的每分每秒。此外，还想感谢我的母亲 Christina Williams 和妹妹 Sharon Williams-Scott。我无时无刻不感激你们一直给予我的爱和支持。

前　言

我已经受够了一场战争，更别提再来一场了。

——托马斯·杰弗逊

我不知道第三次世界大战的武器会是什么样子。但我知道第四次世界大战战场上用的肯定是棍棒与石头。

——阿尔伯特·爱因斯坦

兵法非常简单。找出敌人在哪里，尽快到达那里，尽可能凶狠地打击他，而且要挺住。

——尤利西斯·S·格兰特

本书的目标是帮助培养更多技术精湛的、专注于抵御恶意黑客攻击的安全专家。事实一再证明，对敌方的了解是非常重要的，包括他们的策略、技能、工具和动机。企业和国家所面临的敌手非常专注，而且技艺超群。我们必须携起手来才能理解敌方的行动过程和流程，以确保我们能够正确地挫败敌方具有破坏性的恶意攻击。

本书的作者希望为读者提供他们认为这个行业所需的信息，即对负责任的而且在意图和物质方面真正合乎道德标准的正义黑客技术的整体性讨论。这也是为什么本书一开始就给出正义黑客的定义的原因所在，社会上对正义黑客的理解是非常模糊的。

本书对前两版中的材料进行了更新，并尝试将最全面、最新的技术、流程和材料汇集起来。因此增加了 9 章全新的内容，同时对其他章的内容进行了更新。

本书第 I 部分制定了灰帽黑客必要的伦理和期望基础。该部分内容包括：

- 理清人们对白帽、黑帽和灰帽黑客的定义和特征的混淆认识
- 讨论在实施任何类型的正义黑客行动前应该了解的一些棘手的道德问题
- 讨论漏洞发现报告的难点以及可用于解决这些难题的一些模型
- 调查黑客攻击以及许多其他类型的恶意行为所涉及的法律问题
- 概览适当的漏洞发现流程以及当前提供指导方向的模型

第 II 部分介绍了现如今其他书籍中没有讲到的更高级的渗透测试方法和工具。现在的许多书籍讲的都是一些相同的、被无数次反复翻新的旧的工具和方法，而本书决定更加深入地讲解真正的灰帽黑客正在使用的高级机制。该部分将讨论如下内容：

- 用来实施渗透测试的自动化渗透测试方法和高级工具
- 最新的渗透测试工具
- 潜入攻击、社会工程以及内部攻击

第III部分将深入底层代码，向读者讲解各种操作系统和应用程序的特定部件的工作原理以及如何对它们加以利用。该部分将讨论如下内容：

- 介绍一些基本的编程知识，这些是理解本书剩余内容所需要掌握的概念
- 如何利用栈操作漏洞以及如何识别和编写缓冲区溢出攻击代码

- 如何识别高级的 Linux 和 Windows 漏洞以及如何对它们加以利用
- 如何创建不同类型的 shellcode 来开发自己的概念验证漏洞攻击程序和必要的软件，以测试和识别漏洞
- 最新的攻击类型，包括客户端、Web 服务器、VoIP 以及 SCADA 攻击

第Ⅳ部分将更深入地研究正义黑客技术的最高级主题，甚至当今的许多安全专家都没有理解这些主题。该部分将讨论如下内容：

- 被动和主动分析工具和方法
- 如何识别源代码和二进制文件中的漏洞
- 如何进行软件的逆向工程和组件的反汇编
- 模糊处理和调试技术
- 如何为二进制和源代码打补丁

第Ⅴ部分将讲解恶意软件分析。有时候正义黑客会遇到恶意软件，而且可能需要进行一些基本的分析。该部分将讨论如下内容：

- 收集恶意软件样本
- 分析恶意软件，包括对反模糊处理技术进行讨论。

如果您希望进一步提高和加深对正义黑客技术的了解，那么本书非常适合您。

如果您有任何想法和评论，均可与我们联系，我们的反馈信箱是 wkservice@ vip.163.com，投稿信箱是 bookservice@vip.263.net。此外，如果希望了解与本书有关的额外技术信息和资源，请浏览 www.grayhathackingbook.com 或 www.mhprofessional.com/product.php?cat=112&isbn =0071742557。

目　录

第Ⅰ部分　“合乎道德的揭秘行为”简介

第Ⅱ部分　渗透测试及工具