专业渗透测试（第2版）

Professional Penetration Testing

Second Edition

[美] Thomas Wilhelm 著

王布宏 柏雪倩 李 夏 张 群 译

ELSEVIER

国防工业出版社
National Defense Industry Press

装备科技译著出版基金

专业渗透测试(第2版)

Professional Penetration Testing

Second Edition

[美]Thomas Wilhelm 著

王布宏 柏雪倩 李 夏 张 群 译

国防工业出版社

·北京·

著作权合同登记　图字:军-2017-021 号

图书在版编目(CIP)数据

专业渗透测试:第 2 版/(美)托马斯·威廉(Thomas Wilhelm)著;王布宏等译.
—北京:国防工业出版社,2018.1
书名原文:Professional Penetration Testing(Second Edition)
ISBN 978-7-118-11436-2

Ⅰ.①专… Ⅱ.①托… ②王… Ⅲ.①渗透检验 Ⅳ.①TG115.28

中国版本图书馆 CIP 数据核字(2017)第 330162 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
天津嘉恒印务有限公司
新华书店经售
*
开本 710×1000　1/16　印张 24½　字数 453 千字
2018 年 1 月第 1 版第 1 次印刷　印数 1—2000 册　定价 129.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

译 者 序

随着信息科学与技术的不断发展和广泛应用，网络空间作为继陆、海、空、天之后的“第五维空间”，已成为世界各军事强国战略竞争的制高点。2014 年，我国成立了中央网络安全与信息化领导小组，习主席明确指出“没有网络安全就没有国家安全”。2015 年中国国防白皮书《中国的军事战略》中明确指出“网络空间是经济社会发展新支柱和国家安全的新领域……加快网络空间力量建设……保障国家网络与信息安全，维护国家安全和社会稳定”。为了加快网络空间安全领域高精尖人才的培养，2015 年教育部新增“网络空间安全”一级学科。网络渗透测试是通过黑客攻击的手段和方法对网络系统进行漏洞探测和安全评估的科学，是目前国际上网络安全领域的发展热点，许多发达国家已经建立了相应的行业标准和职业能力认证体系。无论是理论技术发展还是人才培养体系，我国在网络渗透测试领域的发展还相对滞后。目前市面上关于渗透测试技术方面的著作，大都关注于各种黑客工具和渗透测试平台的使用方法。专业的渗透测试人员不仅应能熟练使用各种黑客工具和测试平台，而且还应从方法论的高度对网络渗透测试的组织实施和项目管理具备深刻的认识。

本书系统介绍了专业渗透测试的基础理论和方法，注重基本概念与理论实践的结合，从目前国际上公认的渗透测试方法论、通用执行标准到渗透测试流程中的每个关键环节，为读者详细介绍了如何组织和实施专业化的网络渗透测试。全书共分 15 章：第 1 章对全书的内容进行了简要的介绍；第 2 章主要介绍了黑客的职业道德；第 3 章主要讨论了如何建立渗透测试实验环境；第 4 章主要介绍渗透测试方法论与渗透测试框架；第 5 章主要介绍如何进行渗透测试项目管理；第 6 章介绍如何进行渗透测试信息收集；第 7 章介绍如何进行漏洞识别；第 8 章介绍漏洞的验证与利用；第 9 章介绍本地系统渗透测试；第 10 章介绍提升系统权限；第 11 章主要讨论如何攻击网络的支持系统，特别是数据库服务器和网络共享系统；第 12 章主要讨论如何进行无线网络和网络管理协议的渗透测试；第 13 章主要讨论不同类型的 Web 应用攻击，包括 SQL 注入和 XSS 攻击等；第 14 章主要介绍如何撰写渗透测试报告；第 15 章为如何成为一名职业的渗透测试工程师提供了发展指南。

原著者 Thomas Wilhelm 是科罗拉多理工大学的副教授，之前就职于美国财

富前20强公司,主要从事渗透测试和风险评估工作。其在渗透测试和风险评估领域有超过15年的工作经验,取得了多项信息安全领域的专家证书,在信息系统安全专业领域拥有多年理论研究和实践经验。本书英文原著在美国上市后,引起了强烈的反响。许多IT研究分析师声称,“本书将影响渗透测试人员的整个职业生涯,对网络安全咨询行业的观念影响是不可替代的”。

本书适合作为网络空间安全相关专业高年级本科生的选修课教材,特别适合作为研究生的专业课教材,同时也可供从事计算机网络安全、计算机网络渗透测试和网络攻防工作的技术人员作为必备的参考书。

参加本书翻译工作的有王布宏、柏雪倩、李夏、刘新波、杨智昱。柏雪倩、李夏、刘新波、杨智昱、田继伟、尚福特、李腾耀负责本书校对和文字整理工作,刘新波、刘帅琦参与了本书插图的修改和整理,全书由王布宏和李夏负责统稿。张群审阅了译稿并提出了许多宝贵的意见和建议。

感谢中央军委装备发展部装备科技译著出版基金对本书翻译出版的支持,同时感谢责任编辑牛旭东在本书出版过程中所付出的辛勤劳动。

受译者水平和知识面所限,书中难免有疏漏、不当和错误。恳请读者批评指正。

译者

2017.12

作者简介

Thomas Wilhelm 从 1990 年开始从事信息安全工作，作为信号情报分析员、俄语议员和密码分析员在美国陆军服役 8 年。他曾在包括 DefCon、HOPE 和 CSI 在内的美国各大安全会议上发表讲话，在财富 100 强公司中从事风险评估、参与和领导外部和内部渗透测试、管理信息系统安全项目等任务。Thomas 已取得计算机科学和管理学双硕士学位，正在攻读信息技术博士学位。另外，他还在科罗拉多理工大学兼任副教授，参与编写杂志和书籍在内的多项专著。Thomas 现在主要通过 HackingDojo.com 为公众和政府人员提供安全培训课程，并已获得以下认证证书：ISSMP（信息系统安全管理专家）、CISSP（注册信息系统安全师）、SCSECA（Sun 认证安全管理员）和 SCNA（Sun 认证网络管理员）。

前　言

在本书第1版完成之后，渗透测试领域已经发生了令人震撼的巨大变化。本次第2版增加了许多新元素——不仅仅是对第1版素材的更新和拼凑。笔者认真听取了本书所有读者的意见，将多数内容重新进行编排以方便读者阅读，并且对大部分内容进行了充实，从而对本书第1版中讨论过的概念进行扩展和增补。希望这样的安排能得到各位读者的认可。

本次第2版的另一点不同之处在于，不再随书附赠DVD光盘。原书附赠光盘中包含的内容可以在HackingDojo.com上下载，这一点在本书中将会多次提到。新的资料/渗透测试目标/测试平台随时都有可能发布，而通过网站能够保证在本书的下一版本出版之前及时为读者提供最新的资料。如果你对本书及其内容或者HackingDojo.net网站有任何问题或者批评建议，请直接通过电子邮件info@HackingDojo.com与我联系。

让我们开始探索吧！

Thomas Wilhelm

目　录

第1章 绪 论

章节要点

- 引言
- 新版介绍
- 下载链接和支持文件
- 本章小结

1.1 引言

尽管距离前一版《专业渗透测试》的撰写仅仅只有几年时间，但渗透测试领域已经发生了许多变化，是时候对内容进行更新和扩充了。渗透测试的终极真理在于“系统和网络安全是不断变化和发展的目标”，同时，已经有许多新的资源可以帮助我们成为专业的渗透测试人员。在第2版中，我们将关注渗透测试领域发生的新变化，并详细介绍如何进行内部和外部渗透测试。

读者对本书的第1版给予了许多赞扬，包括我的写作风格、章节练习和内容覆盖面等。然而，也有一些读者对内容提出了许多建议，如不同攻击类型的深入介绍、更复杂的实验环境设置和更多的应用实例等。新版将在这些方面进行修订和更新，以满足读者的以上需求。

过去几年中发生的另一个显著变化是电子书籍的爆炸性增长。本书第1版通过数字方式发行的销售量也相当可观。本书第1版的纸质书籍附带了DVD光盘，但DVD光盘中的内容无法包含在电子版书籍中。从这个新版本开始，随纸质书附赠的DVD光盘中包含的所有材料都可以在支持网站（HackingDojo.com）上下载。这一改变同时也更加方便读者在发现书中错误时及时进行订正和提出反馈，而不必等待再版时再对书中内容做出相应改变。

新版本的最后一个重要变化是，我们将书中的大多数实验和攻击行为限制在实验环境中。以前的版本中，我们包括了连接互联网并与网上资源交互的应用实例。然而，在新版本中我们将试图在实验环境中验证和展示这些攻击实例（虽然我们不会100%的成功，但我们会努力尽可能地接近这一比例）。这其中

包括一些更加复杂的攻击类型,如对网络中的硬件设备实施的攻击。这绝对是一个挑战,但在一个封闭隔离的实验环境中尝试这些攻击是非常重要的,因为它可以方便读者成功复现书中给出的攻击示例。为了让读者能够顺利完成书中的攻击示例,相应的配置数据可以在配套网站上下载和安装。

对于新版中这一系列的变化,我感到很兴奋,希望它可以为你专业渗透测试领域的学习提供最大限度的帮助。

1.1.1 新版介绍

新版书中除了篇幅的增加之外,还有一项更大的变化。在之前的版本中,并没有区分攻击的接入点,无论进行外部渗透测试(以连接互联网的系统作为目标)还是内部渗透测试(在组织的内部网络中进行,好像我们是一个恶意的"内鬼"),我们对这两种测试都同等对待。此外,我们之前内容的组织没有考虑不同技术水平读者的需要,将不同难度的内容混合交织在一起,使读者难以入门。在新版书中,我们将修改内容布局,使不同技能水平的读者可以在这本书的不同阶段开始学习,就自己关注的特定内容有针对性地进行学习和练习。

新版书中的前8章主要集中于基本实验环境的构建、渗透测试的方法论和实施外部渗透测试的相关技术。剩下的章节中,我们将主要针对某些相同的概念进行扩展,并对包括网络设备的攻击、无线黑客攻击和中间人攻击的内部渗透测试技术进行介绍。最后2章我们着重介绍渗透测试报告的撰写方法,并就如何成为专业的渗透测试人员这一点回答读者关心的问题并给予鼓励。下面让我们详细对比一下新旧两个版本各章的具体内容。

准备工作

作为讨论黑客行为的重要部分,我们直接讨论黑客行为的"对与错"。我们首先讨论"道德和黑客"(第2章)。作为专业的渗透测试人员,遵守道德规范的原因依然胜过任何误入歧途参与恶意行为的借口,因此,本章将关注渗透测试领域现存的道德标准和在测试中约束和规范我们行为的法律。尽管大多数读者往往倾向于将这个主题匆匆一带而过,但是,在今天的企业中,职业道德是一个核心问题,通过了解如何在渗透测试项目中规范和约束自己的行为,可以有效改善与客户或雇主的职业关系。

在第3章"建立自己的实验环境"中,我们首先介绍如何构建一个基本的、功能齐全的虚拟实验环境。一个渗透测试的初学者往往会提出下列问题:"需要什么设备建立实验环境"以及"如何学习渗透攻击"。我们将使用虚拟网络快速、简便地搭建一个实验环境,以帮助读者回答上述两个问题。我们还会介绍在实验环境中可以搭建的各种虚拟系统,这些虚拟系统会给读者提供不同的挑

战和学习机会。一旦我们构建了基本的实验环境，我们将讨论如何建立与企业网络环境相仿的复杂实验环境，方便我们对更多高级的渗透主题进行测试和学习。我们将研究如何对交换机和路由器这些实际的网络设备进行设置。读者可以在支持网站上下载实验环境所需的系统配置数据，并借此复现实验内容。对渗透测试实验环境进行升级的目的在于可以通过实验环境对一些系统和网络设备入侵访问的最有效的方法进行介绍，而这些方法往往是渗透测试成败的关键。

在第4章“方法论和框架”中我们将介绍在专业渗透测试领域获得了广泛认可的行业标准和测试基本步骤。在过去20年中，渗透测试这一行业取得了飞速发展，渗透测试高级框架标准的制定梳理工作已经基本完成（虽然仍有很多工作要做，但是更多的是微调而不是推倒重来）。在这一章中，我们将介绍两种基本的渗透测试方法，并比较这些方法的优缺点。

第5章“渗透测试项目管理”主要介绍如何管理渗透测试项目。这一章将会与之前的版本略有不同。在新版书中，我们将对如何在一个组织中管理渗透测试项目重新进行讨论。同时，如何在没有组织基础设施支持的情况下，作为独立顾问管理渗透测试项目，也将是本章的讨论内容。

执行渗透测试

接下来的部分章节中我们将对第4章“方法论和框架”中涉及的具体技术细节展开讨论。一般来说，典型的渗透测试包括识别可利用的漏洞、攻击系统以及提升权限等步骤。

尽管不同的出版物中对“信息收集”术语的表述可能不尽相同，在第6章“信息收集”中，我们将研究被动和主动的信息采集技术，它们将为渗透测试的初始阶段提供引导。根据项目过程中的不同需求，可能需要让测试行为保持隐蔽，因此，我们将分别介绍如何在主动和被动信息收集中使测试保持隐蔽。

第7章“漏洞识别”以上一章节中我们对信息收集的讨论为基础。在这一章中，我们将讨论端口扫描工具和技术、系统和服务识别以及最终的漏洞识别。在漏洞识别阶段，我们还将讨论网络审计人员和渗透测试工程师之间的工作区别，用以区分这两个职业。

由于漏洞利用技术的流动性和多样性，第8章“漏洞利用”可能是这一版书中最难讨论的话题。我们将介绍各种不同的攻击方法，使读者领略到系统攻击方法的多样性。此外，我们还将介绍一些自动化工具，并对使用这些工具的时机和禁忌进行讨论。

在完成上述章节的学习之后，我们关注的焦点将逐渐从外部渗透测试转移到内部渗透测试。