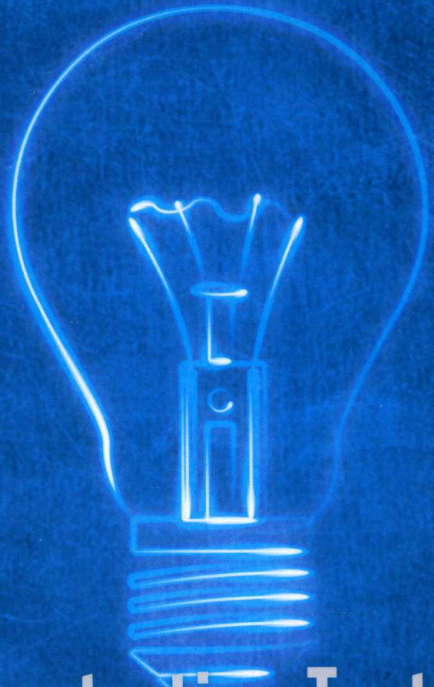
渗透测试

完全初学者指南

[美] 乔治亚·魏德曼（Georgia Weidman）著
范昊 译



Penetration Testing

A Hands-On Introduction to Hacking

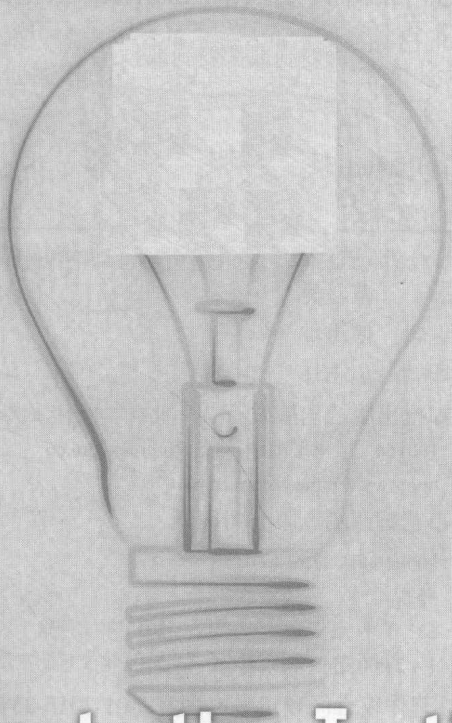
中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

渗透测试

完全初学者指南

[美] 乔治亚·魏德曼（Georgia Weidman）著

范昊 译



Penetration Testing

A Hands-On Introduction to Hacking

人民邮电出版社

北京

图书在版编目（CIP）数据

渗透测试 : 完全初学者指南 / (美) 乔治亚·魏德曼 (Georgia Weidman) 著 ; 范昊译. -- 北京 : 人民邮电出版社, 2019.5
ISBN 978-7-115-50884-3

Ⅰ. ①渗… Ⅱ. ①乔… ②范… Ⅲ. ①计算机网络－网络安全－指南 Ⅳ. ①TP393.08-62

中国版本图书馆CIP数据核字(2019)第036386号

版权声明

◆ 著　[美] 乔治亚·魏德曼（Georgia Weidman）
译　范　昊
责任编辑　傅道坤
责任印制　焦志炜

◆ 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
北京市艺辉印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：30.5
字数：631 千字　2019 年 5 月第 1 版
印数：1－2 000 册　2019 年 5 月北京第 1 次印刷

著作权合同登记号　图字：01-2015-2574 号

定价：118.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

所谓渗透测试，就是借助各种漏洞扫描工具，通过模拟黑客的攻击方法来对网络安全进行评估。

本书作为入门渗透测试领域的理想读物，全面介绍每一位渗透测试人员有必要了解和掌握的核心技巧与技术。本书分为 20 章，其内容涵盖了渗透测试实验室的搭建、Kali Linux 的基本用法、编程相关的知识、Metasploit 框架的用法、信息收集、漏洞检测、流量捕获、漏洞利用、密码攻击、客户端攻击、社会工程学、规避病毒检测、深度渗透、Web 应用测试、攻击无线网络、Linux/Windows 栈缓冲区溢出、SEH 覆盖、模糊测试/代码移植及 Metasploit 模块、智能手机渗透测试框架的使用等。有别于其他图书的是，本书在这 20 章之外还增加了一个第 0 章，用来解释渗透测试各个阶段应该做的工作。

本书内容实用，理论与实战相互辅佐。读者借助于书中提及的各个工具，可完美复现每一个实验操作，加深对渗透测试技术的进一步理解。无论是经验丰富的信息安全从业人员，还是有志于从事信息安全行业的新手，都会在阅读中获益匪浅。本书还适合信息安全专业的高校师生阅读。

序

大约在两年以前的某个会议上，我首次遇见了 Georgia Weidman。那时，她在移动设备安全领域的研究进展已经引人关注，因此我日益关注她的研究成果。从那以后，每逢会议我都会出席 Georgia 的活动。无论是她所独具的分享知识的研究热情，还是她在移动设备安全和智能手机渗透测试框架方面的研究成果，都是那样璀璨夺目。

实际上，移动设备安全只是 Georgia 的研究主题之一。Georgia 已经把渗透测试作为毕生的职业。她经常去世界各地培训渗透测试、Metasploit 框架和移动设备安全的知识。在各种安全会议上，她都愿意分享自己那新颖而独到的与移动设备安全评估相关的创意。

Georgia 不遗余力地修炼在高难主题方面的造诣，而且肯花精力去了解新鲜事物。她曾经参加过我开办的 Exploit Development Bootcamp（exploit 开发训练营）。我敢说她在整个课程中都表现得非常出色。Georgia 一贯乐于在信息安全界分享自己的知识和成果，是当之无愧的真正黑客。因此，当被问到是否可为此书作序时，我深感荣幸。

作为一名首席信息安全官，我绝大部分的工作都以信息安全计划的设计、实现和管理为主。风险管理是信息安全计划中非常重要的一个环节，因为它能够用风险的术语让商业公司客观衡量并深入理解自己的安全状况。商业公司根据自身的核心业务活动、经营使命和业务规划，参照相应法律法规拟定、实现安全措施，从而把业务风险降低到可接受水平——这些运作都离不开风险管理。

识别企业内部的全部关键流程、数据和数据流，是风险管理初期阶段的工作之一。这部分工作包括以 IT 角度，收集所有支撑关键业务流程和数据的 IT 系统（各类设备、网络、应用程序、接口等）的资产详情。这项工作十分耗时。多数人都会忽视那些乍看起来与“支撑关键业务流程和数据”没有直接关系的部分系统。然而这些系统可能起到支撑其他系统的作用，因而它们仍有可能属于关键系统。本质上说，排查资产十分重要，它是风险评估的实质性起点。

定义企业 IT 系统和数据的保密性、完整性和可用性标准，是信息安全计划的目标之一。业务流程的所有者应当能够定义自身业务的目标。为保证业务系统能够满足业务目标的需求，信

息安全专业人员就应当实施相应的安全措施，并且测试这些安全措施的实际效果。

企业系统的保密性、完整性和可用性都面临着现实情况带来的实际风险。有几种方法可以判断这些风险。对手可能会直接攻击信息系统，或攻击具备系统访问权限的有关人员，从而达到突破保密性、损害完整性、影响可用性的破坏目的。企业则可以通过技术评估的手段了解这种破坏行为的难易程度。

这正是渗透测试人员（又有“道德/有道/正义黑客”[ethical hacker]等叫法）展现实力的舞台。称职的渗透测试人员应当具备系统设计、系统组建、系统维护等各方面的知识，应当能够创造性地突破严密的系统防御，从而在揭示和验证信息系统安全状况的工作中发挥举足轻重的作用。

如果你恰巧是有志成为渗透测试方面的专业人员，或者是有意钻研安全测试的系统/网络管理员，那么本书值得一读。它从渗透最初的信息收集阶段入手，深入浅出地介绍渗透测试的各个技术过程。它还讲解了利用网络和程序的安全缺陷进一步地潜入网络的方法，以帮助评估风险可能引发的实际危害。

本书独具一格。市面上的渗透图书多数局限于某些软件工具的使用介绍，然而本书开篇即以渗透测试实验室（在多台虚拟主机上安装一系列具有漏洞问题的应用程序）为测试环境，阐述渗透测试的实践过程。读者可以利用本书推荐的可公开下载的免费工具，毫无顾虑地练习各种渗透技术。

本书每章不仅都介绍有关主题的具体知识，而且还提供了数量不等的练习题目。实际操作的练习题目能够帮助读者深化那些发现和利用安全漏洞的具体认识。实际上，无论是资深人士的亲传师授、真实的生活场景、行之有效的各种技术，还是真实的渗透测试案例中的奇闻趣事，只要你勤于思考，就能从中体会到渗透测试的要诀和技巧。

其实，本书每章主题都足以单独拿出来写一本书（实际上已经有这种图书了），只是作者无意把它打造为渗透测试的百科全书。换而言之，通读本书之后，读者不仅可以从零接触各种攻击方法，了解目标系统的安全评估方法，还可以广泛地接触到其他方面的渗透知识。本书内容循序渐进、面向实践。本书前几章介绍了使用 Metasploit 框架攻击程序缺陷并利用系统防御的单一漏洞规避栅栏式保护（perimeter protection）的所有保护措施，然后潜入网络深处，继而从被测系统汲取数据。在这些基础知识的介绍篇幅之后，还有规避反病毒软件检测、使用 SET（Social Engineer Tookit）实施社会工程学攻击的详细介绍。本书最后几章讲解的是破解企业 WiFi 网络，使用 Georgia（作者）的 Smartphone Pentest Framework 评估公司的“自带设备”策略可能给企业网络带来的实际危害。可以说，本书每章都构思巧妙，都能引起读者学习渗透测试的兴趣。更为难得的是，全书皆为剖析渗透测试工作的第一手资料。

希望本书能够激励读者在某些领域深入钻研，勤奋工作勤勉学习，进行独立的研究并且愿

意在安全界内分享成果。时下，不断发展的新技术已经使得人们的生活环境日新月异，而各种企业的核心业务都日益依赖信息技术。在这样的大背景下，市场对渗透测试专家的需求也会不断升温。亲爱的读者，你就是信息安全界的未来，你就是信息安全行业的未来！

在你打开本书，踏出迈向令人激动的渗透测试世界的第一步之际，祝你学有所成。相信你一定会喜欢本书！

Peter “corelanc0d3r” Van Eeckhoutte

Corelan 团队创始人

作者简介

Georgia Weidman 是一位渗透测试专家和安全研究员，同时还是 Bulb Security 安全咨询公司的创始人。她不仅多次在 Black Hat、ShamooCon 和 DerbyCon 等世界各地的安全会议上发表演讲，而且还亲自传授渗透测试、移动破解和 exploit 开发等专业课程。世界各国的报纸和电视都曾报道过她在移动安全领域的研究成果。DARPA（美国国防高级研究计划局）的 Cyber Fast Track（信息化项目快速通道）就曾为她的移动设备安全主题立项，并给予她专门的资金支持。

献辞

谨将本书献给 Jess Hilden。

致谢

谨在此处表达我对下述个人及单位的感谢（排名不分先后）。

感谢我的父母，感谢他们一直以来对我事业的一贯支持。他们支付了我第一次参加安全会议及第一次考取认证时的开销，那时我还只是一个落魄的大学生。

感谢大学网络防卫竞赛（Collegiate Cyber Defense Competition, CCDC）。特别感谢那个曾经帮助我找到毕生事业的中大西洋地区的红队（Red Team）。

感谢 ShmooCon 组委会给予我第一次演讲的机会，那是我毕生第一次参加的安全盛会。

感谢 Peiter “Mudge” Zatko 和 DARPA Cyber Fast Track 项目的各位前辈。感谢他们给我开办自己的公司，继续开发 Smartphone Pentest Framework 的机会。

感谢 James Siegel，他是我的护身符，并且帮助我准时出席会议活动。

感谢 Rob Fuller，正是他在詹姆斯·麦迪逊大学（James Madison University）的精彩演讲，以及赛后慰问 CCDC 团队的情景，令我立志要在信息安全行业有所作为[①]。

感谢 John Fulmer 为本书无线安全的有关章节丰富了加密学的技术介绍。

感谢 Rachel Russell 和 Micheal Cottingham，他们是我在信息安全界最初的朋友。

感谢 Jason 和 Rachel Oliver 为本书所做的技术审查和内容审查工作。另外，我在 ShmooCon 和 Black Hat 会议上采用的烟熏眼妆，同样是他们的成功之作。

感谢 Joe McCray，他是我的大哥。在我学习业内业务时，他也是我的良师益友。

感谢 Leonard Chin 给予我出席人生中首场大型国际会议的机会。那次的经历令我在此后的会议中不再怯场。

感谢 Brian Carty 帮我建设网络实验室。

① 译者注：Rob Fuller 是 Red Team 赛队的领队，而且连任领队数年。

感谢 Tom Bruch 在我找工作的日子和 DARPA 资金尚未到位的日子里让我住在他的家里。

感谢 Dave Kennedy 多次为我介绍宝贵的业务机遇。

感谢 Grecs 在他的网站上推销我的培训课程。

感谢 Raphael Mudge 帮我联络 DARPA CFT（Cyber Fast Track）项目和其他的重要业务。

感谢 Peter Hesse 和 Gene Meltser 在我职业生涯的关键路口帮我鼓起勇气。

感谢 Jayson Street，感谢上帝让这样一个比我还挑食的家伙做我的朋友。因为他的存在，在异国召开的演讲者晚宴上，我总能显得像个正常的宾客。你最棒了！

感谢 Ian Amit 在我默默无闻的时候向许多知名活动推荐我做演讲。

感谢 Martin Bos，他真的很了不起。

感谢 Jason Kent，他全球首屈一指的技术和精彩的重言式（tautologies）定义语言让我受益颇丰。

感谢詹姆斯·麦迪逊大学里各位传授给我知识的教授。特别感谢 Samuel T. Redwine，我从你那里获得的灵感远比你想象的还多。

感谢 No Starch 的同仁。感谢他们给予我的帮助、指导和支持。在此，请允许我一并感谢 Alison Law、Tyler Ortman 和 KC Crowell。特别感谢我的编辑兼 No Starch 的老板 Bill Pollock。

前 言

在我最初步入信息安全行业的时候，我一直找不到一本适合自己阅读的书，因此我便下定决心，一定要编写一本能够帮助新手的图书。时下，帮助人们自学的网站已经很多，实际上远比在我入行的时候多得多。即使如此，我仍然认为新手还是不容易领会学习的先后次序，很难找到学习必备技能的相应途径。有人会说，书店里的图书已经不少了——介绍高难主题的书和入门图书可谓应有尽有。然而实际情况没有他们想象得那么乐观。那些高难主题的图书，要求读者具有相当充分的背景知识；而面向初学者的图书又太过偏向于理论。曾几何时，每当那些有志于从事渗透测试的网友给我写邮件，询问学习信息安全的具体方法时，由于没有什么资料好推荐，我总是苦恼于如何起笔回信。

后来我成为了一名讲师。我发现，自己最喜欢传授的课程就是渗透测试。参加这门课程的学生总是求知若渴，总是令我乐在其中。因此，在 No Starch 建议我著书立说之际，我就决心撰写一本介绍渗透测试的书。当我公布自己写书这件事时，多数人都认为我会写一本移动安全方面的书。其实，在考虑题材的时候，我就是想写一本渗透测试的书，好在我的受众面前炫耀。

鸣谢

若没有多年的业内从业经验，是无法写出这种题材的书来的。本书介绍了作者和其同事在日常工作中使用的部分工具和技巧。它们都是全球渗透测试专家和安全专家共同努力的成果。我也参加过部分的开源项目（例如 exploit 开发章节介绍的 Mona.py），希望本书能够鼓励你同样为开源项目作出贡献。

借此机会，请允许我向 Offensive Security 表示敬意。感谢他们制作并维护全球渗透测试专家普遍使用的 Kali Linux 发行版。本书采用的操作系统就是 Kali Linux。与此同时，请允许我向 Metasploit Framework 的核心开发团队，以及该项目的全球参与人员表示敬意。此外，感谢所有那些分享知识、成果和技术的渗透测试专家和安全研究专家——没有他们，我们就无法准确、高效地评估客户的信

息安全状况；没有他们，我们这样的讲师就没有什么可以传授给学生的知识。

最后感谢书中提到的各类图书、博客、课程等资料的所有作者。正是他们的文献帮助我成长为渗透测试的专业人员。所谓见贤思齐，我希望我的所学同样能够帮到那些怀有抱负的渗透测试人员。

本书内容

本书的起点不高，只要你能够在自己的电脑上独立安装软件，你就能够看懂它。读者没必要非得是 Linux 专家，也不必非要懂得网络协议的工作原理。当你觉得某些主题非常陌生时，如果本文的讲解仍然不能解答你的疑问，那么可借鉴其他的资料。在介绍各种工具和技术时，本书从 Linux 的命令行开始，循序渐进地进行讲解，尽量照顾各层次的读者。在我初次接触信息安全的时侯，我做的最得意的事情就是把 Windows XP SP2（预览版）开始菜单的 Start 改成了 Georgia。在那个时侯，我为此感到骄傲。

后来，我参加了 CCDC （大学生网络防御竞赛）。我发现所有的红队队员都使用命令行界面。在那届比赛中，他们差不多是“挤”在一个很小的房间里。当他们快速敲打几下键盘之后，我的电脑就不断地弹出窗口。当时我就呆住了，我只知道自己得像他们那样厉害。为了到达今天的水平，我付出了很多的努力。当然，为了达到信息安全的最高境界，我还要付出更多的努力。我只希望本书能够鼓舞更多的人步入这个行业。

■ 第 1 部分：基础知识

本书的第 0 章介绍了渗透测试各个阶段的基本定义。第 1 章讲解了搭建渗透实验室的具体方法。第 1 章搭建的这个实验室就是后文操作的测试环境。在介绍测试环境的搭建方面，其他的渗透图书中都只有 “在你的主机上下载并安装（几款）软件……”这样的寥寥几笔。虽然本书推荐的方法比它们要复杂一点，但是如此搭建的测试环境更为接近渗透测试的实际环境。因此，建议读者抽出时间耐心搭建好自己的实验环境，在阅读的时侯跟随本书的范例进行上手练习。换而言之，本书可以作为现场操作的参考资料和操作备忘。我相信，练习渗透测试的最初场所，无疑还是你自己的家。

第 2 章将初步介绍 Kali Linux 和其他 Linux 系统的大致使用方法。第 3 章则介绍编程方面的基础知识。具有编程相关经验的读者，可以略过第 3 章。在我初出茅庐的时侯，我会一点 C 编程和 Java 编程，但是我不太了解脚本编程，而且基本没有 Linux 方面的编程经验。而我看到的绝大多数的黑客教程都假定读者已经掌握了这两个技能。因此本书提供了编程的入门知识。

如果没有接触过编程，请不要止步于本书的文字，务必花些精力专门研究一下编程技术。基于Linux的操作系统越来越火，主要是因为它们支撑着移动设备和Web服务。因此，即使不打算专门从事信息安全方面的工作，多些这方面的知识仍然会对你有所裨益。此外，无论从事什么职业，只要你使用计算机，采用编程方式来执行重复任务都可以让你的日常工作更为轻松一些。

第4章侧重讲解本书通篇都要操作的平台——Metasploit Framework的基本技巧。虽然我们可以脱离Metasploit完成绝大部分的测试操作，但是Metasploit已经逐渐成为业内的主流操作平台，而且它会不断收录各种最新的威胁和技术。

■ 第2部分：评估

第2部分主要讲解渗透测试的前期工作。第5章将通过公开的网上信息和正面扫描目标系统这两种手段收集目标系统的数据。下一步就要完成第6章介绍的工作，通过查询和研究等手段鉴定目标系统的安全缺陷。若需要捕获目标系统收发数据之中的敏感数据，那么可以参考第7章。

■ 第3部分：攻击

第8章将通过大量的工具和技术利用网络中的安全缺陷，其中不乏各种基于Metasploit的自动化漏洞利用方法和手工操作的漏洞利用方法。在此基础上，第9章将关注网络安全中最为脆弱的一个环节——密码管理。

其后的几章均涉及漏洞利用的高级技术。所谓漏洞，不仅仅存在于面向网络的主机服务，Web浏览器、PDF阅读器、Java和Microsoft Office同样存在安全问题。由于客户越来越重视网络安全，因此客户端攻击往往是获取内网立足之地的关键。第10章将详细介绍客户端攻击。第11章继而以客户端攻击为目标而进行社会工程学攻击。社会学攻击的目标就是操作信息系统的人。作为信息系统的一个组成部分，人是无法被修补程序更新升级的。总之，要触发客户端攻击，存在缺陷的软件必须打开我们精心设计的恶意文件，因而就得诱使操作电脑的人帮我们达成这一目的。实际上多数客户都会部署反病毒软件，因此还要规避反病毒软件的检测。第12章介绍的就是规避检测的相应技术。如果已经获得了目标系统的较高权限，那么此时确实可以直接关闭反病毒软件；不过，“悄然无息地溜过反病毒软件的检测”的做法更为高明，因为我们需要先把恶意程序存储到目标主机的硬盘驱动器上，然后再获取较高的权限。

第13章介绍的是渗透测试的下一个阶段——深度攻击（post exploitation）阶段。曾经有人说过，只有进入了深度攻击阶段，才算开始了真正的渗透测试。在这个阶段，我们要利用已有的权限在网络中探测立足点之外的网络对象，从而提取敏感信息，进而从事一些其他方面的攻

击。如果要进行渗透测试方面的深入研究，那么就得挤出大量时间翻阅最新、最重要的深度攻击技术。

在有关深度攻击的内容之后，本书将介绍顶级渗透测试专家需要具备的几项技能。首先，第 14 章将大致介绍有关 Web 应用安全的评估手段。时至如今，几乎人人都有自己的网站，因此这方面的技能不可或缺。接下来的第 15 章将探讨无线网络的安全评估，并介绍常规加密系统的破解方法。

■ 第 4 部分：exploit 开发

第 16～19 章分别阐述了编写 exploit 的基础知识。这部分内容分为漏洞检测、使用常规技术利用漏洞和编写自己的 Metasploit 模块几大部分。在上手前文各章的渗透测试练习题时，我们使用的都是可通过公开途径下载的软件工具和 exploit。随着业内资历的增长，你可能想要挖掘新的 bug（也就是 0day）然后把它们汇报给厂商。毕竟官方可能会为这种反馈提供奖金。你还可以公开自己的 exploit 和（或）Metasploit 模块，帮助同行检测他们客户的系统是否存在相同的问题。

■ 第 5 部分：移动平台

第 20 章是本书的最后一章。本章将关注渗透测试领域中较为年轻的一个主题：移动设备的安全评估。本将会介绍我自己开发的工具——Smartphone Pentest Framework（智能手机渗透测试框架）。或许在掌握了这本书的所有技能之后，你愿意致力于开发自己的安全工具。

当然，本书不可能全面涉及信息安全的所有方面，它所介绍的工具和技术也十分有限。若要写出那种级别的百科全书，还请等我日后领悟到更高的境界，而且我还得有机会拿出数倍的时间才行；就现实而言，我还需再加把劲。简单来说，本书的定位就是“一本破解入门手册”。若本书能在大家踏入信息安全行业的最初阶段提供帮助，那将是我的荣幸。希望各位读者能在阅读本书的时候有所收获，希望它能鼓励大家继续深造，更希望你们能够在这个令人振奋的、日新月异的行业中成为一名积极分子！

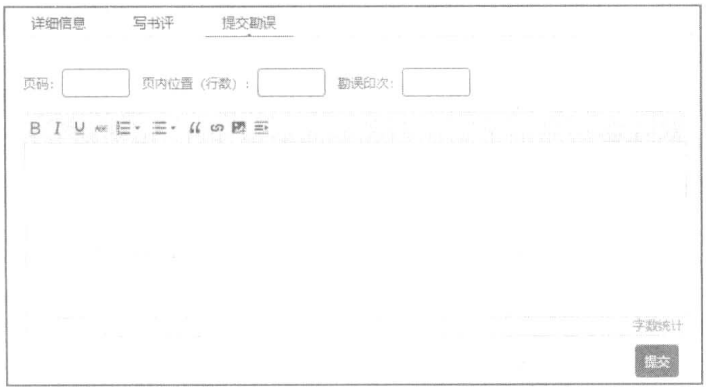
资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书

名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目 录

第 0 章 渗透测试导论 …… 1
0.1 渗透测试的各个阶段 …… 2
0.1.1 明确需求阶段 …… 2
0.1.2 信息收集阶段 …… 3
0.1.3 威胁建模阶段 …… 4
0.1.4 漏洞分析阶段 …… 4
0.1.5 漏洞验证阶段 …… 4
0.1.6 深度攻击阶段 …… 4
0.1.7 书面汇报阶段 …… 5
0.2 小结 …… 6
第 1 章 搭建虚拟渗透实验室 …… 7
1.1 安装 VMware …… 7
1.2 安装 Kali Linux …… 8
1.2.1 网络配置 …… 11
1.2.2 安装 Nessus …… 14
1.2.3 安装其他软件 …… 18
1.2.4 安装 Android 模拟器 …… 20
1.2.5 智能手机渗透测试框架 …… 24
1.3 靶机虚拟机 …… 25
1.4 创建 Windows XP 靶机 …… 25
1.4.1 Microsoft Windows 上的 VMware Player …… 26
1.4.2 Mac OS 上的 VMware Fusion …… 28
1.4.3 安装并激活 Windows 系统 …… 29
1.4.4 安装 VMware Tools …… 32