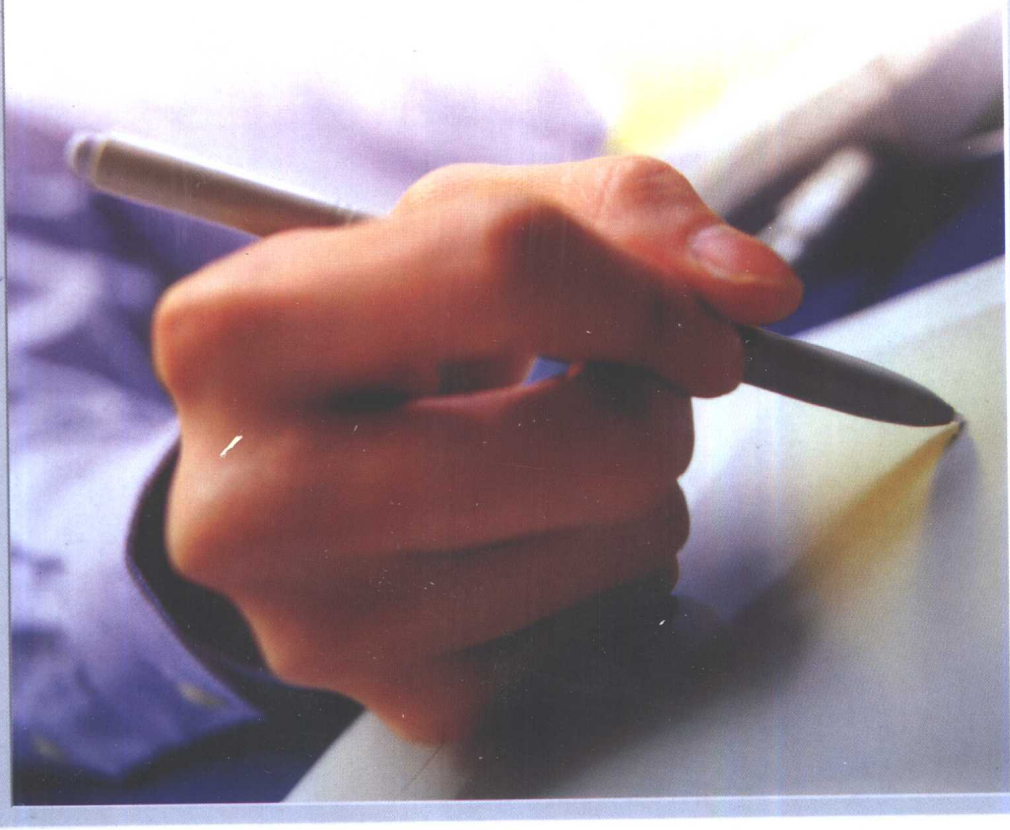
New Riders

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

网络入侵检测分析员手册



Stephen Northcutt 著

余青霓 王晓程 周钢 等 译

周钢 审校

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

网络入侵检测分析员手册

Stephen Northcutt 著

余青霓 王晓程 周钢 等 译

周钢 审校

人民邮电出版社

图书在版编目（CIP）数据

网络入侵检测分析员手册/（）诺斯科特（Northcutt,S.）著；余青霓等译.—北京：人民邮电出版社，2000.3

（信息与网络安全丛书）

ISBN 7-115-08372-X

I.网… II.①诺…②余… 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（2000）第 11549 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

网络入侵检测分析员手册

◆ 著 Stephen Northcutt

译 余青霓 王晓程 周 钢 等

审 校 周 钢

责任编辑 李 际

◆ 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

北京汉魂图文设计有限公司制作

北京鸿佳印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：787 x 1092 1/16

印张：15

字数：347 千字 2000 年 10 月第 1 版

印数：6 001 - 10 000 册 2001 年 1 月北京第 2 次印刷

著作权合同登记 图字：01 - 1999 - 2057 号

ISBN 7-115-08372-X/TP·1511

定价：28.00 元

内容提要

本书从一个非常有名的攻击——Mitnick 攻击开始，列举并分析了多种攻击的详细特点。然后在此基础上，提出了与安全攻击相对应的各种安全对策和安全工具。本书内容包括以下几个方面：

- Mitnick 攻击。
- 过滤器和攻击特征介绍。
- 安全体系结构问题。
- 安全工具之间的互操作性和关联性。
- 基于网络的入侵检测解决方案。
- 对攻击的检测。
- 拒绝服务攻击。
- 情报收集技术。
- 黑客技术介绍。
- 协同攻击技术。
- 其他安全工具。
- 风险管理和入侵检测。
- 对入侵事件的自动和人工响应。
- 入侵检测商业应用事例。
- 将来的发展方向。

书中有一些新颖的理论性内容，引述了 1998~1999 年中的一些论文和研究工作，但绝大部分内容是实用的。书中包含了丰富的攻击实例，描述了多种典型攻击的攻击特征，所有这些都是作者多年从事入侵检测工作的宝贵经验和结晶。这本书适合作为入侵检测分析员的培训和参考手册，对计算机安全有兴趣的计算机爱好者从本书中也能得到不少帮助和启发。

信息与网络安全丛书 审定委员会

名誉主任：朱恩涛
主　　任：谢模乾
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。这些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。

由于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

译者序

目前，人类正向一个新的时代——电子信息时代迈进。计算机网络控制着从战场作战到民用交通管制，从音乐影视到金融活动等各个方面。计算机网络安全问题已经成为影响国家独立和安全，影响经济运行和发展，影响社会稳定和繁荣的重大问题。入侵检测则是网络安全中极为重要的一个领域。

入侵检测研究人员梦寐以求的就是建立一个智能化入侵检测模型。但目前离这一目标还比较遥远，根据译者的研究和开发经验，很难建立一个模型来判定哪一个连接是善意的，哪一个连接是恶意的。即使是目前国际上最先进的入侵检测系统，对某些攻击类型的误报警率也达 90% 以上。所以，对于入侵检测，很大程度上要依靠分析员的经验和直觉，攻击事例和分析员的经验是入侵检测中最重要的两个方面，而这两个方面都需要长时间的原始积累。

这本书适合作为入侵检测分析员的培训和参考手册。书中有一些新颖的理论性内容，引述了 1998~1999 年中的一些论文和研究工作，但绝大部分内容是实用的。书中包含了丰富的攻击实例，描述了多种典型攻击的攻击特征，所有这些都是作者多年从事入侵检测工作的宝贵经验和结晶。希望这本书能很好地为你服务，也希望你喜欢看。

本书的主要翻译工作由余青霓、王晓程、周钢等人完成；唐克、刘向东、韩巍、马瑞萍、高军、李朝虎、胡乔等同志也参加了许多讨论和翻译工作；另外，航天 706 所的谢小权研究员给我们的翻译工作提供了许多帮助和指导。

本书的主要译者在近几年来一直从事计算机网络安全方面的研究和开发工作。但正如本书作者所说的："入侵检测是一个全新的、快速发展的领域"，再加上国内与国外在某些信息、技术和工具上的差距，整个翻译工作对我们来说是一个不断学习和讨论的过程。译者抱着极其认真和谨慎的态度学习并翻译了全文。在翻译过程中，力求准确，忠实原文，但因知识水平和实际经验所限，疏漏之处敬请读者谅解，并希望给予批评指正。

衷心感谢所有为本书的出版付出辛勤劳动的人们！

2000 年 8 月

关于作者

Stephen Northcutt 毕业于 Mary Washington 学院，在进入计算机安全领域之前，他曾从事过多种工作，担任过美国海军直升机搜索和救援的机组人员、制图师和网络设计人员。他还是《事故处理循序渐进》和《入侵检测——Shadow 的风格》的作者，这两本书都是由 SANS 研究所出版的。他是 Shadow 入侵检测系统的最早开发者，并在国防部担任过两年 Shadow 入侵检测小组的领导，目前在弹道导弹防御组织的信息战部门担任主管工作。

关于本书的技术复审人员

Tim Aldrich1990 年从 Oregon 大学毕业时正经营着自己的计算机咨询服务。1991 年他在美国海军接受了一份公务员工作，从事计算机模拟系统的开发，因此来到了加利福尼亚州的圣迭戈。过了几年之后，他移居到弗吉尼亚州，并决定涉足计算机和网络安全领域的工作，开始和 Stephen Northcutt 在 Shadow 小组中共事。1999 年，Tim 离开国防部到华盛顿西雅图一家名为 NEXTLINK Communication 的电信公司工作，担任计算机系统和安全设计人员。

M.Dodge Mumford 作为高级故障排查人员、支持工程师和 Network Flight Recorder(NFR)系统的培训人员，一直在从事运作安全和入侵检测方面的工作。他出席了 1998 年的 SANS 网络安全大会，编写过许多入侵检测 N-CODE 过滤器。到 NFR 之前，他在 BTG 公司承担各种安全方面的任务。他取得过与各种行业有关的不同安全产品系统证书，包括 Checkpoint 公司的 Firewall-1、Axent 公司的 Raptor Firewall 和 Wheelgroup 的 NetRanger。在过去的 8 年里他一直是个活跃的网络和安全管理员。

Judy Novak 在军队研究实验室的计算机安全和入侵响应小组(CSIRT)中担任安全分析员的工作已有两年多了。她在计算机这一行干了 20 多年，主要从事过大型机、UNIX 的相关工作，最近一直在从事安全方面的工作。

Larry Paccone 是信息系统的理科硕士和国际事务的文学硕士，并拥有系统和网络安全、Internet 网络、WAN 产品、Cisco 路由和 Windows NT 方面的专家证书。Larry 目前是 Analytic Science 公司的高级信息/国家安全分析员，他当了 5 年的 Internet 和系统安全分析员，又当过 5 年的国家安全分析员。

致 谢

本书中关于网络入侵检测和分析的见解是由世界各地的许多分析人员提供的。你和我都应该向他们说声谢谢，他们给我们的一份厚礼就是：把一度神秘的东西变成已知的模式。在表达感谢时，我将直呼他们的名字。请记住，我们谈论的这些人是安全界的前沿人物。问候 NFR 开发组的 Marcus、Dodge、Eric 和 Kent，使用 N-code 的第一套样本过滤器真是既有趣又有教育意义。还要感谢 Ken 和 Greg，谢谢你们从 netsec.net 发来的资料。特别感谢 Mudge 博士(l0pht.com)提供了第二章中 N-code 的例子。

谨向 NID 开发小组致以最美好的祝愿。据我所知，你们开发的工具仍旧是顶级的字符串匹配器。如果我的工具箱中没有 NID 的工具，我将非常不愿意进行事例的创建工作。Sandy，好好鼓励他们，他们真是了不起！John，感谢你在我最需要帮助的时候提供了无私的帮助，我会铭记在心的！

在感谢能源部的同时，我要特别感谢编写出 TCPdump 和 libpcap 工具的开发人员。我确实觉得 TCPdump 对网络分析和入侵检测的贡献比任何其他工具都多。

FIWC 的朋友们，我非常想念和你们分享检测结果的时光。Nina、Grace 和 Julie，请你们多保重。我要特别感谢 Raul Amigo，我们一起对付过那么多难懂的资料，正如“Snowy River”中的人物所说，“我的火炉旁永远有你的位置”。

问候 Cisco 公司的 NetRanger 开发小组，你们真了不起。特别感谢与我们合作的 Kevin、Scott 和 Shinn 兄弟。

衷心祝愿 Qualcomm 和 Scott，当我写这些致谢的时候 Scott 正在度蜜月。感谢他们主持了第一届 ID'Net 大会。问候 ODS 公司的 Steve 和 Dave，他们带来了自己的交换技术，并发表了精彩的讲话。来自 sandstorm.net 的 Simson 和 James，谢谢你们，你们的 TCPdemux 工具真不错！还要特别感谢 centraxcorp.com 的技术主任 Paul Procter。没有你，我们不可能完成这项工作，真想立刻再见到你。Chris，你正在为下一届 ID'Net 大会进行有意义的工作，继续努力！

Rob 和 Alan，感谢你们在 Web 安全广播方面给我的帮助；还要感谢 broadcast.com 站点的人们。感谢我们的嘉宾：John、HD、Simson、Steve 和 Paul。Axcent 公司的 Drew 及其他

人，我很遗憾你们对 1999 年 2 月的广播不太满意；我已经写信给 Drew 表示道歉，并提议在本书中介绍你们的系统。希望以后我们能够有机会合作。

问候与我在一个战壕中的特殊朋友，希望我们能够一起不断开创新的战场。Dave，那个算法进展如何？Dick、Mary、Ray 和 Mark，你们什么时候下来？顺便说一句，以后不管我参与组织什么大会，希望你们每人都能交来一篇论文！

衷心祝愿空军 Rome 实验室和 PRC/Litton ACTD 的全体人员。我等不及想看看你们的项目进展如何。

我曾经参观和访问过许多政府机构和实验室，从未发现哪个地方能够像 NSWC Dahlgren 那样既保持开放以满足科研人员的需求又保证安全，能够保持二者之间的平衡关系。不过可千万不能松懈——因为威胁正变得越来越严重。

说到实验室，我向 JNTE 实验室的人学到了有关安全方法论的许多知识，对此我十分感激，希望你们继续努力。感谢 Terry、Vince 和 Dean，你们曾伴我渡过美好的时光。

仍旧是说实验室，军队研究实验室的计算机安全和入侵响应小组(ARL CSIRT)，你们的人员真棒！你们正逐渐成为我们国家在入侵检测和分析领域的领头人。请继续努力吧！

如果没有 SANS 研究所的帮助，Shadow 可能永远不会存在。感谢 Dalas、Zoe、Daragh、Irene、Marsha 和 Rob 为我们付出了辛勤的工作。Shadow 小组特别感谢 SANS 的研究负责人 Alan Paller 所给予的鼓励和支持。

Matt，谢谢你让我和你一起共同主持第一届 IDR 大会，并且教我如何进行会议的组织工作。我也非常感激那些向 IDR、NS'98、ID'99、SANS99 和即将召开的 NS'99 大会提交高质量论文的人。作为一个大会主席，我真有点受宠若惊，你们的参与才是使大会成功的真正决定因素。

如果没有政府发起人——弹道导弹防御组织的参与，也不会有 Shadow 小组的存在。Denny，谢谢你看得起我这个使用捡来的计算机和黑客代码的家伙。感谢 Bob 支持这个项目。还要特别感谢 Chris 和 Rob——虽然金钱不是万能的，但它能给我们很多帮助。

如果没有我在 Shadow 小组的朋友和遍布全国的分析人员对新攻击模式积极投入研究，使攻击模式变得清楚明白，那我将一无所知。Judy、Tim、HD、Lee、Steven 和 Mike，谢谢你们！如果是个十分古怪的攻击模式，那就查个究竟；如果很容易，那么让别人去干吧！我在 NSWC 的 Shadow 队伍中享受到了一生中最大的乐趣。我们度过了不少艰难的日子，然而成功的喜悦是多么令人陶醉！Bill Ralph，是你编写了这个名为 Shadow 的软件；所有使用这个软件的人都要谢谢你！祝你每一天都工作愉快。John，谢谢你为我所做的每一件事情，你我有幸一起参与了 Shadow 的整个开发过程。Adena，你干得真棒！记住不要局限于屏幕信息，要不断探究“还有其他问题吗？”。Dave，你一直掌握着正确的追踪线索，我简直等不及想再看看你那些记录了。Pat，继续努力吧，我们对图形分析工具的急切需要已超出了我能用语言表达的程度。Bill，谢谢你照管我们的超级计算机。Tim，祝你在新的职业

中一帆风顺，“苟富贵，无相忘”！Jim，谢谢你加入 Shadow 的队伍，Shadow Style 的升级工作进行得怎样了？

Fred，你是一个非常理性、和蔼的上司。我知道自己给你带来不少麻烦，但我们也设法干了不少好事。谢谢你这么多年一直作我的诚实可信的朋友。任何时候如果你需要我干什么，只需打个电话。

Vicki，我遇见你的那天一定是个幸运日，之后我们一起经历了许多事情。Shadow 拥有敏锐的分析技术，也应归功于你那不知疲倦的工作态度。你所破译过并为之编写了文档的新攻击数量决不比任何人少——请继续保持。谢谢你为编写“Shadow Style”手册付出的劳动；这本书对分析人员一直是个很有价值的帮手。另外，你和 Hel 一起教授的高级入侵检测课程在这一行中起到了带头作用。

Kathy 和 Hunter，我亲爱的家人，谢谢你们容忍我在写这本书的三个月中对你们的疏忽与怠慢。这种情形马上就会结束了，因为这是我要写的最后一节内容。Kathy，感谢你在我交稿之前花时间帮我检查了一遍。我爱你们！

希望你们喜爱此书！

前 言

这本书是入侵检测人员的培训和参考手册。作为 Shadow——一个世界级入侵检测小组的创始人，我有幸能够与其他一些非常优秀的入侵检测小组和分析人员密切合作。在领导 Shadow 的这些年里，我负责培训过许多分析人员，教学的基本方法就是不断重复，我发现自己在培训每一个新的分析人员时总是不断重复说相同的词。我努力多年创立了一个正式的培训班，在得到机会编写这样一本书后，我把它推迟了一年多，因为知道这需要投入大量的时间和工作。与此同时，对入侵检测分析人员的需求不断增长，已超出了我所能够教学的人数。这一写作项目开始于 1998 年 12 月 22 日，最后一章完成于 1999 年 3 月，为这本书我投入了大量工作，它也值得我这样付出努力。要想成为一名真正技术高超的入侵检测专家，你也需要投入同样的努力，希望这本书能够帮助你早日学有所成。

Shadow 的历史

我们将要提供的所有例子几乎都是由 Shadow 入侵检测系统捕获到的，我把前言的剩下部分全用来介绍 Shadow 的发展历史，如果你想钻研技术问题，可直接转至第 1 章。

如果没有弹道导弹防御组织(Ballistic Missile Defence Organization，BMDO)的 3 个远见卓识的领导，Shadow 可能永远都不会存在。遇见他们时，我正在用从垃圾堆里抢救出来的老式 Sparc 1+s 计算机开发字符串匹配系统，主要的收集引擎就是来自第 45 期 Phrack 中一个经过修改的 Ensnif.c 程序，那就是我的第二代系统！不用说，这种从垃圾堆捡来的硬件和“黑”来的黑客软件限制了我的作为。我第一次遇见 Dennis Poindexter 是在一次 VTC 短会上，我很少碰见谈吐如此有远见的人。第二个星期我就到弹道导弹防御组织去找他，他答应在这个项目上帮助我，并介绍我认识了 Robert Peavey 和 Chris Capilongo，他们为 Shadow 项目提供了第一笔资金。当然，弹道导弹防御组织给予 Shadow 的不仅仅是金钱的资助，他们使我有机会向世界上最为精明的人请教一些非常棘手的问题，并得到他们的建议和忠告。其中最为重要的一条建议可能是非技术性的，我愿意将它和你一起分享，那就是“做一件事情，就一定要将它做得很好。”

有了弹道导弹防御组织提供的资助，我聘用了 John Green，他现在是 Shadow 入侵检测小组的领头人。John 开发的 Dark Shadow 是一个非常强大的入侵检测相关性和趋势分析系统，他是个技术很棒的分析人员，写过一篇 nmap 的论文，那是 1999 年 3 月 2 日一个 Web 广播的基本内容，本书第 11 章中有关 nmap 的部分完全是根据他的工作归纳的。

在 NSWC 这个诞生了 Shadow 的实验室里，大部分研究工作是由努力工作的研究部人员完成的。当 John 从武器系统开发转向研究工作时，他就转到了研究部，到了那儿还不到 3 个星期，他就开始不断地在我旁边嘀咕，说我们应该聘用这个叫 Vicki 的人。

Vicki 现在是 Cisco 公司 NetRanger 开发小组的一名成员，并且是高级入侵检测技术的高级指导。经过一段每天 18 小时的专注工作，她很快就成为一名最好的入侵检测分析人员，她的那种专心程度是我很少见到过的。Vicki 是 3 名 Shadow 设计者中的一员。

1997 年 10 月，我遇到了 Alan Paller 先生，SANS 研究所的研究负责人。当时人们对学习入侵检测有很大兴趣，而我们也正一股劲地从事这方面的工作。SANS 愿意考虑用筛选(非字符串匹配)方法解决入侵检测问题，并帮助将该项目从实验室扩展到教室。正如国防部不是因为它会做广告才闻名的，如果你听说过 Shadow，那也不是因为广告，而完全是因为 SANS。SANS 帮助我们发布了软件让同行复审评价，虽然这是个颇伤自尊的过程，但对改进程序代码绝对有好处。我对这些复审评价进行总结归纳后形成了一本小书：《入侵检测——Shadow 系统的风格》。那时，关于入侵检测方面的书籍很少，而且全都是理论性的，我们却在书中提出了一些有关具体做法的指导，这是我们第一次尝试编写分析人员手册。SANS 还为我们的课程提供了授课场所，利用 Shadow 小组获得的检测结果，我们形成了高级入侵检测实战技术的核心指导课程。

这就是我们三个臭皮匠——John、Vicki 和我自己，每个人以前都从事过 5 年至 15 年的计算机科学研究。我们每个人都是白天编写自己的入侵检测代码，晚上从事分析工作，夜以继日地干。随着代码的不断增多，我们运行系统时都要祈祷一番，希望不要出现什么问题。当 Bill Ralph 加入我们小组的时候，我们的系统由于代码出错“死”了好几个月，Bill Ralph 曾是能源部一个实验室中一群超巨型 Cray 计算机重要系统的程序员，他远不止是这个项目的专业编程人员，他很快就成了那些系统的工程师。从加入我们工作的第二周开始，他就一直是 Shadow 的主要设计者。

Shadow 的朋友

在入侵检测领域有一个特有的奇怪问题：参与这一“游戏”的人互相之间不能好好配合，这一问题体现为以下几点：

- 计算机事件响应小组(CIRT)不向汇报攻击的网络节点反馈信息；
- 各个网络节点之间不共享信息；

- 每个人都要求得到“第一流的、最好的”之类的声誉；
- 明明有对金钱的争夺，但每个人都不愿谈及这个问题。

Shadow 小组的每名成员一致认为我们应改写这样的“游戏”规则，从第一天开始我们就努力与其他人合作，分享我们拥有的信息。虽然遭到不少拒绝和抵制，我们还是与一些小组建立了极好的关系。我无法在此一一列出曾经与我们合作过的每一个小组和检测器的确切位置，但必须特别提到为我们提供数据来源的几个人，“Steve、Mike、Don、Dean 和 Lee，知道我们很爱你们，对不对？”

军队研究实验室的计算机安全和入侵检测小组(CSIRT)是一个愿意分享检测结果、技术和分析观察的小组，基于德克萨斯州 AMU 的 Netlogger，我们两个小组曾经各自独立地开发出几乎完全相同的第一代入侵检测系统。Angelo Bencivenga 是一名优秀的入侵检测小组领头人，在我认识的人里，他对于追查攻击者最富有经验。作为分析人员，最令人激动的经历就是第一次发现某种新的攻击方式，Judy Novak 和我一起处理过许多分析问题，力图从中甄别出攻击者用新的不寻常攻击方式干什么坏事。Judy 还非常友好地担任了本书的技术复审人员。

入侵检测工作中一项令人难以忍受的事情就是：你可能数个月来每天发送出 30 份事故报告，可从来听不到任何回音。然后突然会有一天，哇！每个人都为某一个检测结果感到激动。两个星期前，入侵检测的行业报刊上登载了一篇文章，说国防部副部长在谈及一次攻击时提到了 Shadow 系统，于是所有的人都很兴奋，都想了解这一次检测。唉，我想了解的却是数月来每天发送出去的那 30 份报告到底怎样了。

作为入侵检测小组，发生在我们身上最为离谱的事情就是对协同攻击的观察。从 1997 年 12 月开始，我们不断发现一些奇怪的巧合现象，到了 1998 年 1 月中旬，我们已经收集到大堆数据，正力图将它甄别出来。在我们向一个大学生查询他的主机为什么攻击我们之后，他发来一份攻击者目录，从而使我们获得重大突破。到了 2 月份，我们发表了关于协同攻击的分析论文，那一下子刺激了某些人的神经，他们写信来说是自己先造出“协同攻击”这个专门术语，那是他们个人的知识产权。让我在这儿简单地说一句：Shadow 入侵检测小组使用这一词语只是为了描述我们观察到的一种攻击模式。后来我们决定对协同攻击再进行一次说明，并且向 Usenix 关于入侵检测和网络监测的专题讨论会提交了一篇论文。我很感谢 Usenix 允许我在第 10 章中使用那份材料，我想谢谢 Marcus Ranum 和 Fred Avolio 对我的体谅，还想谢谢与我合作这篇论文的作者：John Green 、Dave Marchette 和 Bill Ralph。

现在你知道我来自何方，对这本书的内容有了自己的预想。书中有一些理论性的内容，我们也会引述了一些论文和研究工作，但书中绝大部分内容是实用性质的。希望这本书能很好地为你服务，也希望你喜欢看。如果你刚刚开始朝着成为一名入侵监检测分析人员的方向努力，我希望你能够获得迅速进步。如果你有一个热门的 DMZ，也就是说有许多攻击者，这项工作可真是要令你发狂了。