网络入侵防范的理论与实践

郑成兴 著

机械工业出版社
CHINA MACHINE PRESS

网络入侵防范的理论与实践

郑成兴　著

机 械 工 业 出 版 社

本书深入论述了网络入侵防范的思想、方法和意义，从军事对抗中引进的主动防御概念出发，讲述了网络数据获取的基础理论；深化传统的检测技术，探讨引入可行的智能技术；阐述了网络监控、网络取证和网络诱骗陷阱系统等；论述了神经网络和小波分析的理论和应用；最后，对信息系统的生存性进行了分析。

本书可供计算机技术、网络技术、电子信息技术领域的专业技术人员、研究人员、管理人员和教师参考，也可供大学生、研究生或网络爱好都阅读。

图书在版编目（CIP）数据

网络入侵防范的理论与实践 / 郑成兴著. —北京：机械工业出版社，2006.9

ISBN 7-111-19880-8

Ⅰ. 网… Ⅱ. 郑… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 107988 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）

责任编辑：吉　玲　（E - mail：jiling@ mail. machineinfo. gov. cn）

责任印制：杨　曦

北京蓝海印刷有限公司印刷

2006 年 9 月第 1 版第 1 次印刷

169mm × 239mm · 8.5 印张 · 347 千字

0001— 4000 册

定价：30. 00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话（010）68326294

编辑热线：（010）88379768

Http://www.machineinfo.gov.cn/book/

封面无防伪标均为盗版

序

郑成兴同志的新作《网络入侵防范的理论与实践》一书与我们见面了，这是一件值得欣慰的事情。该专著的出版，为国内网络安全的防卫研究增添了一本很有价值的参考著作；为广大从事或爱好网络信息系统安全的读者提供了一本精辟而丰富的研究和学习用书，它必将对网络信息系统安全的研究与教学起到推动的作用。

郑成兴同志是国家 973 项目中“网络信息获取、分析与安全监控研究”课题组的主要成员，在从事课题的研究中积累了丰富的经验，这为他的写作奠定了坚实的理论和实践基础。他在书中对网络安全进行了深刻的分析思考，提出了精辟的理论观点，通过新颖的实验观察得出了中肯的论断见解，使该书具有创新性、先进性，并达到很高的学术水准。

20 世纪的计算机技术与网络信息的出现被认为是最伟大的时代发明之一，全世界进入了一个全新的电子时代。许多美好的憧憬引诱着千千万万的人不断地步入网络的世界。然而，就像 20 世纪中期人们发现原子核的规律一样：原子时代是到来了，但是，真正给人们带来的福音却不像大家期待的那样：人类和平利用原子能的技术至今未能完全实现，而大规模杀伤性的核武器却时时威胁着人类自身的生存。时至今日，人们还不得不消耗巨大的精力来遏制并防范原子弹、氢弹之类的核竞赛。进入了电子时代难道就没有同样的阴影在威胁、甚至在毁灭人类辛辛苦苦建设起来的物质与精神文明吗？今天的网民已经体会到黑客、病毒给网络运行带来的麻烦，它不能不使我们正视互联网给我们带来方便的同时，同样也给我们带来日益增加的安全忧患。

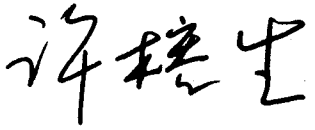
网络的非法入侵问题，一直引起各国业界的高度重视，目前也只能靠局部地添加网络安全设备来增强网络防护的能力。从添设防火墙、入侵检测系统，到网络用户的身份认证，以及网络漏洞扫描、木马病毒的检测等，很长时间里是为原先的网络工程打补丁，处于一种被动的防御状态。从军事对抗中引进的**主动防御**概念启发人们去研究出一批新的网络入侵防范工具，有代表性的是网络监控、网络取证和网络诱骗陷阱系统。这些设备帮助网络管理员通过与入侵者在网上的直接较量，达到知己知彼、使“**敌不知其所攻**”，甚至“**利而诱之，乱而取之，实而备之，强而避之，怒而挠之，卑而骄之，佚而劳之，亲而离之，攻其无备，出其不意。**”同时，在技术和心智上与入侵者一比高低，从而实施有威慑力的网络主动防御策略。当然，除了必要的防范工具外，还要建立严格的内部管理规章制度，

以便网络管理员手中掌握的杀手锏能更好地发挥其致敌死命的效能。这里，还要特别强调的是，在网络安全防范体系中要提供方便高效的网络管理平台，同时包括随时对网络安全的风险评估，也即对网络生存性的分析和应急响应措施的部署。《网络入侵防范的理论与实践》一书尽可能地做到了对整个防范体系的描述和引领，是作者近年来一次较新的尝试。

中国科学院为互联网的最早引进作出过突出贡献，高能所一向重视对网络的管理，力求保障网络的稳定、安全运行。位于高能所计算中心的网络安全课题组从开通网络起就积极跟踪国外先进的管理技术，不断培养出网络安全的专业人才。先后有二十多位硕士生毕业，十多位博士学位获得者，如今他们正活跃在网络安全领域的各个岗位上，成为学科技术的带头人。从技术研究到产品转化上，他们研发的富有创新意识的网络隐患扫描仪、网络取证设备和攻防兼备的网络诱骗陷阱系统等正在社会上投入使用；更多的项目研究和技术开发正在国家的支持下进一步深入开展，不久的将来会陆续产生出新的网络安全产品。

在未来的几年里，计算机网络的需求规模将会越来越大，通信从窄带到宽带，媒介从有线到无线；机型既有大机器，又有超微化的 PDA；网络安全问题也是无处不在。随着各种新的通信协议和传输加密等技术的出现，原本希望能够加强网络安全防线的措施可能也给许多已有的基于网络捕包技术的安全产品带来新的挑战。这一点读者从本书介绍的网络安全原理基础中可以得到清晰的解析。同时，这本身也促使我们现在就下一时期的网络安全技术应该出现什么样的格局进行思考。

通过广大网络安全研究者几年的努力，我国已经在网络安全领域的研究中达到了较好的水平，涌现出一批崭新的成果。“沉舟侧畔千帆过，病树前头万木春”，网络安全研究必须持之以恒、厚积薄发，本书正是反映了一支技术团队在多年的积累中所取得的一系列成果。据悉，该技术团队的实力正在与强大的资本实力结合，在不久的将来她势必为我国在网络安全领域的研究添光增彩。



2006 年 8 月于中科院高能所

试读结束：需要全本请在线购买： www.ertongbook.com

前　言

本书作为一本专著，它来源于科学研究的实践。为了讲清它的渊源，请允许我简述一下有关的科学研究经历。几年前“国家重点基础研究发展规划（973）”项目中分出了一个子课题（G1999035806），当属国家科技部最早立项的网络安全科研项目之一，该课题交由中国科学院高能所许榕生研究员负责主持。我作为该课题组的主要成员，参与课题调研并协助指导其他组员从事该项目的研究工作。

此前，在我国刚开通互联网不久，中国科学院根据许榕生研究员的提议，就委托了高能所及时开展了网络入侵防范技术的研究。一批年青的网络系统管理员和研究生投入了最早的网络安全研究和技术开发，在防范黑客入侵方面取得了引人注目的成绩。高能所的网络安全课题组有过一系列的研究课题，并一度被国内外誉以“反黑客大本营”的美称。在网络无所不在的今天，网络信息系统的安全性非常重要，只靠少数课题组成员的研究是远远不够的，它需要千百万志士的共同努力，因此，研究成果的共享与交流就十分必要。在许榕生研究员的鼓励和支持下，我觉得很有必要写一本书，尝试将研究工作中的方法、思想、观点和论断深刻地表达出来，提供给从事相关技术和科学研究的专业人员参考，给正在新设的信息安全专业的本科生与研究生作为借鉴。

本书具有以下几点特色：

（1）知识性。作为一本专著，所阐述的问题是比较复杂和深刻的。为了使学生和业余爱好者也能逐步理解，在写作过程中，注意对基本概念、定义、性质和功能的精确描述，做到逐层深入。

（2）理论性。网络入侵防范，是当代的一个主流课题，是一个富有挑战性的研究领域。在本书的写作中，以全新的观念去考察它，将独特的方法、开拓的思想、巧妙的构思和灵活的思考结合起来，努力做到理论上给研究以开展，观念上给读者以启迪。

（3）实验性。网络入侵防范，就其本质来说，是一个实践问题。读者会从书中看到许多富有效果的实验。实验是理论的最佳诠释，实验是论断的坚实基础。

（4）成果化。成果指的是观点、看法、见解和论断等。它们贯穿着全书的整个过程。这些观点和结论富有启发性，是学习和使用的最好资源。

本书共有 9 章，围绕着网络信息获取到网络入侵的防范技术这个中心议题，

从各个方向、各个方面来阐述我们所研究的理论与所从事的实验。因而，各个章节相互联系，又有着一定的独特性。

第 1 章　网络入侵防范概述。本章主要论述了网络入侵防范的形势和特点，介绍了网络入侵防范标准、体系设计等概括性内容，是本书的一个概述。

第 2 章　网络数据获取的基础理论。本章主要论述了网络数据获取的原理、方法和工具。

第 3 章　智能化网络入侵检测系统。本章主要阐述了基于数据挖掘和粗糙集理论的网络入侵检测的系统模型、数据预处理方法、检测规则的提取和应用方法等内容。

第 4 章　网络陷阱技术。本章主要阐述了以主动防御为目的的网络陷阱技术。网络陷阱技术主要包括网络陷阱的构造技术、陷阱机技术等。

第 5 章　计算机取证技术。计算机取证为安全防护体系提供取证和事后分析的依据，可解决当前电子犯罪难于取证并难于找到问题根源的问题。本章主要论述了入侵取证的原理、方法、模型和具体系统实现。

第 6 章　网络安全监控的实践。网络信息实时监控系统主要研究数据包捕获技术、协议分析技术和应用恢复技术，来完成对网络上特定服务实现实时监视的功能。本章采用编程的方法实现了网络实时监控。

第 7 章　应用神经网络对网络流量的预测分析。从网络体系架构来说，网络流量是一切研究的基础。网络的行为特征往往可以通过其承载的流量（Traffic）的动态特性来反映。本章阐述了如何将神经网络应用到网络流量分析中，这涉及神经网络模型的设计、训练使用和结果分析等内容。

第 8 章　小波分析基础和应用。本章通过小波变换分析了数据包到达时间间隔，揭示了网络流量的自相似性和多重分形特性，保证和提高现有网络服务质量，推动 Internet 和信息基础结构的健康发展。

第 9 章　信息系统的生存性分析。面对各种入侵，我们的防范措施很难做到百分之百的有效。因此，在入侵防范的基础上，还必须考虑系统被入侵攻陷后的性能情况，这就是系统的生存性。本章对信息系统的生存性概念、分析模型、分析框架和量化分析等研究现状进行了详细的描述。

本书可供计算机技术、网络技术、电子信息技术领域的专业技术人员、研究人员、管理人员和教师参考。

在研究、写作过程中，我得到了课题组研究人员王旭仁、林雪纲、钱桂琼、何发镁、蒋卓明、陈楣和阮航等同志的支持和帮助。同时，刘宝旭博士、杨泽明博士和郑捷文博士卓越的研究工作，及大力协作，也促使了本书的诞生。在此，我对他们表示诚挚的感谢！

北京第二外国语学院领导和中科院高能所领导对本书的写作给予了关心和支

持，在此也对他们表示衷心的感谢！

希望本书的出版能够得到广大读者的认可，书中错漏之处敬请读者指正。

作　者

目　录

试读结束：需要全本请在线购买： www.ertongbook.com

第 1 章　网络入侵防范概述

当提到网络入侵防范的时候，人们自然就会联想到“黑客”。是的，我们在网络安全防护上，是要与黑客过招，与黑客较量的。但本书的宗旨是站在一个网络安全防护的前沿领域里，站在一个网络入侵防范的更高基石上，来全面地阐述网络安全防护的理论与实践。它包括理论上的深入刻画、实践上的详尽描述、观点上的精辟论述和论断上的确切归纳。

本章是全书的总纲，我们将对网络入侵防范的思想方法和技术要领进行简明扼要的阐述，以作为全书其他章节的引子。

1.1　网络安全防护的形势

网络安全的形势是小好，还是大好，这是我们每一个人都关心的问题。即使是接触网络较少的人，也对网络安全局势忧心忡忡。可以说，全民对网络安全形势的重视，是增强网络安全防护的重要原因。

1.1.1　网络安全防护的必要性

Internet 是计算机交互网络的简称，又称网间网。它是利用通信设备和线路将全世界上不同地理位置的、功能相对独立的数以千万计的计算机系统互连起来，以功能完善的网络软件（网络通信协议、网络操作系统等）实现网络资源共享和信息交换的数据通信网。

1. 因特网的建立

因特网是从英文 Internet 翻译过来的，又称为国际互联网，它是一个世界范围内的网络的网络。因特网通过各种通信线路和软件把全球范围内的计算机网络连接成一个整体，而不管这些网络的类型是否相同、规模是否一样以及距离的远近。因特网含有极为丰富的信息资源，是人类巨大的信息宝库，这些资源大得超过任何一个人的想象力。我们可以把它看做一个全球性的博物馆，一个无比神奇的游艺宫，一个发表自己见解的论坛，一个结交朋友的场所。在因特网上可以实现资源共享、相互通信和远程教学等。例如，通过因特网就可以在自己家中的计算机上查阅学校图书馆的书目或北京图书馆的资料；可以到中央电视台的网站上去查阅节目预告甚至收看电视节目；可以在几秒钟内把书信、照片、音乐等传给远在美国的朋友；可以去网上购物；可以到网上学校去获取你所想要学习的知识；也

可以为相隔万里的学生答疑等。

因特网起源于美国的 ARPA 网。20 世纪 60 年代中期开始，一些专家在美国国防部的高级研究计划署（即 ARPA）的资助下，研究如何把美国国内的几个不同的计算机网络连接起来。当时的设想是，当网络的某一部分在战争等特殊情况下受到攻击而损坏时，不影响网络中其他部分的正常工作。因此，ARPA 网采用分布式控制与处理，较好地满足了这方面的要求，网络上的计算机处于平等地位，没有哪一个部分是特别重要、不可缺少的。70 年代他们设计了新的在不同的计算机网络之间实现通信的协议（TCP/IP 组），并公开了所有的 TCP/IP 网络规范和有关的技术成果。这种公开，使得 TCP/IP 得到了广泛的支持和迅速的推广。TCP/IP 应用于 ARPA 网标志着真正意义上的 Internet 出现了。

2. 因特网的发展

从 20 世纪 60 年代起，由 ARPA 提供经费，联合计算机公司和大学共同研制而发展起来的 ARPAnet 网络，最初，ARPAnet 主要是用于军事研究目的。它主要是基于这样的指导思想：网络必须经受得住故障的考验而维持正常的工作，一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其他部分应能维持正常的通信工作。ARPAnet 在技术上的另一个重大贡献是 TCP/IP 簇的开发和利用。作为 Internet 的早期骨干网，ARPAnet 的试验奠定了 Internet 存在和发展的基础，较好地解决了异种机网络互连的一系列理论和技术问题。

1983 年，ARPAnet 分裂为两部分，ARPAnet 和纯军事用的 MILNET。同时，局域网和广域网的产生与蓬勃发展对 Internet 的进一步发展起了重要的作用。其中最引人注目的是美国国家科学基金会（National Science Foundation，NSF）建立的 NSFnet。NSF 在全美国建立了按地区划分的计算机广域网并将这些地区网络和超级计算机中心互联起来。NSFnet 于 1990 年 6 月彻底取代了 ARPAnet 而成为 Internet 的主干网。

NSFnet 对 Internet 的最大贡献是使 Internet 向全社会开放，而不像以前的那样仅供计算机研究人员和政府机构使用。1990 年 9 月，由 Merit、IBM 和 MCI 公司联合建立了一个非盈利的组织——先进网络科学公司（Advanced Network &Science Inc.，ANS）。ANS 的目的是建立一个全美国范围的 T3 级主干网，它能以 45Mbit/s 的速率传送数据。到 1991 年底，NSFnet 的全部主干网都与 ANS 提供的 T3 级主干网相连通。

Internet 的第二次飞跃归功于 Internet 的商业化。商业机构一踏入 Internet 这一陌生世界，很快发现了它在通信、资料检索和客户服务等方面的巨大潜力。于是世界各地的无数企业纷纷涌入 Internet，带来了 Internet 发展史上的一个新的飞跃。

我国自 1994 年正式接入 Internet 到今天的短短几年间，网络技术和应用得到了飞速发展。据 2006 年 1 月 17 日中国互联网络信息中心（CNNIC）在京发布的

试读结束：需要全本请在线购买： www.ertongbook.com