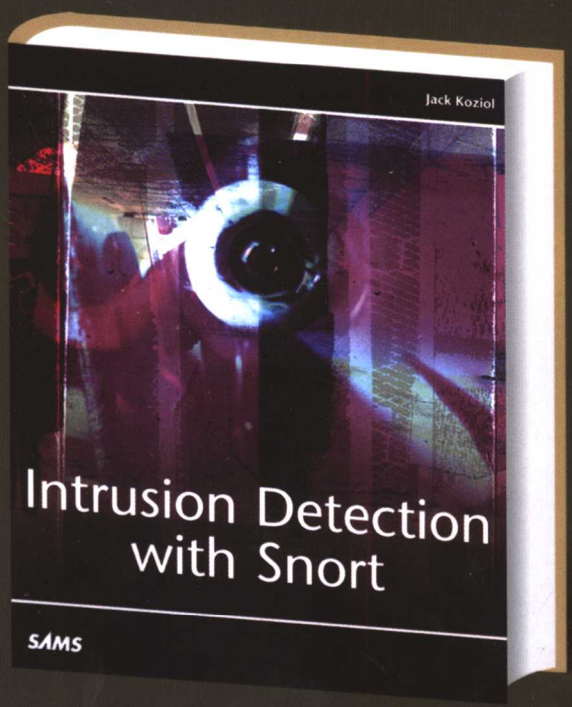
网络与信息安全丛书

SAMS

Snort入侵检测
实用解决方案

Intrusion Detection with Snort

（美）Jack Koziol 著
吴溥峰 孙默 许诚 等译
张玉清 审



机械工业出版社
CHINA MACHINE PRESS

网络与信息安全丛书

Snort 入侵检测实用解决方案

(美)Jack Koziol 著
吴溥峰 孙默 许诚 等译
张玉清 审

机械工业出版社

本书在介绍入侵检测系统的基础上，对 Snort 进行了深入地剖析，详细介绍了 Snort 在实际应用中的安装、使用及维护。全书共 14 章，分别介绍了入侵检测基础、利用 Snort 进行入侵检测、剖析 Snort、安装 Snort 的计划、Snort 运行的基础——硬件和操作系统、建立服务器、建立传感器、建立分析员控制台、其他操作系统下的安装、调整和减少误报、实时报警、基本规则的编写、升级和维护 Snort 以及有关入侵防范的高级话题。本书内容涵盖了 Snort 实际应用的各个方面。

本书无论是对具体的商业应用，还是对教学、科研工作都有相当大的参考价值。

北京市版权局著作权合同登记号：图字 01-2003-4509

图书在版编目（CIP）数据

Snort 入侵检测实用解决方案/(美)科瑞奥(Koziol,J.)著;吴溥峰等译.—北京:机械工业出版社,2005.1
(网络与信息安全丛书)
ISBN 7-111-15701-X

Ⅰ.S... Ⅱ.①科 ...②吴 ... Ⅲ.计算机病毒-防治-软件工具,Snort Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字(2004)第 124430 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：王 颖
责任印制：石 冉

三河市宏达印刷有限公司印刷 · 新华书店北京发行所发行

2005 年 1 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·17 印张·417 千字
0 001—5 000 册
定价：33.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：(010)68993821、88379646
68326294、68320718
封面无防伪标均为盗版

关于作者

Jack Koziol 是芝加哥地区一家主要财政机构的信息安全长官，负责企业范围内的安全。先前，他在一家在线健康护理公司和网络药店的信息安全部门供职。Jack 为信息安全杂志供稿，并发表了一些有关入侵检测的文章。他教授有关 CISSP 考试和“黑客及其防护”的课程。

自从 1998 年以来，Jack 在一些大的生产环境中构建、维护及管理 Snort 和其他的入侵检测系统。他也为一些专门的应用软件撰写 Snort 特征集。

致谢

首先，我要感谢我的父母 Jeff 和 Arlene，他们教导我“只要你专心，你可以做任何事”。我也要感谢我的哥哥 Charlie，他用他的冒险精神鼓舞了我。

我也要感谢 Pearson 教育集团的人们，他们给了我做这个项目的机会并给了一些基础性的指导。我衷心祝福我的资料编辑 Linda Bump，Jenny Watson 和 Stacey Beheler，开发编辑 Lisa Thibault 和 Mark Cierzniak 以及所有为了这本书的出版而辛勤工作的人们。

这本书的质量及其与实际的结合性归功于我的技术编辑 Steve Halligan 和 Bryce Alexander。他们的学识非常渊博，相信在将来会取得更大的成绩。

更要感谢 Snort 工作组的成员，他们开发了世界上最好的入侵检测系统。我自己和我们这个团体都感谢他们在 GPL 发表他们的成果并遵循了开放源代码的精神。

最后我要感谢那些耐心地等待了我 6 个月专心致志、闭门写书的人们。他们是（排名是随机的）：the Koziols，the Beckers，the Spritzers，the Jacobsons，the Noeldners，the Golas，the Hoffmans，Ian Lange，DJ Carlon，Ryan Van Den Elzen，Darren Dalasta，Shawn Swenson，Matt Geesaman，Quasi，当然，还有 Dinesh.

还要感谢 Tracy Hoffman 对我的宽容。

我们期待你的来信！

作为这本书的读者，你们是我们最重要的批评家和评论家。我们很重视你们的意见，想知道我们哪些地方做得对，哪些可以做得更好，你们对出版哪些领域的内容感兴趣，以及其他一些你们想要告诉我们的。

你们可以发电子邮件或直接写信给我，告诉我你们喜欢或不喜欢这本书的哪些内容（也包括我们可以对该书所作的改进）。

在你们的信中，请注意标明该书的主题，作者以及你的姓名、电话和电子邮件地址。我将与编辑一起仔细地评审你们的评论。

Email：networking@samspublishing.com

寄信地址：

Mark Taber
Associate Publisher
Sams Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

读者服务

想得到有关该书更多的信息以及 Sams 出版社其他书目的信息，请浏览我们的主页 www.samspublishing.com. 请在搜索框中键入书的 ISBN 编号(不包括连字符)或书名来查找你需要的书。

译 者 序

入侵检测系统(Intrusion Detection System, IDS)的作用是监控网络和计算机系统是否出现被入侵或滥用的征兆。作为监控和识别攻击的标准解决方案,IDS 系统已经成为安防体系的重要组成部分。

IDS 系统不需要人工干预就可以不间断地运行,能够发现异于正常行为的操作。计算机安防领域的知名专家 Lance Spitzner 对安防问题做了比较形象的比喻:如果把计算机安防问题比喻为城堡,那么防火墙就可以作为城堡的护城桥(只允许自己方面的队伍通过),IDS 可以比作是城堡里的了望哨(监视是否有敌方、或者其他误入城堡的人出现),由此可见 IDS 系统的重要性。一个好的 IDS 系统还要有容错功能,能够适应系统行为的长期变化,而且可以灵活定制,满足个人和组织的需求,同时系统升级要方便,以便保持领先。

Snort 在各种各样的现实环境中都是一种实现入侵检测的实用解决方案,被比喻为安全从业者的瑞士军刀。Snort 的适应性强已在全世界范围内得到证实,Snort 拥有广大的用户群和强有力的 Snort 社区的技术支持。围绕着 Snort 开发了大量的适用于各种需求和各种应用环境的应用工具,相信大家读完该书后会有深刻的体会。

但是另一方面,Snort 难于安装、使用和维护也是大家公认的。Snort 的开发者们倾心于添加新的属性,修正缺陷,因此说明文档的编写做的比较少。虽然有一些关于 Snort 的文档,但是都不够充分,中文方面的权威资料就更少,因此,我们觉得有必要翻译一本关于 Snort 入侵检测方面的书。

本书在介绍入侵检测系统的基础上,详细介绍了 Snort 的使用。书中不但对 Snort 做了简洁明确的介绍,还对它进行了深入的剖析,详细全面地介绍了安装、使用和维护 Snort 的各个方面,并对各个细节也做了具体说明。阅读本书后,读者完全可以建立一个真正实用的 Snort 入侵检测系统。况且 Snort 及其相关软件都是开放源代码的自由软件,可以在书中介绍的相关网站免费下载。本书无论是对具体的商业应用,还是对教学、科研工作都有相当大的帮助,对于入侵检测感兴趣的读者阅读此书后一定会有所收获的。

参加本书翻译的人员除书面署名者外,还有朱静和康效龙两位同志。

由于时间和能力有限,难以做到尽善尽美,不当之处在所难免,恳请读者批评指正。我们的电子信箱是:zhangyq@nipc.org.cn 。

译 者

于国家计算机网络入侵防范中心

目　录

绪　论

我写本书的目的是想给读者提供一本在现实环境下利用 Snort 的第一手的、全面的指导资料。我曾在大大小小的组织中从事过入侵检测工作，并且使用过大量的入侵检测系统技术，在此基础上，我觉得有必要写一本关于安全产业的最有效、最神秘的工具之一——Snort 方面的书。

Snort 常被比喻为安全从业者的瑞士军刀，因为它在各种各样的现实环境中都是一种实现入侵检测的实用解决方案。Snort 的适应性很强，在全世界范围内被广泛安装和使用（据统计已超过 100 000 例），但由于 Snort 被公认是难以安装、维护和使用的，因此，在某种程度上这也是一个难对付的问题。大量必需的设置、特征及与其运行相关的应用程序使得第一次使用 Snort 变得让人难以接受。

失望的用户求助于昂贵的、未开放源代码的其他入侵检测系统，从而失去了灵活配置入侵检测系统以使其适应于具体应用的能力，或者因为缺乏必要的财力而放弃了整个入侵检测。

像许多开放源代码的应用程序一样，Snort 的开发者们倾心于添加新的属性，修正缺陷，而不是专心于说明文档的编写。尽管存在许多有关于 Snort 的文档，但常常都是不够充分的，而且阅读这些文档的前提是读者已有了关于 Snort 或入侵检测的经验（通常假设读者把入侵检测作为一种职业）。这本书的目的就是给读者一个以 Snort 为中心的开放源代码的监测入侵的军械库，以便根据实际需要选择要用的武器。

Snort 构造了一个优秀的入侵检测系统，但仅此而已。这是因为它缺乏易于使用的图形用户界面的管理工具，没有通过寻呼或电子邮件传送警报的方法，呈现出紊乱的没有经过组织的警报信息显示方式。Snort 的开发者致力于使其成为最好的入侵检测系统，把剩下的事留给其他人去做。幸运的是有成百上千的辅助应用程序、工具或脚本可以配合 Snort 一起使用。但与此同时找到适当的应用程序、工具或脚本来配合 Snort 的使用却更加困难。在这本书中我为大家做了资料收集和调查研究的工作，内容涵盖了能与 Snort 配合使用的最流行、最有效的各种辅助应用程序。

本书对拥有图形用户界面的报警管理工具 ACID 做了详细地描述，并且提到了两种产生实时报警的方法（swatch 和 syslog－ng）。对其他特征管理器的使用也做了介绍，比如入侵检测策略管理器将帮助读者使用 Snort。一些高级的入侵防范工具，像 SnortSam 等在最后一章也做了介绍。

如果不仔细彻底地讨论 Snort 的工作方式，这本书就是不完整的。第 3 章“剖析 Snort”专注于介绍 Snort 的内部函数以及一些很少有文档说明的元件，比如像指示 Snort 如何运行的预处理程序。

在读者已经具备了关于 Snort 如何工作的知识后，第 4 章“安装 Snort 的计划”将指导读者如何完成这个艰难的任务。这个任务常会被忽略，但因此会导致整个 Snort 应用的失败。像传感器的布置，事件响应过程及其发展等这些重要的因素在第 4 章也考虑到了。第 5 章“基础——硬件和操作系统”将带领读者完成硬件及操作系统的选择，并且告诉了读者一个通过修改

5 类网线来保护传感器的新颖的方法。

本书的核心部分，第 6 到第 9 章详细地介绍了在家用网络和企业级网络使用 Snort 将会遇到的安装问题及其相关问题的解决方案。接下来讨论了 Snort 工作在多层式拓扑结构的有关问题，包括传感器、服务器和控制台等。同时介绍了在不同的平台上(包括 Windows 和 Linux)安装 Snort 的问题。

即使读者得到一个公开源代码的入侵检测系统，但这个系统也是有一些保留的，这主要是为了提供一个真正有效的入侵检测系统。所有的入侵检测系统面临的一个难题就是错误判断(也即误报警)。如果 Snort 在默认的配置下安装，将会产生大量的误报警。误报警的数量会使得第一次使用 Snort 的用户很失望。通过调整 Snort 来减少误报警的数量势在必行，第 10 章“调整和减少误报”详细地讨论了这一问题。另一个重要的配置任务，使 Snort 能够实现实时报警在第 11 章中做了描述。

第 12 章到第 14 章讨论更高级的话题，像用户对 Snort 特征定制(术语称“规则”)的编写，Snort 的升级与维护，以及将 Snort 作为一个入侵防范工具等问题。Snort 区别于其他不开放源代码的、商业性的入侵检测系统的最大优点就是它允许书写高级规则。这些用户定制的规则使得自己的组织对不愿意接受的或特定的怀有恶意的行为可以实行监听，比如一个从用户的 Web 服务器到一个可疑的国外 IP 地址连接的 TFTP 通信行为。灵活性及类似语言的各种细小规则的定制特性也是 Snort 被广泛接受的重要因素(任何有相关知识的人都可以书写规则并与 Snort 组分享它们)。

最后两个附录作为已存在的 Snort 规则的参考，涵盖了一些最普通的安装及应用话题。

当读完这本书的时候，读者就会拥有一个相当坚固的入侵检测系统，这个系统可与读者花了几百万美元所搭建的商业入侵检测系统相比拟，有时还优于该商用系统。

第1章　入侵检测基础

入侵检测系统(INTRUSION DETECTION SYSTEMS，IDS)已经发展成为安全网络体系中的一个关键性组件。但是，对于许多从事信息安全的人员和系统管理员来说，IDS可能还是一个陌生的概念。本章给出入侵检测的概要描述，并通过例子说明为什么IDS会成为一门重要的技术。

入侵检测系统可以是硬件、软件或者两者的结合，它对单个系统或网络系统中的恶意行为进行监控。入侵检测系统常常被比喻为防窃报警装置。就防窃报警装置而言，传感器通常布置在入口和出口等公共地点。从逻辑上讲，防窃报警装置主要集中于建筑物最薄弱的最易受到入侵者攻击的地方。在保护某些有重大价值的地点时，可以采用一些能检测运动甚至是温度和气压变化的敏感传感器来加强监控力度。传感器收集到数据后递交给某个专业人员，该人员随后必须决定威胁的性质并采取相应的行动措施。IDS在网络世界中采用一套相似的规则运作。传感器被设置在易受攻击的入口等处。对于越有价值的信息资源，受监控所采用的传感器越敏感。就像防窃报警装置一样，IDS也依赖专业人员根据它所收集的数据开展相应的行动措施。

IDS是深度防御信息安全策略的一个关键性组件。深度防御是一种采用一系列重叠防御机制，保护信息资源的方法。其思想是，如果某一防御措施由于某种原因失去作用，其他措施仍然能协调一致地阻止攻击。

提供深度防御必须和加固的主机，安全的路由器，正确放置的防火墙和其他附加设备的配合。IDS透入这一网络基础设施并对滥用进行监控。初学入侵检测的人常常会错误地认为IDS本身就是一整套安全解决方案。实际上应该根据防窃报警装置来考虑IDS：如果你在一座热闹城市的人行道上放置一堆金币，而只用一个报警器来进行保护的话，这些金币很快就会失窃。显然，除了报警器之外还需要一套安全设施。对于IDS也一样，要使IDS有效地发挥作用，一套配置恰当的安全基础设施是必需的。

入侵检测系统是对敌对攻击在适当的时间内进行检测并做出响应的惟一工具。IDS能对现代网络进行完全监控，对一个组织的信息系统所面临的威胁进行实时监控。如果不设置IDS，一个组织可能会被反复攻击并危及安全而毫无察觉。

IDS是一种非攻击性技术。如果正确的进行配置，它不会损害或干扰正常业务。而其他安全技术(比如防火墙)在实施时可能会出现故障并带来很大风险。

本章首先介绍几种不同类型的IDS。然后简单地介绍一下能产生一些普通类别流量的典型攻击。最后，出于客观性，对IDS存在的一些问题进行探讨。

1.1　不同类型的入侵检测系统

IDS从本质上可以分成两类：网络型IDS(NIDS)和主机型IDS(HIDS)。这两种IDS的出现也标志着IDS步入成熟。主机型IDS驻留在一台机器上，监控那些有入侵尝试的机器。网

络型 IDS 更为流行，它对流动在网络中的其他主机发送和接收的流量进行监控。这两种类型各有优缺点，分别适用于不同的情况。

1.1.1 基于主机的入侵检测系统

基于主机的 IDS(HIDS)在操作系统、应用程序或内核层次上对攻击进行监控。HIDS 有权检查日志、错误消息、服务和应用程序权限、以及受监控主机的任何可用资源。另外，HIDS 应该了解应用程序。它应该知道如何区分正常的应用程序数据和异常数据，并且能够监控进行解码和操作的应用程序数据。HIDS 的优点在于它拥有对主机的访问特权。

HIDS 能更好地确定攻击是否成功。由于恶意的流量看起来与正常的流量非常相似，所以网络型 IDS(NIDS)常常会产生错误警报。由于 HIDS 产生误报量比 NIDS 少，因此 HIDS 在检测真正的入侵上更为准确。

误报和漏报

对正常行为产生的警报称为误报。误报是令 IDS 分析家们感到棘手的一个主要问题，因为他们会因误报浪费宝贵的时间和资源。通过调整 IDS 反映网络的方式可以将误报降低到易于管理的水平。

IDS 应该产生相当数量的误报，如果 IDS 不产生任何误报，就很可能会产生漏报。漏报是误报的反面，它是指 IDS 未能检测出真正的攻击。对于 IDS 来说，宁可产生一些误报也不能漏过真正的攻击。因此，出于谨慎，最好调整 IDS，引起一些误报来避免漏报。

HIDS 借助它的访问特权，监控主机中不易被其他系统访问的特殊组件。操作系统的特殊组件，如 UNIX 系统的 passwd 文件和 Windows 系统的注册表，可以被监控以防滥用。如果这一类型的组件被 NIDS 监控则要冒很大的风险。

HIDS 要与它所驻留的系统协调一致，并且要具备该被监控主机的一些深入的仅能为 IDS 所知的知识。因此 HIDS 要具备一些关于主机和其正常行为的特殊知识。发送到主机的流量可能被 NIDS 检测为完全正常，但是可能会被 HIDS 认为是异常和恶意的。因此，HIDS 能发现 NIDS 所不能发现的攻击。

基于主机的入侵检测系统也有一些重大缺点。因为它们驻留在受监控主机，所以对整个网络的拓扑结构认识有限。HIDS 不能检测出针对未安装 HIDS 主机的攻击。攻击者可以控制一台未安装 HIDS 的机器，然后对受保护的主机进行合法访问，这时 HIDS 将毫无用处。为了监控入侵尝试，HIDS 必须安置在每一台危险的主机上。如果一个组织中危险主机的数量不断增长，这将导致成本过高。在主机层次上运行 IDS 意味着你需要为想要保护的每一种操作系统准备一个版本的 HIDS。即使你的组织能够负担这些费用，有勉强够用的版本的 HIDS 或者仅仅能维持系统的运行，也不可能提供完全的保护。

从本质上说，HIDS 是在主机受到攻击之后通过检查日志和错误消息来进行检测的，这带来了各种问题。一些攻击在数据写入日志之前就控制了主机，有效地避开了 HIDS。HIDS 依赖主机与入侵分析员的通信，因此一些使主机完全失去能力的攻击由于阻断了主机与入侵分析员的通讯而可以不被注意地进行。

1.1.2 基于网络的入侵检测系统

网络入侵检测系统(NIDS)放置在网络基础设施的关键区域，监控流向其他主机的流量。