基于网络的入侵检测系统的设计与实现①

Design and Implementation of Network Intrusion Detection System

徐 健 张顺颐 （南京邮电大学计算机学院 南京 210003）

摘要：入侵检测（IDS）技术是一种新兴网络安全技术，它是一种基于主动策略的网络安全系统，是对传统的安全策略的补充，是网络安全系统中的重要组成部分。入侵检测已经成为网络安全不可或缺的一部分，它为网络提供了一个防御层，在这一层中我们可以预先定义可能的入侵行为以便对网络活动进行监视，当发现在可能的入侵行为是就回报警通知系统管理员。本文将基于网络数据的安全性，论述入侵检测系统的基本概念。并论述如何结合 IDS 现有的技术，开发一个简单的网络入侵检测系统的模型。

关键词：网络安全 入侵检测系统；数据库 ODBC

1 引言

网络安全已经成为一个非常热门的话题，而入侵检测是这一两年来在网络安全领域比较热门的技术，而且在今后的一段时间内持续发展。入侵检测是指监视或者在可能的情况下，阻止入侵或者试图控制你的系统或者网络资源的这种努力。由于网络入侵检测系统不像路由器、防火墙等作为关键设备方式工作，因此它不会成为系统中的关键路径。网络入侵检测系统发生故障不会影响正常业务的运行，所以部署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。目前入侵检测方面的技术比过去成熟的多，snort 等开源代码也为入侵检测技术的发展提供了不少借鉴。在本文中我所构建的将是一个轻量级的基于异常的入侵检测系统模型，它具有截取网络数据报文，进行网络数据实时分析、报警、以及日志的能力。

入侵检测最早是由 James P. Anderson 于 1980 年提出来的，其定义是：对潜在的有预谋的未经授权的访问信息、操作信息、致使系统不可靠、不稳定或无法使用的企图的检测和监视。从该定义可以看出，入侵检测对安全保护采取的是一种积极、主动的防御策略，而传统的安全技术都是一些消极、被动的保护措施。所以对入侵检测技术研究是非常有必要的，并且它也是一种全新理念的网络（系统）防护技术。

2 通用入侵检测系统模型

Denning 提出了一个通用的入侵检测系统模型，如下图 1 所示。

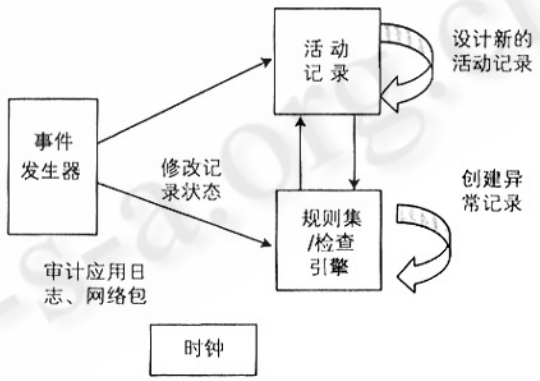

图 1 Denning 的通用入侵检系统模型

该模型的三个主要的部件是事件产生器、活动记录器和规则集。事件产生器是模型中提供活动信息的部分。活动记录器保存监视中的系统和网络的状态。当事件在数据源中出现时，就改变了活动记录中的变量。规则集是一个普通的核查事件和状态的检查器引擎，它使用模型、规则、模式和统计结果来对入侵行为进行判断。此外，反馈也是模型的一个重要部分。现

① 基金项目：国家高技术研究发展计划（863 计划）（2005AA121620）资助项目

有的事件会引发系统的规则学习以加入新的规则或者修改规则。系统的三个子系统是独立的，可以分布在不同的计算机上运行。

3　实用入侵检测系统模型

在通用入侵检测系统模型基础上，采用 Snort（开源代码）的部分源码，构建的基于 Windows 平台的入侵检测系统模型如下图 2 所示。

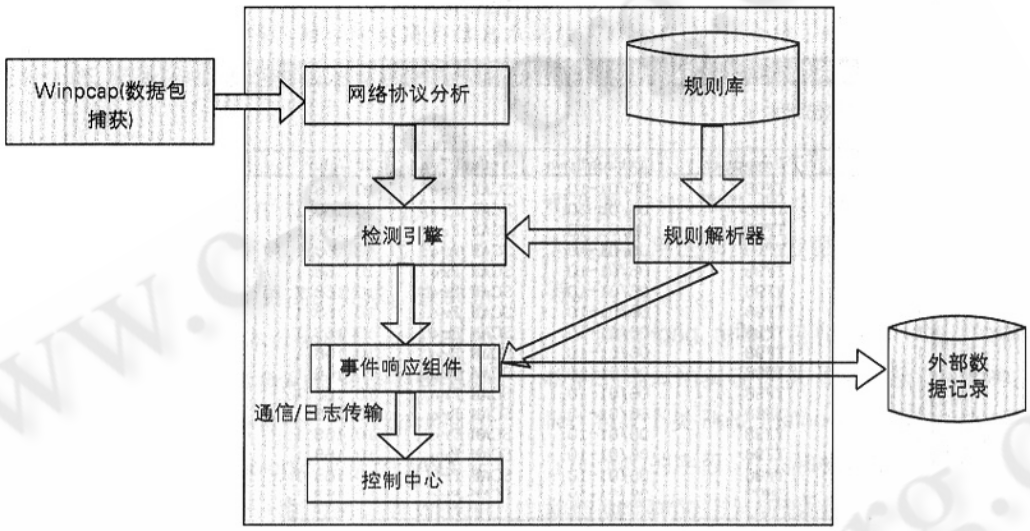

图 2　Win 平台下的实用入侵检测系统模型

Winpcap（windows packet capture）是 windows 平台下一个免费，公共的网络访问系统。winpcap 的主要功能在于独立于主机协议（如 TCP－IP）而发送和接收原始数据报。它不能阻塞、过滤或控制其他应用程序数据报的发收，仅仅只是监听共享网络上传送的数据报。winpcap 提供了重要的灵活的接口 OpenPcap 函数，可直接调用相应函数打开要监视的网卡，开始监听，如捕获到链路层分组就提交到上层，由网络协议解码器（采用 Snort 的部分功能）负责解码成各种网络协议的分组，目前能够分析的协议有 TCP，UDP 和 ICMP。

检测引擎模块是 NIDS 工作的心脏，由三部分组成：规则优化器、多规则搜索器和事件选择器。规则优化器利用集合的方法管理 NIDS 规则。并根据特定的规则参数（如源端口、目标端口和规则内容等）划分规则子集。这使得整个的 NIDS 规则集被划分成许多小的建立在这些独特的参数之上的规则子集。经过这三部分的分析和处理，事件被送往 NIDS 输出系统。

NIDS 的日志传输的特点应该是实时性和多样性，前者指能够在检测到入侵行为的同时及时记录和报警，后者是指能够根据需求选择多种方式进行记录和报警。这里可提供友好的输出界面，在实验中主要是将检测结果可以从控制台上显示，同时将攻击的详细内容记录到数据库中。

事件响应组件接收到经过分析处理的事件分析结果，通过在检测引擎中的相关描述（在实验中将不同攻击类型进行了简单分类），在作记录用的外部数据库中添加相关历史数据。

4　实验仿真及测试结果

考虑到入侵检测程序封装性，在测试中，将入侵检测主程序封装成一个单独的应用程序模块，对外仅提供了一个加载参数的借口，主程序启动参数的设置可通过用户控制修改配置文件来改变。同时考虑到实验结果的实时记录和反馈，在实验中，添加了一个外部的数据库，并且用时钟信号来控制对数据记录的实时监控。仿真测试程序如图 3 所示。

在实验中，主要针对简单的 UDP 攻击进行了测试（TCP、ICMP 类似），在内网使用 UDP 恶意发送数据包（入侵事件标志 1）的程序进行测试，入侵检测程序的仿真测试结果如图 4 所示。

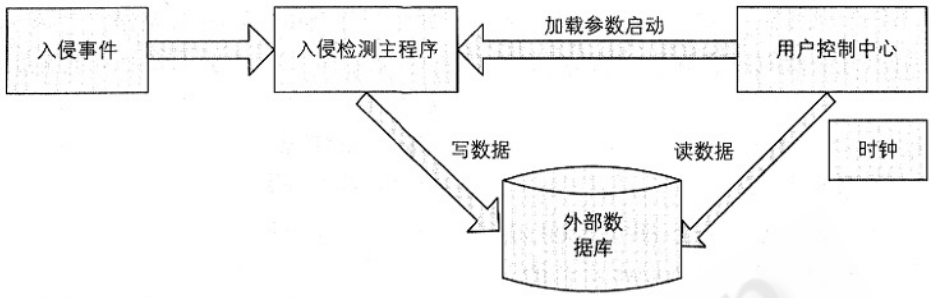

图 3　仿真程序框架图

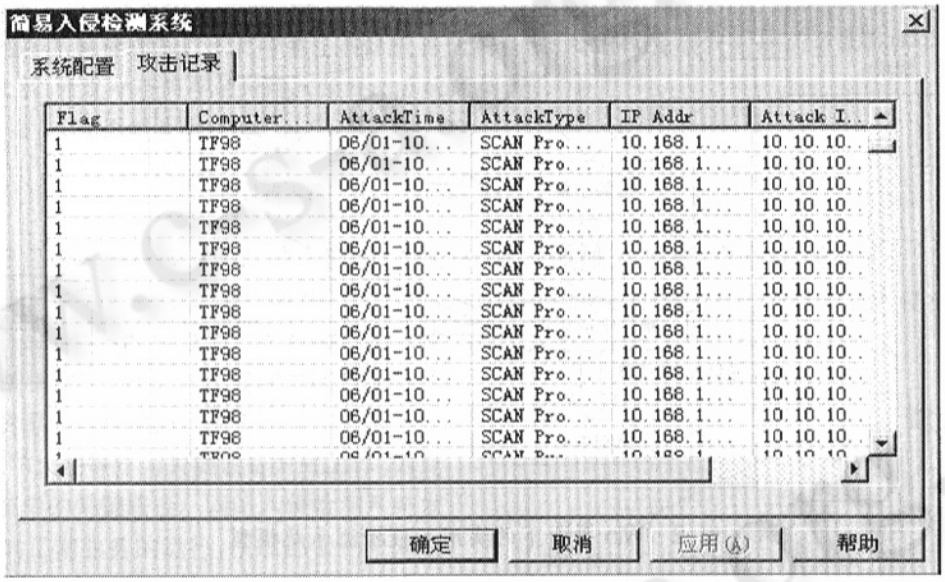

图 4　仿真测试结果

在实验结果的记录中，过滤了一些多余的记录信息，详细结果可以在系统日志中查询到，这里仅按照个人的分类对实验结果进行了处理和分析。

5　结束语

本文在介绍了入侵检测的相关概念以及相对于传统安全技术的优势所在，在研究和分析了相关文献和开源代码的基础上，根据研究需要，构建了实验用的基于异常的网络入侵检测系统。但是目前这个实验系统仅限于单一的网络环境，对于复杂的大型网络环境的监测明显不足。近年来神经网络、专家系统及遗传算法在入侵检测领域的研究，也为入侵检测系统进一步的发展提供广阔的研究前景。

参考文献

1　Denning DE. An Intrusion Dete ction Mode [J]. IEEE Transaction on Software Engineering, 1987, 2 (2): 222 – 232.

2　《入侵检测系统实例剖析》，清华大学出版社，2002 年 5 月第 1 版。

3　Snort 分析报告[EB/OL]. http://sinbad. dhs. org, 2002,12.

4　Terry Escamilla，吴焱，入侵检测[M]，北京 电子工业出版社，1999。

5　http://www. snort. org

6　Northcutt. Network Intrusion Detection. New Riders, 1999