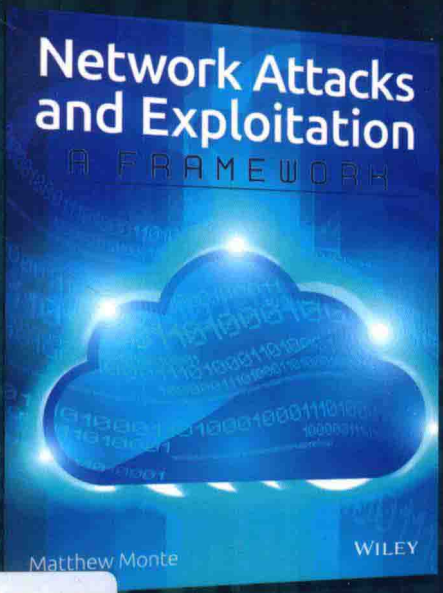
安全技术经典译丛

WILEY

网络攻击与漏洞利用

安全攻防策略

Network Attacks and Exploitation: A Framework

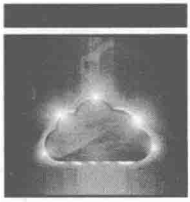


[美] Matthew Monte 著

晏 峰 译

清华大学出版社

安全技术经典译丛



网络攻击与漏洞利用安全攻防策略

[美]Matthew Monte 著

晏 峰 译

清华大学出版社

北 京

Matthew Monte
Network Attacks and Exploitation: A Framework
EISBN：978-1-118-98712-4

北京市版权局著作权合同登记号 图字：01-2016-7773

图书在版编目(CIP)数据

网络攻击与漏洞利用 安全攻防策略/(美)马修·蒙提(Matthew Monte) 著；晏峰 译.
—北京：清华大学出版社，2017
(安全技术经典译丛)
书名原文：Network Attacks and Exploitation: A Framework
ISBN 978-7-302-46667-3

Ⅰ.①网… Ⅱ.①马… ②晏… 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(2017)第 036392 号

责任编辑：王　军　韩宏志
装帧设计：孔祥峰
责任校对：牛艳敏
责任印制：沈　露

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 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：7.375　　**字　　数**：199 千字
版　　次：2017 年 4 月第 1 版　　**印　　次**：2017 年 4 月第 1 次印刷
印　　数：1～3000
定　　价：39.80 元

产品编号：072290-01

译者序

随着计算机互联网技术的飞速发展，在计算机上处理业务已由单机处理功能发展到面向内部局域网、全球互联网的世界范围内的信息共享和业务处理功能。网络信息已经成为社会发展的重要组成部分。涉及政府、军事、经济、文教等诸多领域。其中存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息。很多是敏感信息，甚至是国家机密。由于计算机网络组成形式多样性、终端分布广和网络的开放性、互联性等特征，致使这些网络信息容易受到来自世界各地的各种人为攻击(例如信息泄漏、信息窃取、数据篡改、数据增删、计算机病毒等)。要保护这些信息就需要有一套完善的网络安全保护机制。

国际标准化组织(ISO)将“计算机网络安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护网络系统的硬件、软件及其系统中的数据不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠、正常地运行，网络服务不中断。”

上述计算机安全的定义包含物理安全和逻辑安全两方面的内容。其中逻辑安全的内容可理解为我们常说的网络上的信息安全，

是指对信息的保密性、完整性和可用性的保护，而网络安全的含义是信息安全的引申，即网络安全是对网络信息保密性、完整性和可用性的保护。从广义来说，凡涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

本书共分 9 个章节，从攻防两个侧面介绍了网络安全攻防战略的相关内容。此外，还提供了一些成功的进攻战略供读者研读。读者可以根据自己的需要选取所需的章节进行阅读，这些章节汇聚了多年来作者作为一名网络安全专家所积累的经验和知识。

本书图文并茂，技术新颖，实用性强，列举大量实例对相关内容做了详细解释，是系统管理员不可缺少的实用参考书籍。

参与本书翻译的人员有晏峰、田洪、范园芳、胡训强、余佳隽、张洁、赵翊含、何远燕、任方燕。最终由晏峰负责统稿，在此一并表示感谢。此外，还要感谢我的家人，她们总是无怨无悔地支持我的一切工作，我为有这样的家庭而感到幸福。

译者在翻译过程中，尽量保持原书的特色，并对书中出现的术语和难词难句进行了仔细推敲和研究。但毕竟有少量技术是译者在自己的研究领域中不曾遇到过的，所以疏漏和争议之处在所难免，望广大读者提出宝贵意见。

最后，希望广大读者能多花些时间细细品味这本凝聚作者和译者大量心血的书籍，为将来的职业生涯奠定良好基础。

晏　峰

作者简介

Matthew Monte 是一名拥有 15 年丰富开发经验的安全专家，曾为多家企业和美国政府开发计算机安全工具以及相关战略。在他的职业生涯中，曾在计算机行业和美国情报界担任技术和领导职位。他拥有康奈尔大学计算机科学硕士学位。

技术编辑简介

Dave Aitel 从 18 岁开始就为 NSA 工作了，比 Edward Snowden 还要早。随后加盟@stake，目前开办了一家专门研究进攻信息安全的公司——Immunity, Inc。

致　谢

首先我最应该感谢美丽贤惠的妻子 Jessica。从最初的想法到最终的评审完成，如果没有她的鼓励和支持，本书就不可能顺利完成。谢谢你帮助我判断内容对读者的有用程度，以及当我在电脑面前专注本书的撰写工作时，承担了那么多家务。

其次要感谢我的孩子 Annablelle 和 Levi，正是因为你们，我才有了写作的动力。你们是任何一位父亲都希望拥有的最可爱的孩子。感谢你们的笑容、容忍、理解和受我欢迎的打扰。

感谢我的母亲以及已经离世的父亲，是你们曾经给了我很多的努力，给了我一台 Commodore 64 以及 BASIC 指导，从而帮助我开启了数字世界之旅。

感谢所有为本书贡献了时间和精力的人士，包括：

Dave Aitel对本书进行了审阅并利用其丰富的经验提供了极好的反馈和示例。正是由于他所提出的具有挑战性的评论和建议，才使本书的内容更清晰、更丰富和更全面。

Carol Long 查看了早期的原稿，Tom Dinse 在编辑和出版过程中给予指导。Wiley 的其他工作人员也给予了极大帮助。

David Nadwodny 提出了自己的想法并给予我极大的鼓励，同时

展示了通过独创性和主动性可用胶带和绳子完成哪些工作。

Dave N 早期所提出的许多反馈意见为我提出了许多新想法。

最后，还要感谢那些没有提及的人士，多年来，我一直和他们一起工作，并且学到了很多。本书的最终完成依赖于他们花费大量时间所进行的研究和分析。我感谢那些默默无闻的奉献者。

前　言

兄弟，为什么你还全副武装？你是否曾想过派人去监视木马？

——Menelaus, The Lliad

请记住，黑客(hacking)不仅是一种犯罪，也是一种生存特质。

——Hackers(1995)

本书并不是一本关于Cyberwar、Cyber9/11 或者Cybergeddon的书籍。这些术语通常用来生成页面点击或者确保资金或业务的安全。之所以使用这些术语，主要是为了引起人们的注意，或者使人们感到震撼而采取行动，这样做也许有用，但在考虑如何构建框架来确保计算机真正安全方面却没有实质性帮助。如果Digital Pearl Harbor(表示一种大规模的毁灭性突袭)即将到来，那么你必须采取什么行动来阻止它呢？更新反病毒软件？谨慎使用附件？确保密码至少有两个n3mber5？做这些事并不能帮助我们了解一种攻击，或者阐明一种可以阻止攻击的策略。

Cyberwar 是否永远不会发生，还是即将发生，又或是正在发生？不同的人对于 Cyberwar 定义的理解也不同，所以给出的答案也不一样。不管用什么动词时态来形容 Cyberwar 的状态，毫无疑问的

是，网络间谍是真实存在的并正在行动。计算机安全公司精细地详述带有相关名称的间谍活动，如 Flame 或者 Aurora。与此同时，媒体还持续报道了 National Security Agency 的网络战能力。当人们还在就 Cyberwar 的意义进行辩论时，一个古老职业的最新化身正在蓬勃涌现。

由于报道的入侵次数非常多，使得攻击计算机网络听起来非常容易。攻击者通常是看不见且无法阻挡的，而受害者则往往不知情且无力应付。在看到此类新闻时，你可能会认为由于许多公司都丢失了自己的信用卡数据、被公开了敏感的内部电子邮件或者丢失了军事秘密，所以受到攻击是不可避免的。

这种态度是偷懒的表现。而给出的理由也总是相同的：过时的系统被忽视了，警告标志被错过了，或者粗心的用户判断失误了。如果已经完成了 XYZ，那么攻击将不会成功，然而随着无数的公司和政府机构被一再渗透，仅解释攻击者使用了什么样的战术就显然不够了。

如果想要了解计算机安全失败的原因，就不能仅通过分析某一特定事件来理解计算机操作的固有特性。是否存在内在的进攻优势？哪些因素增强了或者减弱了这种优势？攻击者为了取得成功通常采用什么策略？如何应对相关进攻策略？如何跟上快速的技术变化？

这些都是难以回答的问题。回答这些问题需要在头脑中形成一个框架来推理策略、技术以及用来执行或防护计算机操作的方法。本书将尝试建立这样一个框架，从而帮助解决上述问题以及其他问题，同时还会介绍一些经久不衰的主题。

计算机间谍活动的频率、复杂程度以及影响力都在不断增加。政治、军事、知识产权以及个人金融信息正以前所未有的速度被窃取。随着处理这方面问题的法律和道德学说的不断出现，冲突将会继续。因此，对于企业领袖、IT 专业人士以及政策制定者来说，开始从战略层面解决这些问题是至关重要的，为此，首先必须了解网络攻击和利用的原理。

目　录