学校编码：10384　　分类号＿＿＿密级

学号：X2006230113　　UDC ＿＿

厦门大学

硕　士　学　位　论　文

一种基于 Snort 的网络入侵检测系统设计及应用

Design and Application of Intrusion Detection System Based on Snort

林丽娜

指导教师姓名：段鸿　副教授

专　业　名　称：软件工程

论文提交日期：2009 年 11 月

论文答辩时间：2009 年 12 月

学位授予日期：

答辩委员会主席：＿＿＿＿＿＿

评　　阅　　人：＿＿＿＿＿＿

2009 年 12 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

入侵检测是网络安全技术领域的主要研究方向之一。然而现有的多数入侵检测系统通常只是将采集到的网络数据与已有的攻击模式数据库进行比较，这种模式匹配的方法对已知攻击的检测效率很高，但对于一些未知攻击或者已知攻击的变种却无法准确地检测。将数据挖掘技术应用到入侵检测系统中，有助于提高入侵检测系统的检测准确性和完备性。

本文首先介绍了入侵检测和数据挖掘的相关技术，并重点分析了 Snort 的模块结构和工作流程，为基于数据挖掘技术的 Snort 入侵检测系统的提出提供了理论依据；接着在深入分析关联规则挖掘 Apriori 算法的基础上，针对算法的不足和基于数据挖掘的 Snort 入侵检测系统的需求，在实际应用中采用了基于划分的 Apriori 改进算法。

最后利用 Microsoft Visual Studio 2008 进行开发，语言采用 C#，自主设计了日志分析控制台，该控制台基于 Snort 的平台，利用 Snort 检测的入侵日志，包含了三个功能：规则配置模块，数据分析模块和报表模块。其中，规则配置模块主要是为了方便对 Snort 的规则进行设置和修改；数据分析模块是利用 Snort 对采集到的网络数据包进行预处理，在 Snort 的自身的检测模块之外添加一个基于 Apriori 算法的检测模块，产生新的检测规则集，从而提高检测效率，用于检测未知的网络入侵；报表模块主要是对入侵信息进行输出和整理，方便对入侵信息的查看和汇总。该平台还在仿真的实验环境下进行测试，最终实验结果表明该系统较好地提高了 Snort 的原检测效率。

目前该系统已经在集美大学诚毅学院测试使用中，检测效果很好，有效的防范了网络安全事件的发生，能够及时对攻击事件进行检测，从而采取相对应的防范措施。

关键词： Snort；Apriori 算法；规则检测

Abstract

Intrusion detection is one of the main research directions in network security. However, most of the practical intrusion detection systems usually identify attacks by matching known attacks database with collected network data. These pattern match-based methods are highly effective in detecting known attacks, but they don't work well in detecting unknown attacks or the variations of some known attacks.

This dissertation describes the intrusion detection and data mining related technologies and focuses on analyzing the Snort module structure and work processes, which provides a theoretical foundation for a new Snort NIDS; Secondly, it analyzes Apriori algorithm and proposes its improvements in terms of the algorithm defects and the data-mining-based requirements for Snort intrusion detecting system .

Finally a Snort-based log analysis console is independently designed and developed with Microsoft Visual Studio 2008 and C# language, which consists of three functions: rule configuration module, data analysis module, and report module. Among them, rule configuration module is mainly to facilitate the Snort rule set and modify; data analysis module is to pre-process collected network data packets and to add an Apriori-based algorithm anomaly detection module to its own testing modules, thus generating a new set of rules anomaly detection to enhance detection efficiency for the detection of unknown network intrusion; report module is mainly to organize and put out the invasion information and facilitate the its browse and summary view. The platform is also under an experimental environment simulation testing, the final results show that the system has improved the original Snort detection efficiency.

The system is now being applied to ChengYi college of Jimei University with visible outcome. It has effectively prevented network security accidents with its capacity to detect attacks in a timely manner.

Key words: Snort; Apriori; rules detection

目录

Contents

第一章 绪论

1.1 课题研究背景、目的及意义

近年来随着互联网技术的不断发展，基于网络的计算机系统在现代社会中发挥着越来越重要的作用，已经从独立的主机发展到复杂的分布式开放系统，这给人们在信息处理和资源共享上带来了很大的便利。各种商业、金融和国家政府机构接入到当今最大的信息网络——国际互联网。出于不同的目的，很多这样的目标成为黑客恶意攻击和破坏的对象。在享受着网络技术带来的方便的同时，人们也面临着由于非法入侵系统而引发的一系列安全问题的困扰。随着国际互联网开放性、自由度的提高以及网络应用业务范围的不断扩大，人们对计算机的安全性和保密性也提出了更高的要求。因此，计算机网络必须有足够的保障和防御能力，否则该网络将会给国家安全带来严重的危害和巨大的经济损失。

根据粗略的统计，目前攻击手段大约有两三千种之多，常见的攻击手段有：后门程序、木马、缓冲区溢出攻击、扫描、密码破解攻击、拒绝服务攻击、分布式拒绝服务攻击、FINGER、FTP（File Transportation Protocol，文件传输协议）服务攻击、TELNET（telecommunication net work protocol，电信网络协议）服务攻击、RPC（Remote Procedure Calls，远端程序呼叫）服务攻击、DNS（Domain Name System，域名命名系统）服务攻击、ICMP（Internet Control Messages Protocol，互联网信报控制协议）协议攻击、WEB 服务攻击等等。以上这些只是部分常见攻击类型，每种攻击类型又包括了很多种不同的攻击方法，例如拒绝服务攻击就包括 Syn-Flood、UDP-Flood、Ping-Flood、Land-based-Attack, Smurf Attack, Ping Of Death 等多种攻击方法。由于 Internet 的开放互联性、网络协议自身的缺陷以及操作系统漏洞、系统应用程序漏洞等多方面因素导致了网络环境下的计算机系统存在很多的安全问题。

网络安全问题主要源于黑客的攻击、管理的欠缺、网络的缺陷、软件的漏洞、网络内部的攻击等几个方面[1]。为了尽量保障计算机和网络系统特别是关键部门的信息安全，市场上涌现出了各种安全技术和产品，包括防火墙、安全路由器、身份认证系统、VPN 设备等，这些技术和产品对系统有一定的保护作用，但都属于静态安全技术范畴，不能主动跟踪入侵者，也不能积极有效地防

止来自网络内部的非法行为。为了确保网络的安全，网络系统中拥有的网络安全性分析系统应该能对系统进行漏洞扫描，同时还要能对网络安全进行实时监控、攻击与反攻击，入侵检测系统应运而生。

1.2 国内外发展水平以及研究现状

在上个世纪八十年代，国外掀起了一股入侵检测技术研究的热潮，一些组织开始了入侵检测领域相关的基础理论研究工作。随着计算机系统软、硬件的飞速发展，以及网络技术、系统工程、计算智能、人工神经网络、分布式计算系统等新兴理论与前沿技术的不断完善和发展，入侵检测技术本身也处在不断演变过程中，至今尚未形成一个比较成熟的理论体系。

近 20 年来，作为防火墙的有利补充，入侵检测逐渐成为网络安全领域的一大热点。1980 年，James P. Anderson 发表了一篇名为《计算机安全威胁监测》[2]（“Computer Security Threat Monitoring and Surveillance”）掀起了一股热潮，他在文中首次明确给出了入侵的概念，将入侵划分为外部闯入、内部授权用户的越权使用和滥用三种类型，并提出用审计追踪来监测入侵威胁。

1987 年，Dorothy Denning 的论文《入侵检测模型》[3]（“An Intrusion Detection Model”）提出的理论架构更是启发了很多读者，从而奠定了入侵检测系统商业产品的理论基础。

Dorothy Denning 在论文中给出了一种不依赖于特殊系统、应用环境、系统缺陷和入侵类型的通用入侵检测专家系统框架，简称 IDES 模型。

它的基本思路为：入侵者的行为和合法用户的异常行为是可以从系统合法用户的正常行为中区分出来的。为了定义一个用户的正常行为就必须为这个用户建立和维护一系列的行为轮廓配置，这些配置描述了用户正常使用系统的行为特征。IDES 可以利用这些配置来监控当前用户活动并与以前的用户活动进行比较，当一个用户的当前活动与以往活动的差别超出某些预定义的边界条件，即轮廓配置的各项阈值，这种活动就被认为是异常的，并且它很可能是一种入侵行为。

1990 年，Heberlein 等提出新概念：基于网络的入侵检测——NSM(Network Security Monitor)。从此，入侵检测被分为两个基本类型:基于主机和基于网络。

1991 年，NADIR(Network Anomaly Detection and Intrusion Report)与

DIDS(Distributed Intrusion Detection System)提出了收集和合并处理来自多个主机的审计信息来检测针对一系列主机的协同攻击。

1994 年，Mark Crosbie 和 Gene Spafford 建议在 IDS 中使用自治代理(Autonomous Agents)来提高 IDS 的可伸缩性、可维护性、效率和容错性。

1995 年，IDES 的完善版本 NIDES (Next-Generation Intrusion Detection System)实现了可以检测多个主机上的入侵。

1996 年，GRIDS (Graph-based Intrusion Detection System)的设计与实现使得对大规模自动协同攻击的检测更为便利。

1998 年，Ross Anderson 和 Abida Khattak 将信息检索技术引进了入侵检测领域。

随着人工智能、分布式技术等等的引入，特别是 Internet 的日益膨胀，入侵、攻击事件频频发生。以 2003 年夏天发生的冲击波[4]为例，全球所有安装了微软 Windows 操作系统的 PC 用户，几乎无人幸免，都受到了不同程度的损失。另据国家计算机网络应急技术处理协调中心的统计数据[5]表明，2003 年上半年仅网页篡改一项我国大陆就至少有 150 个网站的网页被篡改，其中包括 87 个政府网站。由此可见，网络用户迫切需要实时的、智能的入侵检测系统及其他安全保障措施的出现，这些需求都进一步的推动了入侵检测的发展。

最近几年来，国内由于电子商务、金融业务、政府机关电子政务的全面铺开，面临黑客攻击的机会越来越大，迫切需要适合自身需求特点的主动防御的入侵检测系统。

1.3 本文的主要结构

第一章绪论：主要介绍本论文研究的背景、目的以及意义，相关领域介绍及课题研究方案和设想。并着重介绍了入侵检测技术的研究现状，突出该问题在研究领域的前沿性和技术上的实效性。

第二章：对入侵检测技术的基本概念、结构、功能、分类进行分析，并介绍应用在入侵检测中的主要技术，介绍了未来入侵检测将要面临的主要问题和挑战。并以典型的入侵检测系统 Snort 为研究对象，对 Snort 的体系结构和工作原理以及规则库进行了详细的分析,最后，还就插件对 Snort 性能的关系进行了讨论。这些分析对今后修改和优化 Snort 系统奠定了基础。

第三章：重点介绍了数据挖掘技术在 Snort IDS 中的应用，利用数据挖掘中的 Apriori 算法对数据库中的历史日志进行挖掘分析,产生新的异常检测规则集，用于检测未知的网络入侵。

第四章：基于改进的 Snort 系统在诚毅学院的设计与实现，详细描述了整个系统的体系结构，搭建完整的系统，尤其是重点介绍了由本人开发及搭建的日志控制分析台，通过具体的实验检测数据，检验改进后的 Snort 系统的实际应用效果。

第五章：结束语，对本文的论述进行工作总结，并提出了进一步的技术讨论和未来的工作展望。

第二章 入侵检测系统、技术分析及 Snort 系统介绍

2.1 入侵检测的基本概念

入侵检测系统(Intrusion Detection System，IDS)是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。

“入侵”(Intrusion)是个广义的概念，不仅包括被发起攻击的人（如恶意的黑客）取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问(Denial of Service)等对计算机系统造成危害的行为。

入侵检测(Intrusion Detection)，顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，进行入侵检测的软件与硬件的组合便是入侵检测系统。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大的简化管理员的工作，保证网络系统的安全运行。

入侵检测的过程一般分为两步：

（1） 信息收集

信息收集也称为数据采集，数据内容主要有：网络流量数据、系统审计数据及用户的活动状态和行为。

（2） 数据分析

数据分析是入侵检测的核心，在这一阶段，入侵检测利用各种检测方法处理第一步中所收集到的信息，并根据分析结果判断检测对象的行为是否是入侵行为。

入侵检测技术是一种主动保护自己免受攻击的网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统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。入侵检测被认为是防火墙之后的第二道安全闸门，它能在不影响网络性能的情况下对网络进行监测。

2.2 入侵检测技术的分类

入侵检测技术虽然可以从不同的角度对其进行分类，但是从实现技术上，一般分为误用入侵检测技术和异常入侵检测技术。

2.2.1 误用入侵检测技术

误用检测技术主要是通过某种方式预定定义入侵行为，然后监视系统的运行，并从中找出符合预先定义规则的入侵行为。基于误用的入侵检测系统通过使用某种模式或者信号标识表示攻击，进而发现相同的攻击。这种方式可以检测许多甚至全部已知的攻击行为，但是对于未知的攻击手段却无能为力，这一点和病毒检测系统类似。因此误用入侵检测具有较高的检测准确性，容易实现，但是它的完整性则取决于数据库的及时更新程度。误用入侵检测系统模型如图 2.1 所示。

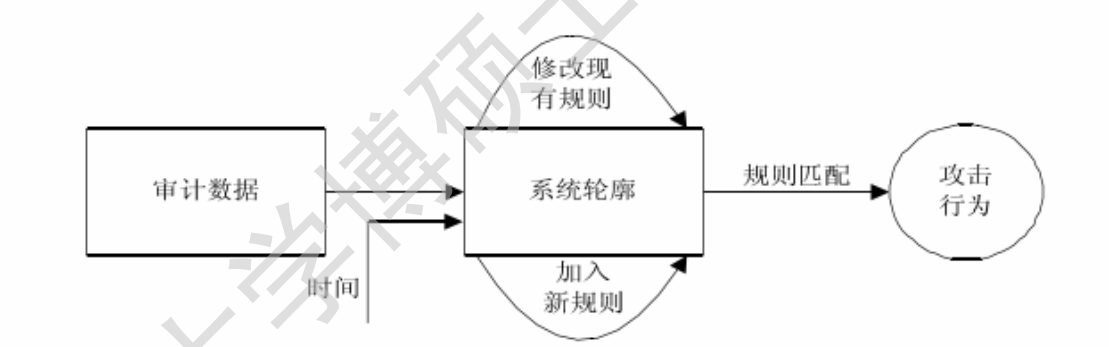

图 2.1 误用入侵检测模型

对于误用入侵检测系统来说，最重要的技术问题是：如何全面描述攻击的特征；如何减少误报率。典型的误用检测系统是基于模式匹配的检测系统，本文研究的 Snort 就是这样的一个系统，它的模式匹配基本上是查找网络包中的存在模式入侵信号，只有少量是利用了规则表示模式入侵信号。这也体现了它轻量级的设计思想。

误用入侵检测技术在实现上多采用以下几类：专家系统、状态迁移分析、模式匹配和键盘监控误用等[6]。

2.2.2 异常入侵检测技术

基于异常的入侵检测方法主要来源于这样的思想：任何人的正常行为都是有一定规律的，并且可以通过分析这些行为产生的日志信息总结出这些规律，而入侵和滥用行为则通常和正常的行为存在严重的差异，通过检查出这些差异就可以检测出入侵行为，此外不属于入侵的异常用户行为（如滥用自己的权限）也能被检测到。

异常入侵检测的主要前提条件是入侵性活动行为作为异常活动的子集[7]。进行异常入侵检测建立在如下假设基础上：任何一种入侵行为都能由于其偏离正常或者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被视为入侵行为。因此，异常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。异常入侵检测系统模型如图 2.2 所示。

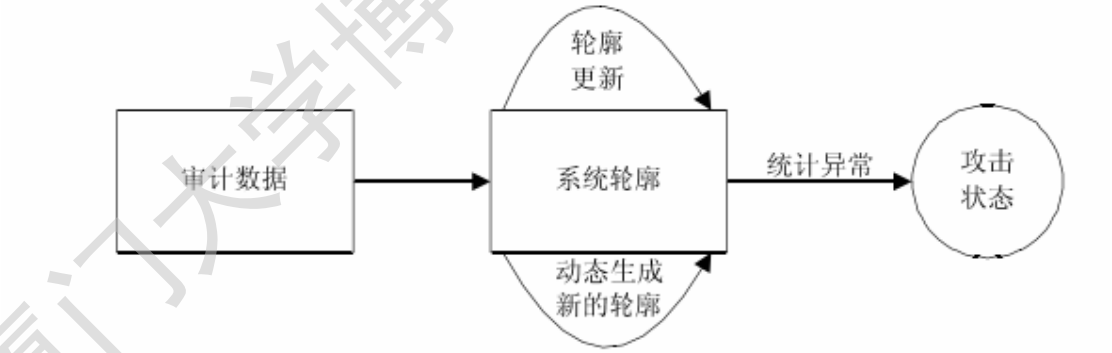

图 2.2 异常入侵检测模型

异常入侵检测系统考虑的主要问题是：选择哪些数据来表现用户的行为；怎样有效表示用户正常的行为。

异常检测是目前入侵检测系统的主要研究方向。常用的异常入侵检测技术有以下几种：基于统计分析的入侵检测技术、基于神经网络的入侵检测技术、基于规则的入侵检测技术等。