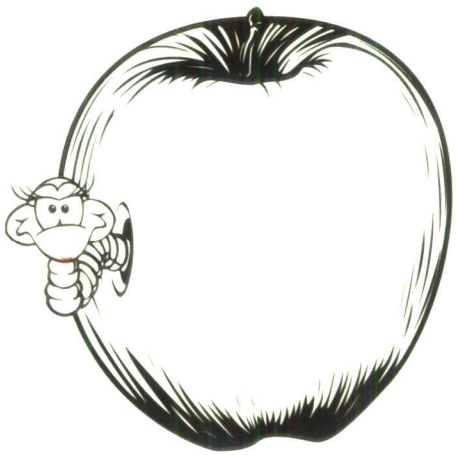
XFOCUS TEAM
From internet,for internet

信息安全焦点丛书

网络入侵检测

——分析、发现和报告攻击

宋劲松 编著



国防工业出版社
http://www.ndip.cn

信息安全焦点丛书

网络入侵检测

——分析、发现和报告攻击

宋劲松　编著

国防工业出版社

·北京·

内容简介

本书由浅入深，全面介绍了关于入侵检测产品和技术的方方面面。全书共分16章，内容由四大部分组成。第一部分为第1章至第3章，介绍入侵检测的概念、选购和使用等内容。读者通过这一部分能了解入侵检测产品的现状，成为一个成熟的使用者。第二部分为第4章至第8章，深入介绍一种开放源码的入侵检测系统(IDS)——Snort的配置、使用、维护等内容，帮助对IDS技术感兴趣的读者了解IDS的原理。第三部分为第9章至第13章，分析了Snort的代码实现，从代码层面剖析IDS的技术，适合IDS的开发者和深入了解IDS技术的专业技术人员。第四部分为第14章至第16章，分析了IDS的弱点，系统讨论了IDS的测试和发展趋势。对IDS的欺骗、IDS的测试和IDS的前景是有一定IDS背景知识的人士所关心的热点问题，本书在这些问题上用专门的章节进行了深入的讨论。

本书可作为网络管理员、对网络安全产品和技术感兴趣的人士、网络安全开发人员和专家的参考资料，也可作为高等院校相关专业高年级本科生和研究生的教学参考书。

图书在版编目(CIP)数据

网络入侵检测：分析、发现和报告攻击/宋劲松编著.
北京：国防工业出版社，2004.9
ISBN 7-118-03537-8

Ⅰ.网… Ⅱ.宋… 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(2004)第077795号

国防工业出版社出版发行
(北京市海淀区紫竹院南路23号)
(邮政编码 100044)
北京奥隆印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 19¼ 436千字
2004年9月第1版 2004年9月北京第1次印刷
印数：1—4000册 定价：36.00元

序 1

世间万物存在阴与阳、黑与白、正义与邪恶等两类势力，并从一定的平衡状态到不平衡，再到新的平衡状态，这是维持世界运行的基础。大到宇宙，小到互联网的攻击防护领域，均无法逃脱这种规律。

对通用计算机系统的攻击最早是 DoS 病毒的攻击，从而兴起了一个新的产业——防病毒软件产业。随着互联网的出现和应用，出现了利用网络攻击，应运而生了入侵检测系统(IDS)。由于网络具有快捷的特点，利用网络传播病毒并达到攻击的目的，成为新的攻击手段，这一方面推进了 IDS 的改进，同时，也对防病毒产业形成了一个重新洗牌的机会。由于目前 IDS 和防病毒采用的主要技术是模式特征匹配技术，所以，需要我们在抗未知攻击方面、处理性能方面有新的突破。

本书全面地阐述了 IDS 的基本原理和发展历程，不论是对入门者，还是对高手都具有极大的帮助。

目前网络攻击已经从单纯的个人破坏嗜好，上升为破坏国家利益、团体利益以及商业利益的行为。攻击的检测与防护对于维持正常的网络社会运行是至关重要的，所以，本书的出版也具有很大的社会意义。

联想集团有限公司 联想研究院 韦卫

2004.6

序2

即将出版的《信息安全焦点丛书》是一套有特点的丛书，突出表现于以下几个方面：

近年来国内对网络信息安全的讨论甚多且泛，理念型的或者说框架上的探讨和具体的一线技术特别是攻防技术的结合较少。乐见焦点丛书是这两个方面结合的一种成功尝试，而几位作者又皆是在一线工作多年的优秀技术人员，丛书中凝结了他们方方面面的工作体验，为学术界、产业界的同事提供了珍贵的一手资料。勿庸置疑，他们流畅优美又带有几分诙谐的笔触，使得书中对信息安全领域一些“焦点”问题的阐述具有良好的可读性。

在我国出版的中文信息安全书籍中，翻译或编译的较多，这套《信息安全焦点丛书》则完全由我国的技术人员原创，是非常可喜的一步。虽然只是一个开端，却表明我国信息安全业内人士视野越发开阔，能够更加准确地把握技术的脉络和产业的动向。从该丛书之创作中，我欣慰地看到了我国培育多年的信息安全产业的核心竞争力。希望我们会有更多的原创技术和著作。

寥寥数笔，记我所感，是为序。

启明星辰信息技术有限公司　严望佳

2004.6

序 3

从有文字记载的历史以来，人类对世界的认识就是在一个不断探索和总结的过程中，从简单到复杂，从单一到多元化，这是认识未知事物的客观规律，贯穿了整个人类的知识发展史。

国内对信息安全的认识从 20 世纪 90 年代开始，经历了单一的产品认知阶段、多种安全产品集成阶段，发展到目前的信息安全产品统一管理阶段，但至今为止仍然较少有企业在进行信息安全建设时针对整个企业的信息安全体系进行规划、组织和建设，大部分信息安全建设还停留在技术和产品堆积的阶段，这种现象主要是因为企业或者部分信息安全行业厂商本身对信息安全认识不够所导致的。

乘着国家重视信息化建设的东风，信息安全已经逐步成为国家安全的组成部分，建立信息安全保障体系，实现一手抓信息化建设，一手抓信息安全的目标，具有重大的社会利益，这也是《信息安全焦点丛书》出版的社会意义，希望“安全焦点”能将这系列丛书一直做下去，为国内的信息安全事业做出更大的贡献！

中联绿盟信息技术有限公司　沈继业

2004.6

目 录

第 1 章　入侵检测概论

1.1　IDS 是什么

入侵检测系统（IDS，Intrusion Detection System)是网络安全防护体系的重要组成部分。IDS 是一种主动的网络安全防护措施，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击。一般来说，IDS 还应对入侵行为做出紧急响应。

1.1.1　为何需要 IDS

对于如何构造网络的安全防护体系，可以参照现实生活中的安全保卫工作，例如某个需要重点保护的大机构。现实中的保卫工作一般会有如下层次：

(1) 在大门的入口会有门卫看守，来客要预先登记，问清楚去哪个部门，得到同意后才给予放行。

(2) 要求各个部门树立安全防范意识，重要的东西要安全保存好，不要放在外来人能随手拿到的地方。

(3) 在机构内安装监控系统，在走廊、房间等需要监视的地方都装上摄像头，建立监控室，集中监控所有的监控画面，由保卫部门派专人监控，发现有异常则立即采取措施。

(4) 在特别重要的地方，对来客进行身份认证，确认身份后才能给予放行；并且可以不对外开放，只有内部人员经过内部通道才能进入。

对安全性的要求越高，则需要采取的措施就越严格，网络体系的安全也大体如此，对比现实中的防护措施，我们可以比较现在做到了什么。

首先，对比第一条，我们可以使用防火墙看守大门，通过规则定义，告诉防火墙和路由器符合什么条件的可以放行或拒绝。同时，对比第四条的要求，可以使用 PKI 加密认证和 VPN 通道达到目的。这样，一切符合要求的访问者就可以进行访问了。

对比第二条，各个部门相当于网络体系内的各个服务器。通过对服务器的系统加固，可以提高安全防护水平，不让来访者随便顺手牵羊。对系统的安全加固是项长期的工作，随时都可能发现漏洞，要做到随时发现随时补。

对比第三条，实现这个功能的就是本书介绍的 IDS。IDS 的出现，解决了安全防护系统中来访者被允许访问后对其所作所为无法控制的难题。我们知道，网络总是要提供服务的，以一些常用的服务，如 WWW，Mail 等为例，防火墙可以做到允许或者拒绝某些访问者访问这些服务，但是这些访问是否是对防火墙的攻击就没法判定了，好像一个访问者进大门后他是不是在偷东西门卫看不到一样。判断这个只有靠墙角的摄像头把来访者的一举一动记录到监视器上。保卫人员由此可以实时看到来访者的行为，一旦发现他

在偷东西，便立刻告警，将其抓获。

1.1.2 IDS 能做什么

IDS 能帮助系统管理员对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。这些都通过其执行以下任务来实现。

- 监视、分析用户及系统活动。
- 系统构造和弱点的审计。
- 识别反映已知进攻的活动模式并向相关人士告警。
- 异常行为模式的统计分析。
- 评估重要系统和数据文件的完整性。
- 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

更详细地说，入侵检测意味着检测未经许可的访问和对一个系统或网络的攻击。一个 IDS 被设计成并且用来探测攻击或对系统、网络和相关资源未经许可的使用，发现后对相关行为予以制止（如果可能的话）。像防火墙一样，IDS 可以是基于软件的或硬件和软件混合的(预先安装和配置好的 IDS 装置)。通常，IDS 软件与防火墙、代理服务或其他的边界服务可以在相同的硬件设备和服务器上运行；但 IDS 和防火墙或其他服务不安装在同一个设备上。虽然这些设备经常被布置在网络外围，但 IDS 却既能发现并且处理外部攻击，又能发现并处理来自内部的攻击。

一个成功的 IDS 不但可以使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，而且能给网络安全策略的制订提供指南。更重要的一点是，它应该配置简单，管理方便，从而使非专业人员非常容易地获得网络安全。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。IDS 在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和告警等。

目前谈到网络安全的实施，人们首先会想到使用防火墙。但随着网络技术的发展，传统的防火墙实际已经不能阻挡入侵者的脚步。致命的原因就是防火墙不是“智能”的。防火墙只能做到允许或者阻止某地址访问某地址的特定端口，但是对于针对开放端口的攻击，防火墙就鞭长莫及了。其次，防火墙完全不能阻止来自内部的袭击。而通过调查发现，50%的攻击都来自于内部，对于企业内部心怀不满的员工来说，防火墙形同虚设。再者，由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于现在层出不穷的攻击技术来说，这显然是致命的弱点。第四，防火墙对于病毒也束手无策。因此，以为在 Internet 入口处部署防火墙系统就足够安全的想法是不切实际的。

国外从 20 世纪 80 年代初就开始了对入侵检测的研究。早期的入侵活动比较简单，通常依靠系统或协议中的明显漏洞来获得非法权限，入侵过程也比较单一，以手工操作为多。这类入侵行为很容易通过简单特征串搜索而捕获，因此这个时期的 IDS 的结构也比较简单，通常可分为引擎部分和控制部分。引擎部分负责检测信息包并发出警报，控

制部分接收警报并产生安全报告，网络入侵特征存放于攻击特征数据库。

近年来，入侵的方法已经变得多样化和复杂化，范围也从针对特定主机的攻击上升为针对网络的全面攻击。例如，分布式拒绝服务攻击（DDoS）就是由分散在互联网上的大量主机系统协同攻击目标主机的。因此，仅仅依靠攻击特征数据库中保存的特征串在主机一级进行检测已不能得到满意的结果。研究人员发展了许多新的技术，而采用代理的分布式系统是一种较好的解决办法。

1.1.3 从不同角度看 IDS

IDS 只是一个符号。在不同人的脑海里或不同的场合中，IDS 代表不同的意思，可能容易引起歧异。例如，经常在论文中看到 IDS 模型，或者听说一个很流行的 IDS 软件叫“Snort”，或者看到国内外的安全厂商推出各自的 IDS 产品等。这些都是 IDS，从不同的角度就有不同的侧重点。

IDS 可描述的角度非常多，从任何一个角度看问题都会形成以管窥豹的片面认识。下面列举一些可以研究 IDS 的角度。

- 在学术界和商业界中存在着对 IDS 的不同研究和发展方向。学术界侧重于入侵检测方法的研究，商业界侧重于入侵检测产品的开发。两者的区别在于很多入侵检测方法很先进，但因为不成熟，在效率、漏报和误报率方面有待提高而不被商业界采用；而入侵检测产品开发中使用的入侵检测技术对学术界来说已无深入研究的兴趣。
- 对攻击者和 IDS 使用者来说，他们对 IDS 的关心是不同的。攻击者关心如何寻找和利用 IDS 的弱点躲避 IDS 的检测，而网络管理员关心如何更好地配置和更有效地利用 IDS。
- 对 IDS 用户和程序员来说，他们看问题的角度又是不同的。程序员更关心 IDS 的实现，对如何开发 IDS 的产品兴趣浓厚，希望知其然更能知其所以然。
- IDS 有开放源码的免费软件，也有价格昂贵的商业产品，二者有何区别。作为一个用户，如何根据自己的情况在免费和付费的软件中做出选择。如何在众多的品牌中选择适合自己的产品。
- IDS 的分类以及各类别间的相互关系。IDS 和其他安全产品的关系如何。IDS 在网络安全体系中的地位如何。
- IDS 分为 HIDS 和 NIDS，它们之间的关系如何。IDS 和其他安全产品的关系如何。IDS 在网络安全体系中的位置是什么。
- 国内和国外分别有各自的代表产品。国外有著名的 ISS，国内有启明星辰、绿盟等厂家。因为国内和国外的用户环境不同，大家分别有着自己的优势和劣势，他们的特点都是什么。
- IDS 技术有着过去、现在和将来。我们可以看到 IDS 的技术演变，可以看到现有的主流 IDS 产品，IDS 将来会向哪些方面发展。
- IDS 产品的好坏众说纷纭，目前尚无统一的标准。但是这方面已经有了很多有益的探索。国内和国外都有哪些值得借鉴的测试标准。

所有这些都是本书要回答的问题。希望通过如此多的角度给 IDS 一个全景式的展现，

读者能够从书中找到自己关心的问题的答案。

1.2 如何检测入侵

1.2.1 信息来源

在现实生活中，警察要证明罪犯有罪，必须先收集证据。只有掌握了充足的证据，才能顺利破案。IDS 也是一样。一般来说，IDS 通过两种方式获得信息。其中一种是网络入侵检测模块方式。当一篇文章从网络的一端传向另一端时，是被封装成一个个小包(叫做报文)来传送的。每个包包括了文章中的一段文字，在到达另一端之后，这些包再被组装起来。因此，我们可以通过检测网络中的报文来达到获得信息的目的。一般来说，检测方式只能够检测到本机的报文，为了监视其他机器的报文，需要把网卡设置为混杂模式。通过在网络中放置一块入侵检测模块，我们可以监视受保护机器的数据报文。在受保护的机器将要受到攻击之前，入侵检测模块可最先发现它。实际应用中网络结构千差万别，用户只有根据具体情况分别设计实施方案，才能让网络入侵检测模块检测到被保护机器的状况。同时，网络入侵检测模块得到的只是网络报文，获得的信息没有主机入侵检测模块全面，所检测的结果也没有主机入侵检测模块准确。网络入侵检测模块方式的优点是方便，不增加受保护机器的负担。在网段中只要安装一台网络入侵检测模块即可。

另外一种获取信息的方式是主机入侵检测模块方式。它是在受保护的机器上安装了主机入侵检测模块，专门收集受保护机器上的信息。其信息来源可以是系统日志和特定应用程序日志，也可以是捕获的特定的进程和系统调用等。

采用主机入侵检测模块方式的缺点是依赖特定的系统平台。用户必须针对不同的操作系统开发相应的模块。由于一个网络中有多种不同的操作系统，很难保证每个操作系统都有对应的主机入侵检测模块，而一个主机入侵检测模块只能保护本机，所以在使用上有很大的局限性。此外，它要求在每个机器上安装，如果装机数量大，对用户来说，是一笔很大的投入。不过，这种模式不受网络结构的限制，在使用中还能够利用操作系统的资源，以更精确地判断出入侵行为。

在具体应用中，以上两种获得信息的方式是互为补充的。

1.2.2 检测办法

当收集到证据后，用户如何判断它是否就是入侵呢。一般来说，IDS 有一个知识库，知识库记录了特定的安全策略。IDS 获得信息后，与知识库中的安全策略进行比较，进而发现违反规定的安全策略的行为。

定义知识库有很多种方式，最普遍的做法是检测报文中是否含有攻击特征。知识库给出何种报文是攻击的定义。这种方式的实现由简单到复杂分了几个层次，主要差别在于检测的准确性和效率上。简单的实现方法是把攻击特征和报文的数据进行字符串比较，发现匹配即告警。这种做法使准确性和工作效率大为降低。为此，开发人员还有很多工作要做，如进行校验和检查，进行 IP 碎片重组或 TCP 重组，实现协议解码等。

构建知识库的多种方法只是手段，目的是准确定义入侵行为，这是 IDS 的核心，也

是 IDS 和普通的网上行为管理软件的差别所在。虽然它们都能监视网络行为，但是 IDS 增加了记录攻击特征的知识库，所以比网上行为管理软件提高了一个层次。定义攻击特征是一项专业性很强的工作，需要具有丰富安全背景的专家从众多的攻击行为中提炼出通用的攻击特征，攻击特征的准确性直接决定了 IDS 检测的准确性。

实际上，大多数商业环境中混合使用基于网络的 IDS（NIDS）、基于主机的 IDS（HIDS）和基于应用程序的 IDS 观察网络上所发生的一切，并更好地监视关键的主机和应用程序。IDS 也可以按照它们对事件的不同分析方法进行区分。一些 IDS 主要使用特征检测技术，这和很多防病毒软件的工作原理类似：基于病毒库特征来识别并阻止被感染的文件、程序和动态网页内容进入计算机系统。只不过 IDS 使用的是攻击库，库里的内容是已知攻击的行为特征。现在，特征检测已经是商用入侵检测系统中使用最广泛的技术。另一种检测的方式叫做基于异常的检测技术。它预先定义了什么是“正常”和“反常”的系统活动 (称为启发式)，以从正常的系统行为中区分出异常的行为。当有异常行为发生时，就可以检测到并采取报告、阻止等响应方式。一些异常检测 IDS 可以让用户定义一个正常行为的基准线，这个基准线可以用抽样统计，基于规则的聚合或神经网络等方法构造出来。入侵检测系统就按照此基准线工作，发现有超出此基准线的行为即告警。

数以百计厂商提供各种不同形式的商业 IDS 解决方案。其中最有效的解决方案是同时使用 NIDS 和 HIDS。同样，在某些特定的产品或解决方案中，主要执行特征检测，辅以异常检测。最后，最现代的 IDS 包括有限的自动响应能力，但是这些通常以自动流量过滤、阻断或分离作为最后的手段。 虽然一些系统宣称能够对攻击作出还击，但实践证明，记录和分析是这些系统所能提供的最有用的方法。

1.3 IDS 的分类

根据 IDS 工作的特点，我们可以看出 IDS 是分布式的结构。还是以监控系统比喻，装在各个地方的摄像头我们叫做“探测器”，探测器的作用是收集信息并且加以分析，发现异常。根据安装的位置不同，探测器可以分为基于主机的和基于网络的。基于主机的探测器安装在被监控的服务器上，通过收集服务器的信息来进行分析告警。基于网络的探测器安装在被监控的服务器的同一个 HUB 或交换机上，通过监听网络上到达服务器的报文来分析告警。基于主机的探测器就像装在各个房间的摄像头，基于网络的探测器就像装在各个走廊的摄像头。两个位置不同，互为补充。

1.3.1 NIDS

NIDS 的名称来自于它的工作模式——监视整个网络。更精确地说，它监视整个网络的一部分。正常情况下，计算机的网卡（NIC）工作在非混杂模式，在这种模式中，只有数据包的目的地址是网卡的 MAC（Media Access Control）地址时，网卡才会接收这个数据包并处理。NIDS 在混杂模式下监视不流向自己的 MAC 地址的网络流量。在混杂模式中，NIDS 可以得到所有网络中的数据包。虽然设置混杂模式是为了保护自己的网络，但是考虑到可能会出现秘密规则，所以监测网络通信一定要得到重视。

基于网络的探测器收集信息没有基于主机的探测器准确，并且因为使用了监听功能，所以对于 HUB 可以正常使用，但对于交换机则需要交换机厂商支持。交换机必须有调试端口能够得到别的端口的报文，这样在交换机上配置后就能使用。基于网络的探测器一般不影响服务器的正常工作，而且可以监控多个服务器的工作。

从图 1-1 中我们看到这个网络使用了 3 个 NIDS，这些 NIDS 都被放置在网络最关键的地方，能监视到关键部位处所有设备的网络流量。这是一个典型的网络保护方案拓扑图，提供公共服务的服务器子网被 NIDS 保护着，但子网中的一台服务器被入侵后，这台服务器会变成一个继续攻击整个子网的跳板。所以为了预防更深层次的危险，必须监视这个子网。

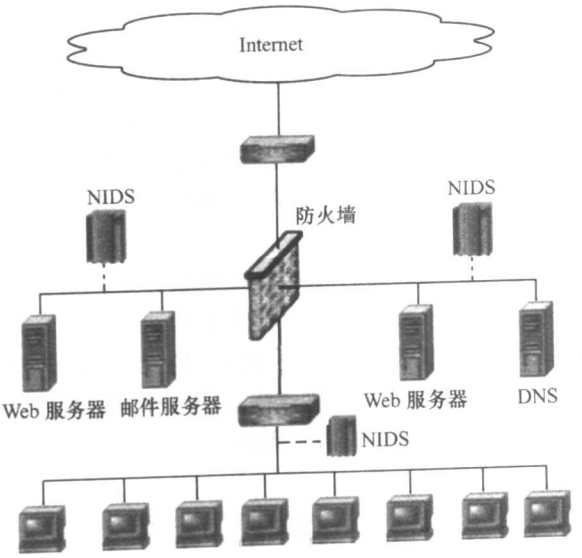


图 1-1　NIDS 网络

内网中的主机被其他的 NIDS 保护着，这样可以减少内网主机被入侵的危险，在网络中布置多个 NIDS 是深层安全防护的一个很好例子。

1.3.2　HIDS

HIDS 和 NIDS 有两点不同。HIDS 只能保护它所在的计算机。计算机网卡设置的是非混杂模式，非混杂模式在有些情况下有其自身的优势，因为不是所有的网卡都能设置成混杂模式的。另外，对配置低的计算机来说，混杂模式对 CPU 的占用会很明显地体现出来。

HIDS 的另一个好处是可以精确地根据自己的需要定制规则。例如，如果运行 HIDS 的计算机上没有运行域名服务（DNS），就不需要加上那些检测 DNS 攻击的规则集。减少了不相关的规则可以提高检测效率和降低处理器的负荷。

图 1-2 描述了一个在一些服务器和个人计算机上安装了 HIDS 的网络。正如前面所提到的，安装在邮件服务器上的 HIDS 主要设置和邮件服务器相关的规则，使其免受入侵，而安装在 Web 服务器上的 IDS 主要设置和 Web 服务器相关的规则，检测对 Web 服务器的