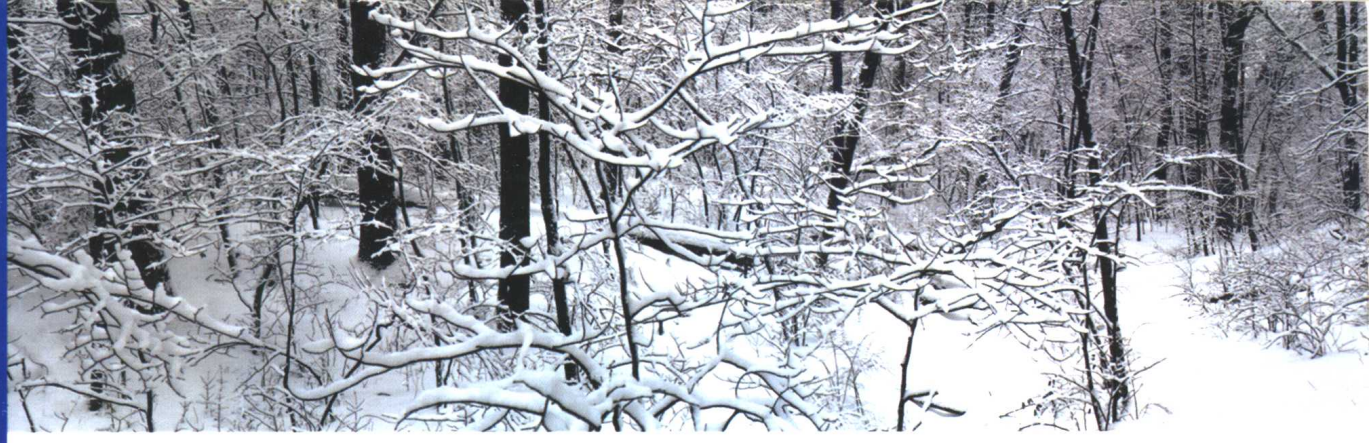

入侵检测实用手册

The Practical Intrusion Detection Handbook

Paul E. Proctor 著

邓琦皓 许鸿飞 张斌 译

PH
PTR

中国电力出版社
www.infopower.com.cn

入侵检测实用手册

The Practical Intrusion Detection Handbook

Paul E. Proctor 著

邓琦皓 许鸿飞 张斌 译

中国电力出版社

内 容 提 要

本书由入侵检测领域的顶级专家编写，介绍了如何使用入侵检测系统来检测、阻止以及响应威胁。还通过使用现实世界中的一些案例介绍了入侵检测软件的功能，并介绍了如何将其整合到用来保护信息和电子商务资产的综合策略中。本书包括基于主机、基于网络以及混合入侵检测系统介绍；入侵检测系统的选择标准以及 RFP 样例；成功部署入侵检测系统的关键要素；入侵检测的 6 个神话及其真实情况等。

本书适合于任何需要选择、部署、操作、管理或者是以别的方式使用商用入侵检测系统的读者。

图书在版编目（CIP）数据

入侵检测实用手册/（美）普罗科特著；邓琦皓等译 —北京：中国电力出版社，2002.8
ISBN 7-5083-1129-9

Ⅰ. 入… Ⅱ. ①普…②邓… 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（2002）第 058424 号

著作权合同登记号 图字：01-2001-2225 号

中国电力出版社出版、发行
（北京三里河路 6 号 100044 http://www.infopower.com.cn）
汇鑫印务有限公司印刷
各地新华书店经售
*
2002 年 10 月第一版 2002 年 10 月北京第一次印刷
787 毫米×1092 毫米 16 开本 17.5 印张 385 千字
定价 35.00 元

序　言

20 世纪 90 年代中期，Neil 是加拿大一个重要政府机构的审计员。一个内部人员从该机构盗走了几百万美元，Neil 受命协助调查该事件。Neil 花了六个多月查阅了大量事务日志来追踪公款的踪迹，随后推断出了公款是怎样被侵占的。大笔公款却永远无法追回了。

2000 年 2 月 9 日，Amazon.com（亚马逊电子交易网站）和其他一些电子商务公司的排头兵遭受了分布式拒绝服务攻击（distributed denial of service attack），这次攻击造成的损失总计几百万美元。这次电子“滑铁卢”彻底改变了电子商务的现状，突出地表明了在任何成功的在线商务中，有效的检测和响应非常重要。

1986 年，Dorothy Denning 写了一篇论文，提出了商业技术的发展进程，即应该提供检测（detection）、响应（response）、威慑手段（deterrence）及毁坏情况评估（damage assessment）。入侵检测（intrusion detection）（经常被误解）为在动荡的在线世界中寻求安全提供了最好的条件。

我的职业是尽量将入侵检测带出研究室，并将其投入到实际环境中去。1988 年，我为美国海军工作，致力于入侵检测研究，其目的是为了在海军工作环境中部署（deploy）入侵检测系统。1990 年，我继续从事普通的范例测试，以量化入侵检测的价值。1992 年，我在 SAIC 设计了 CMDS（Computer Misuse Detection System，计算机误用检测系统），它是首批商用入侵检测系统之一。CMDS 投入使用，并且在 20 世纪 90 年代中期被很广泛地采用。1997 年，我离开了 SAIC，与他人共同创建了 Centrax 公司，并将入侵检测引入了 Windows NT 平台。我在 Cybersafe 帮助开发了最早的一种综合了网络和基于主机技术的混合入侵检测系统。

我曾经研究、开发、部署、销售过入侵检测系统，举办过相关主题的研讨会，帮助进行过相关的调查。这本书是我的下一步。其实目的很简单：写下我所知道的有关入侵检测系统的一切，让读者理解入侵检测，帮助商家部署实用的系统。

读者可以自己控制阅读的进度、成效。本书将解释入侵检测，消除读者的神秘感，并提供需求指导，通过完整的工程生命周期（project lifecycle）来帮助读者得到某个入侵检测系统并使其有效地运作起来。本书介绍的奇闻逸事将入侵检测信息与真实世界联系起来。重要之处都进行了强调，被单独列出来，使读者能更容易看到要强调的内容。

本书大致分成了三部分。第一部分描述了技术，第二部分介绍了如何有效地操作，第三部分则是关于工程生命周期的。本书最后，用了一章的篇幅来介绍商用产品，这些产品是读者必备的工具。

Paul E. Proctor

于太平洋上空 35000 英尺某处

致　谢

感谢 Tom Trebelhorn 这些年对我的信任，感谢他的支持，感谢他为实现我们的梦想所做的牺牲。感谢 TT 为我所做的一切。

Dorothy Denning 的工作一直在激励着我。如果没有她在我们相遇之前所做的关于入侵检测方面的工作，就没有今天的我。感谢 Dorothy 为我所做的一切，感谢 Dorothy 从总体上对入侵检测行业的帮助。

Chris Byrnes 是我的好朋友。我要感谢 Chris，他是我商业上的良师，总是适时地给我提出建议。Harry Schessel 是我多年的合作伙伴和朋友，我们一同奋斗。我要感谢 Harry，他使我摆脱了没有收益的窘境，让我得到了回报。Scott Chapman 是我所知道的最好的一个项目经理/程序员/技术专家。感谢 Scott 的加入，感谢他夜以继日的工作。继续听着音乐，月亮一定会在 Austin 上空升起。

我曾在三个不同的机构中从事入侵检测工作，最先是在 SAIC。Bob Barnhart 是我启蒙阶段的良师益友，我知道的所有东西确实都是他教的。我要感谢 Bob Collins，他帮助我从整体上把握我所从事的工作。John Hyon 和 Luis Cuatok 都是非常优秀的程序员，他们一开始就与我一同工作。伙伴们，谢谢你们。

我所在的第二个机构是 Centrax。我要感谢 Tom Zipoli，他是我的上司，为人正直，也是我的好朋友。Zip. Lynn Hassler 使我们从一开始就没走弯路，我们有时都要为此欢呼。感谢 Lynn 的忠诚和他的努力工作。感谢最好的销售团体（他们甚至可以管理我），他们是 Craig Straube、Scott Anderson、Mark Bonsack、Mark Eberle、Dave Eschliman、Paul Innella 和 Linnea Sandler。感谢 Mary Thomas 帮助我组织机构（这是一个永远不会结束的任务）。

我所在的第三个机构是 Cybersafe。Jim Cannavino、Bob Carberry 和 Pete Fiorito 组成了一个梦幻小组。感谢 Jim Cannavino 的远见和支持。感谢 Bob 给我展示了商业的另一面。感谢 Pete 敏锐的洞察力。

我遇到 Jim Hurley 时，他还在 Data General。入侵检测并不是那么容易掌握的，但是 Jim 能够理解，现在也是这样。感谢 Jim 精通入侵检测。

Stephen Northcutt 和 Teresa Lunt 是两个入侵检测天才，我要感谢他们出色的工作。我也要感谢 Steve Snapp、Kathleen Jackson、Hank Vaccaro 和 Matt Bishop 在本行业的出色工作。

实用入侵检测方面的书当然要有一些实践者。下面这些人从各方面帮助本书得以完成。特别感谢 George Collins 的远见和指导。George，谢谢你这些年的付出。Scott Kennedy 是网络入侵检测权威，是实践者中的佼佼者。他首先在 SANS 上运行了 IDNet，他一直走在相关技术的前沿。Scott，谢谢你所做的贡献。感谢 Don Goldstein，他是个安全人员，给我提供了进行入侵检测的反馈意见，其价值是无法衡量的。感谢整个 DB 小组成员，他们是 Neil Todd、Phil Venebles 和 Andrew Kennedy。他们为本书所做的付出会使许多人受益。特别感谢 IBM 公司的 Paul deGraff，他为大型机入侵检测提供了资料。

感谢 Tad 阐明了操作模式，他了解读者的需求。感谢 Bob，他了解该技术，在操作需

求方面具有敏锐的洞察力。

下面这些人也是我要感谢的，他们也为本书做出了贡献。Engarde Systems 的 Mike 和 Dianna Neumann 提供了大部分网络入侵检测的例子。Dan Masters 为复合标志（compound signatures）提供了帮助。Mark St. John 博士检查了人工智能部分并进行了评论。最后，要特别感谢 Eric Rohy 这么多年的付出和辛勤劳动。

感谢 Network Ice 的 Robert Graham、ODS 的 Steve Schall 及 Dave O'brien、Network Associates 的 Rama Moorthy、Network Wizards 的 Ron Gula、Network Flight Recorder 的 Barnaby Page 及 Marcu Ranum、Cisco Systems 的 Joe Sirrianni、Pentasafe 的 Janette Deyhle、Mission Critical 的 Neil Bremmner、Internet Security Systems 的 Dan Nadir、Axent 的 Scott 及 Mark Ungerman 以及 Computer Associates 的 Christine Rogers，这些厂商的职员提供了关于他们产品的有用信息。

写这本书花了我一年时间，这期间我得到了产品部的一些朋友的帮助。Sue Heim 一直帮助我编辑，使这本书最终得以面世。Glenn Van Houten 制作了精美的插图。感谢 Dude 的制图。我还要感谢我的责任编辑 Tim Moore，他一直引导着我完成手稿。

感谢我最好的朋友 Tom 和 Jen。特别感谢 Gromit 和 Farley，他们是许多范例的主角。

我的爱妻 Sherry 一直在默默付出。她放弃了周末，在工作之余帮助完成本书，还要掌管 www.practicalsecurity.com 网站。我无法表达谢意。这点，我的爱妻是知道的。

最后，要感谢我的父母。他们在我需要时总是给我支持。这一点我永远感激他们，我也将会这样对待我的孩子们。

本书导读

读者：本书适合于任何需要选择、部署（deploy）、操作、管理或者是以别的方式使用商用入侵检测系统的读者。本书几乎未提及研究信息。

组织结构：本书大致分为四部分。第 1~6 章描述了入侵检测技术。7~10 章介绍了怎样有效地使用入侵检测系统，并给出了许多现实世界中的范例。11~14 章是关于工程生命周期的，包括需求定义、论证入侵检测的可行性、工具的选择以及商用产品。第 15、16 章是关于入侵检测的组织机构、标准和法律问题的一些综合信息。

- 初学者在阅读其他章节前，应掌握第 1~5 章的内容。
- 管理者应该阅读第 1~7、11 和 15 章。
- 选择、操作入侵系统的技术人员应该阅读第 6、7、8、9 和 14 章。
- 法律工作者可以直接阅读第 15、16 章。

要点

读者可以看到本书中多次出现这个图标。它表示文中出现的重要之处需要重点指出来。这也使读者能够很快地找到重要信息。

补充说明：补充说明是一些真实的故事或奇闻，用来举例说明文中的重要之处。

我将本书写得通俗易懂，而且使读者易于找到信息。“要点”和“补充说明”这样的形式使读者能够更好地阅读本书，并且获得在自己的企业中成功部署入侵检测系统所需要的信息。

真实故事及案例研究

第 12 章，**保持需求的灵活性**。在整个过程的早期保持需求的灵活性能增加系统的整体有效性。（第 153 页）

第 12 章，**比重量：计算标志数**。具有最多标志的产品不一定是最适合你的环境的工具。（第 157 页）

第 12 章，**不可能什么都监控得到！**如果你想成功的话，你就必须确定合理的监控需求。（第 159 页）

第 13 章，**合理性检查！**检查购买过程中的互斥需求。（第 172 页）

前　言

20 世纪 80 年代中期，当我在 SRI 国际组织中从事入侵检测工作时，只有少数几个人在从事这个领域的工作，没有商用产品，也没人确信这个概念可以起作用。当有人确信它没用时，我们知道传统的计算机安全方式需要用别的方式来替代。访问控制（access control）和其他安全机制并不很安全，有决心的黑客（hacker）通常只要稍微努力一点就可以突破安全防线。更糟的是，已有的防范体系根本不能防止来自内部的威胁。入侵检测看起来是个有希望的替代方式。

1987 年离开 SRI 时，我停止了入侵检测的工作，但我作为旁观者看到了这个领域在兴旺、成熟起来。它从理论上的概念发展为实用的方法，从研究梦想成为一个重要的产品领域，从一个有研究价值的想法发展为计算机安全方面的国家计划中的关键部分。它从一个监控单一的计算机的工具演变成可以监视整个网络。

在这方面没有人比 Paul Proctor 懂得更多。Paul 在 SAIC 工作时设计了第一个商用入侵检测产品 CMDS。随后他与人共同创建了 Centrax，最终研制成功了 Centrax 入侵检测系统。从一开始，Paul 就意识到应该怎样让入侵检测在操作环境中获得成功。他不仅懂技术，而且知道顾客的需求。他将技术和顾客需求综合起来，创建了能满足现实需要的很好的产品。

Paul 的这本独一无二的书是他渊博的知识和开发商用入侵检测产品的经验这两者的结晶。当其他人注意技术时，他却引导读者经历选择、部署和使用入侵检测产品的整个过程。同时，他还解释了入侵检测技术的工作原理，澄清了常见的误解。

他用真实的案例来阐明概念和解决方法。他讨论了哪些能起作用，哪些不能，指出了这些工具的缺陷及使用开销。他没有因为自己的商业利益而说假话。

对于期望购买入侵检测产品的或已做出决定购买但正在确定购买哪种产品并怎样部署产品的人，本书是必不可少的。本书为这些人的实际操作做了颇具价值的指导。研究人员也能从本书受益，因为本书的内容证实了他们的一些想法，而且指出了需要进一步研究的领域。最后，本书给那些对入侵检测有兴趣的读者提供了很有价值的资料。

Dorothy E. Denning

目　录

第 1 章　介绍

验证才能信任。

——Ronald Reagan

随着电子商务对经济发展的支配和对 Internet 的推进，各种规模的商业成功已经开始依赖于计算机的互连性。我们要和合作伙伴、供应商、顾客连接起来，甚至还要与竞争对手互连。正因为处于这些互连环境下，所以必须为商业开发出基于计算机安全控制的某种程度的信任关系。通过验证（verification）这样的控制可以增强信任。而验证是由入侵检测提供的。

计算机安全学科涉及下面三个基本要素：

- 预防（prevention）。
- 检测（detection）。
- 响应（response）。

这三者对计算机系统的综合防护都很关键。但是最近 30 年来，许多资源都花费在预防方面，几乎将检测和响应排除在外，这简直不成比例。从根本上来说，预防总归比别的方式要好一些。毕竟，如果防止了威胁，那就不需要检测和响应。不幸的是，预防方式并不能完全保护公司资产，仍然会引起损失。1999 年 6 月，《纽约时报》报道全美 1999 年由于计算机误用造成的损失超过 70 亿美元。

要点

1999 年 6 月，《纽约时报》报道全美 1999 年由于计算机误用造成的损失超过 70 亿美元。

1.1　安全 vs 商业

为什么商店在关门时要把门锁上呢？这个问题凸现了商业面临着安全问题这样一个矛盾。商店开着门是为了让顾客可以进来买东西，简而言之，这样才能进行交易。进门的顾客也许经常会偷盗或挥舞着枪支把钱柜里的钱都抢走。这种事件的威胁是店主锁门的原因之一。现在安全的矛盾很明显：锁上门来保证安全，或者是打开店门做生意。

要点

安全矛盾：商店可以锁上门来保证安全，或者是打开店门做生意。

商业依赖于计算机。计算机要能够允许进行相当程度的访问，以便完成交易。厂商、顾客、合作伙伴和职员需要能以不同的访问级别访问计算机网络。此外，这些必需的访问

会导致本地计算机连接到 Internet 上或使用别的技术。例如，使用调制解调器会使网络容易遭受不具有访问权的外部人员的攻击。

允许访问计算机当然就具有潜在的威胁，但是现在信息的交换对于商业来说比其他任何因素都更为关键。即使是在情报搜集、涉及国家安全这样的秘密事件中，授权者之间的数据交换也是成功的关键。

对于安全威胁的传统响应是建立堡垒，即设计一系列预防措施来阻止非授权用户的访问。为让读者理解计算机中的堡垒的概念，可以用一个日常生活中的例子来比喻说明，即保护一个装满了盒子的仓库（这些盒子里装着重要信息），如图 1-1 所示。

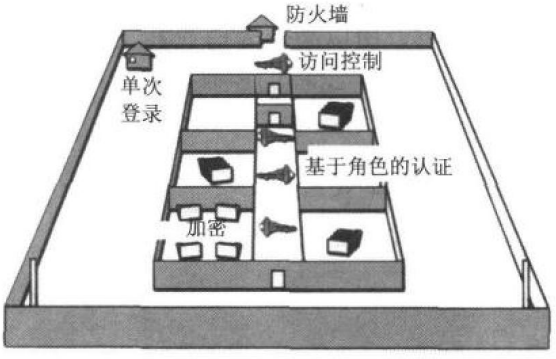

图 1-1　访问控制机制

当一层层剥开安全“洋葱”时，读者可以看到许多预防措施的例子。在这个用来比喻的现实世界中，用路灯来表示物理安全，路灯可以比作计算机世界中的防盗设备，包括标记设备（tagging device）、硬件锁（hardware lock）、驱动器锁（drive lock）和告警器（alarm）。比路灯更近一点的是环绕着仓库的围墙，它可以比作计算机领域中的防火墙。

前门有几把钥匙，有从岗亭处进入仓库的钥匙，也有进入仓库各个房间的钥匙，这很像是计算机中经过签名授权的证书。随后就可以进入仓库了，而在具有访问控制方式的计算机领域中则要用密钥或口令登录。进入仓库后，要进每个房间还需要有相应的钥匙，这就像计算机中的基于角色的认证（role-based authentication），它只允许用户访问指定的文件、文件夹。最后，可以将仓库中的盒子锁上，这样，即使盒子被盗也不会导致非授权泄密，这与计算机使用的加密方式相似。

避免外部人员侵害的预防措施不胜枚举，一种典型的方式就是再加一层保护。但是这样的方式有其局限性。

不幸的是，预防性安全措施只致力于信息交换的安全，很难有效地对访问控制进行管理，而且其代价是减慢交易的速度。防火墙能限制进入网络的访问者，但同时会引起延迟。例如，允许通过防火墙访问一个新商业伙伴的过程也许要等上好几天。另一个影响商业的访问控制的例子是，回拨式（dial-back）调制解调器要求预先确定位置，这就减少了它的用处。

预防外界威胁的另一个问题是，大多数损失都是由内部人员引起的。1999 年 CSI/FBI（Computer Security Institute/Federal Bureau of Investigation，计算机安全协会/联邦调查局）的计算机犯罪及安全调查局指出，82%的损失是内部威胁造成的。从 1997 年到 1999 年，由于与信任关系相关的威胁，其中包括盗取私有信息、破坏数据或网络、内部人员滥用网络访问、金融诈骗、非授权的内部人员访问及电信欺骗，造成了总计为 293890505 美元的损