中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

入侵检测

[美] Rebecca Gurley Bace 著

陈明奇 吴秋新
张振涛 杨晓兵 译

人民邮电出版社
www.pptph.com.cn

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

入侵检测

[美] Rebecca Gurley Bace 著

陈明奇 吴秋新 张振涛 杨晓兵 译

人民邮电出版社

图书在版编目（CIP）数据

入侵检测/（美）贝思（Bace, R.G.）著；陈明奇等译. —北京：人民邮电出版社，2001.6
（信息与网络安全丛书）
中国计算机学会计算机安全专业委员会推荐参考书
ISBN 7-115-09287-7

Ⅰ. 入… Ⅱ. ①贝… ②陈… 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（2001）第 22798 号

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书
入侵检测

◆ 著 Rebecca Gurley Bace
译 陈明奇 吴秋新 张振涛 杨晓兵
责任编辑 陈冀康

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ pptph.com.cn
网址 http://www.pptph.com.cn
读者热线 010-67129212 010-67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：14.75
字数：323 千字 2001 年 6 月第 1 版
印数：1－5 000 册 2001 年 6 月北京第 1 次印刷

著作权合同登记 图字：01－2000－2860 号
ISBN 7-115-09287-7/TP·2210

定价：30.00 元

内容提要

本书是关于入侵检测技术的一本实用性手册。书中详细介绍了入侵检测技术发展的过程，系统深入地讨论了入侵检测的设计和实施过程中需要考虑的问题。通过讨论和分析影响入侵检测的各方面因素，读者将了解到入侵检测系统的历史、现状和未来，进而可以评估所设计的或已有的入侵检测系统。

本书适合于网络管理员、关注网络安全的技术人员以及从事网络安全咨询服务的人员阅读。

信息与网络安全丛书 审定委员会

名誉主任：朱恩涛

主　　任：谢楷乾

副 主 任：杜肤生

顾建国

徐修存

委　　员：（以下以姓氏笔划为序）

王亚明　冯登国　刘凤昌　吕晓春　杨智慧　屈延文

赵世强　赵战生　卿斯汉　高新宇　崔书昆　缪道期

丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999年好莱坞推出的以网络安全为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从CIH噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全，在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局领导及部分计算机安全专家组成的审定委员会对图书进行了审阅，

从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

版权声明

译者的话

随着计算机信息技术与网络技术的迅猛发展，信息与网络安全形势也日趋严峻和复杂化。各种计算机安全事件不断发生，从技术、管理、法律等多方面采取综合措施保障信息与网络安全已成为世界各国计算机技术人员的共同的目标。入侵检测则是信息与网络安全保障中非常关键的一个技术领域。

本书的作者长期从事入侵检测和网络安全技术及策略方面的咨询工作。本书适合于对入侵检测技术感兴趣的安全技术人员：它介绍了入侵检测的历史，详细阐述了入侵检测所涉及的技术主题。本书也适合于需要了解如何评估和选择入侵检测产品的读者：它介绍了如何评估和选择及如何配置使用入侵检测产品。此外，本书所讨论的与入侵检测相关的问题对所有的信息安全技术人员都有较高参考价值。

本书的全部翻译工作由陈明奇、吴秋新、张振涛、杨晓兵和张大鹏等完成。陈明奇翻译了第 1 章，并负责全书校对与统稿，吴秋新翻译了第 5 章、第 6 章、第 7 章，张振涛翻译了第 2 章、第 11 章、第 12 章、第 13 章及术语表，杨晓兵翻译了第 3 章、第 4 章，张大鹏翻译了第 8 章、第 9 章、第 10 章。

本书的主要译者近几年一直在从事信息与网络安全方面的研究与开发工作。入侵检测是一个较新的且正在快速发展的领域，整个翻译工作对我们而言也是一个不断学习的过程。译者抱着认真负责的态度翻译了全文。在整个翻译过程中我们力求语言流畅并忠实原文，但因知识水平和实际经验所限，疏漏之处在所难免，希望广大读者给予批评指正。

衷心感谢所有为本书的出版付出辛勤劳动的人们！

2001 年 3 月

作者简介

Rebecca Gurley Bace 是 Infidel. Inc 的总裁，专长是入侵检测和网络安全技术及策略方面的咨询业务。

在成立 Infidel 之前，Bace 女士在美国政府部门工作了 15 年，前 12 年是国家安全局(NSA)的雇员。1989 年至 1995 年，作为 NSA 的信息安全(Infosec)研究和技术办公室(R2)的创办者，她领导了计算机不正当使用和异常检测(CMAD)研究计划。

作为 CMAD 研究计划的领导者，Bace 女士在入侵检测的早期研究中付出了许多努力，在 Purdue 大学(COAST 项目)、California 大学 Davis 分校(安全实验室)、New Mexico 大学和 Tulane 大学发起了学术研究。她还曾在 Los Alamos 国家实验室的 Wisdom and Sense 及 STAR 异常检测研究项目中作为政府的技术监督员。

Bace 女士和联邦调查局(FBI)David Icove 博士的合作研究成果包括《计算机犯罪调查手册》的出版和有罪黑客的政府研究报告。她和由她发起并资助的 CMAD 工作组于 1995 年一起参与对 Kevin Mitnick 的监测、跟踪和拘捕。Kevin Mitnick 是当时被 FBI 通缉的头号计算机罪犯。关于她的这段经历在 Tsutomu Shimomra 的 *Takedown* (Hyerion Press 1995)一书中也被提及。Bace 女士于 1995 年被授予 NSA 的杰出领导奖，以表彰她在建立全国的 CMAD 团体方面的贡献。

1996 年，离开 NSA 后，Bace 女士在 Los Alamos 国家实验室的计算/信息/通信部门任安全副主管。她负责制定保护策略，以使实验室在安全需求和可用性及性能之间取得平衡。

Bace 女士是 Alabama 州 Leeds 人，在纽约州立大学获科学学士学位，并在 Loyal 学院获工程科学硕士学位。

关于技术评审人

这些评审人以他们的丰富的实际经验对本书的整个写作过程都做出了突出的贡献。

在本书的写作过程中，这些专家审阅了所有材料，包括技术内容、结构和流图。他们的反馈意见保证了《入侵检测》满足读者对高质量的技术信息的需求。

David Neilan 已经在计算机/网络界工作了 8 年多，最近 5 年主要致力于网络和 Internet 安全。从 1991 年至 1995 年，他在 Intergraph 从事图形系统和网络方面的工作。此后 4 年，David 在 DEC 公司从事 DEC 防火墙和网络安全方面的工作。自 1998 年起，David 在 Present Online Business Systems 公司从事 LAN/WAN 和 Internet 安全方面的工作，为采用 Internet 创建安全的 VPN(Virtual Private Network)的不同公司设计网络基础结构，以支持安全的 LAN/WAN。

Robin Roberts 已经在信息安全界工作了 10 年多。1997 年起，她在 BTG 公司从事技术集成和服务工作。在 BTG 公司，她被认为是信息安全方面的专家，并且管理一个信息和网络安全服务组，该小组主要服务对象是来自情报组织的客户。1986 年至 1997 年，Robin 在中央情报局 (CIA)工作，管理信息安全的研发计划和对各种中介项目提供相关主题的专家意见。

Stephen E.Smaha 是 Haystack Labs 公司的创始人和 CEO(首席执行官)。从 1989 年起，他设计、实施并安装了基于软件的入侵检测和不正当使用的检测系统。1993 年，在发布他们的第一个商业产品之前，Haystack Labs 公司为各个政府机构和他们的签约方做了入侵检测系统的研究开发工作，这些机构包括联邦调查局(FBI)、国家安全局(NSA)、能源部、美国空军和其他一些不宜公开的机构。Haystack Labs 公司 1997 年 10 月被 Trusted Information Systems(TIS)公司收购。在 TIS 公司，Smaha 担任主管技术的副总裁直至 1998 年 4 月该公司被 Network Associates 收购。此后，他服务于数家计算机公司董事会和技术咨询委员会，并且积极地参与了一些启动公司的顾问活动。在成立 Haystack Labs 公司之前，Smaha 曾为 Tracor Applied Science 的军用客户开发了计算机安全系统；曾管理一个在 Schlumberger 的人工智能软件小组；曾在 Sytrex 公司设计办公自动化工作站，并且为 Health Products Research 编写生物统计软件。Smaha 是个知名的演说家，是 Interop、COMDEX、Internet World 和各

类安全相关论坛的撰稿人。他曾在联邦和州一级的关于安全和隐私的专家委员会任职。Smaha 在 Princeton 大学获数学和哲学学士学位，在 Pittsburgh 大学获哲学硕士学位并在 Rutgers 大学获计算机科学硕士学位。

Fred Chris Smith 在 New Mexico 的 Santa Fe 开始律师职业。自 1978 年他一直生活在那里。1985 年后，他时常针对 Los Alamos 国家实验室开发的不同数字证据分析工具和其它计算机犯罪取证技术为该国家实验室提供咨询。目前他为 Los Alamos 国家实验室正在开发的新计算机犯罪取证工具和公开执法及计算机安全个人专用的技术提供咨询。他作为特别诉讼和调查的主管，连续四次任 New Mexico 的首席检察官。从 1989 年起，他开始在 SEARCH 工作，最近帮助他们为州和当地执法官员开设了高级互联网调查课程，他在 California 的 Sacramento 也开设这门课。现在他在 Virginia 的 Richmond 全国白领犯罪中心执行董事咨询委员会任职。过去 10 年中，Fred 还开发了训练课程并向许多州和联邦机构介绍了由于商业上网络化软件应用的增加而导致计算机犯罪和法律责任方面的理论新进展。他为团体及私营的调查公司和诉讼策略公司的涉及电子证据的案件提供咨询。他最近的出版物是为全国防止经济犯罪联合会写的《为起诉计算机网络入侵形成合作伙伴》一书，该书将在 2000 年后出版。Fred 曾在 Michigan 大学就读并于 1972 年从 Stanford 获法学学位。

Christopher Wee 从 1991 年以来就是入侵检测和网络安全的研究人员。他的研究兴趣包括基于主机的审计监视、网络协议中的脆弱性及安全策略规范。作为 California 大学 Davis 分校的研究生和博士后，他参加了 DIDS、LAFS、GrIDS 和 IDIP 等入侵检测系统项目的研究工作。Chris 现在是 Intel 在线服务公司的高级信息安全分析专家。他在 California 大学 Davis 分校获电气电子工程学士学位，并在该校获得计算机科学的硕士和博士学位。

致 谢

在本书的写作过程中，正如我的一生，人们给了我太多不同寻常的祝福，正是这些人们在我周围织起了支持我的网。

我深深感谢 Steve Smaha，对我而言，他多年来一直是我从事入侵检测方面研究的缪斯。他、Jessica 和 Rebecca 已经成为过去十几年中支持激励我的源泉。应 Steve 的要求，我写了此书，在整个写作过程中，他是愉快而富有启发的讨论的源泉。

我愉快地同 Macmillan Technical Publishing 的 Jennifer Garrett、Katie Pendergast、Alissa Cayton 和 Linda Engelman 一起工作，在本书出版过程的不同阶段他们不断鼓励并指点我。

在网络和信息安全界的同事构成了一个睿智聪明和令人难以置信的愉快而有趣的团体。对我的征求意见和解释的请求，他们曾经用不失幽默有趣的电子邮件、流行的闲聊话题和深刻的见解慷慨地给予我信息和鼓励。特别感谢 Jim Anderson、Dorothy Denning、Gene Spafford、Bob Abbott、Marv Schaefer、Ruth Nelson、Marcus Ranum、Kevin Ziese、Adam Shostack、Chris Wee、Fred Smith、Drew Gross、Carolyn Turbyfill、Robin Roberts、Stephanie Fohn、Gene Kim、Ron Gula 和 Dave Icove。

我以前在国家安全局的同事们都是非常聪明和有献身精神的专家，他们履行着对社会非常关键的职能，然而这些人平常却很少为人们所想起。我为自己曾是该组织的成员而感到骄傲，并为他们对整个民族的支持而向他们致敬。

最后，我的家庭是我巨大的快乐和启迪的源泉。这包括我出生的家庭和聚集在我周围亲密持久的朋友而组成的家庭。我非常幸运地拥有如此多的向我敞开他们的心胸和生活的人们。尤其，我要感谢 Terri Gilbert 和 Paul Bace，谢谢他们在我写作此书时给予的爱、支持和耐心。

前 言

计算机和网络技术在相当程度上支配了我们今天的生活。我们日常生活中的许多事，包括工作、娱乐、社区、交通和通信，都依赖于这些技术。Y2K 及其相关问题对公共基础设施所带来的威胁广为传播，它表明了我们是如何依赖于最终由计算机控制的支持结构。

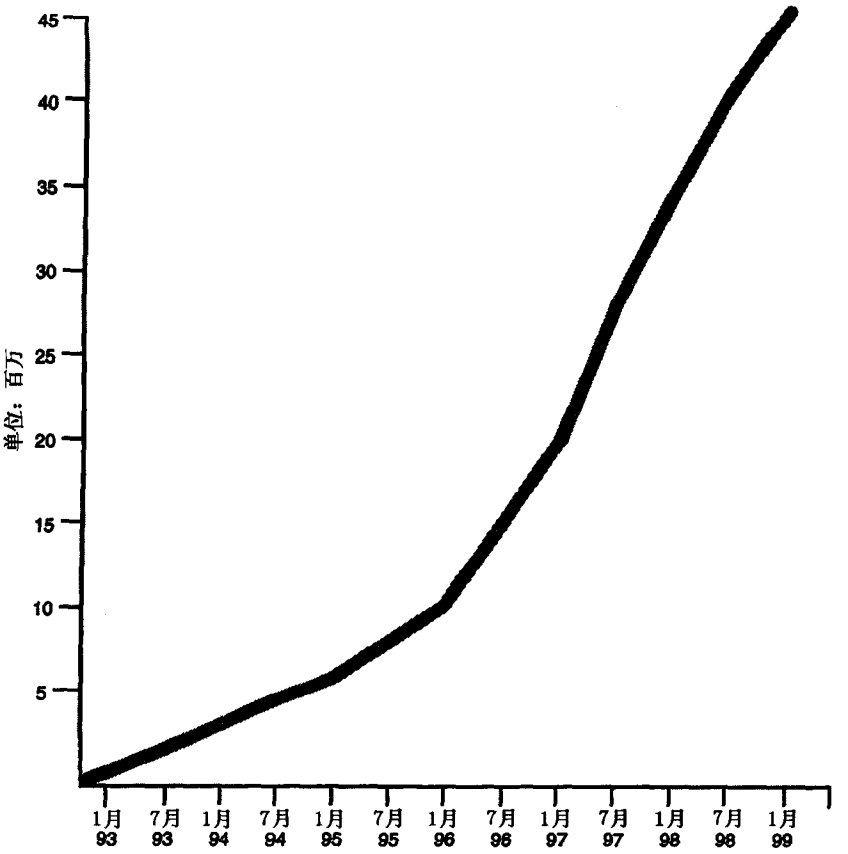
正是由于过分依赖于这些系统，我们已痛苦地意识到了它们的缺点和不足。从大至航班坠毁到小至医疗设备失效而导致的灾难都被归咎于系统失效。公众媒体上关于黑客事件和灾难性系统失效的报道吸引了人们的注意力，而且使公众对这些太容易出问题机器的可依赖程度更为关注。但是，提供了近乎魔术般功能的新技术的诱惑力缓和了这些关注。甚至社会的商业模式也转变为在虚拟的市场上提供商品和服务。虚拟市场中的店面由字节和网络数据包构筑而成，而不再是由水泥和砖块构成。

长期以来，新消费技术的大规模推广遵循着一定的可预测的模式。首先是这种技术的引进，随后该技术的早期拥护者采用这种技术并成为它后来流行的先驱者。接下来的阶段是社会主流接受该技术，这依赖于技术本身和社会环境。随着对新技术了解的增加，一些用户会利用它的能力来取得进步。但不幸的是，还有一些用户利用该技术对他人造成伤害或者更方便地实施犯罪活动。最终，由于公众的关注，法律及执法部门制定法令并且执行措施以处理这些问题。

计算机和网络的发展也不例外。最初，人们缺少接触计算机的机会而且制造、维护计算机的费用高昂，这些都限制了相关安全问题的发生。当系统上托管的关键信息越来越多，而且系统远程访问的能力也随之而增加时，安全问题开始变得突出了。

作为政府和学术界合作的成果，ARPANET 的出现和迅速成长，加速了安全问题的暴露。ARPANET 原来是为一个小团体设计的，团体中的成员是相互信任的，而且信息很少有可察觉的价值。“握手”协议是那时的规则，拥有帐户的人很少，网络中的许多用户彼此认识。

下图表明了在过去数年中 Internet 的增长情况。很明显，Internet 发展的早期已过去，高度信任的网络社区文化也随之而去。许多商业组织把 Internet 作为他们最重要的商业运作的手段，政府机构把 Internet 作为向公众提供访问公共记录和信息的渠道，将来的计划是把网络作为选举和投票的基础。



Internet 域名调查，1999 年 1 月，DNS 中的主机数

在这个网络世界中，对安全和相应的系统控制的需求是显而易见的。对那些保卫计算机系统和网络安全的人来说，所要达到的目标的确雄心勃勃。因此，达到的安全性必须是合理且充分的，同时在可说明性和几乎同样重要的隐私保密要求之间取得平衡。此外，必须有足够的灵活性以容纳全球范围内的法规制度，但在跨越多个司法权追踪犯罪分子的能力上应保持足够的一致性。

对感兴趣的研发人员而言，组合必要的管理措施和技术手段以满足这些安全需求的方法是丰富而复杂的，这就像瑞典式自助餐。安全审计和入侵检测已经变成计算机和网络安全的重要部分。这些技术所要提供的功能服务于直接、间接两个方面的安全目标：直接的安全目标包括跟踪和检测；间接的安全目标是监视系统中其他安全机制的情况和可信任度。

*入侵检测*监视发生在计算机系统或网络中的事件，分析它们中隐藏的安全问题的迹象。入侵检测可以想象为其他领域中的监视系统，包括便民店和银行中的警铃或录像监视系统。广义上，民防系统和军事上的早期预警系统也可以划入这种功能分类。尽管监视的策略和目标不同，但总的思想是相同的。这些系统提供警戒功能；当所关注的活动发生时，则发出警告提醒对此负责任者。

入侵检测这个术语在军事上还用来指那些监视系统，它们监视物理实体(如通信电缆)以发现损害的证据或其它的物理改变。军用标准中描述了系统的功能和针对该领域的测试基

准。在本书中，入侵检测是指监视、检测计算机系统和网络中的目标活动并作出反应的功能。

总的来说，入侵检测作为非密码学的计算机安全技术，是相对年轻的技术。1980 年以来，人们才对入侵检测进行了大量的研究和开发。这方面的研究已经产生了相当广泛的解决策略以达到入侵检测的目标。

入侵检测因年轻(因而不成熟)带来了其它复杂的问题。在入侵检测的理论研究和实际应用两者之间还是存在差距的，这种局面导致了那些研究开发产品人员的各种不良倾向。例如，有倾向定义无用的术语，而且开发出的解决方法同系统安全的其它部分或管理基础设施没有互操作性。另一个倾向是声称自己所中意的解决方案或方法可以解决所有的问题而不顾自己的声明是否真实有效。

在顾客需求的驱动下，随着研发资金的增加，这些问题最终将会得到解决。入侵检测的重要性在防御性信息战中是不言而喻的。政府已经宣布计划在该领域追加投资。

过去 10 年中，我一直沉浸在入侵检测的研究中。在那段时间里，我看到了太多的问题综述、提出的解决策略、商业化产品和专家，可谓“你方唱罢，我便登场”。在这段时期里，我一直负责政府对该领域的研究，试图将研究兴趣和运作需求两者结合起来。我自己也进行过研究，探索黑客们所采用的挫败安全机制的技术。在研究领域工作了多年后，我转换到了一个安全管理岗位工作，在一个具有挑战性的运行环境中使用一些产品。在过去十年的最后几年中，我主要是同安全领域新手一起工作，使用一些已有的商用产品并且开发新产品。在这段时间，我很高兴地看到许多入侵检测产品成功转向商业市场。

然而，这些高兴还受到一些问题的影响。我看到这个商业产品市场，仅利用了过去 15 年研究已经积累的成果的一小部分；我看到从业者和开发者在规定和构建系统之前，甚至没有问问最终用户真正需要什么，如何才能最好地将入侵检测功能和现有系统集成，以及如何才能最好地实施；我看到起初的研究和开发显然并没有理解用户所面对的问题或已有的工作。最终，我还看到自由公开地讨论入侵和脆弱性的阻力仍然存在。这些阻力来自于那些不顾一切地需要控制信息来保护他们的系统的人。

尽管有这些问题，我仍然相信入侵检测作为计算机安全的重要部分的价值和前景。做得很好的安全系统，可以保护我们的隐私和那些定义在这个虚拟网络世界中的关于我们究竟是谁的信息，它还可以使 Internet 用户形成新的可变化的社区，使我们在新千年中合作解决许多摆在我们面前的迫切问题。

我写本书的目的就是：记录我获得的经验，见证一项技术从概念至商业化产品的成长过程。我希望本书中的信息能使读者将入侵检测作为工具库中的利器，帮助自己达到系统的安全目标。

目 录