计算机专业人员书库

网络入侵检测

网络入侵检测系统的设计与实现

唐正军　等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

计算机专业人员书库

网络入侵检测系统的设计与实现

唐正军　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

这是国内第一本全面覆盖网络入侵检测系统从设计基础到源码实现的技术书籍。本书所介绍的知识清晰全面，从入侵检测的概念、网络数据流的捕获技术开始，到入侵检测的不同方法，如基于专家系统的入侵检测、基于统计分析的入侵检测等等，最后是对系统具体源代码实现内核的深入剖析，可使用户对于入侵检测技术有一个比较全面的理解。读者如果想要学习入侵检测技术，可以从阅读本书中介绍的知识开始。

图书在版编目(CIP)数据

网络入侵检测系统的设计与实现/唐正军等编著. —北京：电子工业出版社，2002.4
(计算机专业人员书库)
ISBN 7-5053-7414-1

Ⅰ.网… Ⅱ.唐… 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(2002)第 002974 号

责任编辑：郭 立　　特约编辑：程清源
印　　刷：中国科学院印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：35　字数：886.4 千字
版　　次：2002 年 4 月第 1 版　2002 年 4 月第 1 次印刷
印　　数：6 000 册　定价：58.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：(010)68279077

前　言

当前在全球范围内，对计算机及网络基础设施的攻击行为已经成为一个越来越严重和值得关注的问题，特别是各种政府机构的网站，更是成为黑客攻击的热门目标。对类似猖獗的入侵行为的察觉和防护成为各种机构，无论是商业或是政府机构的一个日益迫切的要求。

为何要选购本书?

现有的安全机制通过访问控制，例如口令和防火墙技术，来保护计算机和网络不受非法和未经授权的使用。然而，如果这些访问措施被泄漏或者被绕过，则一个滥用权利者将可能获得未经授权的访问，从而可能导致巨大的损失和系统运行的崩溃。比如说目前流行的防火墙技术，一个常见的缺陷就是如果其安全性配置得特别强大，就会影响到网络系统的处理性能。更严重的情况是防火墙把所有的安全问题都集中在一起。一旦防火墙被突破，那么内部网络就很容易被破坏。因此，可以说防火墙是网络的瓶颈，它们建立了一个把所有防卫措施都放置到一个集中位置的环境。对网络安全来说，这是一个潜在的危险因素。

另外一个实际的问题是，不能够在所有情形下都依靠访问控制机制来防范内部人员的攻击行为。几乎所有的安全系统对内部人员的滥用权力行为都是脆弱的，而审计记录痕迹几乎是检测授权用户滥用行为的唯一手段。

入侵检测系统(IDS, Intrusion Detection System)是用来检测针对计算机系统和网络系统的非法攻击的安全措施。本书在以往的基础上尝试对入侵检测系统的设计与实现技术做一个比较完整的介绍，其中包括设计基础、具体实例和源码实现3大部分。通过本书的写作，作者希望对广大安全技术工程人员能够有所帮助。

本书的内容组织和特点

本书共分为三大部分。

第一部分介绍网络入侵检测系统的相关设计基础知识。首先，对入侵检测系统的发展作了概括介绍，力图使读者有一个先入为主的全面印象。接着简要介绍了相关的网络编程基础知识，包括分层协议模型和相关协议报文格式等。有经验的读者可跳过其中的若干小节，但是强烈建议对报文格式的内容再次浏览，以便理解本书后面对系统实现源码的分析过程。在第3章中，着重分析了网络数据流的截获技术，其中包括基本的数据包"嗅探"(Sniffer)技术以及先进的BPF数据包过滤机制。这是网络入侵检测系统实现的技术基础，建议仔细阅读。接下来的第4章则对入侵检测引擎的设计进行了剖析，其中主要是分析了统计分析引擎的设计并以著名的IDES系统为例说明。入侵检测引擎的另一种常用设计技术——专家系统放在第5章进行介绍，主要是结合一个实际专家系统的使用情况来说明其基本应用原理。最后，在第6章中介绍了入侵检测规则语言N-Code，主要目的是供读者作为借鉴进行进一步的研究工作。

第二部分包括第7章内容。如标题所示，为给读者一个关于实际入侵检测系统的直观和

全面的印象，本书选择了 NFR 公司的 IDA(Intrusion Detection Applliance)系统，对其系统架构设计、主要功能以及使用界面和方法等作了详实的介绍。希望读者在阅读完毕后，能够在脑海中建立起一个完整的系统远行图景。

第三部分是本书的精华部分，包括第 8 章内容。该部分从源代码级别上彻底剖析了著名的自由软件 Snort 入侵检测系统的实现原理和设计要旨，包括整个系统的架构设计思路、模块化插件的设计特色以及核心规则系统的分析等内容。通过仔细和耐心地阅读第 8 章中的分析内容，读者将会发现其中所揭示出来的若干设计原理和实现特色，就构成了目前市面上若干商用入侵检测系统的工作基石。感兴趣和有头脑的读者，还可以进一步在此基础上再做更加深入的探讨努力，其中特别包括借鉴和发展自己的代码实现模块。

技术发展前景

在网络技术快速发展和网络应用环境不断普及的同时，安全问题也越来越引起各种组织机构、社会团体和大众的关注。在传统的加密和防火墙技术已不能完全满足安全需求的同时，入侵检测技术作为一种新的安全手段，正受到越来越大的重视。现在入侵检测技术正处于第一代技术向下一代检测技术的过渡时期，在未来的发展过程里，将越来越多地与其他学科和技术领域进行交融汇合，如数据融合、人工智能以及网络管理等。特别是针对大规模网络环境下的技术应用，更加是前景光明。

入侵检测技术已经成为当前网络安全技术领域内的一个研究热点。它的快速发展和极具潜力的应用前景需要有更多的研究和工程技术人员投身其中，在基础技术原理的研究和工程项目开发等多个层面上同时开展工作，才有可能做出领先的产品系统。

致谢

本书是作者在完成国家自然科学基金重点项目“信息防护关键技术研究”的过程中编写完成的。在本书的编写过程中，得到了解放军第二炮兵工程学院刘代志和宋建社教授的指导和帮助，在此表示感谢。同时，对具体参与编写工作的田仲、王兵、高伟亮、张蕾、吴越勇和刘起等人表示深深的谢意。没有他们的努力，就没有本书的最终面世。

最后感谢电子工业出版社责任编辑郭立女士的辛勤工作。

技术支持

本书的写作只是在飞速发展的网络安全技术领域内的一次努力尝试，由于本书是首本全面覆盖从入侵检测系统的设计到源码实现的图书，所以仓促中难免存在错误和不当之处，欢迎广大读者和技术人员提出批评和建议，可发电子邮件至 zj_mkt@263.net。同时，积极欢迎志同道合者共同研究和探讨。

再次感谢您选择并阅读本书！

唐正军

2002 年 2 月

目　录

第1章 概 述

入侵检测系统（IDS, Intrusion Detection System）用来识别针对计算机系统和网络系统，或者更广泛意义上的信息系统的非法攻击，包括检测外界非法入侵者的恶意攻击或试探，以及内部合法用户的超越使用权限的非法行动。使用 IDS 的目的各有不同。有的人是对法律方面的事务感兴趣，包括对入侵者的跟踪、定位和起诉，而有些人使用 IDS 是为了保护自己重要的计算资源。还有一些使用者则对发现和纠正系统安全漏洞更加感兴趣。

本书中所指的“网络入侵检测系统”是一个相对广泛意义上的概念，包括针对网络基础设施以及其中主机系统的非法攻击行为的检测。

1.1 入侵检测系统的组成部分

从功能逻辑上讲，入侵检测系统由探测器（Sensor）、分析器（Analyzer）和用户接口（User Interface）组成。下面分别对这 3 大部分进行简要介绍。

1）探测器（Sensor）

探测器主要负责收集数据。探测器的输入数据流包括任何可能包含入侵行为线索的系统数据，比如说网络数据包、日志文件和系统调用记录等。探测器将这些数据收集起来，然后发送到分析器进行处理。

2）分析器（Analyzer）

分析器又可称为检测引擎（Detection Engine），它负责从一个或多个探测器处接受信息，并通过分析来确定是否发生了非法入侵活动。分析器组件的输出为标识入侵行为是否发生的指示信号，例如一个警告信号。该指示信号中还可能包括相关的证据信息。另外，分析器组件还能够提供关于可能的反应措施的相关信息。

3）用户接口（User Interface）

IDS 的用户接口使得用户易于观察系统的输出信号，并对系统行为进行控制。在某些系统中，用户接口又可称为“管理器”、“控制器”或者“控制台”等。

除了以上 3 个必要组件之外，某些 IDS 可能还包括一个所谓的“蜜罐”（Honeypot）诱饵机。该诱饵机被设计和配置成为具有明显的系统安全漏洞，并对攻击者明显可见。诱饵机能够作为 IDS 中一个专门提供给攻击者进行入侵的探测器来使用，从而提供关于某次攻击行为发生过程的相关信息。

根据检测引擎的实现技术，入侵检测系统可分为“滥用检测（Misuse detection）”和“非规则检测（Anomaly detection）”两种系统。下面将对这两种系统做一个分析和比较。

1.2 滥用入侵检测系统

滥用入侵检测系统的应用是建立在对过去各种已知网络入侵方法和系统缺陷知识的积累之上，它需要首先建立一个包含上述已知信息的数据库，然后在收集到的网络活动信息中寻找与数据库项目匹配相关的蛛丝马迹。当发现符合条件的活动线索后，它就会触发一个警告，这就是说，任何不符合特定匹配条件的活动都将会被认为是合法和可以接受的，哪怕其中包含着隐蔽的入侵行为。因此，滥用入侵检测系统具备较高的检测准确性，但是，它的完整性（即检测全部入侵行为的能力）则取决于其数据库的及时更新程度。

可以看出，滥用入侵检测系统的优点在于具有非常低的虚警率，同时检测的匹配条件可以进行清楚地描述，从而有利于安全管理人员采取清晰明确的预防保护措施。然而，滥用入侵检测系统的一个明显缺陷在于，收集所有已知或已发现攻击行为和系统脆弱性信息的困难性以及及时更新庞大数据库需要耗费大量精力和时间，这是一项艰苦工作。另一个存在的问题是可移植性，因为关于网络攻击的信息绝大多数是与主机的操作系统、软件平台和应用类型密切相关的，因此带来的后果是这样的入侵检测系统只能在某个特定的环境下生效。最后，检测内部用户的滥用权限的活动将变得相当困难，因为通常该种行为并未利用任何系统缺陷。

在滥用入侵检测系统中，研究者们提出基于各种技术类型的检测器，如专家系统（Expert system）技术、特征分析（Signature Analysis）技术、Petri 网络分析、状态转移分析（State-transition analysis）等等。

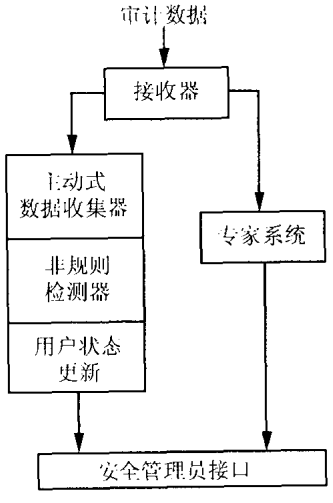

图 1.1 IDES 原型系统的结构

专家系统技术在各种开发模型（Prototypes）中得到广泛应用。通常，专家系统中包含一系列描述攻击行为的规则（Rules），当审计数据事件被转换成为能够被专家系统理解的包含特定警告程度信息的事实（Facts）后，专家系统应用一个推理机（Inference engine）在事实和规则的基础上推理出最后结论。这里，原始的审计数据被抽象成系统能够理解的事实，有利于进一步应用更高层次的各种分析技术。

采用专家系统技术的典型例子有 SRI 公司开发的入侵检测专家系统（IDES，Intrusion Detection Expert System），其系统结构如图 1.1 所示。

由于处理速度的原因，专家系统技术目前只是在各种研究原型中得到应用，而商业化的软件产品采用了其他效率更高的技术，其中目前应用最广泛的就是特征分析技术。与专家系统技术比较，相同之处是同样要收集关于网络入侵行为的各种知识，不同点是特征分析技术更直接地运用收集到的各种知识，例如入侵行为可以被转化成它们在实施过程中所产生的一个事件序列或某种系统审计文件以及网络数据包中的数据样板模型。

1.3 非规则入侵检测系统

非规则入侵检测系统的工作是建立在如下假设基础上的，即任何一种入侵行为都能由于其偏离正常或者所期望的系统和用户的活动规律而被检测出来。描述正常或者合法活动的模型是从对过去通过各种渠道收集到的大量历史活动资料的分析中得出来的。入侵检测系统将它与当前的活动情况进行对比，如果发现了当前状态偏离了正常的模型状态，则系统发出警告信号，这就是说，任何不符合以往活动规律的行为都将被视为入侵行为。因此，非规则入侵检测系统的检测完整性很高，但要保证它具备很高的正确性却很困难。

此类检测技术的优点在于它能够发现任何企图发掘、试探系统最新和未知漏洞的行为，同时在某种程度上，它较少依赖于特定的操作系统环境。另外，对于合法用户超越其权限的违法行为的检测能力大大加强。

较高的虚警概率是此种方法的主要缺陷，因为信息系统所有的正常活动并不一定在学习建模阶段就被全部了解。另外，系统的活动行为是不断变化的，这就需要不断地在线学习。该过程将带来两个可能后果，其一是在此学习阶段，入侵检测系统无法正常工作，否则生成额外的虚假警告信号。还有一种可能性是，在学习阶段，信息系统正遭受着非法的入侵攻击，带来的后果是，入侵检测系统的学习结果中包含了相关入侵行为的信息，这样，系统将无法检测到该种入侵行为。

在非规则入侵检测中，最广泛使用的技术是统计分析（Statistics Analysis）。系统或者用户的当前行为通过按一定时间间隔采样并计算出的一系列参数变量来描述，如每个会话进程的登录和退出时间，占用资源的时间长短及其在每个进程中占用的 CPU—内存—硬盘等资源的多少等。采样的时间间隔从几分钟到一个月，时间长短不等。在最初的模型中，系统计算出所有变量的平均值，然后根据平均偏差检测当前行为是否超过了某一阈值，当然，这样的模型是很简单和粗糙的，无法准确检测异常活动。进一步的算法将单个用户的参数变量数值与积累起来的群体参数变量值进行比较，但是检测能力的提高还是不大。目前在几种非规则检测系统中使用了一种更加复杂的模型，检测系统同时计算并比较每个用户的长期和短期活动状态，而状态信息随着用户行为的变化而不断更新。

另一种主要的非规则检测技术是神经网络技术。神经网络技术通过学习已有的输入—输出矢量对集合，进而抽象出其内在的联系，然后得到新的输入—输出的关系；这种技术在理论上能够用来在审计数据流中检测入侵行为的痕迹。然而，目前尚无可靠的理论能够说明神经网络是如何理解学习范例中的内在关系的，所以同样也无法清楚地解释它是如何发现并理解入侵行为的。神经网络技术和统计分析技术的某些相似之处已经被理论证明，而使用神经网络技术的优势在于它能够以一种更加简洁快速的方式来表示各种状态变量之间的非线性关系，同时，能够自动进行学习/重新训练的过程。

1.4 两种分析技术的比较

本节将从以下 3 个方面来描述上述两种分析技术的不同之点。