HZ BOOKS 华章IT
ELSEVIER 爱思唯尔

信息安全技术丛书

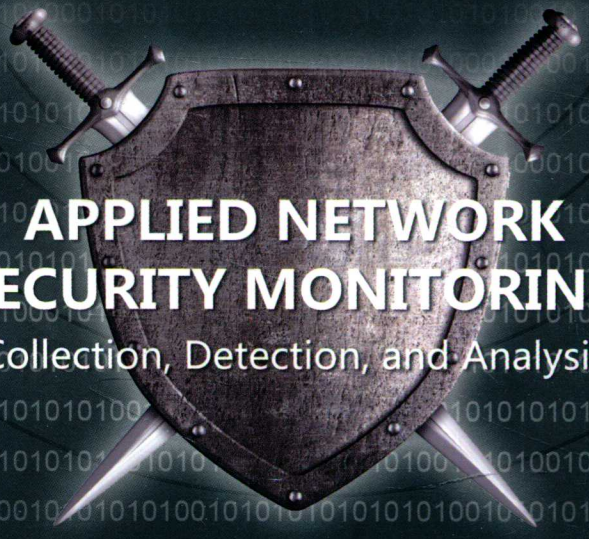
国际信息安全技术专家亲力打造，是系统化建立网络安全监控体系的重要参考

既详细讲解网络安全监控的相关工具和技术，又通过多个完整的真实案例阐述网络安全监控的关键理念与最佳实践，是由菜鸟到NSM分析师的必备参考

网络安全监控

收集、检测和分析

[美] 克里斯·桑德斯（Chris Sanders） 杰森·史密斯（Jason Smith） 著 李柏松 李燕宏 译



APPLIED NETWORK SECURITY MONITORING

Collection, Detection, and Analysis

机械工业出版社
China Machine Press

信息安全
技术丛书

网络安全监控

收集、检测和分析

[美] 克里斯·桑德斯 (Chris Sanders) 杰森·史密斯 (Jason Smith) 著 李柏松 李燕宏 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络安全监控：收集、检测和分析 /（美）桑德斯（Sanders，C.），（美）史密斯（Smith，J.）著；李柏松，李燕宏译 . —北京：机械工业出版，2015.11
（信息安全技术丛书）
书名原文：Applied Network Security Monitoring: Collection, Detection, and Analysis

ISBN 978-7-111-52009-2

I. 网… II. ① 桑… ② 史… ③ 李… ④ 李… 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（2015）第 260809 号

网络安全监控：收集、检测和分析

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：吴　怡　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2016 年 1 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：24.25
书　　号：ISBN 978-7-111-52009-2　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjt@hzbook.com

华章IT
HZBOOKS | Information Technology

The Translator's Words 译者序

一直以来，在企业网络安全的攻、防对抗中，防御者都是处于不利位置的。这不仅因为攻、防双方力量对比悬殊，更重要的是，防御方往往需要全面防守，一着不慎则满盘皆输；攻击方只需要单点成功突破，借助内网横向渗透手段，就可以在企业网络环境中肆无忌惮地获取所需资源。另外，“敌在暗，我在明”，防御者往往无法及时发现、分析、处置网络安全事件，只能在安全事件发生后，被动响应，收拾残局。假设防御方能够有效地部署网络安全监控产品，全面地收集网络数据，准确地检测安全威胁，深入地分析调查安全事件出现的原因，就可以及时发现防御工事的脆弱之处，有针对性地调整防御策略。

本书全面地介绍了网络安全监控“收集、检测、分析”各环节的技术要点。对于一些关键步骤，作者结合大量的实战案例，详细地讲解具体操作方法。即使是初学者，也可以在本书的指导之下轻松上手。对于具有一定基础的分析人员，书中提供了大量的实用脚本和公共网络资源，以及作者根据多年实战经验总结出的若干最佳实践。虽然这是一本专业性较强的技术书籍，但作者行文生动活泼、语调轻松诙谐，读起来饶有趣味。

值得一提的是，在本书第 12 章“使用金丝雀蜜罐进行检测”中，作者介绍了蜜罐文档（Honeydoc）的使用方法，这是一个简便易行的攻击者溯源的技术手段，能够以极低的实施成本，在一定程度上对网络安全事件作出预警，甚至可以辅助定位到攻击者。在 2015 年度中国互联网安全大会（ISC2015）的“APT 与新威胁论坛”中，我曾在相关议题中介绍了作者提出的这种思路。另外，在本书第 15 章“分析流程”中，作者创造性地将刑侦调查和医学诊断这两套分析模型应用于网络安全事件的分析中。这两个模型的引入，将原本错综复杂的分析方法解释得通俗易懂。

由于译者水平有限，译文中难免存在纰漏，恳请读者批评、指正。读者在阅读本书的过程中，如果对译文有任何意见或建议，或者对书中（尤其是对检测、分析这两部分的内容）提及的技术手段、实现方法有什么想法或思路，欢迎给我发邮件：libaisong@antiy.cn，或通过我的新浪微博“@ 安天李柏松”深入交流。

最后，感谢家人给我的支持，感谢安天的同事们给我的帮助，感谢吴怡编辑和合译者燕宏给我的鼓励。

李柏松

2015 年 10 月 25 日于哈尔滨

作者简介 *About the Author*

Chris Sanders，第一作者

Chris Sanders 最初是肯塔基州 Mayfield 的一名信息安全顾问、作家和研究员。那个无名小镇距离一个叫 Possum Trot 的小镇西南方向 30 英里，距离一条叫 Monkey's Eyebrow 的公路东南方向 40 英里，刚好位于道路的拐弯处。

Chris 是 InGuardians 的高级安全分析师。他有支持多个政府、军事机构以及财富 500 强企业的丰富经验。在美国国防部的众多角色中，他有效地促进了计算机网络防御服务提供商（CNDSP）模型的角色作用，协助创建了多种 NSM 模型以及多款目前在用智能化工具，以保卫国家的利益不受侵害。

Chris 曾撰写了多本书籍和学术文章，其中包括国际畅销书《 Practical Packet Analysis 》，目前已发布了第 2 版。Chris 目前拥有多项业界认证，包括 SANS、GSE 以及 CISSP。

2008 年，Chris 创立农村科技基金（RTF）。RTF 是一个 501(c)(3) 非营利组织，为来自农村地区攻读计算机技术学位的学生提供奖学金机会。该组织还通过各种支持计划促进了技术在农村地区的宣传。RTF 目前已为农村学生提供成千上万美元的奖学金和帮助支持。

当 Chris 不埋头于数据包分析的时候，他喜欢观看肯塔基大学野猫篮球队的比赛，擅长 BBQ（美国真人秀节目），业余无人机制作爱好者，在海滩上消磨时光。Chris 目前与他的妻子 Ellen 居住在南卡罗来纳州的 Charleston。

Chris 的博客地址为 http://www.appliednsm.com 和 http://www.chrissanders.org。他的推特账号为 @chrissanders88。

Jason Smith，合著者

Jason Smith 白天是一名入侵检测分析师，晚上则是一名垃圾场工程师。起初来自于肯塔基州的 Bowling Green，作为一名有潜质的物理学家，Jason 以大数据挖掘和有限元分析为切入点开始他的职业生涯。偶然的运气，对数据挖掘的热爱将他引向了信息安全和网络安全监控，

一个让他痴迷于数据处理和自动化的领域。

Jason 有很长一段时间都在帮助州和联邦机构强化他们的防御功能，现在在 Mandiant 担任安全工程师。在部分开发工作中，他创建了诸多开源项目，很多已成为 DISA CNDSP 计划的最佳实践工具。

Jason 经常在车库里度过周末，从街机柜到开轮式赛车，他都可以建造。其他爱好诸如家居自动化、枪械、大富翁游戏、吉他以及美食。Jason 对美国乡村有着深沉的爱，热衷于驾驶，同时对学习有着孜孜不倦的欲望。Jason 现在生活在肯塔基州的 Framkfort。

Jason 的博客地址为 http://www.appliednsm.com。他的推特账号为 @automayt。

David J. Bianco，贡献者

David 在 Mandiant 担任一名狩猎团队领导之前，花了 5 年的时间为一个财富 500 强企业建设了一套智能驱动的检测响应系统。在那里，他为一个部署了近 600 个 NSM 传感器覆盖超过 160 个国家的网络设置了检测策略，主导响应了一些国家遭受到的最严重的针对式攻击事件。他在安全社区、博客、演讲和写作上持续活跃着。

他经常在家看《 Doctor Who 》节目，或演奏他的四套风笛，或与孩子们一起玩耍。他还喜欢在除了海滩之外的任何地方长走。

David 的博客地址为 http://detect-respond.blogspot.com。他的推特账号为 @DavidJBianco。

Liam Randall，贡献者

Liam Randall 是旧金山 Broala LLC（Bro 核心团队专家组）的首席合伙人。最初，他来自于肯塔基州的 Louisville，在 Xavier 大学以系统管理员角色为学校工作，同时也获得了学校的计算机科学学士学位。在那里，他第一次开始了设备驱动安全编程和基于 XFS 的自动柜员机软件研发。

目前他正为财富 500 强企业、研究机构和教育网络、军队服务分支、其他安全焦点小组提供高容量安全解决方案咨询。他曾在 Shmoocon、Derbycon 和 MIRcon 等会议做过演讲，并经常在安全事件上做 Bro 训练班的培训。

作为一名丈夫和父亲，Liam 在周末时做发酵酒，在他的花园里工作，修理小工具，或制作奶酪。作为一名户外运动爱好者，他和他的妻子喜欢铁人三项，长距离游泳，享受他们的社区活动。

Liam 的博客地址为 http://liamrandall.com/。他的推特账号为 @Hectaman。

序 言 *Preface*

学习如何建设与运营一个网络安全监控基础设施是一项艰巨的任务。Chris Sanders 和他的团队制定了 NSM 的框架，为读者编纂了一个将网络安全监控付诸实践的有效计划。

大中型组织正面临令人崩溃的大量数据。面对着某些情况下过亿的事件量，有一个可扩展的监控框架和标准化运营流程是当务之急。

寻找即寻见，反之亦然。数据收集工作本身没有太大意义，甚至对检测环节来说很可能也一样，而分析工作却非常重要。这本书将给你一把钥匙，打开 NSM 的大门，展示其中的每一步骤：收集、检测和分析。

在 20 世纪 30 年代末期，许多民间飞行员主张使用他们的技能来捍卫国家。如今，民间组织积极投身保卫国家的时代再次到来。我们常常无故遭到攻击，制造业、化工业、石油和天然气行业、能源业以及我们社会中许多重要领域，在一系列有协作有计划的攻击中首当其冲。当专家们已在思考未来爆发网络战争的可能性时，身处一线的从业者们仍对其重视不足。

当然，我不是在宣扬战争，而是想强调分析的重要性。你的系统被 root 提权了？那么你必须分析你的日志。大多数网络攻击会留下痕迹，这得靠每一个系统管理员对入侵迹象做日志审查。尽管如此，管理员查看日志大多数是为了提升系统性能和商业分析。单单提升系统性能就可以帮助企业获得投资上的回报，而正手上的商业分析就更加不用说了，能为企业带来的价值无法估量。

在 InGuardians 公司，我们常被叫去响应网络安全事故以防止大规模数据破坏。大多数组织现在通常是从核心网络的设备、代理、防火墙、系统和应用中保存了相关数据，这些数据已存储了相当长的一段时间，看不到明显的投资回报率。在大多数情况下，我们通过独立的日志分析就可以识别出现在或过去发生的数据泄漏事件。

当你在你的控制台上回溯一些日志时，可能会手足无措地想：“我不知道要寻找些什么”。请立足于你所知道的，所理解的，不要再去想其他，勇敢面对，一切都将是有趣的。

Semper Vigilans

Mike Poor

Preface 前 言

我喜欢抓坏人。当我还是个小孩子的时候，就想以某些方式抓住坏人。例如，就近找一条毛巾披上作斗篷，与小伙伴们满屋子跑，玩警察抓小偷的游戏。长大后，每当看到为百姓伸张正义，让各种坏蛋得到应有的惩罚，我都特别开心。但不管我多努力去尝试，我的愤怒也无法让我变成一个绿巨人，不管我被多少蜘蛛咬了，我也无法从我的手臂里发射出蜘蛛网。我也很快意识到我并不适合做执法工作。

自从认识到这个现实，我意识到我没有足够的财富建一堆华丽的小工具，并身着蝙蝠衣在夜里绕飞巡逻，所以我结束了一切幻想，将我的注意力转向了我的电脑。事隔多年，我已走出了童年梦想中想活捉坏蛋的角色，那已不是我最初想象的那种感觉。

通过网络安全监控（NSM）的实战抓住坏人，这也是本书的主旨。NSM 是基于防范最终失效的原则，就是说无论你在保护你的网络中投入多少时间，坏人都有可能获胜。当这种情况发生时，你必须在组织上和技术上的位置，检测到入侵者的存在并及时做出响应，使事件可以得到及时通报，并以最小代价减小入侵者的破坏。

“我要怎样做才能在网络上发现坏人？”

走上 NSM 实践的道路通常始于这个问题。NSM 的问题其实是一种实践，而这个领域的专家则是 NSM 的实践者。

科学家们通常被称作科技领域的实战者。在最近的上世纪 80 年代，医学上认为牛奶是治疗溃疡的有效方法。随着时间的推移，科学家们发现溃疡是由幽门螺旋杆菌引起的，而奶制品实际上会进一步加剧溃疡的恶化[⊖]。虽然我们愿意相信大多数科学是准确的，但有时不是这样。所有科学研究是基于当时可用的最佳数据，当随着时间的推移出现新的数据时，老问题的答案就会改变，并且重新定义了过去曾经被认为是事实的结论。这是医学研究的现实，也是作为 NSM 从业者面对的现实。

遗憾的是，当我开始涉猎 NSM 时，关于这个话题并没有太多参考资料可用。坦白地说，

⊖ Jay, C.（2008, November 03）. Why it's called the practice of medicine. 见 http://www.wellsphere.com/chronic-pain-article/why-it-s-called-the-practice-of-medicine/466361

现在也没有。除了行业先驱者们偶尔写的博客以及一些特定的书籍外，大多数试图学习这个领域的人都被限制在他们自己设备的范围内。我觉得这是一个合适的时机来澄清一个重要误解，以消除我先前说法的潜在疑惑。市面上有各式各样的关于 TCP/IP、包分析和各种入侵检测系统（IDS）话题的书籍。尽管这些书本中提及的概念是 NSM 的重要方面，但它们并不构成 NSM 的全过程。这就好比说，一本关于扳手的书，会教你如何诊断汽车，但不会教你如何启动。

本书致力于阐述 NSM 的实践。这意味着本书并不只是简单地提供 NSM 的工具或个别组件的概述，而是将讲解 NSM 的流程以及这些工具和组件是如何应用于实践的。

目标读者

本书最终将作为执业 NSM 分析师的指南。我每天的职责也包括对新分析师的培训，因此本书不仅为读者提供教育素材，也为培训过程提供支持性教材。既然如此，我的期望是读者们能将本书从头到尾阅览，对成为一名优秀分析师的核心概念能有入门级的掌握。

如果你已经是一名执业分析师，那么我希望本书将为你打下一个良好基础，让你可以增强分析技能，提升现有的工作效率。目前我已与数名优秀分析师共事，他们将成长为伟大的分析师，因为他们可以用本书中提及的一些技术和信息去提高他们的效率。

NSM 的有效实践需要对各类工具有一定程度的熟练运用。因此，本书将会讨论到数款工具，但仅限于从分析师的立场去讨论。当我讨论 Snort IDS、SiLK 分析工具集或其他工具时，那些负责安装维护这些工具的人会发现我并不会很长篇大论地讲这些过程。但在有需要的时候，我会将其他相关资源补充进来。

此外，本书完全专注于免费和开源工具。这不仅是为了吸引更多可能没有预算来购买诸如 NetWitness、Arcsight 等商业分析工具的人，也是为了展示使用基于开源分析设计的工具带来的内在优势，因为它们在数据交互的过程能够提供更高的透明度。

所需基础知识

最成功的 NSM 分析师在开始安全相关工作之前，通常在其他信息技术领域已经拥有丰富的经验。这是因为他们已经具备了作为一名分析师的其他重要技能，比如对系统、网络管理的理解。如果没有这样的经历，建议阅读一些书，我罗列了一份我十分喜爱的主要书籍清单，我认为这些书能够帮助读者深入了解一名分析师必备的重要技能。我已尽了最大努力，让读者在不需要太多基础知识的前提下阅读本书。但如果读者感兴趣，我强烈推荐阅读部分书籍作为本书的补充。

- 《TCP/IP 详解，卷 1，协议》，作者 Kevin Fall 和 Dr. Richard Stevens（Addison Wesley 出版社，2011）。对 TCP/IP 的核心理解是让 NSM 更加有效的重要技能之一。早期 Dr. Richard Stevens 的经典文著已经被 Kevin Fall 更新，增加了最新的协议、标准、最佳实践、IPv6、协议安全，等等。

- 《The Tao of Network Security Monitoring》，作者 Richard Bejtlich（Addison Wesley 出版社，2004）。Richard Bejtlich 帮助定义了很多概念，这些概念奠定了 NSM 实践的基础。基于这样的事实，我在整本书中会经常引用他的书或博客的内容。尽管 Richard 的书已经有将近 10 年的历史，但书中的许多材料仍然使它成为 NSM 范畴内相关文案。
- 《Practical Packet Analysis》作者 Chris Sanders（No Starch Press 出版社，2010）。我不是王婆卖瓜。鉴于 Dr. Stevens 的书已为 TCP/IP 协议提供全面深入的阐述，这本书则是使用 Wireshark 作为首选工具从实践层面讨论数据包分析。我们在书中讲述如何做数据包检测，如果你之前从未看过数据包，我建议你将此书作为基础。
- 《Counter Hack Reloaded》作者 Ed Skoudis 和 Tom Lison（Prentice Hall 出版社，2006）。我一直认为这本书绝对是最佳常规安全书籍之一。它覆盖的范围非常广，我向任何经验级别的读者都推荐此书。如果你从未做过安全相关的工作，那么我会说《Counter Hack Reloaded》是必读的一本书。

本书的组织

本书划分成三部分：收集、检测和分析，每章重点讨论相关的工具、技术和核心领域流程。我是一个来自肯塔基州的普通乡村男孩，所以我将尽我所能地用一种不加太多修辞的简单基调来阐述。我也将尝试引入典型的先进概念，并尽可能把它们分解成一系列可重复的步骤。正如任何书籍阐述广义概念一样，当一个概念被提出时，请记住，它并不会覆盖每一种可能的场景或边缘案例。尽管我可以举出一些案例作为一个最佳实践，但本书最终构建的理论是基于集体研究、经验以及合著者的观点。因此，可能会有这样的场景，你的研究、经验和观点导致你对提及的话题有不同的结论。这是完全正常的情况，这就是为什么 NSM 是一门实践。

第 1 章：网络安全监控应用实践 这章专门定义了网络安全监控和它在现代安全环境的相关性。它讨论了很多整本书将会用到和引用到的核心术语和假设。

第一部分：收集

第 2 章：数据收集计划 这是 ANSM 收集部分的第 1 章，介绍了数据收集和它的重要性。本章将介绍数据收集实施框架，它使用一种基于风险的方法来决定哪些数据应该被收集。

第 3 章：传感器平台 这章介绍 NSM 部署中最重要的硬件组成：传感器。首先，我们对 NSM 的各类数据类型和传感器类型做简要概述。接着，引出讨论购买和部署传感器的重要考虑因素。最后我们将谈及 NSM 传感器在网络上的位置，包括创建网络可视化地图分析的入门。

第 4 章：会话数据 该章讨论会话数据的重要性，同时详细介绍用于收集 NetFlow 数据的 SiLK 工具集。我们还将就会话数据的收集和解析对 Argus 工具集进行简要分析。

第 5 章：全包捕获数据 该章开头对全包捕获数据的重要性作概述。接着分析了几款允

许全包捕获 PCAP 数据的工具，包括 Netsniff-NG、Daemonlogger 和 Dumpcap，引出对 FPC 数据存储和保存计划，包括裁剪 FPC 数据存储数量不同考虑因素的讨论。

第 6 章：包字符串数据 该章介绍了包字符串数据（PSTR）以及它在 NSM 分析过程里的有效性。我们将介绍几种生成 PSTR 数据的方法：使用工具 Httpry 和 Justniffer，我们还将了解用于解析和查看 PSTR 数据的工具：Logstash 和 Kibana。

第二部分：检测

第 7 章：检测机制、受害信标与特征 该章讨论检测机制与妥协指标（IOC）之间的关系。我们介绍 IOCs 是如何被逻辑组织，以及它们是如何被纳入到 NSM 计划进行有效管理的。这里面将会包含对指标分类的系统，以及部署在各种检测机制里的，用于计算和跟踪指标精确度的度量。我们也将看到两种不同格式的 IOC ：OpenIOC 和 STIX。

第 8 章：基于信誉度的检测 该章将讨论第一种特定类型的检测：基于信誉度的检测。我们将讨论基于信誉度检测的基本原理，以及一些分析设备信誉度的资源。此次讨论将倾向于过程自动化的解决方案，并演示了如何使用简单 BASH 脚本，或通过使用 Snort、Suricata、CIF 或 Bro 来完成这一过程。

第 9 章：基于 Snort 和 Suricata 特征的检测 基于特征的检测是入侵检测最传统的方式。本章将介绍这种检测类型的入门，并讨论入侵检测系统 Snort 和 Suricata 的使用方法。这里面包含 Snort 和 Suricata 的用法，以及为两种平台创建 IDS 特征的详细讨论。

第 10 章：Bro 平台 该章将介绍 Bro，比较流行的基于异常的检测解决方案之一。本章将综述 Bro 的架构、Bro 语音和几个实际案例，来演示 Bro 作为一款 IDS 和网络记录引擎真正惊人的威力。

第 11 章：基于统计数据异常的检测 该章将讨论使用统计数据进行网络异常识别。这将侧重于使用各种 NetFlow 工具，如：rwstats 和 rwcount。我们将讨论使用 Gnuplot 和谷歌画图 API 进行可视化统计的方法。本章将提供几个能从 NSM 数据中生成有用统计的实际案例。

第 12 章：使用金丝雀蜜罐进行检测 金丝雀蜜罐以前仅用于研究目的，现在却是一种能用于有效检测的操作型蜜罐工具。本章将提供不同类型的蜜罐概况，以及什么特定类型能在 NSM 环境中被应用。我们将介绍几款能用于监控用途的流行蜜罐应用程序，如：Honeyd、Kippo 和 Tom's Honeypot。我们也将简要讨论 Honeydocs 的概念。

第三部分：分析

第 13 章：数据包分析 这是 NSM 分析师最重要的技能，是具备解读和解密关键网络通信数据包的能力。为了有效做到这一点，需要对数据包是如何被分割有个基本的了解。该章将为读者提供基础支持，并说明如何逐字节单位地分解数据包字段。我们通过使用 tcpdump 和 Wireshark 来证实这些概念。该章也将通过使用 Berkeley 包过滤器和 Wireshark 显示过滤器来介绍高级包过滤技术的基础。

第 14 章：我方情报与威胁情报 我方情报与威胁情报的生成，能够影响事件调查的好坏。

本章首先介绍了传统的情报循环如何用于 NSM。紧跟着，介绍通过网络扫描产生资产数据和扩充 PRADS 数据来生成我方情报的方法。最后，我们将分析威胁情报的种类并讨论关于敌对主机的战略威胁情报研究的几个基本方法。

第 15 章：分析流程 最后一章讨论整体的分析过程。开始只是讨论分析过程，后来分解成两个不同的分析过程：关系调查和鉴别诊断。紧跟着，讨论了从失败的事件中学到的教训过程。最后，我们以几个最佳分析实例来结束本书。

IP 地址免责声明

在本书中，提及的例子、原始数据和截图中涉及一些 IP 地址。在这些案例中，除非另外指明，这些 IP 地址已被各种工具随机化。因此，任何引用涉及某个组织的任意 IP 地址，纯属巧合，绝不代表是由那些实体产生的实际流量。

本书配套网站

还有相当多的东西我们想在本书中介绍，但我们根本找不到地方容纳进来。于是，我们创建了一个配套网站，包含不同 NSM 话题的各种额外想法，以及代码片段、技巧和窍门。如果你喜欢本书内容，那么可以考虑查阅配套网站 http://www.appliednsm.com。虽然在本书完成出版前本站点并没有太多的更新，我们计划在本书发行后定期更新这个博客。本书的任何勘误也将在这里持续更新。

慈善支持

我们很自豪地声明，本书所得版税将 100% 捐赠出去，用于支持以下五个慈善事业。

农村科技基金

农村学生，特别是那些成绩优异的、接触到技术的机会通常会比他们在城市或城郊的同行少。2008 年，克里斯·桑德斯创立了农村科技基金（RTF）。RTF 的主旨是减少农村社区与他们的城市和城郊同行之间的技术鸿沟，方法是通过有针对性的奖学金计划、社区参与，以及在农村地区全面推广和宣传技术。

我们的奖学金是针对那些生活在农村社区、对计算机技术拥有热情并打算在这个领域继续深造的学生。本书版税的一部分将用于支持这些奖学金计划，并提供树莓派计算机给农村学校。

更多信息请参见：http://www.ruraltechfund.org

黑客慈善组织（HFC）

由 Johnny Long 创立，HFC 雇佣黑客志愿者（无条件），让他们从事于短暂的“微型项目”，旨在帮助那些无法提供传统技术资源的慈善机构。除此之外，HFC 也在乌干达、东非地区支持援助组织帮助世界上最贫穷的公民。他们提供免费的电脑培训、技术支持、网络服务等。

他们已经帮助许多当地学校增设电脑和培训软件。此外，HFC 还通过他们的食物计划为东非的儿童们提供食物。

更多信息请参见：http://www.hackersforcharity.org

Kiva

Kiva 是第一个允许通过多领域公司直接捐钱给发展中国家人们的在线借贷平台。Kiva 记录了每一个需要贷款的人的个人故事，让捐赠者能够直接联系他们。简单地说，Kiva 方便了改变生活的借贷。该基金的捐赠来自于本书的销售所得，并为有需要的人提供这些贷款。

更多信息请参见：http://www.kiva.org

Warriors 希望工程

Warriors 希望工程（Hope for the Warriors）的任务是提升后 911 服役人员的生活品质，包括他们的家人，以及那些曾在工作岗位上因持续的生理和心理创伤而倒下的家庭。Warriors 希望工程致力于恢复自我意识，恢复家庭单位，以及恢复我们的服务人员和我们的军人家属对生活的希望。

更多信息请参见：http://www.hopeforthewarriors.org

自闭症演讲组织

自闭症是一种非常复杂的病症状态，患者在社交互动、沟通、重复的行为上均存在不同程度的困难。美国疾病控制中心估计，88 个美国儿童当中会有 1 个存在某种形式的自闭症。自闭症演讲组织是一个致力于改变那些与自闭症作斗争的患者们的未来的组织。他们通过为生物医学研究提供资金来做到这一点，研究的范围涉及自闭症的病因、预防、治疗和治愈。自闭症演讲组织也提供自闭症宣传，以及为自闭症患者的家庭提供支持。

更多信息请参见：http://autismspeaks.org

联系我们

我和我的合著者们投入了大量的时间和精力在本书上，所以当我们听到有人读过我们的书并想分享他们的想法时，我们总是很兴奋。无论你想在什么时候联系我们，你可以把所有问题、意见、威胁和婚姻的建议直接发给我们，我们的联系方式如下：

Chris Sanders, 第一作者

E-mail: chris@chrissanders.org

Blog: http://www.chrissanders.org; http://www.appliednsm.com

Twitter: @chrissanders88

Jason Smith, 合著者

E-mail: jason.smith.webmail@gmail.com

Blog: http://www.appliednsm.com

Twitter: @automayt

David J. Bianco，贡献者

E-mail: davidjbianco@gmail.com

Blog: http://detect-respond.blogspot.com/; http://www.appliednsm.com

Twitter: @davidjbianco

Liam Randall, 贡献者

E-mail: liam@bro.org

Blog: http://liamrandall.com; http://www.appliednsm.com

Twitter: @liamrandall

致谢

《哥林多后书》第 12 章节如是说："但他对我说，'我的恩典够你用的，因为我的能力是在人的软弱上显得完全。'因此，我更喜欢夸自己软弱，好让基督的能力庇佑我"。

写这本书的过程简直证明了上帝的力量对人性弱点的完善。本书是我曾经参与的最困难的项目之一，对上帝的信念让我能够最终坚持下来。因为上帝，这本书以及我所做的一切都是可能的，我真诚地希望我的这次工作可以作为上帝神奇力量的见证。

这本书之所以能完成，离不开许多朋友直接或间接的帮助。我想借此机会感谢他们。

Ellen，你是我的挚爱，我的后盾，我的力量，也是我的头号粉丝。没有你，这一切是不可能成功的。我要感谢你曾经承受过的压力与绝望，以及本书写作过程中那些疯狂的日日夜夜。同时我还想感谢你帮助修改本书。我想，你的英语专业终于派上了用场。我爱你，成为你的丈夫我感到很自豪。

爸爸妈妈，在你们的影响下成长，使我成为一个独特的人。作为子女我所能做的将会继续坚持，传承你们赋予的性格并分享你们给予的爱。我爱你，爸爸；我也爱你，妈妈。

我的家庭，尽管我们只是一个小团体，我们之间分享的爱却是浓厚的，这对我来说太重要了。虽然我们相距甚远，但我知道你们爱着我并支持我，我很感激这一点。

Perkins 的家庭，感谢你积极地让我走入你的生活，我很幸运，有你的爱和支持。

Jason Smith，毫不夸张地说，你是我遇到过的最睿智的人，与你相处非常愉悦。你不止是一个伟大的同事和合着者，你更是一个久经考验的朋友。我可以毫不犹豫地说，你已经是我的兄弟。我永远感激这一切。

David Bianco 和 Liam Randall，我已经不知道怎么感谢你们对本书的巨大贡献。你们的贡献价值实际已远远超出你们的想象。

至于我的同事（过去的和现在的），我一直认为，如果一个人周围都是好人，他会成为一个更好的人。很幸运我在公司工作中能够与一些优秀、正直的人共事。我要特别感谢我的 InGuardians（公司名）大家庭：Jimmy、Jay、Suzanne、Teresa、John、Tom、Don、Rad、

Larry、Jaime、James、Bob 和 Alec。我还想感谢 Mike Poor，是他为本书写的序言，他也依然是我心目中的数据包忍者偶像之一。

Syngress 的工作人员，谢谢你们让我有机会写成这本书，并帮助我将这个梦想变成现实。

本书的技术内容和方向涉及的领域可能超出了我的认知能力，但我会尽力做到最好。除了上面提到的亲朋好友，我还要感谢以下人员作出的贡献，是他们协助对每个章节做了细致的审查，让我从他们身上获得不少好的创作灵感，本书的成功离不开他们的支持，人员罗列如下（排名不分先后）：

Alexi Valencia、Ryan Clark、Joe Kadar、Stephen Reese、Tara Wink、Doug Burks、Richard Bejtlich、George Jones、Richard Friedberg、Geoffrey Sanders、Emily Sarneso、Mark Thomas、Daniel Ruef、CERT NetSA 团队的其他成员、Joel Esler、Bro 团队、Mila Parkour、Dustin Weber、and Daniel Borkmann。

Chris Sanders

Contents 目 录