信息系统安全入侵检测技术

入侵检测技术概述

入侵检测分类与评估

入侵检测产品概况

缘起

传统网络安全技术存在着与生俱来的缺陷

- **程序的错误**
- **配置的错误**

需求的变化决定网络不断发展

- **产品在设计阶段可能是基于一项较为安全的技术**
- **但当产品成型后，网络的发展已经使得该技术不再安全**

传统的网络安全技术是属于静态安全技术，无法解决动态发展网络中的安全

定义

入侵检测是用来发现外部攻击与内部合法用户滥用特权的一种方法

它还是一种增强内部用户的责任感及提供对攻击者的法律诉讼依据的机制

预防措施的局限性

- 预防性安全措施采用严格的访问控制和数据加密策略来防护，但在复杂系统中，这些策略是不充分的。这些措施都是以减慢交易为代价的。
- 大部分损失是由内部引起的
  - **1999年CSI/FBI（Computer security institute/Federal Bureau of Investigation)指出，82%的损失是内部威胁造成的。**

入侵检测的特点 - 1

入侵检测是一种动态的网络安全技术

利用各种不同类型的引擎，实时地或定期地对网络中相关的数据源进行分析

依照引擎对特殊的数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制

入侵检测的动态性

- 入侵检测的实时性
- 对网络环境的变化具有自适应性

网络安全工具的特点

	优点	局限性
防火墙	可简化网络管理，产品成熟	无法处理网络内部的攻击
IDS	实时监控网络安全状态	误报警，新的攻击模式
Scanner	简单可操作，帮助系统管理员和安全服务人员解决实际问题	并不能真正扫描漏洞
VPN	保护公网上的内部通信	可视为防火墙上的一个漏洞
防病毒	针对文件与邮件，产品成熟	功能单一

入侵检测的特点 - 2

与防火墙不同的是，IDS入侵检测系统是一个旁路监听设备，没有也不需要跨接在任何链路上，无须网络流量流经它便可以工作。

因此，对IDS的部署的唯一要求就是：IDS应当挂在所关注流量都必须流经的链路上。

IDS的接入方式：**并行接入(并联)**

IDS在交换式网络中的位置一般选择为：尽可能靠近攻击源，尽可能靠近受保护资源。这些位置通常是：

- 服务器区域的交换机上
- 边界路由器的相邻交换机上
- 重点保护网段的局域网交换机上

入侵检测的内容

外部攻击检测

- 外部攻击与入侵是指，来自外部网络非法用户的威胁性访问或破坏
- 外部攻击检测的重点在于，检测来自于外部的攻击或入侵

内部特权滥用检测

- 内部特权滥用是指，网络的合法用户在不正常的行为下获得了特殊的网络权限并实施威胁性访问或破坏
- 内部特权滥用检测的重点集中于，观察授权用户的活动

入侵检测的功能

检测和分析用户和系统的活动

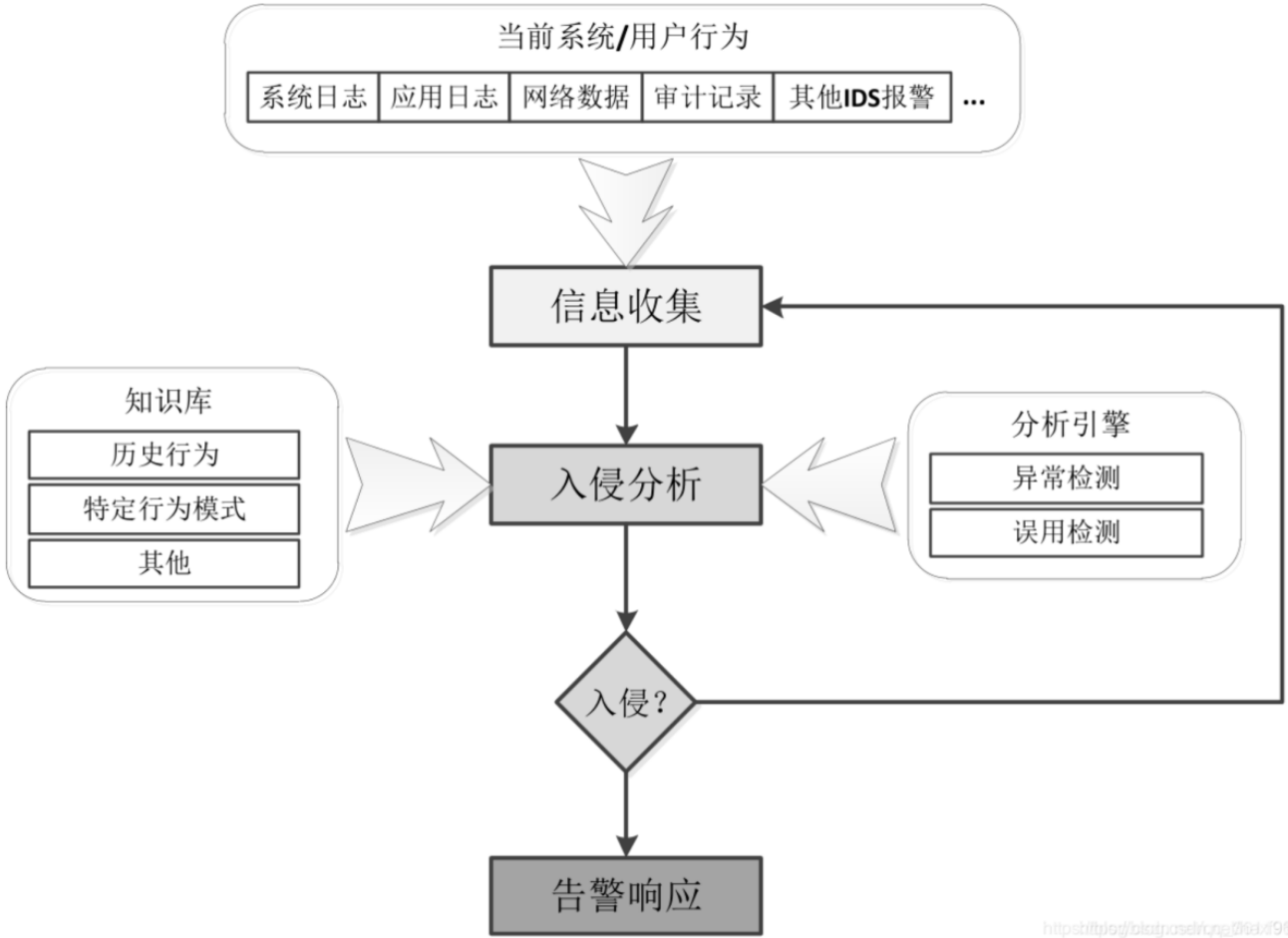
识别反映已知攻击的活动模式

非正常活动模式的统计分析

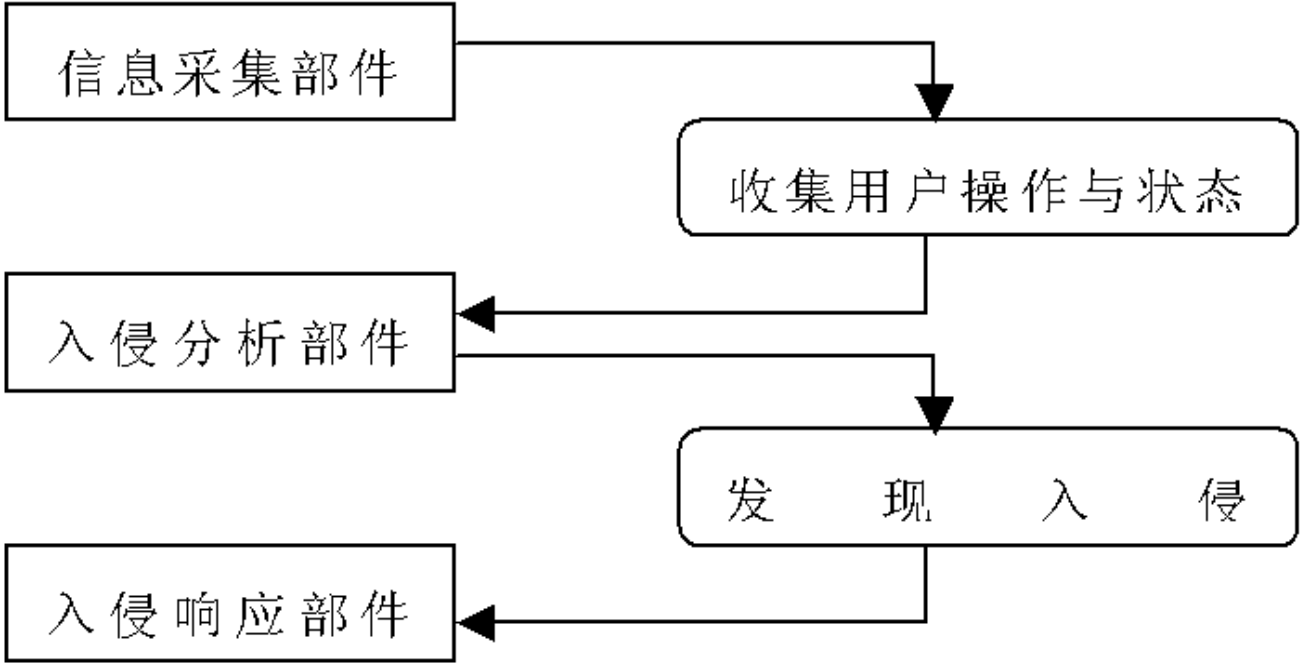
通过对操作系统的审计，分析用户活动、识别违规操作

审计系统配置和脆弱性、评估关键系统和数据文件的一致性

入侵检测原理图


当前系统/用户行为
系统日志
应用日志
网络数据
审计记录
其他IDS报警
...
信息收集
知识库
历史行为
特定行为模式
其他
入侵分析
分析引擎
异常检测
误用检测
入侵?
告警响应

入侵检测系统构成 - 1



入侵检测系统构成 - 2

信息采集部件

- **对各类复杂、凌乱的信息进行格式化，并交付于入侵分析部件**

入侵分析部件 误用检测(模式匹配)、异常检测(统计分析)、完整性分析

- **按着部件内部的分析引擎进行入侵分析，当信息满足了引擎的入侵标准时就触发了入侵响应机制**

入侵响应部件

- **当入侵分析部件发现入侵后，由入侵响应部件根据具体的情况做出响应**
- **响应部件同信息采集部件一样都是分布于网络中，甚至与信息采集部件集成在一起**

入侵分析——信息收集

- 入侵检测很大程度上依赖于收集信息的可靠性和正确性。
- 要保证用来检测网络系统的软件的完整性。
- 特别是入侵检测系统软件本身应具有相当强的坚固性，防止被篡改而收集到错误的信息。
- 在一个环境中，审计信息必须与它要保护的系统分开来存储和处理。因为
  - 防止入侵者通过删除审计记录来使入侵检测系统失效
  - 防止入侵者通过修改入侵检测器的结果来隐藏入侵的存在
  - 要减轻操作系统执行入侵检测任务带来的操作负载

入侵分析——信息收集

- 数据来源可分为四类：
  - 来自主机的：基于主机的监测收集通常在操作系统层的来自计算机内部的数据，包括操作系统审计跟踪信息和系统日志
  - 来自网络：检测收集网络的数据
  - 来自应用程序：监测收集来自运行着的应用程序的数据，包括应用程序事件日志和其它存储在应用程序内部的数据
  - 来自目标机：使用散列函数来检测对系统对象的修改。

工作机理 - 1

技术分析的依据

- **历史知识**
- **现有行为状态**

实时的监测是保证入侵检测具有实时性的主要手段

根据实时监测的记录不断修改历史知识，保证了入侵检测具有自适应性

工作机理 - 2

入侵检测的技术的核心在于入侵检测过程

对行为与状态的综合分析，基于：

- **知识的智能推理**
- **神经网络理论**
- **模式匹配**
- **异常统计**

入侵检测分类与评估

按引擎分类

按实现方式分类

按技术路线分类

按系统各模块的运行方式

按时效性分类

按引擎分类 – 误用检测

首先根据已知的入侵，定义由独立的事件、事件的序列、事件临界值等通用规则组成的入侵模式

然后观察能与入侵模式相匹配的事件，达到发现入侵的目的

入侵模式需要定期更新

按引擎对比 – 误用检测

优点

- 误用检测具有很强的可分割性、独立性，可缩小模式数据库规模
- 具有很强的针对性，对已知的入侵方法检测效率很高
- 有能力提供模糊入侵检测引擎

缺点

- 可测量性与性能都和模式数据库的大小和体系结构有关
- 可扩展性差
- 通常不具备自学习能力，对新攻击的检测分析必须补充模式数据库
- 攻击行为难以模式化

按引擎分类 – 异常检测

原理

- 通过检查统计量的偏差，从而检测出不正常的行为

实现方法

- 将各个主体、对象的行为量化
- 以历史数据设定期望值
- 将与期望值有偏差的行为定义为入侵

按引擎对比 – 异常检测

优点

- 符合数据的异常变化理论，适合事物的发展规律
- 检查算法比较普适化，对变量的跟踪不需要大量的内存
- 有能力检测与响应某些新的攻击

缺点

- 数据假设可能不合理，加权算法在统计意义上可能不准确
- 对突发性正常事件容易引起误判断
- 对长期、稳定的攻击方法灵敏度低

按实现方式分类

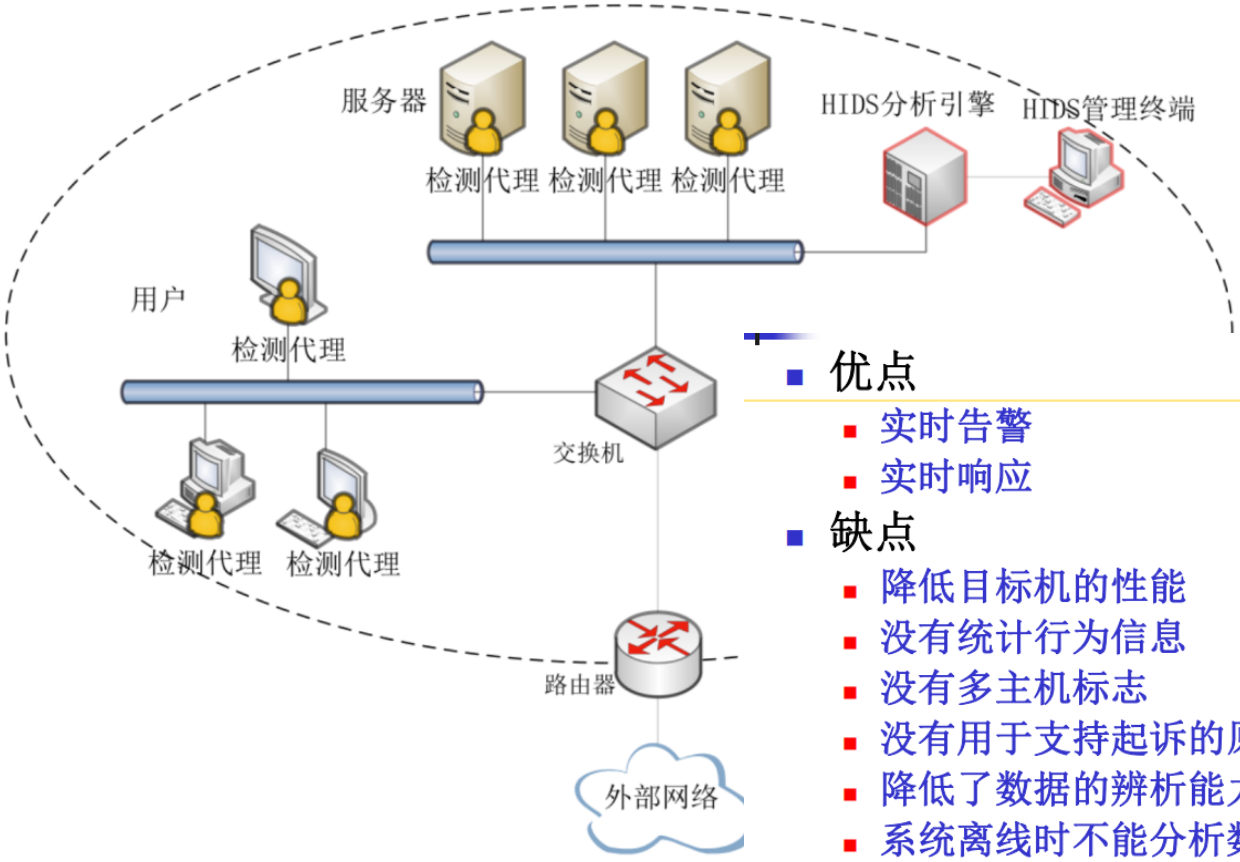
基于主机的IDS（HIDS)

- 安装在被重点检测的主机之上
- 对该主机的网络实时连接以及系统审计日志进行智能分析和判断

基于网络的IDS（NIDS)

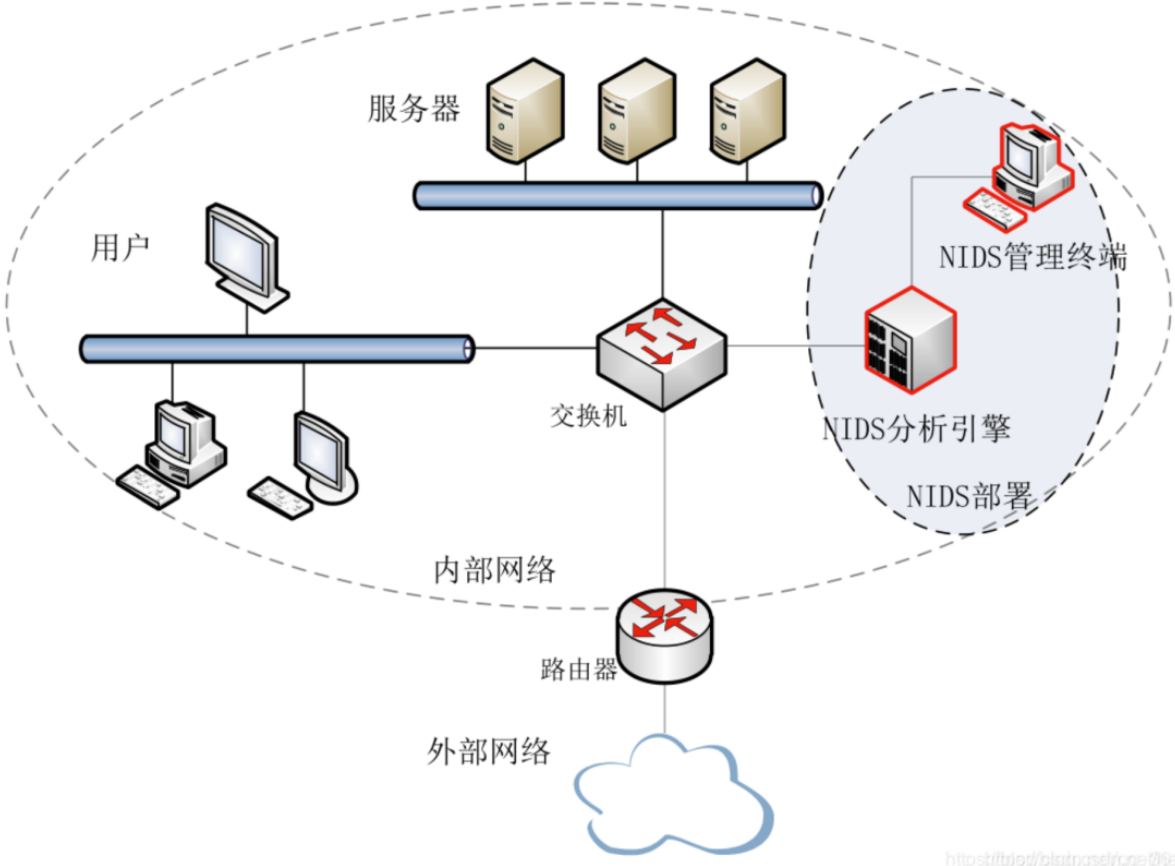
- 放置在比较重要的网段内
- 不停地监视网段中的各种数据包
- 对每一个数据包或可疑的数据包进行特征分析

基于主机的IDS



- 优点
  - 实时告警
  - 实时响应
- 缺点
  - 降低目标机的性能
  - 没有统计行为信息
  - 没有多主机标志
  - 没有用于支持起诉的原始数据
  - 降低了数据的辨析能力
  - 系统离线时不能分析数据

基于网络的IDS



按实现方式 – HIDS

优点

- 能够获得更详尽的信息
- 误报率低
- 对分析“可能的攻击行为”非常有用
- 适用于不需要广泛的入侵检测、或者传感器与控制台之间的通信带宽不足的环境

缺点

- 依赖于服务器的日志与监视功能，降低应用系统的效率，可能需要中断服务
- 全面布署HIDS代价较大
- 对入侵行为的分析的工作量将随着主机数目增加而增加

按实现方式 – NIDS

优点

- 能够检测来自网络的攻击
- 能够检测到超过授权的非法访问
- 易于安装，不影响业务系统的性能，风险小

缺点

- 监测范围受网段的限制，全网段部署传感器会使成本大大增加
- 数据量大使得NIDS很难检测一些需要大量计算和分析才能检测的攻击
- 传感器的分析能力的增强常伴随着协同能力的减弱
- 难以处理复杂协议，如：加密、高层协议

网络IDS vs 主机IDS对比

网络IDS

- 侦测速度快
- 隐蔽性好
- 视野更宽
- 较少的监测器
- 占资源少

主机IDS

- 视野集中
- 易于用户自定义
- 保护更加周密
- 对网络流量不敏感

按技术路线分类 - 1

基于统计分析的入侵检测技术

- 基于对用户历史行为进行统计，同时实时地检测用户对系统的使用情况
- 根据用户行为的概率模型与当前用户行为进行比较，一但发现可疑的情况与行为，就跟踪、监测并记录，适当时采用一定的响应手段
- 有一定的自适应能力，稳定，但误警率高

按技术路线分类 - 2

基于神经网络的入侵检测技术

- **将神经网络模型运用于入侵检测系统，可以解决基于统计数据的主观假设而导致的大量虚假警报问题，同时由于神经网络模型的自适应性，使得系统精简，成本较低**
- **但是不成熟**

按技术路线分类 - 3

基于专家系统的入侵检测技术

- **根据专家对合法行为的分析经验来形成一套推理规则，然后在此基础上构成相应的专家系统，由此专家系统自动地进行攻击分析工作**
- **推理系统的效率较低**

按技术路线分类 - 4

基于模型推理的入侵检测技术

- **对已知入侵行为建立特定的模型，监视具有特定行为特征的活动，一但发现与模型匹配的用户行为，就通过相关信息证实或否定攻击的真实性**
- **又称为模式匹配，是应用较多的入侵检测方法**

按系统各模块运行方式分类

按系统各模块的运行方式

- **集中式：系统的各个模块包括数据的收集分析集中在一台主机上运行**
- **分布式：系统的各个模块分布在不同的计算机和设备上**

- 优点
  - 实时告警
  - 实时响应

- 缺点
  - 降低目标机的性能
  - 没有统计行为信息
  - 没有多主机标志
  - 没有用于支持起诉的原始数据
  - 降低了数据的辨析能力
  - 系统离线时不能分析数据

按时效性分类

时效性

- **脱机分析：行为发生后，对产生的数据进行分析**
- **联机分析：在数据产生的同时、或者发生改变时，进行分析**

IDS评估标准

准确性

- **误警：IDS将用户正常的操作当作入侵行为，予以报警（1%~10%）**
- **漏警：IDS将入侵行为当作用户正常的操作，不予报警（10%~50%）**

处理性能

完备性

容错性

及时性

入侵检测系统的局限性

对用户知识要求较高，配置、操作和管理使用较为复杂

网络发展迅速，对入侵检测系统的处理性能要求越来越高，现有技术难以满足实际需要

高虚警率，用户处理负担重

由于警告信息记录的不完整，许多警告信息可能无法与入侵行为相关联，难以得到有用的结果

在应对对自身的攻击时，对其他数据的检测也可能会被抑制或受到影响