ET Distribution Firewall

Requirement Analysis

目录

1.产品限制条件

1.1 产品的目标

1.1.1 该项目工作的用户问题和背景

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。误用检测和异常检测是入侵检测系统的主要方法。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。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。为广大互联网用户提供一个安全、方便的工作环境，免去不断下载更新特征库的麻烦。

1.1.2 产品总目标：

本项目的总目标是建立一个在 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。

1.1.3 产品具体目标：

具体目标：
1．
目标：实现分布式网络监控
优势：打破以往入侵检测软件单打独奏的做法，实现网络联防，共同对付网络入侵。
说明：服务器可以监控域内各客户端的情况，并发出警告。

2.
目标：误用检测
优势：提高检测效果
说明：为了提高监测效果，除了提供异常检测模块，还同时提供误用检测模块，以提高监测效果。

3.
目标：基于统计的异常检测
优势：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。而且有自动学习能力，不断适应新环境。
说明：不依赖特征库，可以查到特征未被确定的攻击数据。

4.
目标：提供其他网上安全工具。
优势：方便用户检查计算机当前状态。
说明：如文件监控，进程监控等。

1.2 客户，顾客和其他风险承担者

1.2.1 客户

各种局域网提供者

1.2.2 顾客

该产品的用户范围广泛，各种局域网，如校园网、公司或社区的局域网等的服务器和用户端都可以使用本系统。本系统使用不需要特殊的专业知识，几乎所有的互联网使用者都有可能成为用户。关键顾客有：

1．各中小型企事业单位，他们需要更高的网络安全又不愿出资购买硬件防火墙设备。
2．单独的个人用户，他们不愿不断下载更新攻击特征库，而使用本系统的异常检测的功能。

1.2.3 其他风险承担者

无

1.3 产品的用户

1．顾客（见 1.2.2）
2．网站管理员

1.4 需求限制条件

1.4.1 解决方案限制条件

1．产品必须运行在 Windows2000\XP\2003\NT5.0 (不支持 Windows98)系统下并使用,framework1.1(运行期)
2．硬件要求：PII 300 以上处理器，64M 内存，50M 以上可用磁盘空间。

1.4.2 实现环境

1．电子商务网站是在托管服务器上运行。
2．对用户的访问平台不作其他任何假设性的限制

1.4.3 商业上架销售软件

本产品开发利用的均是 IBM 提供的比赛软件包，无需购买其他软件包。

1.4.4 开发者构建该产品需要多长时间

开发时间大约为一年

1.4.5 该产品的财务预算是多少

暂无。

1.5 命名标准和定义

待定

1.6 相关事实

1.7 假定

通过对比找到最优的算法模型，以及相关的实验数据

2.功能性需求

2.1 产品的范围

2.1.1 工作上下文范围

由于本系统实现了高度的人工智能，能够自动学习，自动拦截能对系统产生不良影响的数据包，除了在已开始安装时需要进行一定的训练，用户在使用时一般感觉不到本系统在运行。

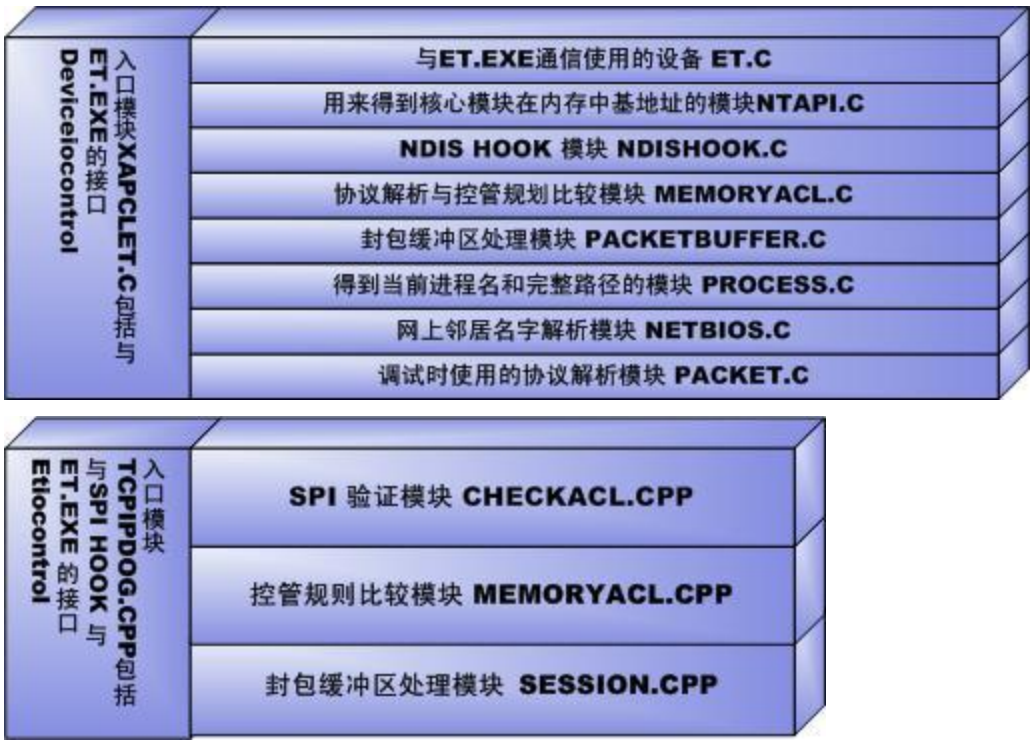
2.1.2 工作切分

2.1.3 产品边界

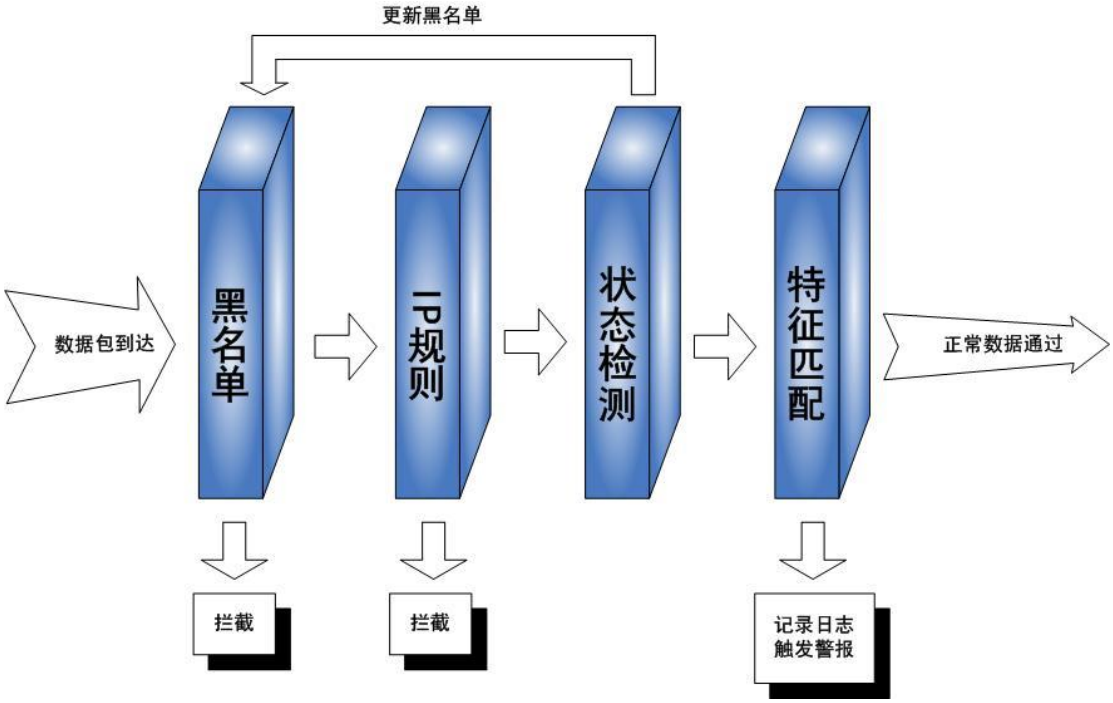
基本设计概念和处理流程

- **Driver Layer（驱动层）**

- **Application Layer（应用层）**



- **Network Layer（网络层）**
- **DataAccess Layer（数据层）**



2.2 功能性需求与数据需求

功能性需求

1．用户可以不必经常下载更新.
2．平时系统在后台工作，用户不必理会或注意到其存在.
3．在用户受到袭击发出警报.
4．自动在后台与服务器连接区的最新黑名单及其他需要的数据。
5．占用尽可能少的系统资源。

数据需求

需要自用户的机器上采集状态样本数据作为日后判断是否异常的标准。

3.非功能性需求

3.1 观感需求

操作界面应该有好，美观

3.2 易用性需求

操作界面应该有好，美观

3.3 性能需求

服务端应能监测到所有的在线用户，并对这些用户及时发送更新信息。

3.4 操作需求

界面友好，易操作

3.5 可维护性和可移植性需求

无。

3.6 安全性需求

本系统 必须有足够高的检出率和足够小的漏查率，以保障用户的信息安全。

3.7 文化和政策需求

无

3.8 法律需求

1，不得使用其他公司或个人未授权的专利
2，图案不得侵犯其他公司的版权。

4.项目问题

4.1 开放式问题

4.2 商业上架式软件解决方案

无

4.3 新问题

无

4.4 任务

无

4.5 迁移

无

4.6 风险

无

4.7 费用

无

4.8 用户文档

详见使用说明

4.9 后续版本需求

无