ET Distribution Firewall

Feasibility Analysis

GB8567——88

可行性研究报告

1 引言

1.1 编写目的

网络上的入侵事件层出不穷,这对信息资源的安全构成了严重威胁。应对这些恶意行为的重要措施之一就是入侵检测。而作为该技术的两个分支--异常检测和误用检测,本项目就是想通过实验和修正来研究具体不同的检测模型和算法之间的差异和优劣,具体重点研究不同的基于统计的异常检测模型,并尝试通过实验对比和论证,对已有的算法模型进行修正,找出最具有通用性、可移植性和精度令人满意的算法模型并最终建立一个在 windows 平台上基于.NET 框架的具有防火墙功能的 IDS 系统。

1.2 背景

说明:

经过前期对防火墙和入侵检测系统的开发,本研究小组已经开发一套适合作本次研究课题的实验系统平台,系统平台的具体设计请参考“概要设计”。并且本研究小组已有相当的网络安全和入侵检测的专业知识,并且对已有的基于统计的异常检测模型也有一定认识。通过本课题的研究,本研究小组想通过实验分析对网络安全领域甚至扩展到其他模式识别领域,寻求一种基于统计的具有通用性、可移植性和精度高的识别模型,并以此模型改进现有系统。

1.3 参考资料

- **[1]Selection, Combination, and Evaluation of Effective Software Sensors for Detecting Abnormal Computer Usage *KDD’04*, August 22–25, 2004, Seattle, Washington, USA.**
- **[2] Simple, State-Based Approaches to Program-Based Anomaly Detection C. C. MICHAEL and ANUP GHOSH Cigital Labs**
- **[3]Documents of Snort**

- **[4]Documents of Bro**
- **[5] Analysis and Mathematical Justification of a Fitness Function used in an Intrusion Detection System, Pedro A. DiazGomez, Dean F. Hougen**
- **[6] http://www.ll.mit.edu/IST/ideval/index.html**
- **[7] Immunity-Based Intrusion Detection System Design, Vulnerability Analysis, and GENERTIA's Genetic Arms Race,** Haiyu Hou, Gerry Dozier
- **[8] Characterization of Network-Wide Anomalies in Traffic Flows,** Anukool Lakhina, Mark Crovella, Christophe Diot
- **[9] http://www.xfilt.com**
- **[10] http://www.xfocus.net**
- **[11] http://www.checkpoint.com**

2 可行性研究的前提

2.1 要求

A. 功能：集分布式网络监控、异常检测、误用检测于一身，还有其他安全工具如文件监控，进程监控等。

B. 性能：符合一般服务器的硬件配置要求，资源占用率相对较低。

C. 最终成果为建立一个在 windows 平台上基于.NET 框架的具有防火墙功能的 IDS 系统。

D. 完成期限：预计一年。

2.2 目标

1、通过实验对现有的基于统计的异常检测模型的作较全面对比分析。

2、建立一个在 windows 平台上基于.NET 框架的具有防火墙功能的 IDS 系统，具有占用资源少，检测准确率高，误报率低，适应性强，符合家用和桌面办公需求等特性。并通过分布式协作机制使网络安全信息更合理、有效地流动，打破以前单机防火墙各自为政的被防护局面，开创网络联防的新时代。

3、把算法模型推广到其他模式识别领域，建立具有一般性意义的基于统计的模型框架。

2.3 需要的条件

a．适当的老师指导

b．有一定数量的适合长时间做实验的机器

2.4 进行可行性研究的方法

通过上网搜索资料，了解国内外相关技术的发展状况；
通过了解市场上相关产品的信息，把握本项目的实际价值；
学习掌握相关的专业知识，分析论证本项目技术上的可行性。

2.5 评价尺度

本系统的好坏评价：

1、用户使用的难易度

2、机器配置要求，内存、cpu 等资源占用率

3、开发所需的人力物力

4、维护工作量的大小

5、检测效率和准确度

6、是否具有推广性

7、与实验平台的无关性（即可移植性）

3 对现有系统的分析

3.1 工作负荷

现有系统能在一定程度上阻止各种网络攻击，保护用户的计算机免受外来不良数据的影响。

3.2 局限性

现有的 IDS 系统大多数基于误用检测，很少基于异常检测，基于统计的异常检测就更少了。其三者的对比如下：

	误用检测系统	非基于统计的异常检测系统	基于统计的异常检测系统
发现未知的攻击的能力	不能	可以发现	可以发现
升级要求	需要频繁升级	根据环境变化升级	基本不需要升级
通过学习适应各种不同的环境的能力	没有学习能力	有一定学习能力，但适应性不强	有一定学习能力且
达到很高的检测率	可以但会消耗很大的系统资源(>90%)	可以，但也会消耗一定的系统资源(>40%)	可以且基本不占用系统资源（<3%）
对系统的依赖性	依赖性很强	依赖性很强	不强，比较容易移植
适用的领域	专用领域	专用领域	多个领域，需要重新学习
训练需要的时间	不用训练	较短	较长
可靠性	低	高	高
误报率	低	高	低
系统资源占用程度	很高	较高	低
可扩展性	有一定可扩展性，但需要重新编写模块	有一定可扩展性，但需要重新编写模块和重新学习	可扩展性强，只需更新算法插件和重新学习
稳定性	低，因资源占用太大经常造成 Crash	较好，但资源占用较高	好，且不影响系统正常运转

现有的大多数 IDS 都采用误用检测技术，该技术具有大量的局限性。这种系统最致命的缺陷就在于其只能发现特征已被确定的攻击。这种技术完全依赖于特征库，而特征库的更新速度远远跟不上新病毒或新入侵手段的产生速度，而且特征匹配比较死板。如果攻击者采用新的攻击方法或者只需稍微改变一下原有的攻击方式，就可以骗过这种 NIDS ，从而达到入侵的目的。另外，由于需要对大量数据进行匹配，需要占用很多宝贵的系统资源。而特征库的升级，也需要大量专

业人员对新特征进行研究，人力物力耗费大。

列出本系统的主要的局限性，例如处理时间赶不上需要，响应不及时，数据存储能力不足，处理功能 不够等。并且要说明，为什么对现有系统的改进性维护已经不能解决问题。

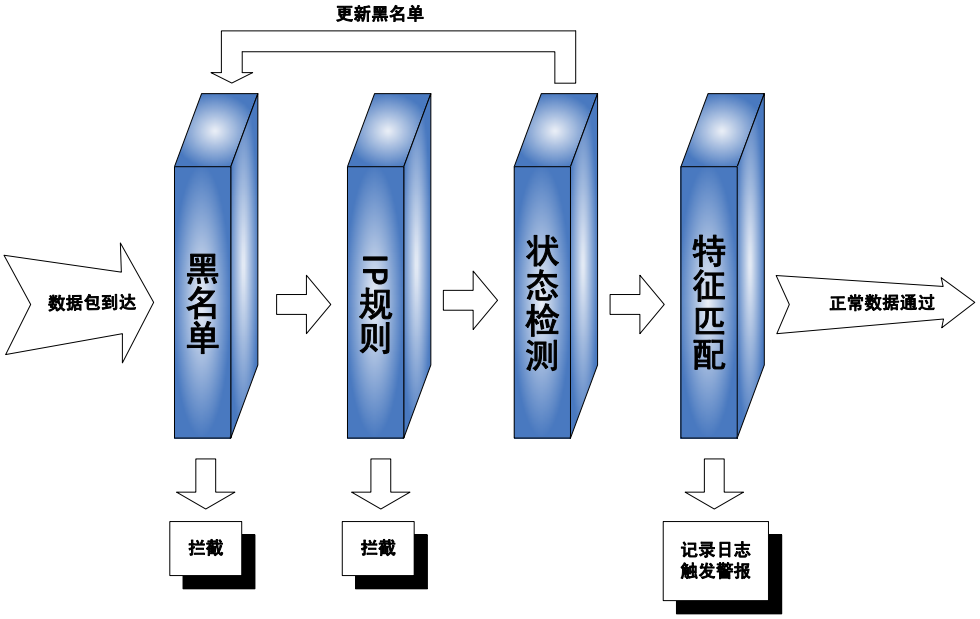
4 所建议的系统

4.1 对所建议系统的说明

建议建立一个在 windows 平台上基于.NET 框架的具有防火墙功能的 IDS 系统，具有占用资源少，检测准确率高，误报率低，适应性强，符合家用和桌面办公需求等特性。并通过分布式协作机制使网络安全信息更合理、有效地流动，实现网络联防。

4.2 处理流程和数据流程

本系统对数据包的处理流程如下图所示：



从网络端口读取的数据包必须经过四层过滤才能正常通过。第一层是黑名单，如果系统从数据包中提取的来源 ip 地址在黑名单中，则直接将数据包丢弃。第二层采用现在流行的 snort 规则集和 Bro 规则集对数据包进行 ip 规则匹配，对不符合 ip 规则的数据包进行拦截。第三层是状态检测，系统将检测受到数据包之后机器各个状态参数，并与原先建立的正常状

态进行比较，若与正常状态偏离太大，则将该数据包认为攻击数据，如果一定时间内从同一来源多次收到攻击数据包，则将对方 ip 列入黑名单。最后对数据包进行特征匹配，拦截记录具有特征的数据包并触发警报。

4.3 改进之处

本系统中由通过实验得到的新算法编写的异常检测模块，能发现绝大多数使系统偏离正常状态的数据包。

更少地占用系统资源，更加高速、有效。

打破以往单打独奏的的入侵防御模式，本系统使用分布式算法，实现网络联防。

4.4 影响

对开发的影响

为了适应不同机器不同操作系统，本系统安装之后需要进行一定的训练，以产生一个正常状态空间，这个训练过程需要一定的时间。但训练完后，系统正常工作，用户即可享受本系统带来的安全方便的工作环境。

4.5 局限性

说明所建议系统尚存在的局限性以及这些问题未能消除的原因。

4.6 技术条件方面的可行性

本项目使用的是基于统计的异常检测的方法，目前国内外在该方面的研究为我们的项目提供了很多有用的信息和参考，我们研究了很多的该方面的著作，同时进行了大量的开发工作，在秉承前人的基础上已开发了一个可供项目进行实验的系统。

基于统计学进行检测技术上更容易实现，这方面的理论、数学模型的发展也比较完善，能让我们学习借鉴。

异常检测方面，我们主要参考了麻省理工大学的一个成功的实验项目，并借鉴了对方一

部分研究数据，在此基础上，我们有信心与能力将这一技术更进一步发展，得到自己的科研成果。

5 社会因素方面的可行性

5.1 使用方面的可行性

本系统高度智能化，使用简单，工作时用户基本感觉不到该系统的存在，不要求使用者拥有某一领域的专业知识，容易被广大的计算机用户接受；而且资源占用小，对机器性能要求不高，可移植性强，适用于绝大多数的办公室和家用电脑。

6 结论

综上所述，本项目可以立即开始进行。