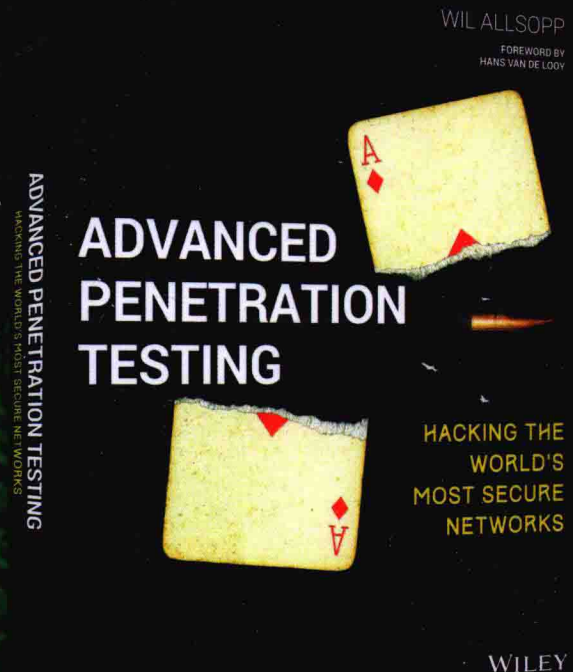
安全技术经典译丛

WILEY

渗透测试高手
打造固若金汤的安全网络

Advanced Penetration Testing:
Hacking the World's Most Secure Networks



[美] Wil Allsopp 著

杨 雪 译

清华大学出版社

安全技术经典译丛

渗透测试高手

打造固若金汤的安全网络

[美] Wil Allsopp 著

杨 雪 译

清华大学出版社

北 京

Wil Allsopp
Advanced Penetration Testing: Hacking the World's Most Secure Networks
EISBN：978-1-119-36768-0

北京市版权局著作权合同登记号 图字：01-2017-4035

图书在版编目(CIP)数据

渗透测试高手　打造固若金汤的安全网络 / (美) 威尔·奥尔索普(Wil Allsopp)　著；杨雪　译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文：Advanced Penetration Testing: Hacking the World's Most Secure Networks
ISBN 978-7-302-49780-6

Ⅰ. ①渗…　Ⅱ. ①威…　②杨…　Ⅲ. ①计算机网络－网络安全　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 037091 号

责任编辑：王　军　于　平
封面设计：牛艳敏
版式设计：思创景点
责任校对：曹　阳
责任印制：刘海龙

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：北京鑫丰华彩印有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：12.5　　字　　数：318 千字
版　　次：2018 年 3 月第 1 版　　印　　次：2018 年 3 月第 1 次印刷
印　　数：1～4000
定　　价：49.80 元

产品编号：075957-01

译 者 序

本书作者 Wil Allsopp 是渗透测试领域的专家，他为我们提供了一个全新的渗透测试视角。与其他介绍渗透测试的书籍相比，本书并未花费笔墨介绍 NMap、Kali Linux 等常规工具，而是以为不同行业的客户执行的渗透测试为例介绍高级持续性威胁(Advanced Persistent Threat，APT)建模，并给出一系列实用的工具和解决方案。

作为高校老师，在教学和科研压力繁重的情况下，我为什么还要翻译这本书？原因有二。第一，了解并掌握渗透测试技术非常重要；第二，我非常愿意为国家网络空间安全战略贡献自己的绵薄之力。我国国家计算机网络应急技术处理协调中心在《2016 年中国互联网安全报告》中指出：高级持续性威胁目前已常态化，我国面临的攻击威胁尤为严重。360 威胁情报中心发布的高级持续性威胁研究报告称：2016 年针对我国境内目标发动攻击的 APT 组织有 36 个。更多攻击者依托商业攻击平台和互联网黑色产业链数据等成熟资源实施 APT 攻击，不仅降低了发起 APT 攻击的技术和资源门槛，还加大了受害方溯源分析的难度。

强烈建议对网络安全感兴趣或正从事网络安全工作的读者阅读本书。Wil Allsopp 详细描述了如何针对不同目标定制攻击，即使读者不具备编程背景也能了解攻击者如何隐蔽地从“安全的”网络中窃取数据。作者通过大量示例展示了社会工程学在网络攻击中的作用。2017 年 5 月，WannaCry 蠕虫大规模感染计算机并植入勒索软件加密用户的数据，受害者需要支付约 300 美金的比特币才能解锁。读者可以在本书中了解到勒索软件的机制。此外，作者针对英国某军事计算机网络执行的 APT 建模令人大开眼界，而他对银行等高安全性机构执行的渗透测试会让许多同行啧啧称赞。

感谢清华大学出版社的编辑，她们为本书的翻译投入了巨大的热情并付出了很多心血。她们不断地给予我鼓励，对译稿提出了许多宝贵的意见，其专业精神令人佩服。没有她们，本书不可能顺利付梓。

Wil Allsopp 对渗透测试理解透彻，译者本着“诚惶诚恐”的态度，在翻译过程中力求“信、达、雅”，但鉴于水平有限，错误和失误在所难免，如有任何意见和建议，请不吝指正。感激不尽！本书全部章节由杨雪翻译，参与翻译的还有罗军、杨朝祥、刘玉平、罗贤旺、杨凤娥。

最后，希望读者在阅读本书后有所收获！

译者

作 者 简 介

Wil Allsopp 喜欢将物品拆卸成零件，但他偶尔又将它们重新组装起来。Wil 对渗透测试的热情就如同许多人热衷于逛酒吧(Wil 也经常会去酒吧喝上一杯)。1999 年，Wil 在 Zaltbommel 一家名为斯塔特的咖啡店里偶遇了一位志趣相投的伙伴，随后他辞去 IBM 软件开发工程师的职位，转而成立了老虎队安全公司。由于时间的原因(至少 Wil 这么认为)，这家公司后来被并入库拉索安全公司。

二十年过去了，Wil 仍在不断搞破坏，而不同的是，目前是一些世界知名的企业花钱请他进行“破坏”。

Wil 目前和妻子一起居住在荷兰，与他们一同生活的还有一大群猫、狗、鸡和一只名叫马尔科姆的癞蛤蟆。

我们在黑暗中劳作，竭尽所能并奉献所有。我们的怀疑出自热情，而保持热情是完成任务所必需的。剩下的就是艺术的疯狂。

—— Henry James

技术编辑简介

Elias Bachaalany 具有长达 14 年的计算机编程和软件逆向工程经验，他是 Wiley 出版社出版的书籍 *Practical Reverse Engineering* 和 *The Antivirus Hacker's Handbook* 的合著者，并单独撰著 *Batchography: The Art of Batch Files Programming* 一书。Elias 精通多种技术及编程语言，如网页编程、数据库编程和 Windows 设备驱动编程(boot loader 和小型操作系统)等，能够设计.NET 托管代码[①]，编写脚本和软件保护程序，并开发逆向工程和桌面安全工具。

① 译者注：托管代码(managed code)指由公共语言运行库(Common Language Runtime，CLR)而非直接由操作系统执行的代码。公共语言运行库提供许多核心的运行时服务，如跨语言集成、垃圾回收、运行库类型检查、安全支持等。

致　谢

非常遗憾无法在此感谢所有人，但我要特别感谢 Tim 和 Courtney，在你们的帮助下本书才得以完成。感谢 D. Kerry Davies，你是我们所有人的榜样。感谢英国国家通信总局(Government Communications Headquarters，GCHQ)的宝贵建议。最后，还要感谢我们这个时代最被低估的音乐家之一 Gary McGath。

此外，感谢渗透测试领域的同行、黑客以及这些年来与我共事过的网络安全宣传人员。没有你们就没有这本书的问世。

序　言

我从一开始接触计算机就对这些强大系统的安全性颇感兴趣。作为一名荷兰学生，我在高中学习 ALGOL 60 编程时有幸通过一个 300 波特率的调制解调器拨号接入并使用埃因霍温理工大学的飞利浦 P9200 系统。那时个人计算机并未普及，像 P9200 这样的计算机系统价格不菲。使用调制解调器接入系统并编程解决大量的计算问题对我来说已非常神奇，参观计算机更是梦寐以求的事情。由于该计算机位于大学校园内，因此要参观它还不算太困难。那时，“安全”这一话题并未受到关注，我只需要扮作年轻学者请求参观该设备就能达到目的。

我在埃因霍温理工大学校园内了解到 P9200 只是一台“很小的微型计算机”。真正强大的是美国宝来 B7700 主机。我费了很大力气寻找 B7700 主机系统的接入号，不停游说管理人员以获取登录该系统的账号，并最终获得成功。虽然我并未入侵 B7700 系统，但这一经历证明掌握社会工程学(能够说服对方以博取信任并获得信息)具有极高价值。

我在攻读计算机科学专业时开始使用 Prime 计算机。当时计算机安全并不受重视。PrimeOS 操作系统存在很多缺陷，我们甚至能在其修复安全问题的补丁程序中发现新的安全缺陷。我就是从那时起开始关注信息安全，直至现在。毕业前夕，我开始在一家名为宝西电子的小公司从事核工业系统开发工作，这些核工业系统的规模从小型的基于 6502 处理器的便携式放射物计量器到大规模自动测量系统不等。他们使用 PDP-11 系统控制参与核反应的燃料棒。我从那份工作中不仅了解到安全的重要性，还学会了如何编写安全的计算机代码。我们不能拿多种燃料棒处理程序冒险并泄露高放射性材料，这会引发致命的后果。

1989 年，我接触到一本鲜为人知的地下刊物 *Hack-Tic*，这是一个不定期出版的黑客杂志，该杂志拓宽了我的视野。我注意到更多对信息安全感兴趣的人，他们发表了大量的信息，包括使当时的荷兰电信运营商 PTT 公司(直到今天运营商仍未意识到通过隐蔽而实现安全的思想是完全错误的)大为恼火的电话系统信息和开锁信息等。与志同道合的人在杂志上探讨这些话题最终发展为每月聚会、不定期举行派对和(在酒店、露营地——通常要能够快速连接互联网)开展黑客活动。如今，我们拥有不仅可以编写或破解软件，还可以通过不同方式使用各种现代技术的黑客空间。曾经的地下活动已经很好地融入了现代社会。

回想 2000 年，在经历了几次跳槽后，我在荷兰最大的计算机中心之一担任渗透测试部门负责人。然后我和两个朋友决定一起创业。当时，互联网泡沫刚刚破灭，我们认为应该创建一家专注于信息安全的咨询公司。尽管当时我们对未来一无所知，但幸运的是，我们一直坚守这一信条：“即使没能成功，但至少我们经历过。”

我在斯堪的纳维亚半岛游览时接到了第一单生意，我不得不一边与客户交谈，一边在路过的一家酒店的房间里起草一份渗透测试合同，并用宾馆的传真机将合同发送给客户。

当时，我们的公司甚至还没有名字。

即使泡沫破灭，许多互联网公司倒闭，但我们仍继续营业。由于没有找到与我们要提供的服务相近的域名，我们为公司命名为 Madison Gurkha[①]。这个颇具异域风情的名字有多种好处，例如：你至少需要拼读三次才能完整念出它的名字(这会给客户留下深刻印象)，还会让人们猜想我们是一家总部在荷兰境外的大型跨国集团。

那时我们不需要销售或市场部门。我们的个人关系网在不断扩大，从事相同业务的公司不多，因此在客户中的口碑为我们带来了很多生意。我们当时仅从事基本的 Web 应用与信息、通信和技术(Information Communications Technology，ICT)基础设施的漏洞评估，并在客户对真实攻击给其 ICT 环境带来的影响确实感兴趣时执行一些渗透测试。由于可用的工具很少，我们必须自己编写漏洞利用程序和脚本以减轻工作量。漏洞利用程序有时会发布在互联网上(通常发布在新闻组[②]中)，但你必须重新编译这些程序。由于这些漏洞利用程序中往往包含一些缺陷，而那些仅编译这些程序的脚本小子无法真正理解问题所在，因此无法使用这些代码(你必须修改代码以使其可用)。到本书写作时，Metasploit 和 Nessus 等工具已经非常普及，电视剧《黑客军团》展示了这些工具的使用。

然而，信息安全也在进步。信息安全一直而且很可能永远是在攻击与防守之间寻求不稳定的平衡。可用工具的功能在增强，并将出现更多、更高级的工具。但这些工具只有在那些了解工具的优缺点并能解释结果的专家手中才能真正发挥价值。

Wil Allsopp 就是这样的专家。Wil 于 2006 年加入 Madison Gurkha 后，我有幸与他共事。经过多年的发展，我们已由一个三人的初创公司变为如今专门从事信息安全咨询的企业。一直以来，Wil 帮助我们进一步拓宽安全测试的范围。他一直在寻找漏洞并希望企业和机构能够意识到安全威胁。本书包含了许多介绍高级威胁的有价值的例子。

如果你所在的机构并不只满足于遵循“处于可控范围”的检查列表实施安全防御，而是真正想了解自己能否抵御当前世界范围内正在发生的各种高级威胁，则你应该阅读这本书。请确保你花钱雇来的公司能够真正执行此类攻击。Wil 再次展示了一个真正的信息技术专家不但知道如何使用工具，还会在必要时创新性地思考并实施其他高级的攻击。常规的漏洞扫描有助于你的基础设施保持正常，而真正采用本书介绍的高级技术的渗透测试能够为你提供必要的信息，让你了解自己是否真正掌控了信息安全，还是仅依照所谓的“检查列表”进行防御而对真正的危险视而不见。

2016 年 10 月 5 日于阿姆斯特丹

汉斯·冯·卢瓦

Madison Gurkha 公司创始人

① 译者注：Madison Gurkha 公司已于 2017 年 10 月 5 日更名为 Secura。

② 译者注：新闻组(newsgroup)是一个电子讨论组，它集合了对某一主题具有共同兴趣的人发表的文章。

前　言

认为好运青睐勇敢的人是一种错误的理念。事实上，好运总是青睐有准备的人。当公司经历严重的安全事故时，你所做的准备以及对这一事件必然性的理解决定了公司能否从事故中成功恢复。不论你是本地社区大学的安全负责人，还是国际银行的首席信息安全官(Chief Information Security Officer，CISO)，上述事实同样适用。

霍华德·拉夫曾说，“诺亚建造方舟时，天并未下雨。”

做好准备的第一步就是要树立意识。

攻击的相似性

我们总是认为自己必须为系统安装补丁程序并确保网络的安全，因为黑客会大范围扫描网络地址，寻找未执行上述操作的受害者，这些黑客会入侵他们遇到的任何脆弱的系统。从某种程度来说这种认知是对的——总有人喜欢攻击那些能被轻松入侵的系统。20 世纪 80 年代也是如此——如果你清楚自己面临的攻击，防御公共交换电话网络(Public Switched Telephone Network，PSTN)上的战争拨号很容易。然而，如果你被某个既有时间又有资源的攻击者盯上，问题则变得截然不同。简单地说，无论是 20 世纪 80 年代还是现在，耐心地针对某些用户实施攻击以入侵目标公司的系统通常都是最好的方式。然而，与其他行业一样，安全公司也在不停地以不同的时髦名词销售“新的”产品和服务，这个新名词就是高级持续性威胁。

高级持续性威胁(Advanced Persistent Threat，APT)

与传统入侵不同，APT 特别具有目标导向性。攻击者试图寻找一些内容(例如某些专用数据)并用足够的耐心去获取它们。虽然我不建议将复杂的流程分解成简单的列表或流程图，但所有 APT 通常具有以下特征：

- 初始化攻击——通常借助社会工程学实现。针对某一终端的攻击通常包括某一核心技术组件(例如 Java 小程序)，但如果缺少令人信服的托词，攻击通常注定会失败。尽管可以自主地选择托词，但若想取得成功，你通常需要针对目标公司或其雇员定制托词。随意尝试不同的攻击传递方式然后攻击上钩的对象并不是合适的 APT 建模方式，攻击者通常不会这样做。
- 建立攻击的前沿阵地——确保不需要重复初始化攻击就能进一步访问被攻陷的网络资产。命令与控制(Command & Control，C2)可以实现这一功能，你最好创建自

己能够完全理解并在必要时可根据需求定制的 C2。本书在介绍 C2 各方面时强调的一个关键点是在确保 C2 安全性的同时必须使其网络流量看上去合法。这个问题很容易解决。

- 权限提升——获取本地管理员和域管理员权限。实现这一目的的方法有很多，本书将着重介绍一些最实用且可靠的方法以及一些关键概念。
- 内部侦察——从周边基础设施、信任的关系以及 Windows 域结构中收集信息。对任何 APT 活动来说，获得成功的一个关键因素是态势感知。
- 扩大控制的网络范围——借助收集到的管理员凭据或其他攻击扩大对其他网络设施的控制。这种方式又称为“内网漫游”，攻击者在目标网络内部创建稳定的操作平台后，通过这种方式扩大自己在基础设施中的影响力并利用其他主机。
- 持续性——确保能够通过命令与控制持续地控制目标。持续性主要意味着无论目标机器是否重新启动，你都能随时访问目标。
- 完成任务——渗漏窃取到的数据。这是 APT 中最重要的一部分。攻击者对破坏系统、篡改网页或窃取信用卡账号(除非这些内容对达成最终目标有所帮助)不感兴趣。一般来说，攻击者的目标非常明确——通常是专有数据——当他们定位并渗漏出这些数据后攻击就完成了。

我是一名职业渗透测试工程师(你也可以称我为专业“黑客”)，在过去二十年的大部分时间里，我为每一种可能的客户和市场工作。本书介绍了这些工作经历。我想向读者介绍传统渗透测试在保护机构免受有针对性的 APT 攻击时几乎失效的原因。现代渗透测试的方法陷入了停滞，只有打破僵局才能实现对 APT 的防御。

下一代技术

有许多技术宣称自己能够防御 APT 攻击并阻止未知的恶意软件。其中一些产品表现尚可，它们的确通过提供某种程度的行为分析增强了安全性——例如，通过查看.exe 文件的行为而不是易被绕过的反病毒特征来捕捉 Metasploit 回调函数。然而，在这种情况下，APT 建模依然很容易，因为理解上述工具的行为非常容易。真正的 APT 攻击由专业的攻击者实施，这些攻击者非常了解现代入侵检测和防御系统的工作原理，并能开发出自己的攻击工具。因此，我在介绍 APT 建模技术时主要使用 SSH 协议，因为该协议在解决许多问题的同时还能够使生成的流量看上去合法。我们有必要思考 APT 的本质及其原因。许多商业机构或其他组织错误地理解了高级持续性威胁，却仍在提供建议及销售服务。下面这篇发表在 InfoWorld[①]上的文章恰好能够反驳我最近在网上看到的一些错误观念。

- 判断是否遭受 APT 攻击的特征一：夜间登录次数激增——纯属无稽之谈。攻击者在攻陷目标后(无论采用何种攻击方式)不会使用任何会被审计的登录方式，因为他们已经部署了自己的命令与控制基础设施。无论是深夜还是其他时间你都不会看到他们的登录记录。

① 译者注：InfoWorld 是美国国际数据集团(International Data Group, IDG)旗下的出版机构。

当一个老练的攻击者创建自己的C2后，审计日志很有可能无法记录任何信息。攻击者很可能会绕开这些机制。

- 判断是否遭受APT攻击的特征二：查找被广泛部署的后门木马——我将在本书中反复向读者灌输反病毒软件和其他恶意软件检测工具对APT无效的观念。“A”代表高级，攻击者不仅能够开发自己的工具，还可以伪装可用的公开工具。你所发现的后门木马(不管其是否被广泛部署)往往是外部攻击者事先部署的、故意让你发现的诱饵。
- 判断是否遭受APT攻击的特征三：意外信息流——“我希望所有的电子邮件客户端都能够显示用户最近一次登录、查收电子邮件的位置以及访问上一条信息的位置。Gmail和其他云电子邮件系统已经向用户提供此项功能。”

  任何电子邮件系统(或其他系统)都可以记录远程IP地址并执行实时分析以检测异常行为。但是，如果攻击者在你的网络内部访问电子邮件，源IP地址将来自你自己的网络。随着浏览器攻击的频发，这种情况将变得更加常见。
- 判断是否遭受APT攻击的特征四：发现意外的数据压缩文件——寄希望于偶然发现包含有价值数据的ZIP文件(查找这些文件很方便)并不是实现信息安全的好方法。尽管此类文件的存在很可能是系统被入侵的标志(Indicator of Compromise, IoC)，但这种方法不可靠也无法重复。你应该认为，既然攻击者能够进入内部网络窃取宝贵的数据，他们就一定知道如何使用删除命令。
- 判断是否遭受APT攻击的特征五：检测哈希传递攻击工具——我并不清楚为何唯独关注“哈希传递攻击”——特别是它们应作为攻击框架的一部分，而不是单独存在。尽管如此，虽然此类工具的存在可以被认为是IoC，但你将在本书中了解到APT攻击者不会以这种方式在被攻陷的主机上部署能够被检测到的攻击软件。隐蔽性和耐心是APT的标志。

“黑客”

我们对“黑客”的认知已经发生了翻天覆地的变化。“黑客”一词已经过时，其所呈现的内涵完全是错误的，我倾向于使用中性的术语，如：攻击者或外部活动者。你会了解到目前从事攻击活动的人比当年那些拥有大把时间的青少年无政府主义者要糟糕得多。在黑客活动的“黄金年代”，马克·阿贝尼[②]、凯文·普尔森[③]和凯文·米特尼克[④]等是典型的英雄人物，与今天相比那个年代竟然难以置信的纯真。当下的情形比20世纪80年代激励了许多黑客的计算机科幻小说中描述的场景还要光怪陆离。

这几年我异常忙碌。斯诺登的披露震惊了全世界，这直接导致科技行业对安全的态度

② 译者注：马克·阿贝尼是来自纽约的计算机黑客，他是骗局大师(Master of Deception)的创始人之一，激励了美国成千上万的青年人“钻研”国内电话系统的内部工作原理。

③ 译者注：凯文·普尔森经常使用马甲“黑暗但丁(Dark Dante)”作案，他因攻击洛杉矶电台的电话线路而出名。

④ 译者注：凯文·米特尼克是第一个被美国联邦调查局通缉的黑客，有评论称他是世界上“头号计算机黑客”。凯文·米特尼克现在是一名网络安全咨询师，他出版了《反欺骗的艺术》《反入侵的艺术》等著作。

发生了广泛变化。2013 年，我与一家客户开展了一场在披露发生前无法想象的沟通——他们想要规避的对象是美国国家安全局(National Security Agency，NSA)。该客户并非暴民，而是一家具有良好口碑的世界 500 强公司。知识产权盗窃呈上升趋势且规模不断扩大。出于我的工作性质，我可以肯定地说读者所了解到的只是那些披露给媒体的攻击事件，与未被媒体报道的内容相比，它们仅是冰山一角。我每天都会接触到此类安全事件。不幸的是，对更广泛的科技行业来说，入侵目标系统(包括恰当执行的渗透测试)比保护其不受攻击要容易得多。系统从安全变得脆弱就像上千人中有人犯一个小错误那样简单。

忘记你对渗透测试的所有认知

没有什么是安全的。读者至少应该收获这样一条经验——一个坚定的攻击者总是处于优势地位，并且(极少数除外)企业越大，不安全因素越多。因为大企业意味着更多的待监控对象、更多的网络出站和入站点、业务单元间的边界模糊不清以及更多的用户。当然，这并不意味着大型企业应该放弃希望，但仅“遵照安全程序”是不够的。

尽管这种全面的或开放范围的测试的好处显而易见，但至少与传统的渗透测试相比，APT 建模在现实中极少执行。其原因有二：人们认为 APT 建模收费更高(事实并非如此)以及企业极少想做这一等级的审查。企业只想遵从他们的安全政策和法定要求。你一定听到过遵从 HIPAA[⑤]、SOX[⑥]或 PCI[⑦]标准之类的术语，供应商将他们打包在一起就好像它们有什么具体含义似的，但它们的存在只是让律师们开心并获得高薪，而且该产品包很容易销售。即使你的企业遵从 PCI 标准，但仍可能极度脆弱。读者可以去了解一下 T.J.Maxx[⑧]或索尼公司，T.J.Maxx 花费多年才恢复人们对其品牌的信心，而大量的数据泄露意味着索尼公司所受的损害目前仍在评估中。这足以说明以追求合规的心态看待安全性是有害的。我在此反复强调这一点，因为我想确保读者彻底理解遵从安全策略和安全并不是一回事。

本书组织架构

如前所述，我将在本书中探讨在现实世界中执行 APT 建模，但本书的内容并不完全拘泥于此。我将介绍一个可行的 APT 测试框架，并在每章中添加一些解决不同问题所需的功能，并将结果应用于所讨论的目标环境。在介绍时，我将尽可能做到与源代码无关，但由于你需要开发自己的工具——有时需要使用不熟悉的编程语言——因此，坚实的编程知识是必不可少的。

本书每一章都介绍了我对某特定行业的 APT 建模经验。因此，每一章都会引入新的概念、思想并启发读者。我认为从不同的行业背景、对安全的态度以及能力差异巨大的网络

---

⑤ 译者注：HIPAA 法案全称为 Health Insurance Portability and Accountability Act，其目的是简化管理以降低日益增长的医疗费用开支。

⑥ 译者注：萨班斯法案(Sarbanes-Oxley Act, SOX)是美国政府出台的改革会计职业监管、公司治理、证券市场监管等方面的法律。

⑦ 译者注：支付卡行业(Payment Card Industry, PCI)数据安全标准由 PCI 安全标准委员会创始成员制定，旨在鼓励国际上采用一致的数据安全措施，确保持卡人的信用卡和借记卡信息安全。

⑧ 译者注：T.J.Maxx 是美国的名品打折连锁店。

防御人员等角度来介绍 APT 建模很有价值。如果你是一名渗透测试工程师，你会有所收获。如果你的职责是防止攻击者入侵所在单位的系统，你会了解到一些让你半夜睡不着的内容，但本书也会告诉你如何构建更具弹性的防御措施。

我无意写作一本枯燥乏味的技术手册，本书的每个章节都采用了类似的格式——以不同的行业作为背景，我们在其上探究新的技术、攻击方式及主题。这不仅包括成功的攻击向量，还包括权限提升、规避恶意软件检测、态势感知、内网漫游以及多种能够帮助读者深入理解高级可持续威胁和 APT 建模的关键技术。虽然我给出了许多示例，但本书的目标并不是简单地提供一些代码和脚本，而是鼓励读者更宽泛地、从根本上理解这些问题，从而能够以新的方式思考并开发自己的工具。

- 第 1 章“医疗记录的安全性”讨论针对医院基础设施的攻击，阐述宏攻击和浏览器攻击等概念，并初步介绍 C2。
- 第 2 章“数据窃取研究”以一所研究型大学遭受的攻击为背景探讨使用 Java 小程序作为攻击向量，并讨论更高级的 C2。
- 第 3 章“21 世纪的抢劫”讨论如何针对银行等高安全性目标执行渗透测试和采用了 DNS 协议的高级 C2 技术。
- 第 4 章“制药业”介绍一场针对制药公司的攻击，并以此为背景介绍客户端利用及将 Metasploit 等第三方框架集成到 C2。
- 第 5 章“枪支弹药”介绍勒索软件仿真以及使用洋葱路由(The Onion Router，Tor)隐蔽服务来掩盖 C2 基础设施的物理地址。
- 第 6 章“犯罪情报”以入侵某警察总部为背景描述，当能够短暂访问攻击目标时使用“爬虫盒”实现长期的攻击活动。此外，该章还将介绍权限提升和通过 HTML 应用程序部署攻击等概念。
- 第 7 章“战争游戏”探讨针对保密网络的攻击，并阐释公开资源情报收集和命令与控制中的高级概念。
- 第 8 章“攻击出版社”展示了如何利用出版社采用的技术和工作流程来攻击。本章探讨新兴的多元媒体及实验性的 C2 方法，并介绍社会工程学中的高级概念。

现在，让我们一同开启高级渗透测试之旅。

目　录