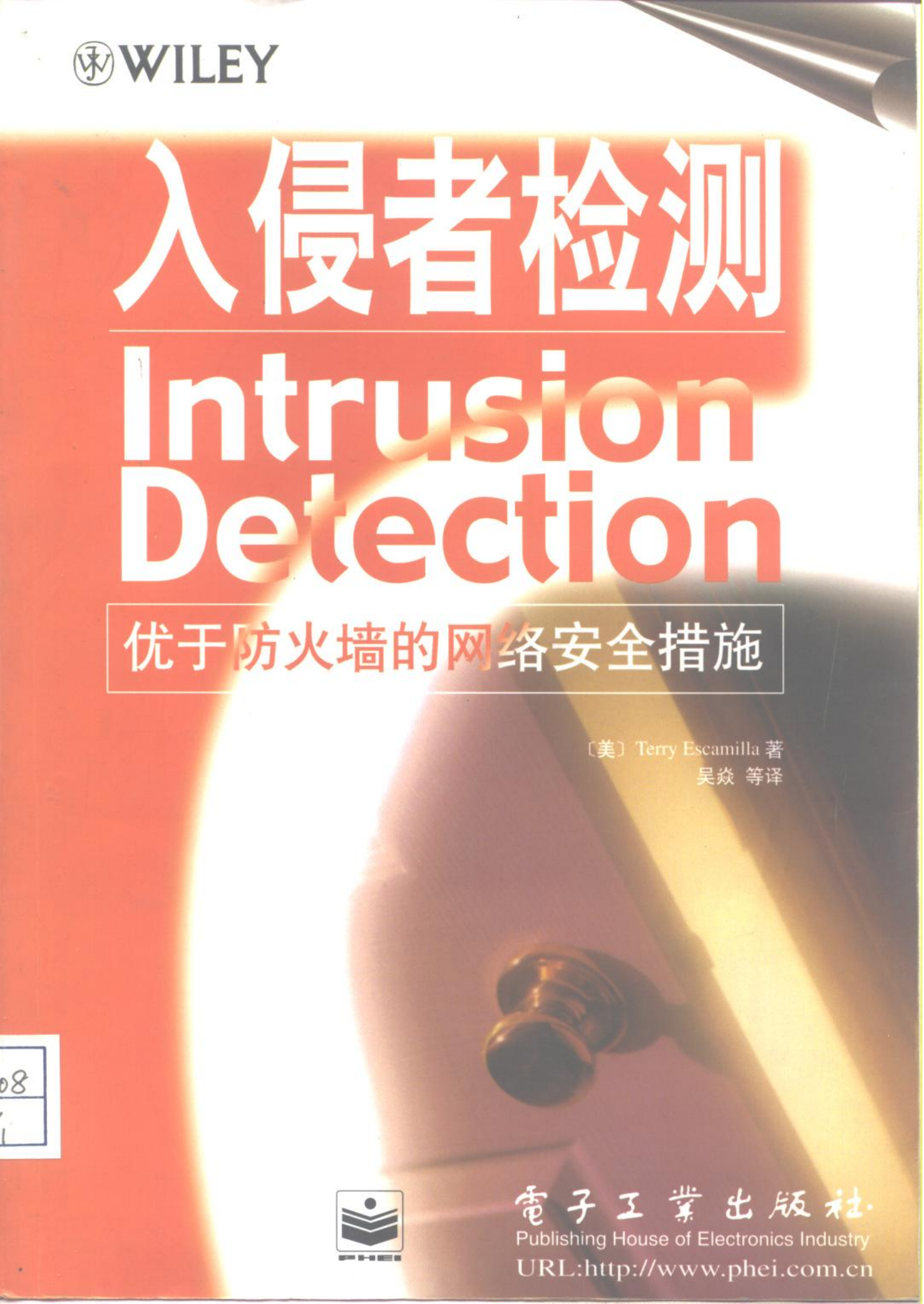
WILEY

入侵者检测

Intrusion Detection

优于防火墙的网络安全措施

〔美〕Terry Escamilla 著
吴焱 等译



電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

WILEY: Intrusion Detection

入侵者检测

T. 埃斯卡米拉
〔美〕 Terry Escamilla 著

吴焱 等译

電子工業出版社
Publishing House of Electronics Industry

内 容 提 要

随着计算机应用技术的迅速发展，计算机和网络日益深入到人们的生活中，而随之产生的安全问题却没有得到应有的重视，特别是在商业和生产领域，人们往往在遭到黑客攻击之后才发现系统中的漏洞。

本书介绍的是各种类型的网络入侵检测系统（IDS）及其在不同环境中的应用。本书共分为三个部分。第一部分介绍了传统的安全领域：识别与验证、访问控制和防火墙的作用。第二部分详细描述了三种主要的IDS，它们的作用已超越了传统的“保护系统”的概念，目的是抓住系统内部和外部的入侵者。第三部分回顾和总结全书内容。当你读完这本书时，就会对入侵检测产品的差异和互相覆盖的部分有了一个清楚的了解。

本书是网络入侵检测方面较高水平的实用书籍，适合于大型系统的管理员和计算机专业读者。

书　　名：**入侵者检测**
著　　者：〔美〕Terry Escamilla
译　　者：吴焱 等
责任编辑：郭小湘
印 刷 者：北京天竺颖华印刷厂
装 订 者：三河金马印装有限公司
出版发行：电子工业出版社出版、发行
北京市海淀区万寿路173信箱　邮编：100036　发行部电话：68279077
北京市海淀区翠微东里甲2号　邮编：100036　发行部电话：68207419
URL:http://www.phei.com.cn
经　　销：各地新华书店经销
开　　本：787×1092 1/16　印张：13.75　字数：350千字
版　　次：1999年7月第1版　1999年7月第1次印刷
书　　号：ISBN 7-5053-5344-6/TP・2671
定　　价：24.00元
著作权合同登记号　图字：01-1999-0942

前　言

1997年夏天，John Wiley & Sons公司的人第一次请我考虑写一本关于计算机安全方面的书。经过与Carol Long的几次会晤，我认为写一本关于网络入侵检测这一引人入胜领域的书确有必要。过去的几个月里，这本书的内容经过了多次修订，主要是为了反映计算机安全领域不断变化的情况。

Carol和Pam Sobotka核准本书第一个写作提纲时，我正在位于德克萨斯州奥丝汀的Haystack实验室工作。我本打算对黑客袭击计算机系统的多种途径进行分类以便其它的书可在此基础上展开。不过我看到将其与其它计算机安全手段进行对比来对网络入侵检测提供一个概述也很有价值。很多次碰上顾客问我诸如此类的问题：网络入侵检测与防火墙有什么不同？我已经加密了，难道这还不够吗？与其在下几个月里不断向商业伙伴或顾客重复同一些问题的答案，还不如干脆把它们写成一本书。

本书有几部分写于1997年，却不得不在1998年进行修订，以加入近期在产品定位方面的变化。

这本书写了大概四分之三的时候，Haystack被可信信息系统（Trusted Information System）收购了。我们已经预测到安全产业里会有合并与收购，但就像Web一样，谁也没想到事情进行得那么快。TIS不久就成为Network Associates的一部分，而当主要安全销售商们转向较佳解决方案时，其它的合并与收购也相继发生。尽管环境诱人，我还是决定回到先前的雇主IBM那儿，致力于安全性的实际应用。

做任何事情都不可避免地要有所取舍。与Wiley小组的人讨论了几次之后，我们决定写一本网络入侵检测方面实用的高水平的书，而不是一个中等水平的论述。因此我们的目标是来比较网络入侵检测与计算机安全的其它形式的区别，并说明每种类别的产品如何发挥作用。随着时间的发展，经销商们提供的产品可能有更多的重复，可能已推出升级版。我们不想过多谈论产品的细节，毕竟总体理论比起一年要改好几次的产品细节要重要得多。与此同时，我们也避免把这本书写成产品购买报告。这种报告还是留给商业出版社或是你的实验室自己做更好。

我尽力不对黑客和CRACKER作评判。许多安全漏洞都是由想堵漏洞而非那些想利用漏洞的人说出来的。我们假设你想保护信息资产不受破坏，因而你需要了解系统是如何受到危害的以及如何防御和监视。我提供的方法是实用而有针对性的。道德和法律上的争论最好还是留给那些领域的专家吧。

遗憾的是本书未用太多篇章概括介绍入侵检测研究。尽管我对这一领域充满了兴趣，但并不认为仅用一章或一个附录就可以写清楚。一整本详述入侵检测研究的历史和现状的书可能更合适些。感兴趣的读者能够在SRI、LLNL、COAST和U.C. Davis管理的站点处找到原文和指南。

在国外，我的头衔是安全专家和研究员。其他国家也有许多杰出的项目和产品，但由于我对它们所知甚少，就没有提及。有希望的是你可以自己对这些同类事物进行一下研究。

我想强调一点，本书及其内容并未经由IBM同意。著述计划的设想和付诸笔端大多是我在Haystack和TIS时的事儿。虽然一个人的观点总会不经意地流露到他的文章中，但是对重要题目的表述我还是尽量做到公正无私。

本书所交版税的一部分将捐赠给慈善机构。在一次防火墙会议上，我有幸和Peter Neumann分在一个讨论小组里。当时他把他的那份酬金捐给了一个对他本人有重要意义的基金，并提醒我，作为研究人员与专业人士，我们有责任通过其它方式为社会尽力。

接受捐赠版税的机构可能每年都换，不过我一开始就选择了全国儿童代言中心（fly.hiwaay.net/~ncacadm/）。尽管我以及我的任何家人都不是危害儿童事件的受害者，但是我看到危害儿童已成为当今世界重要问题之一。当你将本书纳入收藏之列时，你应当为其他那些没有我们这样幸运的人将从中受益而感到欣慰。如今互连网上发生的危害儿童事件的数目呈上升趋势。儿童们通常是通过e-mail或聊天室被电子“跟踪”。如今一些安全工具能提供保护。URL加锁、Web站点排名以及查找数据包中不受欢迎词语的扫描器都能帮助降低对儿童的危害。尽管本书没有提及，对因特网的这些安全贡献是发展中的产品的一个重要组成部分。本人在这里郑重声明：本书的任何错误都是无意识的。错误都是我自己的。这里提到了经销商和产品的名称，但并不表明他们对本书内容的赞同或支持。你的收获因所述解决方案而异。

——特瑞D. 艾斯凯米拉博士
一九九八年 六月
科罗拉多州 伯德

介　绍

这本书用来帮助你了解入侵检测系统（IDS）如何适用到你的安全产品库中。当你读完这本书时，就会对入侵检测产品的差异、产品之间的覆盖部分，以及它们如何为你的站点提供综合的保护有一个清楚的了解。

本书的概貌和入侵检测

本书的重点是入侵检测，然而要理解为什么入侵检测是重要的，就需要知道一些背景知识。

即使你想掌握公共域源代码和熟悉一套工具，也应该先读一下这本书。所有的应用程序中出现的问题和解决办法在商业软件和免费软件中都是一样的。你也应该明确地了解公共域工具的优点和局限性。当你读到仔细描写一些商业软件的部分时，就做一些笔记，而再当你考虑要从因特网上下载的免费软件时，就使用它们来完成类似风格的分析。顺便提一下，许多新出现的商业软件产品都可以从网上免费下载，如TIS防火墙工具包（TIS Firewall Toolkit）。

要从这本书的内容中获益，你并不需要购买任何产品。这里的每一章都不需要你使用任何特殊的计算机或特殊的软件程序来完成任何练习。当然，如果你有机会试用一些产品就会学到更多的知识。许多销售商都提供产品的测试版或者发送带有软件密钥的全功能版本。

什么人应该读这本书

你可能正在考虑是否需要入侵检测。另外一个问题是，是收集一些免费的有用工具还是买商业软件。市场上有很多图书充分地覆盖了公共域工具的范围，这些工具是非常有用的，并且完成了入侵检测任务中的一部分。在这本书的第二部分“入侵检测：优于传统意义上的安全”，主要针对的是商业软件而不是免费软件。这将使你的知识更完满。

如果你是站点安全工作人员，就一定想读这本书来了解IDS与其它安全产品有什么关系。你也当然想知道IDS能检测到什么和IDS不能检测到什么。如果你计划用IDS支持你的站点上安全策略，你就必须知道IDS的长处和短处。

对任何了解计算机的人来说，这本书的内容都是很丰富的。对那些喜欢更深入了解的人，书中详细地阐述了几个主题。因此，如果你是一个CIO或者只是对计算机安全感兴趣，阅读这本书一定会让你获益匪浅。如果你对建立你自己的IDS感兴趣并要开始着手时，这本书会给你提供许多信息。

你不会在这本书找到黑客如何进入系统的方法，这里也没有描述已知的攻击方法。对那些知道如何得到这些信息的人来说，这些信息很容易得到。这个问题的讨论需要另外的一

本书，才能充分地详细地描述普通性的攻击。现在已知道的入侵方式有一百多种，而且每天都在出现新的方法。

本书是如何组织的

本书分成三个主要部分。第一部分“在入侵检测之前：传统的计算机安全”，在这部分中提供了背景知识并证实为什么说入侵检测是重要的。第二部分“入侵检测：优于传统意义上的安全”分成入侵检测和增加入侵检测能发挥什么作用两个部分。第三部分“改善系统环境推荐”介绍对付入侵的方法，并建议你如何使用新学习到的知识建立一个完全安全的解决方案。

要想完全获得本书介绍的知识，请按顺序读每一章节。当然，如果你认为自己是在初学者这一级以上，在浏览完第1章“入侵检测与经典安全模型”后感到比较轻松，就可以向后读了。如果你发现你自己正寻找更宽或更深的东西，就查找附录中的参考资料。在你读完这本书之前，或者说到你读完这本书为止，你不会成为安全专家。

第一部分“在入侵检测之前：传统的计算机安全”从第1章“入侵检测与经典安全模型”开始。这一部分是入门，通过构建一个安全模型来讨论计算机安全的几个重要方面。如果你了解了基本的安全模型应该做什么，也就学会了提出关于安全产品深刻的、批评性的问题。对基本模型的理解会使你明白不同的产品解决的是哪一方面计算机安全问题。

在第2章“识别与验证在系统中的作用”中，将对识别与验证I&A（Identification and Authentication）进行比较细致的介绍。在与计算机交互中的第一步就是用户的识别与验证。因为I&A要确认在系统中你是谁，所以它对入侵检测有很大的影响。黑客的一个目标就是通过利用I&A过程来获得进入系统的权限。在第2章中，你将会明白I&A是如何受到攻击的，你怎样能提高I&A的能力，和为什么即使你有很强的验证功能也同样需要IDS。

第3章“访问控制在系统中的作用”将转向下一个逻辑步骤访问控制。当你完成了I&A过程后，根据在你正在使用的系统中定义的访问控制策略，将限制你可以做什么。在这一章中，你将学到底层的操作系统如何处理访问控制，和如何利用其它工具来提高访问控制性能。你也将会明白为什么即使在网络中加入了其它访问控制产品，在访问控制之上还需要入侵检测。

在第4章“传统网络安全方法”中探讨了防火墙的作用和网络安全的其它几方面。当你读完第4章，你将明确了解在I&A和访问控制之上防火墙都提供了什么服务。你也将会明白为什么就算你有了防火墙也一样需要入侵检测。顺便提一下，如果你的站点连到Internet上了，而没有安装防火墙（或者至少是一个筛选路由器“screening router”），先别看书了——赶紧安装一个防火墙。

在你理解了三个传统安全领域——I&A、访问控制和防火墙的作用后，第二部分“入侵检测：优于传统意义上的安全”将带你进入入侵检测中去。在第5章“入侵检测及其必要性”中，将对你介绍三种主要的IDS。在这一章中，也将向你简短介绍扫描器（scanner）、系统级的IDS和网络IDS的概貌。你应该知道，虽然检测从外部试图闯入系统的人非常有意义，但是FBI和其它信息源的报告中提到，由计算机犯罪所造成的损失通常有80%或更多与内部人员有关系。入侵检测试图抓住内部的和外部的入侵者。

第6章“系统上的入侵检测有趣且简单”进一步指明了IDS如何真正发现黑客攻击。你将会明白检测黑客通常不是简单的事情。如果黑客攻击范围覆盖一个大的网络，就更不容易发现黑客在做的每一件事情。尽管扫描器、系统IDS和网络IDS之间有少量的覆盖，但每一个都完成基于它们检测黑客的类型的重要功能。

第7章“脆弱性扫描器”详细讨论了入侵检测扫描器工具。在这一章中通过与现在市场中正在使用的商业扫描器工具的对比，重点讨论了扫描器能检测什么和不能检测什么。这里虽然对一些扫描器工具进行了讨论，但你还是应该听听销售商的意见，因为他们有关于扫描器的最新信息。由于入侵检测工具的变化是有规律的，所以最好知道，与其在现有的扫描器之间进行比较，不如了解这一类工具的问题。

第8章“UNIX系统级IDS”的主要内容就是系统级IDS。正如你将看到的那样，仅通过监视站点上的每个系统就能发现一些黑客攻击。这里讨论了许多取舍的问题。这里还描述了一些特殊UNIX黑客攻击，以便你能理解系统级的IDS是如何捕获入侵者的。当然在这里，也提到系统级IDS的弱点以及为什么要在系统监视器之上添加扫描器和网络IDS。入侵检测中最早的一些研究都是集中在系统级工具上的。

第9章“嗅探入侵者”中根据网络IDS性能将IDS分类。一般来讲，这些工具都是通过智能地查找网络数据数据包来工作的。网络查询能够查出一些攻击，但也会漏掉一些。但是它是与其他两种类型IDS协同工作的。到你读完第9章，就会掌握许多关于入侵检测的知识了。这时你应该可以清楚地知道IDS是如何完善传统安全工具功能的，也就是说IDS是如何提高I&A、访问控制和网络安全性能的。

在第10章“NT的入侵检测”中特殊考虑了NT入侵检测的问题。正如你将要看到的，NT系统已经成为许多黑客攻击的主要目标。尽管NT的源代码不是随便可以得到（而UNIX正相反），但是NT的黑客却是越来越多。在这章中将对NT的黑客攻击和IDS如何检测它们结合在一起来讨论。至本章结束，就完成了对入侵检测的全面介绍，但还有一些事情需要你考虑。

第三部分“完善系统环境”以两个重要的主题结束本书。第11章“你已经遭到攻击！”中根据不同的资源状况推荐了一些方案并提供了处理安全事件的基本框架。要知道准备熟悉的解决方案对于事件处理小组来说是非常重要的。如果你正受到攻击的威胁，尽快跳到第11章的建议部分。

第12章“入侵检测并不是安全问题的终结”回顾全书，帮助你理解入侵检测的过程。在这里你将回顾经典计算机安全的威胁、弱点和解决方案。三类主要的IDS的关键点也在这里更新。然后，这章提供了一些关于如何在你的站点上配置几个补充的安全产品的建议。最后预测了入侵检测在近期的发展方向。

最后，在附录“信息热链接”中提供了许多有用的网址。

取舍的事实

在开始之前，有必要提及以下重要的两点。

首先，成功的销售商要受到市场需要驱动来做取舍。因为你也在市场之中，所以你应该知道，一般来讲市场需求很少是相似的。许多商店和公司投资最可能受益的新产品，而却

在竞争激烈的市场中建立市场失败，或失去与已受保护的竞争对手竞争的资格。公司根据不同的原因向其产品中增加功能，如竞争、上市时间、时机、开销等。如果你不喜欢现在IDS的做法，就向销售商反映你的想法。现在你可能被迫做一些取舍，但可能在这个产品新版本发行时，你的需要就得到了满足。

其次，在完善你的站点安全时，你也需要做一些取舍。首先，你的资源是有限的。经常更换密码技术也需要足够的钱和时间，因此密码解决方案也就不得不中断了。因此，一开始你就处于不利地位。因为你不可能有足够的钱和时间，所以建立一个理想化的安全环境是不可能的。

人们购买产品的原因是不同的——可能是因为他们最好的朋友推荐的；可能是因为它便宜；可能是因为他们喜欢这个产品的广告；可能是因为他们老板推荐使用的；可能是因为他们的竞争对手也使用；可能是因为该产品的服务比较好；也可能只是因为它支持某种特殊的语言（如日语）。最畅销的IDS可能不是功能最多的，也可能不是性能最好的，也可能不是最早使用。产品的畅销可能是因为被一个广受尊敬的机构认可的，或是被大部分计算机用户认可。你可能因为有影响的团体发布的一些标准，甚至是因为世界上90%的人都使用与你不同的产品，而被迫接受一种产品。

正是因为上述原因，有一些取舍是你控制不了的。当然还有其它的一些取舍你是可以控制的。可能是因为你是两个公司的董事会成员之一，所以你的公司正使用着那种产品。你可以选择不同的安全产品，但是你却还受着限制。这就是市场的事实。针对这种情况你能做些什么？这本书将又如何帮助你呢？

你应该精确地知道一个产品能做什么和不能做什么。这本书就是要你清楚地知道一个产品是如何工作的、它提供什么样的特殊功能和你为什么需要它。没有安全的计算机网络是非常危险的。由于使用了有错误的产品或是错误配置了的产品，所产生的对计算机安全的错误认识是非常可怕的。第一种情况，人们至少还知道环境不安全，还会小心处理。而在后一种情况下，网络事实上不安全时，人们却认为它是安全的。他们会更大意，而在他们认为网络传输安全的情况下，会在网络上向其它站点发送机密信息。

有时取舍是在配置中而不是在产品中。这些取舍包括负相关的一些参数。例如：如果你想让所有用户的口令存放在一个中央服务器里，你就一定要在网络等待时间和网络传输之间做取舍。早上8点钟，当有10,000名公司雇员要通过这个站点进行登录时，你就会希望有网络延迟并使网络传输失效。而另一方面，如果你将所有用户口令存放在一个或多个物理上安全的授权服务器上，为防止口令窃贼盗窃口令就必须牺牲一些网络性能。尽管以一些网络以性能作为代价提高了网络安全性，但是对系统的威胁还是存在的。你还是要担心诸如社会工程，不安全的口令代码，一些可能会在网络客户机的本地缓存区中留下一些口令的错误或其它的一些问题。取舍在计算机技术中是不可避免的。只有拥有这方面的知识才能选择正确的方案。

本书提到的所有产品都有能力解决你的问题，这些产品对解决你的问题将会大有益处。事实上，所有的销售商都在日益增长的计算机安全性的挑战面前获得赞扬。象你要面对选择一样，这些销售商也要对不同的参数组进行取舍。丰富你的知识吧，并用这些知识来提高你对这些参数选取的理解。

这本书是针对入侵检测的。与其它研究的问题一样，入侵检测也有自己丰富的历史，来说明为什么市场需要它。这本书将向你说明经典计算机安全问题的背景，并解释经典安全产品是如何处理这些问题的，以及为什么在I&A、访问控制和网络安全产品，如防火墙，之上还需要入侵检测。计算机安全是一个非常吸引人的领域，因为它带有许多反复、周折、秘密、欺骗和非常强烈的感情色彩。你将会看到入侵检测包含计算机安全的所有特点。

目 录

第 一 部 分

在入侵检测之前：传统的计算机安全

许多人都认为计算机安全的目的是为了防止故障发生。即使在近期，包括防火墙在内，这个目的也没有达到。在本书的第一部分，你将明白常规配置的计算机安全产品是如何满足你的需要的，以及它们还遗留一些什么样的问题。了解不同类型计算机安全产品的优缺点是明白入侵检测如何加强站点安全性的关键所在。要达到这个目的，你需要掌握下面的知识：

- 用标准安全模型来仔细考虑计算机安全产品如何适合你的策略。
- 识别与验证产品的作用及它们可解决和不可解决的问题。
- 标准访问控制在操作系统中的作用及如何通过它来提高系统的防御能力。
- 防火墙和其它技术如何增强网络安全性以及它们带来的遗留问题。
- 为什么即使加入了其它安全产品仍需要入侵检测。

第1章 入侵检测与经典安全模型

入侵检测是个热门话题。在近几个月中，有好几家入侵检测公司已被大型安全技术公司吞并了。所有的销售商都希望自己的安全技术解决方案与他们的竞争对手不同，从而获得优势，而增加入侵检测系统（IDS）就是其中方法之一。但是为什么所有人都需要入侵检测呢？为彻底理解这个问题，我们需要回顾一下关于计算机安全的基础知识。

计算机安全是个非常复杂的问题。为统一不同的说明方法，我们采用简单的方式。因此在这一章中，我们用最基本的安全模型来描述系统环境中的这个核心部分。无论你的计算机或网络多么复杂，都可以认为是从基本安全模型中抽象出来的，并以主体、对象和访问控制来表达。

回到起点：经典安全模型

宇宙是复杂的，但你却可以用几个亚原子级的简单名词和动词来分解它，而不用了解在亚原子级宇宙是如何运转的。为了理解计算机安全解决方案，的确有必要仔细考虑环境的每一部分的基础细节，以减少可能的安全漏洞。你应敢于去理解自己站点中每个部件的功能并敢问“喂，在这下面究竟运行着什么？”。如果有人想让你开发新的应用程序，每一次都要以同样的问题开始：主体是谁？对象是什么？一般性的访问控制是如何操作的？谁管理安全？

你可能还会问许多其它的问题，而这些问题都是由你对基本的计算机安全模型的理解产生的。本章的第一部分将介绍计算机安全中一些普遍认可的目标。当你知道你想从计算机安全中获得什么后，下一步就是找到一个方法来判定你的要求是否得到满足。要完成这项工作，就要从最简单的计算机安全准则开始，逐步构造安全模型。本章的最后给出一个分类表，这个表对于理解站点上可能使用的不同产品之间的相互关系，和IDS如何满足你的设计是非常有帮助的。

每个站点都有一个准确定义的安全策略，这个策略用来描述信息将如何处理。即使相同的安全策略也可能由不同的安全模型的组合，而得到不同的效果。安全模型是可以用许多方法实现的一个抽象，而可完成安全模型任务的产品为增强安全策略提供了媒体。相同的安全模型也可以支持不同的安全策略。每一个用来增强站点安全的产品都可以导出它自己的安全模型。例如：防火墙与同它共同工作的操作系统为你的公司提供安全的因特网连接。为完成整个目的，防火墙和操作系统有着各自不同的功能和职责。防火墙要依靠操作系统提供安全的环境来运行防火墙程序。如果操作系统的核心出了问题，那么防火墙也就不能完成它的功能。正是由于这种交互作用的存在，你需要知道基本安全模型的结构和如何评价一个安全模型。

简单说来，安全模型定义了许多实体以及实体之间交互和参考的规则。你已经熟悉网络上的不同实体——用户、组、文件、路由器、工作站、打印机、磁盘驱动器、用户程序、

客户、服务器和网络适配器。这些实体在计算机网络中以不同的方式进行着相互之间的交互和参考。访问控制规则定义实体之间如何交互和参考。常见的一个访问控制规则是在一个计算机上对某个特殊文件可读用户的限制。如果你能想到几个其它的例子，就说明你已经理解了安全模型的基本概念。

在研究基本安全模型之前，首先考虑一下为什么需要安全。由一个或几个产品完成的安全模型通过满足三个基本目标。

计算机安全目标

为理解为什么入侵检测现在被加入到其它产品中来提高安全性，你就有必要了解安全产品试图满足什么样的目标。正是由于传统安全产品没有完全达到这些目标，才有许多公司开发或投资于入侵检测的解决方案。

字首连缀字CIA非常容易记住，它代表计算机安全中的三个中心目标：

保密性（Confidentiality） 保护数据不受非授权操作的破坏。

完整性（Integrity） 保证非授权操作不能修改数据。

有效性（Availability） 保证非授权操作不能获取保护信息或计算机资源。

当有人问为什么认为计算机安全如此重要的时候，他们的回答通常是保密性。我们中大多数人当然不希望那些对别人医疗记录非常感兴趣的人很容易就知道自己的医疗记录。信用卡的记录和财产信息当然也是希望受保护的信息。考试成绩、操行评语等个人文件一般也都是希望受保护的信息源。同样地，由手工完成的对银行交易的大量保护措施已在几百年前就完成了。可见，即使计算机没有出现，如何完成保密性的历史早就有了。

信息的完整性在日常生活中也是必然的。非授权的对信用卡记录的改变说明其系统在维护数据完整性的控制下有缺陷。在网络通讯中，如果在数据数据包没有到达目的地前就发生了改变，则信息的完整性就受到了破坏。如果你正在浏览一个Web站点而一个心怀叵测的人却可以从你的个人电脑上获得信息并使用这些信息从你的银行帐户上窃取你的钱，你就成了破坏完整性和保密性的受害者。

由安全问题导致的缺乏数据有效性是要主要考虑的问题。如果一个证券经纪公司对原始交易数据库突然不可访问，每一分钟将会损失上百万。人们可以从容地面对由于软件故障而导致的数据不可访问，甚至磁盘驱动器的错误和数据库的崩溃都不会令人惊奇。然而由于工业间谍的原因数据库变得不可用，那就看看报纸的头版吧！而忽略这些潜在问题的人们，却仍旧用大量的钱用来购买多余的供电设备、多余的网络适配器、多余的服务器和多余的磁盘，而不买安全监测产品。

那么我们又如何展示安全产品提供的保密性、完整性和有效性呢？使用计算机理论科学的一些技术，我们可以在一个特殊的计算机系统的上下文中来形式化定义保密性和完整性。做为一个结论，我们可以说保密性和完整性都是可计算的。这个结论是非常有用的，因为它使计算机安全研究人员明确地知道一个特殊的计算机系统加强了保密性和完整性（Brinkley和Schell，1995）。在商业产品中这些形式化方法很少用到。然而它却可以让我们很轻易地从理论上知道，我们可以严格保证产品关于完整性和保密性的声明。

证明有效性更复杂一些。对有效性的说明不能象完整性和保密性那么有把握。主要原

因是确定影响一个特殊计算机系统中有效性的所有因素是不可能的。也就是说，这些影响因素用数学的表达式不可能穷举，或是说用形式化的方法证明有效性太难了。在这本书中没有使用形式化的证明和结论，但如果你愿意学习更多关于计算机安全的形式化方法，有许多很好的参考资料（Bell，1990；LaPadula，1990；Williams and Abrams，1995），按本书参考书目可以找到这些参考资料。

若以计算机安全的术语来总结就可以说，我们可以用较高的水准保证保密性和完整性，但不能在同一水平上保证一个特殊系统的有效性。至少在假设销售商采用的合理设计和开发过程的基础上，我们确定用来保证系统的保密性和完整性的产品可以证明是安全的。

在计算机安全的其它文献中，你有时还会发现其他的计算机安全目标包括验证（authentication）和认可（nonrepudiation）。验证是核实某人或某事标识的过程，如当用户键入一个密码时。认可是指证明一条信息从一个发送者发出而不是从其他人处发出的过程。正如你将在本章看到的一样，验证被定义为基本安全模型所需要支持的功能，而不是一个显式的目标。在站点上可能需要认可，但它通常不是必要的，它在上述的三个基本目标中被省略掉了。

现在你已经知道了网络安全的目标，下面通过完成一个安全模型来了解这些目标是如何达到的。

学会问一些难的问题

安全模型是一个抽象，它用来定义实体和实体之间是如何被允许进行交互的。在论文中安全模型都是由一系列定义开始的，但最后都由软件，硬件或软硬件来完成的。我们当然希望这个成果是正确的并符合模式的规格。如果这个结果有错误，系统将缺少提供保密性、完整性和有效性的能力。

每个操作系统中都有安全模型。作为安全模型的一部分，在大多数操作系统中对每个文件的访问权限都通过特殊的方法进行限制。在传统的UNIX系统中有一个规则规定，只有Joe这个用户可以读名为JoeMail的文件。这个例子中的实体是Joe和JoeMail，并且在操作系统的上下文中他们必须是唯一的标识。任何模糊的东西都会降低模型满足这三个目标的能力。访问控制规则，也就是授权，是用来说明安全策略中由{Joe, JoeMail, read}三元组构成的这个特殊部分。显然，这几个实体和这个规则只是整个操作系统和安全模型基础的一小部分。其他操作系统实体有文件、进程、线程、队列、消息、处理器和操作系统核心本身。

在网络中配置的安全产品通常也要遵循一个安全模型。你必须知道每一个正在使用的安全模型的目的和范围。要理解为什么这样，我们就拿向操作系统中加入数据库管理系统时发生的情况考虑一下。操作系统和数据库管理系统有不同用户标识。在这种情况下，不需要操作系统中的用户名也要在数据库管理系统中进行标识。事实上，用户名可以由完全不同的字母和字符产生。这两种产品中定义了不同的实体。操作系统定义的实体如文件和目录，而数据库管理系统使用的实体却是记录、域和表。操作系统和数据库管理系统控制的范围也不一样，包括时间的和空间的。操作系统管理是否允许用户安装数据库管理系统，而数据库管理系统却决定用户可以访问数据库的哪一个部分。