HZ BOOKS
华章IT
no starch press

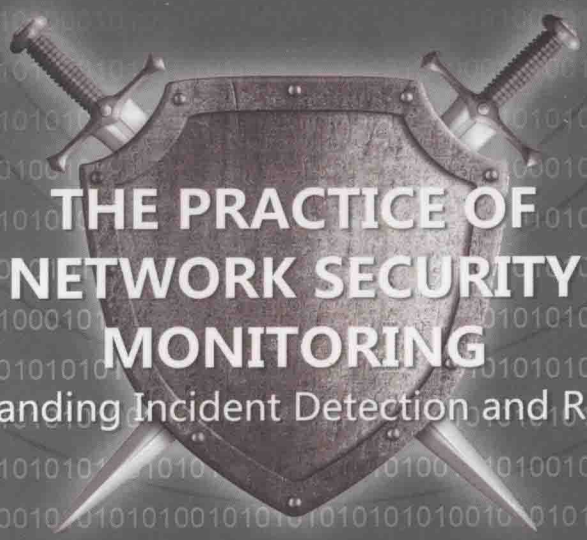
信息安全
技术丛书

- 全球顶尖安全公司FireEye首席安全战略官、Mandiant公司首席安全官撰写，深入解读网络安全监控的核心思想、工具和最佳实践
- 从网络安全监控的原理、工具选型、环境部署到攻击的识别、发现与截击，系统且全面地讲解网络安全监控的主流工具，帮助你有效检测和响应网络入侵

网络安全监控实战

深入理解事件检测与响应

[美] 理查德·贝特利奇（Richard Bejtlich）著 蒋蓓 姚领田 李潇 张建 译



THE PRACTICE OF NETWORK SECURITY MONITORING

Understanding Incident Detection and Response

机械工业出版社
China Machine Press

网络安全监控实战

深入理解事件检测与响应

[美] 理查德·贝特利奇（Richard Bejtlich）著 蒋蓓 姚领田 李谦 张建 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络安全监控实战：深入理解事件检测与响应 /（美）贝特利奇（Bejtlich，R.）著；蒋蓓等译．
—北京：机械工业出版社，2015.4
（信息安全技术丛书）
书名原文：The Practice of Network Security Monitoring：Understanding Incident Detection and Response

ISBN 978-7-111-49865-0

I. 网… II. ①贝… ②蒋… 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 067987 号

本书版权登记号：图字：01-2014-3563

网络安全监控实战：深入理解事件检测与响应

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：高婧雅　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2015 年 4 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：18.5
书　　号：ISBN 978-7-111-49865-0　　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）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

The Translator's Words 译 者 序

安全是一个动态过程，充其量是过程中攻与防的暂时平衡，而不是一种持续存在的状态。在企业安全周期中，它在不停地被打破、重建，再打破、再重建，攻守双方围绕各自的目标开展针锋相对的较量。然而，“千里之堤毁于蚁穴”、“短板效应”的训诫决定了入侵者具有天生的优势。攻在暗，只需渗透一个点；防在明，需要防护一个面，任何不重视每一个细节的安全人员都可能在本已可怜的夹缝中打包走人。外有强行入侵者，内有规则破坏者，内忧外患并存，究竟是谁把木马带进了固若金汤的城堡？

当今社会，企业网络安全还没有引起足够的重视，从人力配备到资金投入，从话语权到政策，都得不到足够的支持，这也正是网络安全事件层出不穷的现实基础之一。从另一个层面看，策划、研发、市场直至企业的保洁人员都有可以量化评定的业绩，安全人员的工作仍无可量化的方法或度量的标准。在这样的环境中，成功阻止入侵的次数可以用来判定安全人员工作的优劣吗？网络安全的确不能为企业带来直接收益，但它或许可以成就你的竞争对手，甚至为你带来最直接、最致命的危害。从企业高层到普通职员，都应深刻认识到这一点。虽然没有哪个企业因网络安全防护做得好而蒸蒸日上，但远不乏因网络安全事件导致企业关门破产的案例。尤其在实名制大背景下的私人信息安全，更成了每个人不容忽视的问题。

智者驾驭工具，愚者役于工具。工具主义者认为花大价钱购置一大批盒式设备，搭积木似地堆在网络中，就可以高枕无忧了，事实上这些很可能只是提供了一种虚假的安全感。他们看不到方法在安全模型中的作用，方法是构建模型的基石，是安全策略的组成元素。只有把策略应用于设备和工具，它们才能得以新生，才能发挥出应有的作用，这也是作者一再强调的一个重要方面。就像每个人都有优缺点一样，每种工具也都有自己的专长和不足，要想真的驾驭工具，能在面对不同的任务时选择适合自己的工具，除了掌握各种工具的使用方法和增强工具效率的技巧外，还要了解它们的实现原理，比较其技术优劣。在这种基础上，才能用其所长、避其所短，发挥出它的最大效益。因此，作者也在书中详细介绍了一些主流监

控工具的优缺点，以供读者在需要时做出科学的选择。

作者认为以检测为中心的哲学核心是防护，但终将会失败，也就是说安全破坏不可避免。但是，请各位读者改变审视入侵的方式，防御者尽管无法规避破坏，然而最终将会阻止入侵者，换句话说，志坚意决的入侵者最终会突破你的安全防护，但他们或许不能实现预期的目标。CIRT 要做的是，在入侵者实现其目标之前阻止他们，从入侵者未能达成目标的角度来看，GIRT 就是赢家。译者认为这种哲学核心才是本书最具启蒙性的思想。希望企业高层、安全管理人员及普通职员都能认识到这一点，从而改变对安全破坏的认识，采取有效的措施，最大程度地降低威胁，减少安全事件造成的危害程度。

除封面署名译者蒋蓓、姚领田、李潇、张建以外，参加本书翻译的还有朱曾志、李石、王少刚、张振顶、姚晓玉、王建国、贺丹、于伟华、郑永、高守传、姚金凤等，全书由姚领田进行技术审校。感谢本书的编辑们，是他们的热情和激励促使我顺利完成了全书的翻译。尤其要感谢张振顶先生及他的家人，他们对我的关心、指导和影响，我始终铭刻在心。

最后，感谢我的妻子。她是 70 后的尾巴尖，具有 70 后女子典型的美德：勤劳善良、娴淑典雅，还兼具 80 后女性的知性之美、独立率性。是她带给了我的女儿和我无限的幸福，以此译作献给她。

在翻译过程中，译者完整保留了原作者的称谓、举例和观点，但这并不代表译者支持或认可这些观点，请读者在阅读过程中注意甄别。由于水平有限，在翻译中难免出现一些问题，恳请读者批评指正。

姚领田

湖南·宁乡

Preface 序

这或许是你读过的最重要的书籍之一。网络安全是既涉及国家安全又涉及经济安全的问题，每天网络空间都在进行着秘密的斗争。对我们的安全和幸福至关重要的基础设施（譬如电网）正在遭受着攻击，关乎我们经济繁荣的知识产权也正在被迅速地“吸出”（suck out）。大大小小的公司时常处在数字世界的风险之中。

正是矛盾的这种全民化使得本书显得如此重要。借用老生常谈的说法：如果你的组织不是解决方案的一部分，那么它就是问题的一部分。保护你的组织，阻止它被利用来攻击你的供应商、合作伙伴、客户以及世界上的其他组织。而且，通过检测攻击，你可以提醒其他人或组织，避免它们遭受同样技术或同一入侵者的攻击。

很少有人或组织被号召保护他们的国家免受传统恐怖主义攻击或者军事侵犯，但是在网络空间并非如此。阅读本书不会把你的团队变成专业网络安全防护组织，但是它提供了增强安全态势的知识，使你的组织或世界变得安全一点。

在 1986 年 8 月，一个 75 美分的账目错误导致了网络安全监控行业的诞生。1988 年，Cliff Stoll 在其论文“ Stalking the Wily Hacker”以及后来的《 The Cuckoo’s Egg》（杜鹃蛋）一书中记述的那样，他被要求找出该组织的两个会计系统中不一致的原因。接下来他就过上了对国际间谍多年调查的奇幻历险生活，在此期间，他曝光了攻击者和防御者使用的技术，这些技术在今天仍然有重要意义。

Stoll 的对手攻击的其中一个站点是劳伦斯 - 利弗莫尔国家实验室（Lawrence Livermore National Laboratory，LLNL）。同时，像优秀的管理者经常做的那样，LLNL 的一个管理者借此获得了资金资助的机会。1988 年，LLNL 在三种网络安全工作上获得资金支持：反病毒软件、“安全概要检测程序”（Security Profile Inspector）应用软件，以及一个基于网络的入侵检测系统，该系统被称作网络安全监控器（Network Security Monitor，NSM）。在这些领域中，LLNL 没有太多的经验，于是向加利福尼亚大学戴维斯分校的 Karl Levitt 教授求助，在

LLNL 启动资金的支持下，创立了加利福尼亚大学戴维斯分校计算机安全实验室（UC Davis Computer Security Laboratory）。据我所知，LLNL 管理者创造了网络安全监控器一词，但是让戴维斯分校来实现具体的思想[⊖]。

我在网络安全监控领域的最初工作记录于在 1990 年的题为“网络安全监控器”的论文中，类似于入侵检测中偏学术性的工作，这种入侵检测依赖基于统计分析的异常检测。但是随着时间的流逝，在拥有了操作经验以后，NSM 开始看起来越来越像 Cliff Stoll 从事的活动了。1988 年，Stoll 写道：“我们知道研究人员正在开发监视异常活动的专家系统，但是我们发现自己的方法比较简单、廉价而且或许更加可靠”。[⊜]

Stoll 将打印机附加到输入线路（line）上，这样他可以打印用户的活动，同时还能观察攻击者实际正在做的事情，我开发的“ transcript”程序是从网络包中产生基本相同的输出。NSM 对于验证可疑的活动实际上是否是一次入侵以及弄清攻击者的本性来说是完全必要的。

Stoll 及其同事 Lloyd Belknap 构建了一款逻辑分析程序，在串行线上运行它就能够寻找登录的特定用户，我向我们的网络监控器增加了字符串匹配代码以便查找关键字（登录默认账户的尝试、登录失败的消息、访问密码文件等）。

Stoll 还增加了自动的响应机制，当攻击者登录时，这种机制会提醒他，当攻击者过于接近敏感信息时会中断连接，并交叉关联来自其他站点的日志。多年之后，入侵检测系统中所有的特征都会变得类似。

到 1991 年，NSM 系统在实际检测和分析网络攻击方面的价值得到证明。我在加利福尼亚大学戴维斯分校定期使用它，LLNL 偶尔使用它（隐私方面是一个问题），很快美国空军和国防信息系统局（Defense Information Systems Agency，DISA）也在使用它。

然而，在某些方面，运行 NSM 系统变得有点令人沮丧。我能知道网络上有多少攻击者，却几乎没有人意识到正在发生的情况。实际的例子是，DISA 被召唤到一个地方，因为某种可疑的活动来自他们那里的拨号交换机。无独有偶，该组织正在预订一套具有较高性能的系统，因为当前的平台能力已经饱和。当 DISA 将其 NSM 传感器挂钩上之后，竟发现大约 80% 的连接都是来自攻击者，他们设备能力饱和的原因不是来自合法用户而是攻击者。

到 1992 年，NSM 系统（或许其他基于网络的监控器）的使用引起司法部的注意，但并非是以一种好的方式关注。然后，首席检察官助理 Robert S.Mueller III（我为本书作序时他担任 FBI 主管）向国家标准与技术研究院（National Institute of Standards and Technology，

⊖ “网络安全监控器”一词和 NSM 一样，现在一般用于描述基于安全的网络监控。然而，对我而言，在 20 世纪 90 年代早期，这些用于特指我的项目。在本书序中，我使用这些词和术语来特指我的项目的情况。

⊜ *Communications of the ACM* 31, no.5（May 1988）：484.

NIST）的 James Burrows 发送了一封信件，说我们在做的网络监控可能涉嫌非法窃听，因为使用类似 NSM 系统的工具，我们将面临欺诈和罪犯的指控。Mueller 鼓励 NIST 广泛地传播这封信件。

尽管引起了法律的关注，这个领域的工作仍以极快的速度持续进行。到 1993 年夏季，LLNL 向我发送一封邮件，告诉我停止分发 NSM 软件（他们想控制软件的分发），在此之后，我便开始缩减自己关于 NSM 的开发工作。LLNL 将其 NSM 软件拷贝重新命名为“网络入侵检测程序”（Network Intruder Detector，NID），空军将其拷贝重新命名为自动化安全事件测量（Automated Security Incident Measurement，ASIM）系统，DISA 将其系统重新命名为联合入侵检测系统（Joint Intrusion Detection System，JIDS）。到 20 世纪 90 年代晚期，空军已将 ASIM 推广到全球的约 100 个站点，并将其摘要整合到他们的通用入侵检测指示器（Common Intrusion Detection Director，CIDD）中。

同时，商业产品也涌现出来。到 20 世纪 90 年代晚期，Haystack 实验室（使用了由我们共同的 DIDS 工作开发的 NSM 软件）发布了名为 Net Stalker 的基于网络的 IDS，WheelGroup（由使用 ASIM 的空军人员组成）发布了 NetRanger，ISS 发布了 RealSecure，其他公司也竞相涌入了这个市场。

到 20 世纪 90 年代晚期，开源社区也以像 Snort 这样的系统涉足进来。到 21 世纪初期，一些小组开始建立企业“安全运行中心”（Security Operations Center，SOC），这些中心在很大程度上基于开源组件创建。当 Richard Bejtlich（另一位空军校友）为 Ball Aerospace & Technologies 公司建立了名为 NETLUMIN 的系统时，我结识了他。虽然很少有人听说过 NETLUMIN，但它的很多设计和概念留存了下来，而且在本书中会有所体现。

人们往往过于关注技术和产品，但是构建一种有效的事件响应能力涉及的内容远比安装工具需要的技术要多得多。关于如何最佳地使用这些工具，在过去 20 年的基础上已经积累了大量的知识。未能正确部署的技术可能迅速地变为运行这些技术的人的负担，甚至提供给人们虚假的安全感。例如，在 12 年以前，我正致力于 DARPA 项目，我们组成的团队正在进行一项任务，即将大量的网络安全工具汇集到一起。防御者已经安装了 3 种基于网络的 IDS 来监视他们的边界，但是攻击者使用从承包商那里窃取的凭证通过合法的 SSH 连接侵入。在攻击期间，没有 IDS 报警。这种情况最初令防御者出乎意料而且非常失望，但是它可以得当地指出基于网络的 IDS 边界监视检测技术和部署策略在防御上述攻击时存在的基本限制（我不确定程序管理者像我一样发现了如此精彩的具有教育意义的时刻）。

20 世纪 90 年代早期，当空军致力于分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）时，我们的程序管理者将系统的预期用户描述成“军士的甜甜圈袋子”

（Sergeant Bag-of-Donuts），预期若将“魔法箱子”（magic box）部署在网络上或者将一套软件部署在终端系统上，则组织的所有安全问题都将不复存在。安全公司的销售部门乐此不疲地推销“魔法箱子”，而且管理部门和投资者也常常买进。

产品和技术不是解决方案，它们只是工具而已，防御者（和组织的管理部门）需要明白这一点，没有闪亮的银弹可以解决所有网络安全问题。攻击也有生命周期，这些生命周期的不同阶段以不同的数据源形式留下不同的证据，使用不同的分析技术可以最佳地揭示和理解这些数据源。

组建一个明白这一点且知道如何有效地安置团队资产（包括工具、人员和时间），知道如何往返穿梭于不同的数据源和工具之间的团队（即使是一个人的团队），这对于创建有效的事件响应能力至关重要。

Richard Bejtlich 凭借自己的卓越能力而为人所知——从 1998 ~ 2001 年在 AFCERT 工作，到设计和部署系统，再到在 GE 组建一个大型的事件响应团队，最后到以首席安全官职位在世界上实力最强的信息安全公司之一工作。他丰富的经验使他对于事件响应问题有一种相对独特的历史观。虽然本书没有自称为“经验教训的”书，但是它清晰地提炼出作者大量的经验，他的这些经验都可以应用在实际工作中。

正如狡猾的黑客 Cliff Stoll 展示的那样，国际网络间谍已经出现了近 30 年，但是在最近 5 ~ 10 年，发生了一些根本性的转换。在过去，黑客行为主要被视为一种业余爱好，在很大程度上，黑客由于工作、结婚和建立家庭而放弃这种爱好。但是如今，个别黑客行为已成为一种职业途径，这也是我们写这本书的原因。

几乎未来的所有冲突——无论经济、宗教、政治还是军事，都将会包括网络元素。我们拥有的防御者越多，我们对他们的调遣越有效，我们大家就生活得越舒适。本书将有助于实现这种美好的愿望。

Todd Heberlein

网络安全监控器系统开发人员

写于加利福尼亚大学戴维斯分校

2013 年 6 月

Preface 前　言

网络安全监控（Network Security Monitoring，NSM）是关于收集、分析和增强预警（Indications and Warnings，I&W）以检测和响应入侵的技术。

——Richard Bejtlich 和 Bamm Visscher[⊖]

欢迎阅读本书。本书旨在帮助你使用以网络为中心的操作、工具和技术检测并响应数字入侵。我已试图使背景知识及理论需求保持最低水平，而且结合以往实践撰写此书。我希望本书改变你看待计算机安全或者力图影响的对象的方式。我的焦点不在于安全周期的规划和防御阶段，而在于处理已经被攻陷的或者处于被攻陷边缘的系统所采取的行动。

本书是我之前关于 NSM 作品的续篇和补充。

- 《The Tao of Network Security Monitoring：Beyond Intrusion Detection》（Addison-Wesley, 2005；832 页）。Tao 提供了背景、理论、历史以及案例研究来指导你的 NSM 操作。
- 《Extrusion Detection：Security Monitoring for Internal Intrusions》（Addison-Wesley, 2006; 416 页）。在阅读 Tao 之后，你会发现《Extrusion Detection》扩展了 NSM 架构（抵御客户端的攻击）的概念以及网络取证。
- 《Real Digital Forensics：Computer Security and Incident Response》与 Keith J.Jones 和 Curtis W.Rose 合著（Addison-Wesley, 2006; 688 页）。最后，RDF 说明了如何将 NSM 与以主机和内存为中心的取证整合，这可以使审查者调查绑定在计算机上的 DVD 中的犯罪证据。

本书会激发你的 NSM 行动，而且我的方法已经经过时间的检验。2004 年，我的第一本书就包含了我提倡的“以检测为中心”的哲学核心思想：防护终将失败。一些读者质疑这种

⊖ SearchSecurity webcast,December 4,2002(slides archived at *http://www.taosecurity.com/bijtlic visscher techtarget webcast 4 dec 02.ppt)*。

结论，他们认为如果“恰当地”综合应用防护、软件安全或者网络架构，阻止所有入侵还是有潜在可能性的。他们认为，如果你能够阻止攻击者对网络的非授权访问，那么检测就不必要。那些仍然信奉这种哲学的人很可能遭受某种长期、系统化的入侵，就如我们每周在媒体上看到的那样。

几乎在十年之后，安全行业和更加广泛的信息技术（IT）社区开始认识到，有决心的入侵者总能够找到危害其目标的方法。成熟的组织现在不仅试图阻止攻击者，还开始寻求快速检测攻击者，通过调查事件的影响程度来进行有效响应，同时，彻底牵制入侵者以限制其可能产生的危害。

殚精竭虑地看待企业安全是明智之举。事件响应不再是一件罕见、特别的事情，相反，它应当是具有确定度量和目标的持续商业过程。本书会提供一组数据、工具和使用网络的程序以便于你使用，同时它们可帮助你将安全操作转化成应对频繁遭受危害的利器。如果不知道上季度有多少次入侵使你的企业遭受折磨，或者不知道你能够多快地检测和控制这些入侵，本书将会向你展示如何实施这些活动并且跟踪这两种关键度量。

读者对象

本书面向不熟悉 NSM 的安全专业人士，也适用于更高级的事件处理人员、架构师以及需要向管理层、初级分析师或者其他不擅长技术的人讲解 NSM 的工程师。也许熟练的 NSM 实践者不能从本书中学到令人惊讶的新技术细节，但是我相信今天的安全专业人士很少有人已经学会如何恰当地实施 NSM。对入侵检测系统或防护系统（Intrusion Detection /Prevention System，IDS/IPS）仅提供报警感到泄气的读者，你会发现使用 NSM 将是一种令人愉悦的体验。

预备知识

我尽量避免重复其他作者已经讲解透彻的知识。我假定你理解 Linux 和 Windows 操作系统的基本使用方法，掌握 TCP/IP 网络及其他网络攻击和防御的基本知识。如果你对 TCP/IP 或网络攻击和防御的知识掌握不够，请考虑参考下面的这些书籍：

- 《The Internet and Its Protocols：A Comparative Approach》，Adrian Farrel 著（Morgan Kaufmann, 2004; 840 页）。Farrel 的书不是最新的，但是它涵盖了广泛的协议范围——包括应用协议和 IPv6，对于每一种它都具有位级的图表和动人的描述。
- 《Wireshark Network Analysis》（第 2 版），Laura Chappell 和 Gerald Combs 著（Laura Chappell University, 2012; 986 页）。所有的网络和安全分析人员都需要理解和使用 Wireshark，本书涵盖描述、屏幕快照、实际案例研究、复习题（附答案）、动手实践以及几十个网络追踪（联网获取）。

- 《Hacking Exposed》，第 7 版，Stuart McClure 等著（McGraw-Hill Osborne Media, 2012; 768 页）。在攻击与防御 IT 类的书中，《Hacking Exposed》保持着单册销量最佳的记录。感谢它新颖的介绍方法：① 介绍一种技术；② 破坏方法；③ 修复方法。

对这些书中的核心概念感到满意的读者或许想考虑下列书籍来更深入地理解：

- 《Network Forensics：Tracking Hackers through Cyberspace》，Sherri Davidoff 和 Jonathan Ham 著（Addison-Wesley, 2012; 592 页）。《Network Forensics》采取以证据为中心的方法，使用网络流量（有线和无线的）、网络设备（IDS/IPS、交换机、路由器、防火墙和 Web 代理）、计算机（系统日志）和应用程序来调查事件。
- 《Metasploit：The Penetration Tester's Guide》，David Kennedy、Jim O'Gorman、Devon Kearns 和 Mati Aharoni 著（No Starch Press, 2011; 328 页）。Metasploit 是一个利用目标应用程序和系统的开源平台，本书说明了如何有效地使用它。

关于软件和协议的声明

本书中的例子都是以 SO（Security Onion，安全洋葱）发行版（http://securityonion.blogspot.com/）中集成的软件为依托。Doug Burks 创建了 SO，这可以使管理员和分析人员使用类似 Snort、Suricata、Bro、Sguil、Squert、Snorby、Xplico 以及 NetworkMiner 这样的工具执行 NSM 更容易一些。SO 是免费的，可通过可引导的 Xubuntu ISO 映像或者通过向你喜爱的 Ubuntu 添加 SO Personal Package Archive（PPA）并安装。尽管 FreeBSD 仍然是一个强大的操作系统，然而 Doug 为 SO 所做的工作，连同 Scott Runnels 的贡献，使得 Ubuntu Linux 分支成为我的 NSM 工具的首选。

我主要使用在 SO 中集成的软件，而且本书中的例子均使用开源工具来演示攻击和防御，而不是商业工具。尽管商业工具提供了许多有益的特征、付费支持以及推卸责任给开发商的可能，但我还是建议读者考虑首先使用开源工具来看看它们的功能。毕竟，几乎很少有组织为购置商业软件提供大量的预算来启动 NSM 行动。

本书主要关注 IPv4 流量。一些用 SO 打包的工具支持 IPv6，但有一些则不支持。当 IPv6 在生产网络中的应用变得更加广泛时，我期望 SO 中更多的工具可集成 IPv6 能力。因此，本书的未来版本或许会讨论 IPv6。

本书内容

本书由下列部分和章节组成。

第一部分——介绍 NSM 及如何放置传感器。

第 1 章 解释了为什么 NSM 会奏效，以获得在环境中部署 NSM 的必要性支持。

第 2 章 论述了围绕从物理访问到网络流量带来的挑战和解决方案。

第二部分——主要讨论了如何在硬件上有效安装 SO 并进行配置。

第 3 章 介绍了 SO 并说明了如何以较低的成本或零成本在备用硬件上安装软件以具备基本的 NSM 能力。

第 4 章 扩展了第 3 章的内容，进一步描述了如何安装分布式 SO 系统。

第 5 章 讨论了顺利安装 SO 所进行的维护活动。

第三部分——主要讨论了 SO 中的关键软件及如何使用这些应用。

第 6 章 解释了 SO 中的 Tcpdump、Tshark、Dumpcap 及 Argus 工具的关键特征。

第 7 章 补充介绍了 NSM 工具链中基于 GUI 的软件，涵盖 Wireshark、Xplico 和 NetworkMiner。

第 8 章 说明了如 Sguil、Squert、Snorby 及 ELSA 这样的 NSM 套件如何启动检测和响应流程。

第四部分——讨论了如何使用 NSM 程序和数据检测及响应入侵。

第 9 章 分享了笔者创建和领导全球计算机事件响应团队（Global Computer Incident Response Team，CIRT）的经验。

第 10 章 给出第一个 NSM 案例研究，你将会学到如何应用 NSM 原理识别和验证连接到因特网的应用程序遭受到的攻击。

第 11 章 给出第二个 NSM 案例研究，本章提供了一个因客户端攻击而遭受侵害的用户案例。

第 12 章 用所讲过的工具和技术来扩展 SO 的能力。

第 13 章 讲解如何克服两种挑战来执行 NSM。

结论 提供了一些关于未来 NSM 的思想，尤其考虑到了云环境。

附录包含了 SO 开发人员 Doug Burks 关于核心 SO 配置文件和控制脚本的信息。

致谢

首先，必须感谢我可爱的妻子 Amy，感谢她对我工作的支持，包括写作文章、博客及其他在我们结婚之前就已开始创作的作品。自从在 2004 年年中出版了我的第一本书以来，我们有了两个可爱的女儿。Elise 和 Vivian 激发我启动这项计划，因为你们三个人，我每天都感谢上帝。我的父母和姐妹也一直在支持我，而且我还要感激 Michael Macaris（我的第一任功夫导师）向我浇灌的智慧之水。

除了在我第一本书中感谢过的 NSM 专家以外，我还必须补充感谢通用电气计算机

事件响应团队（General Electric Computer Incident Response Team，GE-CIRT）成员，他们陪同我从2007年到2011年走过难以置信的安全之旅。我们拥有世界上最好的NSM实践（operation）。Bamm Visscher、David Bianco、Ken Bradley、Tyler Hudak、Tim Crothers、Aaron Wade、Sandy Selby、Brad Nottle以及30多位其他GE-CIRT成员，与你们共事令我非常快乐。还感谢Grady Summers——我们当时的首席信息安全官（Chief Information Security Officer），感谢他创建了我们的团队，还感谢Jennifer Ayers和Maurice Hampton，感谢他们使我们具备了唐·吉诃德式的想象力。

我要感谢Mandiant（曼迪昂特）的同事的支持，包括首席执行官Kevin Mandia和主席Travis Reese，他们早在2011年就雇用了我，但是首次对我展示信任分别是在2002年的Foundstone和2004年的ManTech。感谢曼迪昂特的销售团队和我们的合作伙伴，因为他们为我们提供了一个向世界分享信息的平台和机会。感谢在撰写此书时防护曼迪昂特自身安全的那些坚强灵魂——Doug Burks、Dani Jackson、Derek Coulson以及Scott Runnels，赞赏你们的奉献、专业水准和出色的职业道德。特别感谢Doug Burks和Scott Runnels，感谢他们对SO项目的辛勤工作，这个项目把强大的NSM工具带到了想要试用它们的任何人身边。我还要感谢SO中的所有开源软件开发人员的辛勤努力：你们的帮助使我们所有的网络更加安全。

感谢那些通过对话、新颖的项目以及合作方式质疑我对NSM理解的人们，他们包括Doug Steelman、Jason Meller、Dustin Webber和Seth Hall。那些自2003年阅读我博客（http://taosecurity.blogspot.com/）或者自2008年阅读我推特动态的人鼓励我进行创作。也感谢Black Hat（黑帽大会）的安全专业人士，我自2002年就开始随他们一起授课：前领导人Jeff Moss和Ping Look以及现领导人Trey Ford。还需要特别地提及Steve Andres和Joe Klein，无论何时，当我的学生数量变得太多而难以独自应对时，他们都会帮助我授课。

最后，感谢帮助我创作本书的令人惊讶的团队。首先是来自No Starch出版社的创始人Bill Pollock、产品经理Serena Yang以及宣传人员Jessica Miller。Marilyn Smith和Julianne Jigour编辑了本书，Tina Salameh绘制了优美的封面。Susan Glinert Stevens是排版师，Ward Webber对本书进行了校对。技术编辑David Bianco、Doug Burks及Brad Shoop提供了无与伦比的评论，Brad的妻子Renee Shoop志愿进行了另一个层面的审阅。Doug Burks、Scott Runnels、Martin Holste和Brad Shoop也从文字编辑方面为本书提供了有价值的借鉴。最后同样重要的是，Todd Heberlein为本书作序。感谢Todd开发了网络安全监控软件，这款软件使NSM概念在20世纪90年代早期就进入了人们的生活。

目　录 *Contents*

译者序

序

前言

第一部分　准备开始

第 1 章　网络安全监控基本原理 …… 2

1.1　NSM 简介 …… 3

1.1.1　NSM 阻止入侵吗 …… 3

1.1.2　NSM 和持续监控的区别 …… 6

1.1.3　NSM 与其他方法相比如何呢 …… 7

1.1.4　NSM 为什么有效 …… 8

1.1.5　如何配置 NSM …… 8

1.1.6　NSM 何时无效 …… 10

1.1.7　NSM 合法吗 …… 10

1.1.8　在 NSM 作业期间如何保护用户隐私 …… 11

1.2　一个简单的 NSM 测试 …… 11

1.3　NSM 数据的范围 …… 12

1.3.1　完整内容数据 …… 13

1.3.2　提取的内容数据 …… 15

1.3.3　会话数据 …… 17

1.3.4　事务数据 …… 18

1.3.5　统计数据 …… 19

1.3.6　元数据 …… 21

1.3.7　警报数据 …… 23

1.4　所有这些数据的关键是什么 …… 25

1.5　NSM 的缺点 …… 26

1.6　在哪购买 NSM …… 26

1.7　到哪里寻求支持或更多信息 …… 27

1.8　结论 …… 27

第 2 章　收集网络流量：访问、存储和管理 …… 28

2.1　试验性 NSM 系统的网络示例 …… 28

2.1.1　简单网络中的网络流 …… 29

2.1.2　NSM 的潜在位置 …… 32

2.2　IP 地址与网络地址转换 …… 33

2.2.1　网络块 …… 33

2.2.2　IP 地址分配 …… 34

2.2.3　地址转换 …… 34

2.3　选择实现网络可见性的最佳位置 …… 37

2.3.1　观察 DMZ 网络流量的位置 …… 37

2.3.2 观察无线网络和内网流量的位置 …… 37
2.4 对流量的物理访问 …… 39
2.4.1 用交换机实现流量监控 …… 39
2.4.2 使用网络窃听器 …… 40
2.4.3 直接在客户端或服务器上捕获流量 …… 40
2.5 选择 NSM 平台 …… 41
2.6 10 条 NSM 平台管理建议 …… 42
2.7 结论 …… 43

第二部分 SO 部署

第 3 章 单机 NSM 部署与安装 …… 46
3.1 单机或服务器加传感器 …… 46
3.2 选择如何将 SO 代码安装到硬件上 49
3.3 安装单机系统 …… 50
3.3.1 将 SO 安装到硬盘上 …… 50
3.3.2 配置 SO 软件 …… 53
3.3.3 选择管理接口 …… 55
3.3.4 安装 NSM 软件组件 …… 56
3.3.5 检查安装 …… 59
3.4 结论 …… 61

第 4 章 分布式部署 …… 62
4.1 使用 SO 的 .iso 映像安装 SO 服务器 …… 62
4.1.1 关于 SO 服务器的一些考虑 …… 63
4.1.2 创建 SO 服务器 …… 63
4.1.3 配置 SO 服务器 …… 64
4.2 使用 SO 的 .iso 映像安装 SO 传感器 …… 66
4.2.1 配置 SO 传感器 …… 66
4.2.2 完成配置 …… 68
4.2.3 验证传感器正在工作 …… 68
4.2.4 验证 autossh 隧道正在工作 …… 69
4.3 使用 PPA 创建 SO 服务器 …… 69
4.3.1 安装 Ubuntu 服务器作为 SO 服务器操作系统 …… 70
4.3.2 选择静态 IP 地址 …… 71
4.3.3 更新软件 …… 73
4.3.4 通过 PPA 配置 SO 服务器 …… 74
4.4 使用 PPA 创建 SO 传感器 …… 75
4.4.1 安装 Ubuntu 服务器作为 SO 传感器操作系统 …… 75
4.4.2 将系统配置为传感器 …… 77
4.4.3 运行设置向导 …… 78
4.5 结论 …… 81

第 5 章 SO 平台的日常管理 …… 82
5.1 及时更新 SO …… 82
5.1.1 通过 GUI 更新 …… 82
5.1.2 通过命令行更新 …… 83
5.2 限制对 SO 的访问 …… 84
5.2.1 通过 SOCKS 代理连接 …… 85
5.2.2 改变防火墙策略 …… 86
5.3 管理 SO 数据存储 …… 87
5.3.1 管理传感器存储 …… 88
5.3.2 检查数据库驱动器的使用 …… 88
5.3.3 管理 Sguil 数据库 …… 89

5.3.4 跟踪磁盘使用 …… 89
5.4 结论 …… 90

第三部分 工具

第 6 章 命令行下的数据包分析工具 … 92
6.1 SO 工具种类 …… 92
6.1.1 SO 数据表示工具 …… 92
6.1.2 SO 数据收集工具 …… 93
6.1.3 SO 数据传送工具 …… 93
6.2 运行 Tcpdump …… 94
6.2.1 用 Tcpdump 显示、写入和读取流量 …… 95
6.2.2 使用 Tcpdump 过滤器 …… 97
6.2.3 从 Tcpdump 输出中提取细节 …… 99
6.2.4 用 Tcpdump 研究完整内容数据 …… 99
6.3 使用 Dumpcap 和 Tshark …… 100
6.3.1 运行 Tshark …… 101
6.3.2 运行 Dumpcap …… 101
6.3.3 使用 Tshark 分析 Dumpcap 捕获的流量 …… 102
6.3.4 对 Tshark 使用显示过滤器 …… 103
6.3.5 Tshark 显示过滤器应用示例 …… 105
6.4 运行 Argus 和 Ra 客户端 …… 106
6.4.1 停止及启动 Argus …… 106
6.4.2 Argus 文件格式 …… 107
6.4.3 研究 Argus 数据 …… 107
6.5 结论 …… 110

第 7 章 图形化数据包分析工具 …… 111
7.1 使用 Wireshark …… 111
7.1.1 运行 Wireshark …… 111
7.1.2 在 Wireshark 中查看数据包捕获 …… 112
7.1.3 修改默认的 Wireshark 布局 …… 112
7.1.4 Wireshark 一些有益的特性 …… 115
7.2 使用 Xplico …… 121
7.2.1 运行 Xplico …… 122
7.2.2 创建 Xplico 实例和会话 …… 123
7.2.3 处理网络流量 …… 123
7.2.4 检查解码的流量 …… 124
7.2.5 获取元数据和汇总流量 …… 126
7.3 使用 NetworkMiner 检查内容 …… 127
7.3.1 运行 NetworkMiner …… 127
7.3.2 收集和组织流量细节 …… 128
7.3.3 描绘内容 …… 130
7.4 结论 …… 131

第 8 章 NSM 控制台 …… 132
8.1 以 NSM 为中心查看网络流量 …… 132
8.2 使用 Sguil …… 133
8.2.1 运行 Sguil …… 134
8.2.2 Sguil 的 6 个关键功能 …… 135
8.3 使用 Squert …… 144
8.4 使用 Snorby …… 145
8.5 使用 ELSA …… 148
8.6 结论 …… 151