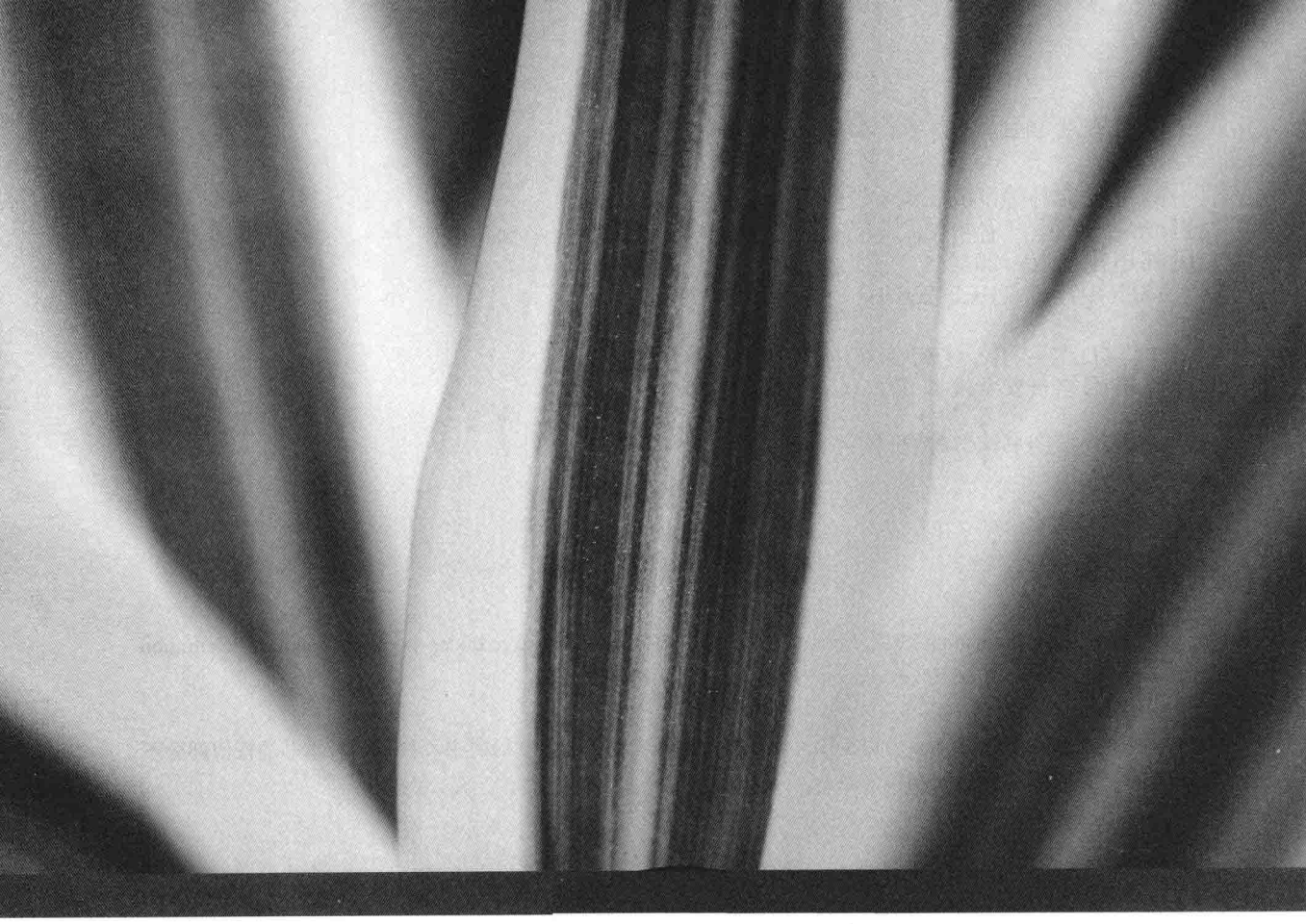
PACKT PUBLISHING

高度安全环境下的高级渗透测试

Advanced Penetra[redacted]r Highly-Secured Environments: The Ultimate Security Guide

[英] Lee Allen 著
孙松柏 李聪 陈力波 译

人民邮电出版社
POSTS & TELECOM PRESS



高度安全环境下的高级渗透测试

[英] Lee Allen 著
孙松柏 李聪 陈力波 译

人民邮电出版社
北京

图书在版编目（CIP）数据

高度安全环境下的高级渗透测试 / （英）阿伦（Allen, L.）著 ; 孙松柏, 李聪, 陈力波译. -- 北京 : 人民邮电出版社, 2014.4
ISBN 978-7-115-34256-0

Ⅰ. ①高… Ⅱ. ①阿… ②孙… ③李… ④陈… 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(2013)第311085号

版 权 声 明

◆ 著 [英] Lee Allen
译 孙松柏 李 聪 陈力波
责任编辑 傅道坤
责任印制 程彦红 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：21.25
字数：455 千字 2014 年 4 月第 1 版
印数：1－3 000 册 2014 年 4 月北京第 1 次印刷

著作权合同登记号 图字：01-2012-7223 号

定价：69.00 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

本书是一本介绍高级安全渗透测试的安全技术图书，采用步骤方式讲解了在安全环境下进行渗透测试的相关技术、工具和知识。

本书分为 11 章，分别讲解了如何计划和界定一次成功的渗透测试，用来进行侦查以求获取信息的技术和方法，进行系统识别和网络扫描的方法，远程漏洞利用，Web 应用攻击，客户端渗透攻击与利用，后渗透攻击，如何绕过防火墙和规避入侵检测系统，如何收集测试数据并对结果进行验证，以及如何搭建各种类型的虚拟环境等知识。本书最后一章还通过建立一个真实的测试环境，让读者在其中从头至尾地执行渗透测试，以确保其完全掌握了书中的内容。

本书适合渗透测试人员、网络安全管理人员、信息安全专业的学生，以及对渗透测试、信息安全感兴趣的读者阅读。

译者序

记得第一次将翻译稿交给本书的责任编辑，应该是差不多一年之前的事情了。如今，2013 年即将收官，在我忙着进行年度总结和来年规划的时候，突然收到了责任编辑的通知：该书即将出版，请提交最终版本的译者序。顿时感觉眼前一黑，心中一颤。忙而不乱的年终节奏终于要被这本拖延已久的图书给打断了。于是赶紧抽出半小时不到的时间，匆忙写就该序。

近些年来，渗透测试是计算机安全行业中非常抢手的一项工作，究其原因，是因为渗透测试已经成为网络中对抗各种脚本小子、骇客、黑客的有效手段。而要想成为一名合格的渗透测试人员，则需要具备大量的计算机基础知识、计算机安全知识，学会从黑客的角度、思维来渗透网络系统，从而发现问题，并及时修复，只有这样，才能最大限度地低于各种入侵行为。然而，由于黑客都是那些痴迷计算机技术，且具备超高水平的一类人，这些人的能力和思维远非一般人可以比拼，因此，想要真正模拟黑客的思维和攻击手段实属不易。正是在这样的情况下，渗透测试人员和安全从业者需要不断地学习各种黑客攻防技术，学习国外安全技术专家的实战经验和思维方式。

本书作者 Lee Allen 就是一名值得我们学习，而且具有丰富经验的安全研究和渗透测试人员。他在安全业界已经浸淫了 15 年之久，本书是他多年从事渗透测试的经验总结，事无巨细地涵盖了渗透测试的各个环节。另外，作者在本书中体现出来的严谨态度，以及滴水不漏的描述让我深深折服。毕竟，渗透测试面对的环境复杂而且多变，描述稍有不慎，则可能导致最终的测试差之毫厘谬以千里。

本书主要是基于 Linux 系统的渗透测试，由于译者从事渗透测试工作已经有多年，深知国内同行在这方面的不足，而本书很好地起到了填补空白的作用。需要重点提及的是，本书还得到了国际上几位知名“黑客”的倾力推荐，比如，知名的渗透测试框架 Metasploit 项目的发起者和创始人 HD Moore 就对本书大加赞赏。

尽管本书由很多优点，但是作为译者，我们也先指出其中的不足：书中的示例普遍比较简单，作者的原意是通过这些简单但常见的案例来讲解渗透测试中最常碰到的问题，因此如果您打算从本书中学到一些高深莫测的技术，那么您就要失望了。另外，由于本书涉及的面很广，包括了渗透测试过程的各个环节，因此无法做到面面俱到。从这一点上来说，本书更像渗透测试的参考手册。

最后，我首先要感谢本书的合作译者：我的兄弟、同窗波波童鞋和聪哥，在研究生阶

段和你们的学习、交流是我人生道路上一笔重要的财富，我从你们身上学到很多东西，没有你们的辛苦付出，也不可能在短时间内完成本书的翻译工作。翻译期间，波波的儿子刚刚出生，晋升为奶爸的他尽管非常忙碌，但还是按时按质完成了翻译工作，他的责任感让我由衷敬佩。另外，感谢本书责任编辑傅道坤为本书所做的协调以及细致的审查。最后，感谢远在家乡的父母和年近 90 的奶奶，祝你们平安、健康。你们永远是我的精神支柱。

末了，还需要不能免俗的来一句，“由于时间和水平有限，译者有时候并不能完全准确地理解本书作者要表达的意思，书中也可能存在一些语法错误，如有翻译不到位之处，还请各位读者谅解”。

孙松柏

2013 年 12 月于朝阳公园

关于作者

Lee Allen 目前是一家世界 500 强公司漏洞管理项目的领导，主要负责安全评估和渗透测试等工作。

Lee 对渗透测试和安全研究相当具有激情。在 20 世纪 80 年代，Lee 借助他挚爱的 Commodore 64 电脑，在满地都是 5.25 英寸磁盘的房间里登录到 BBS，由此步入激动人心的安全世界。经过在安全行业和社区内多年的浸淫，他一直是这个圈子里最伟大的专家。

他持有多个行业认证，其中包括 OSWP，而且已经在 IT 领域工作了 15 年之久。他爱好并执着于对概念攻击代码的验证和评审、编程、安全研究、出席安全会议、技术探讨、写作、3D 游戏开发和滑雪。

我要感谢我的爱妻 Kellie，她一直是我的贤内助，还要感谢我的孩子 Heather、Kristina、Natalie、Mason、Alyssa 和 Seth，他们让我的多任务处理艺术得以进一步完善。我还要感谢我的女婿 Justin Willis，谢谢他对我们国家所做的服务。此外，我还要感谢 Kartikey Pandey 和 Michelle Quadros，谢谢他们在我写作本书期间给予的帮助和指导。我还要特别感谢 Steven McElrea 和 Aaron M. Woody，他们花费了大量的时间来验证本书中的所有示例，并指出了其中的错误。正是得益于你们这样的人存在，安全社区才变得格外有趣。

关于审稿人

Steven McElrea 以 Steven McElrea 以 Microsoft Windows 和 Exchange 服务器管理员的身份，在 IT 领域工作了 10 多年。在被安全 bug 折磨过几次之后，他开始学习和研究 InfoSec，而且已经学习了好多年。他有一个很不错的小型博客（www.kioptrix.com），并在上面竭尽全力地为新手讲解和演示信息安全的基本原理。他当前在安全领域工作，而且他真的很热爱这份工作。将工作领域专项 InsoSec 是他所做的最好的选择。

谢谢 Amelie、Victoria 和 James，我爱你们。谢谢 Richer 让我一开始就从事该书的审校工作，尽管我曾经为此焦头烂额。我还要感谢 Dookie，是他帮助我冷静下来并理清头绪。我还要感谢我的父母，是你们的支持让我们度过了最艰难的时光。我爱你们！

Aaron M. Woody 是信息安全领域的一位专家，拥有 14 年以上的工作经验，先后涉及过多个垂直行业。他的经历包括执行、实施外设安全和取证调查，以保护世界上一些大型金融机构的安全。当前，Aaron 是一家领先的信息安全公司 Accuvant Inc.的解决方案工程师，该公司位于科罗拉多州的丹佛。他是一位活跃的讲师，主要讲解破解和取证技术，同时还负责 n00bpentesting.com 博客的维护。大家可以通过@shai_saint 在 Twitter 上找到他。

衷心感谢我的爱妻 Melissa 和爱子 Alexis、Elisa、Jenni，谢谢他们能够与我分享在编写本书时的得失欢乐。我还要感谢 Steven McElrea（@loneferret）对本书评审期间所做的完整性检查。我还要特别感谢 Lee Allen，谢谢他邀请我参与到该书的编写中来。

前言

渗透测试人员需要面对由防火墙、入侵检测系统、基于主机的保护、加固后的系统以及知识渊博的分析人员团队构成的整体环境，其中分析人员会对通过其安全信息管理系统收集到的数据进行分析处理。在这样的环境中，仅仅运行自动化工具通常不会得到什么结果。而且由此导致的这种虚假安全感可以很容易地丢失关键数据和资源。

本书则对基本的自动扫描之外的内容进行了讲解。通过本书讲解的知识，读者可以进行复杂而艰巨的测试任务，以有效地衡量传统上的安全环境所遭受的整个攻击平面。

本书只使用了可以免费获取的工具和资源来讲解这些概念。其中将要用到的一个工具是知名的渗透测试平台 BackTrack。BackTrack 的团队开发人员会不断更新该平台，以提供一些可用的最佳安全工具。我们用来模拟渗透测试的大多数工具都包含在 BackTrack 的最新版本中。

渗透测试执行标准（Penetration Testing Execution Standard[PTES]，地址为 http://www.pentest-standard.org），是我们执行测试的指南。尽管我们不会讲解该标准中的所有内容，我们会尽可能地让本书中的知识符合标准中的基本原理。

本书采用步骤式讲解，并使用 VirutalBox、pfSense、snort 和类似的工具在自己的系统上模拟一个高度安全的环境。这可以让读者在一个安全的环境中来练习书中所学的知识。而且在你执行测试时，也可以有机会通过安全响应小组的视角来看待渗透测试。

本书在讲解时，会先提出一个挑战，其中你将使用虚拟实验室来从头到位地模拟整个渗透测试。渗透测试人员需要能够向其客户来解释相应的缓解策略。我们还会讲解一些不同的缓解策略来应对书中所列的攻击。

本书内容

第 1 章，计划和界定一次成功的渗透测试，将为您剖析渗透测试的各个环节。你将学习如何正确界定一次渗透测试的范围和限制，比如遇到第三方的设备或环境时。我们还会讨

论使用各种技术的优先顺序。

第 2 章，高级侦查技术，将会引导你学习一系列不引起目标系统警告的数据收集技术。我们将会关注各种侦查策略，包括深入挖掘目标系统的 Web 站点和其他特殊网站中包含的信息。

第 3 章，扫描：明智地选择目标，将描述一系列关于系统识别和网络扫描的方法，从而让你能够明智地选取目标。本章的目标是扫描目标环境，从而讲解如何从中选取目标系统。本章将涉及到高级 Nmap 技术以及使用 PBNI 来检测网络中的变化。本章最后将会介绍如何躲过一些扫描手段，以此来迷惑攻击者（为应急响应团队争取时间）。

第 4 章，远程漏洞利用，深入讲解了 Metasploit 框架，还描述了使用 Armitage 进行的团队测试。我们还将看到来自 Exploit-DB.com 的概念利用代码的证明，我们稍后会重写以及编译。本章还将讲解用于密码攻击的 THC Hydra 和 John the Ripper。

第 5 章，Web 应用攻击，主要讲解 Web 应用攻击。本章首先通过步骤方式来讲解如何构建一个 Web 应用攻击实验室，然后再详细讨论 w3af 和 WebScarab 的使用。在很多环境中讲解的负载平衡现在也有了一些特性。本章将通过示例来讲解用来检测 Web 应用防火墙和负载平衡的方法。本章最后讲解了 Mantra 浏览器。

第 6 章，客户端渗透攻击与利用，本章讨论了如何绕过 AV 特征，以及 Social Engineering Toolkit 的更多高级特性。本章还详细讲解了缓冲区溢出和 fuzzing。

第 7 章，后渗透攻击，讲解了在完成一次成功的攻击之后，所要执行的行为。我们会讲解权限提升、高级的 Meterpreter 功能，在不同类型的 OS 中设置账户权限，以及在攻击结束之后进行清理，以免留下蛛丝马迹。

第 8 章，绕过防火墙和规避入侵检测系统，讲解了在进行渗透测试时，用来绕过检测的方法。这包括避免入侵检测系统和高级的逃避技术。我们还讲解了可以提升恶意用户或应用的可检测性的方法。

第 9 章，数据收集工具与结果汇报，可以帮助你利用测试期间收集到的数据创建报表和统计。你将学到如何收集所有的测试数据，以及如何对结果进行验证。你还将学到生成报告的所有过程。

第 10 章，建立虚拟的测试实验环境，帮助你创建一个测试环境来模拟一个具有多层 DMZ 环境的公司。该公司是使用 IDS 和某些加固系统以及 app 来实现多层 DMZ 环境的。这包括设置 VBOX、BackTrack、虚拟防火墙、IDS 和监控。

第 11 章，综合挑战，通过使用书中学到的技巧来获得实践经验。我们将会给读者设置一些挑战，它会要求你在自己的测试环境中从头到尾地执行渗透测试。我们还为该挑战提供了一个步骤式的解决方案，来确保你确实已经完全掌握了书中的内容。

学习本书的先决条件

为了练习书中内容，你需要一台计算机，而且该计算机具有足够的能力和空间来运行虚拟化工具，我们稍后会使用这些工具来创建实验室。如果计算机的硬盘空间有限，则无法胜任该任务。书中描述的虚拟化工具可以在大多数现代的操作系统中运行。

本书读者对象

本书适合对安全测试持有热忱和学习意愿的人士阅读。本书假定读者具有基本的安全概念以及不同的操作系统知识。如果你是一名渗透测试人员、安全顾问，或者仅仅是对安全测试有兴趣，都可以阅读本书。

请注意：

- 本书中的信息只能用于合法目的；
- 未经设备拥有者的书面许可，不得在其设备上使用本书中讲到的知识；
- 如果你利用本书中的内容执行非法行为，则会导致你身陷囹圄；
- 如果因为滥用本书中的信息而导致惩罚，我们不承担任何责任。

书中的内容只能在得到授权和许可的测试环境中使用。

本书体例

提示框中的警告或重要提示以如此形式出现。

技巧与窍门则以这样的形式出现。

目录