

# 9 入侵检测

2019年5月27日 10:02

## 0 概述

### 1 入侵检测技术的历史

### 2 入侵检测的相关概念

### 3 入侵检测的信息源

- [3.1 操作系统的审计记录](#)
- [3.2 系统日志](#)
- [3.3 应用程序的日志信息](#)
- [3.4 基于网络数据的信息源](#)
- [3.5 其他的数据来源](#)
- [3.6 信息源选择的基本原则](#)

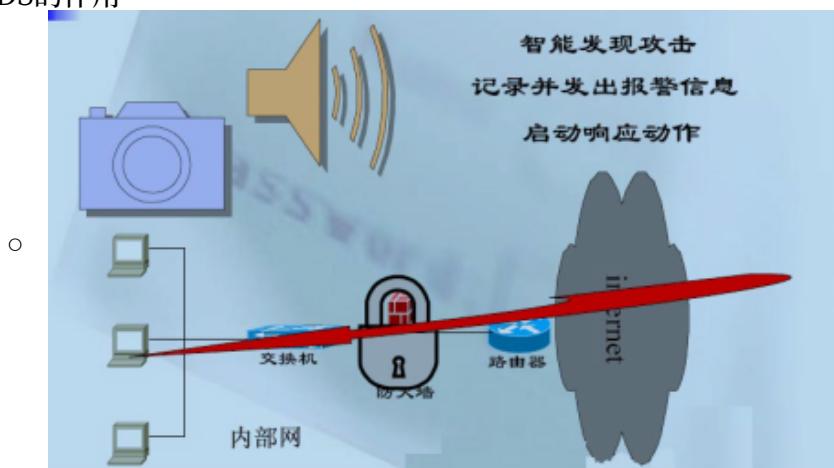
### 4 入侵检测技术的分类

- [4.1 按照信息源的分类](#)
- [4.2 按照检测方法的分类](#)
- [4.3 其他的分类标准](#)

### 5 具体的入侵检测系统

## 0 概述

- IDS存在与发展的必然性
  - 网络攻击造成的破坏性和损失日益严重
  - 网络安全威胁日益增长
  - 单纯的防火墙无法防范复杂多变的攻击
- IDS的作用



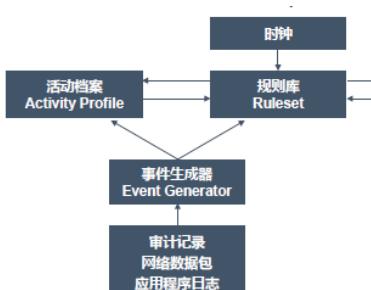
- 为什么需要IDS
  - 单一防护产品的弱点
    - 防御方法和防御策略的有限性
    - 动态多变的网络环境
    - 外部和内部的威胁
  - 关于防火墙
    - 网络边界的设备，只能抵挡外部来的入侵行为
    - 自身存在弱点，也可能被攻破
    - 对某些攻击保护很弱
    - 即使透过防火墙的保护，合法的使用者仍会非法地使用系统，甚至提升自己的权限
    - 仅能拒绝非法的连接请求，但是对于入侵者的攻击行为仍一无所知
  - 入侵很容易
    - 入侵教程随处可见
    - 乌云、freebuf、Xfocus
    - 各种工具唾手可得
- 网络安全工具的特点

优点	局限性
防火墙	可简化网络管理，产品成熟
IDS	无法处理网络内部的攻击 误警率高，缓慢攻击，新的攻

ID	类的监控和安全状态	设置较高，较慢攻击，新的攻击模式
Scanner	完全主动式安全工具，能够了解网络现有的安全水平，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	并不能真正了解网络上即时发生的攻击
○ 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

## 1. 入侵检测技术的历史

- 主机审计
  - 主机审计出现在入侵检测技术之前，其定义为：产生、记录并检查按照时间顺序排列的系统事件记录的过程。
  - 目的：早期情况下，统计用户的上机时间，便于进行计费管理。
  - 美国军方在20世纪70年代支持一项关于计算机系统安全的研究计划，最终的研究成果包括了一项重要的计算机安全评估标准——TCSEC（可信计算机系统评估准则）
  - James-Anderson在1980完成的技术报告《计算机安全威胁的监控》提出了安全审计的目标。Anderson在报告中定义了三种恶意用户：
    - 伪装者（Masquerader）：此类用户试图绕过系统安全访问控制机制，从而利用合法用户的系统账户。
    - 违法者（Misfeasor）：在计算机系统上执行非法活动的合法用户
    - 秘密活动者（ClandestinedUser）：此类用户在获取系统最高权限后，利用此权限以一种审计机制难以发现的方式进行秘密活动，或者干脆关闭审计记录过程。
- 入侵检测模型的建立
  - 1987年DorothyDenning发表了入侵检测领域内的经典论文《入侵检测模型》



- 技术发展的历程
  - 入侵检测技术是20世纪80年代早期提出的
  - 1984-1986年，Denning和Neumann在SRI公司内设计并实现了著名的IDES，该系统是早期入侵检测系统中最具有影响力的一个
  - 1987年，DorothyDenning发表的经典论文“AnIntrusionDetectionModel”，提出入侵检测模型
  - 1989-1991年，StephenSmaha设计开发了Haystack入侵检测系统，该系统用于美国空军内部网络的安全检测目的
  - 1990年，加州大学Davis分校的ToddHeberlien在IEEE上发表了“ANetworkSecurityMonitor”，标志着入侵检测第一次将网络数据包作为实际输入的信息源
  - 1992年，加州大学圣巴巴拉分校的Porras和Ilgun提出了状态转换分析的入侵检测技术，并实现了原型系统USTAT，之后发展出NSTAT、NetSTAT等系统
  - 同一时期，KathleenJackson在LosAlamos国家实验室设计开发了NADIR入侵检测系统，该系统用于监控LosAlamos的内部计算网络环境，采用了以每周计算活动档案的统计技术来描述用户的活动情况，并使用了专家系统规则来检测异常的用户行为
  - SAIC和HaystackLabs分别开发出CMDS系统和Stalker系统，这两个系统是首批投入商用的主机入侵检测系统
  - 1994年，Porras在SRI发出IDES系统的后继版本NIDES系统，进一步SRI开发了用于分布式环境的EMERALD系统
  - 1995年，普渡大学的S.Kumar在STAT的思想基础上，提出了基于有色Petri网的模式匹配计算模型，并实现了IDIOT原型系统
  - 1996年，新墨西哥大学的Forrest提出了基于计算机免疫学的入侵检测技术
  - 1997年，Cisco公司开始将入侵检测技术嵌入到路由器，同时ISS公司发布了基于Windows平台的RealSecure入侵检测系统，自此拉开了商用网络入侵检测系统的序幕

- 1999年，LosAlamos的V.Paxson开发了Bro系统，用于高速网络环境下的入侵检测系统。
- 1999年，加州大学的Davis分校发布了GrIDS系统，该系统试图为入侵检测技术扩展到大型网络环境提供一个实际的解决方案
- WenkeLee提出了用于入侵检测的数据挖掘技术框架
- 2000年，普渡大学的DiegoZamboni和E.Spafford提出了入侵检测的自治代理结构，并实现了原型系统AAFID系统

## 2 入侵检测的相关概念

- 入侵的定义
  - 计算机安全的三个目标：
    - 机密性.保证系统信息不被非授权的用户访问
    - 完整性.防止信息被非法的修改或破坏
    - 可用性.保证系统信息和资源能够持续有效，并能按照用户所需的时间地点和方式加以访问
  - 安全策略用于将抽象的安全目标和概念映射为现实世界中的具体安全规则，通常定义为一组用于保护系统计算资源和信息资源的目标、过程和管理规则的集合
  - 任何潜在的危害系统安全状况的事件和情况都可以称为“威胁”，Anderson在1980年的技术报告中建立了威胁的早期模型，并按照威胁来源分为三类。
    - 外部入侵者：系统的非授权用户
    - 内部入侵者：超越合法权限的系统授权用户
    - 违法者：在计算机系统上执行非法程序的合法用户
  - 入侵：表示系统内部发生的任何违反安全策略的事件，除了上述威胁外，还包括：
    - 恶意程序的威胁
    - 探测和扫描系统配置信息和安全漏洞
  - 美国国家安全通信委员会（NSTAC）下属的入侵检测小组（IDSG）在1997年给出了关于“入侵”的定义：
    - 入侵是对信息系统的非授权访问以及（或者）未经许可在信息系统内进行的操作
- 入侵检测的定义
  - 检测对计算机系统的非授权访问
  - 对系统的运行状态进行监视，发现各种攻击企图、攻击行为或者攻击结果，以保证系统资源的机密性、完整性和可用性
  - 识别针对计算机系统和网络系统，或者更广泛意义上信息系统的非法攻击，包括检测外部非法入侵者的恶意攻击和试探，以及内部合法用户的超越使用权限的非法行为（违法者-秘密活动者）
  - 美国国家安全通信委员会（NSTAC）下属的入侵检测小组（IDSG）在1997年给出了关于“入侵检测”的定义：
    - 入侵检测是对企图入侵、正在进行的入侵或者已经发生的入侵进行识别的过程
  - 所有能够执行入侵检测任务和功能的系统，都可以称为入侵检测系统，包括软件系统和硬件系统。
- 入侵检测与通用入侵检测系统模型



- 数据收集器（探测器）：主要负责收集数据
- 检测器（分析器/检测引擎）：负责分析和检测入侵的任务，并发出报警信号
- 知识库：提供必要的数据信息支持
- 控制器：根据报警信号，人工或自动做出反应动作
- 另外，绝大多数入侵检测系统都会包含一个用户接口组件，用于观察系统的运行状态和输出信号，并对系统行为进行控制

## IDS基本结构

入侵检测系统包括三个功能部件

- [信息收集](#)
- [分析引擎](#)
- [响应动作](#)

### 信息收集

- 入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为
- 需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息
  - 尽可能扩大检测范围
  - 从一个源来的信息有可能看不出疑点
- 入侵检测的效果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
- 信息收集的来源
  - 系统或网络的日志文件
  - 网络流量
  - 系统目录和文件的异常变化
  - 程序执行中的异常行为

### 分析引擎

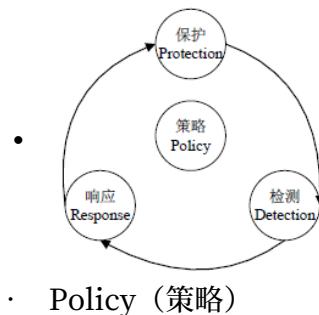
- 模式匹配
  - 模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为
  - 一般来讲，一种攻击模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）
- 统计分析
  - 统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）
  - 测量属性的平均值和偏差被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生
- 完整性分析
  - 完整性分析主要关注某个文件或对象是否被更改
    - 包括文件和目录的内容及属性
    - 在发现被更改的、被安装木马的应用程序方面特别有效

### 响应动作

- 简单报警
- 切断连接
- 封锁用户
- 改变文件属性
- 最强烈反应：回击攻击者

### 入侵检测与PPDR模型

- PPDR模型是Policy（策略）、Protection（防护）、Detection（检测）和Response（响应）的缩写，特点是动态性和基于时间的特性



- PPDR的核心内容。规定了系统所要达到的安全目标和为达到安全目标所采取的各种具体安全措施及其实施强度
- Protection (防护)
  - 具体包括制定安全管理规则、进行系统安全配置工作以及安装各种安全防护设备
- Detection (检测)
  - 采用各种安全措施后，根据系统运行情况的变化，对系统安全状态进行实时的动态监控
- Response (响应)
  - 当发现了入侵活动或入侵结果后，需要系统做出及时的反应并采取措施
- PPDR模型阐述的结论：
  - 安全的目标实际上就是尽可能的增大保护时间，尽量减少检测时间和响应时间

### **3 入侵检测的信息源**

- 对于入侵检测而言，输入数据的选择是首先需要解决的问题，其原因包括：
  - 入侵检测的输出结果，首先取决于所能获得的输入数据的数量和质量
  - 具体采用的入侵检测技术类型，也常常因为所选择的输入数据的类型不同而各不相同
- 几种常用输入数据类型
  - [3.1 操作系统的审计记录](#)
  - [3.2 系统日志](#)
  - [3.3 应用程序的日志信息](#)
  - [3.4 基于网络数据的信息源](#)
  - [3.5 其他的数据来源](#)
  - [3.6 信息源选择的基本原则](#)

#### **3.1 操作系统的审计记录**

- 最早采用的用于入侵检测任务的输入数据源就是操作系统的审计记录
- 操作系统审计记录被认为是基于主机入侵检测技术的首选数据源，原因为：
  - 操作系统的审计系统在设计时，就考虑了审计记录的结构化组织工作以及对审计记录内容的保护机制
  - 操作系统审计记录提供了在系统内核级的事件发生情况，反映的是系统底层的活动情况并提供了相关的详尽信息
- 操作系统的审计记录--SunSolarisBSM：
  - BSM安全审计子系统主要概念包括：审计日志、审计文件、审计记录和审计令牌
  - 审计日志是由一个或多个审计文件组成，每个审计文件包含多个审计记录，而每个审计记录则由一组审计令牌构成
  - 每一个BSM审计记录都揭示了一次审计事件的发生
  - BSM审计记录以二进制形式进行存储，其字段结构和数据结构大小都实现了预先定义，从而提供了在不同平台系统间进行移植的兼容性

#### **3.2 系统日志**

- 操作系统日志
  - 操作系统日志是指与主机信息源相关的，使用操作系统日志机制生成的日志文件的总称
- 应用程序日志
  - 应用程序日志是指由应用程序自己生成并维护的日志文件的总称
- 系统日志的安全性较操作系统的审计记录差，原因为：
  - 产生系统日志的软件通常是在内核外运行的应用程序，而不是像操作系统审计记录是由系统内核模块生成，因而这些软件容易受到恶意的修改或攻击
  - 系统日志通常是存储在普通的不受保护的文件目录里，并且常常以简单文本文件格式存储，容易受到恶意的篡改和删除等操作，而审计记录通常以二进制文件的形式存放，且具备较强的保护机制

#### **3.3 应用程序的日志信息**

- 应用程序日志可作为分析检测的数据源，原因如下：
  - 应用程序日志是用户级别的系统活动抽象信息，所以更加容易理解和处理
  - 网络化计算环境的普及，导致入侵攻击行为的目标越来越集中于提供网络服务的各种特定应用程序

- 应用程序日志作为分析检测的数据源的问题和风险：
  - 应用程序的日志信息通常更容易遭到恶意的攻击，包括篡改和删除等操作
  - 尽管很多操作系统提供应用程序级别的审计功能，但是很多特定的应用程序中并不包括这些审计特性，或者是审计功能并没有提供足够详细的信息
  - 特定应用程序同样存在是否值得依赖的问题

### 3.4 基于网络数据的信息源

- 采用网络数据源有以下优势：
  - 通过网络被动监听方式获取网络数据包，作为入侵检测系统输入信息源的工作过程，对目标监控系统的运行性能几乎没有任何影响，并且通常无须改变原有网络的结构和工作方式
  - 嗅探器模块在工作时，可以采用对网络用户透明的模式，因而降低了其本身遭到入侵者攻击的概率
  - 基于网络数据的输入信息源，可以发现许多基于主机数据源所无法发现的攻击手段，例如基于网络协议的漏洞发掘过程
  - 网络数据包的标准化程度，相对主机数据源而言要高许多，例如目前几乎大部分网络协议都采用了TCP/IP协议族

### 3.5 其他的数据来源

- 其他安全产品提供的数据
  - 如防火墙
- 网络设备提供的数据
  - 网络管理系统
  - 路由器
  - 交换机
- “带外”信息源
  - 所谓“带外”数据源通常是指人工方式提供的数据信息，例如人工记录下的各种类型的系统事件和相关信息等

### 3.6 信息源选择的基本原则

- 根据入侵检测系统设计的检测目标来选择所需的输入数据源
- 在不影响目标系统运行性能和实现安全检测目标的前提下，最少需要多少信息，或者是最少数目的输入数据源

## 4 入侵检测技术的分类

- [4.1 按照信息源的分类](#)
- [4.2 按照检测方法的分类](#)
- [4.3 其他的分类标准](#)

### 4.1 按照信息源的分类

- 基于主机的入侵检测
  - 基于主机的入侵检测通常从主机的审计记录和日志文件中获得所需的主要数据源，并辅之以主机上的其他信息，在此基础上完成检测攻击行为的任务
  - 优点：
    - 能够较为准确地监测到发生在主机系统高层的复杂攻击行为
  - 缺点：
    - 无法移植
    - 影响性能
    - 无法对网络环境下发生的大量攻击行为做出及时的反映
- 基于网络的入侵检测
  - 基于网络的入侵检测通过监听网络中的数据包来获得必要的数据来源，并通过协议分析、特征匹配、统计分析等手段发现当前发生的攻击行为
  - 优点：
    - 能够实时监控网络中的数据流量，并发现潜在的攻击行为和做出迅速的响应
    - 可移植性好
    - 不影响宿主机性能
  - 缺点：
    - 准确率
    - 发生在应用进程级别的攻击行为无法依靠基于网络的入侵检测来完成

## 4.2 按照检测方法的分类

- 滥用入侵检测
  - 滥用入侵检测的技术基础是分析各种类型的攻击手段，并找出可能的“攻击特征”集合
- 异常入侵检测
  - 通常都会建立一个关于系统正常活动的状态模型并不断进行更新，然后将用户当前的活动情况与这个正常模型进行对比，如果发现了超过设定阈值的差异程度，则指示发现了非法攻击行为
- 滥用入侵检测与异常入侵检测的比较
  - 滥用入侵检测比异常入侵检测具备更好的确定解释能力
  - 滥用入侵检测具备较高的检测率和较低的虚警率
  - 开发规则库和特征集合方便、容易
  - 滥用检测只能检测到已知的攻击模式，模式库只有不断更新才能检测到新的攻击方式
  - 异常检测可以检测到未知的入侵行为

## 4.3 其他的分类标准

- 非实时处理系统
  - 通常在事后收集的审计日志文件基础上，进行离线分析处理，并找出可能的攻击行为踪迹，目的是进行系统配置的修补工作，防范以后的攻击
- 实时处理系统
  - 根据用户需求而定的变量，系统分析和处理的速度处于用户需求范围内

## 5 具体的入侵检测系统

- NFR公司的NID
  - 基本上是一种基于规则检测的网络入侵检测系统，同时具备一些异常入侵检测功能
  - 最大的特点就是独一无二的设计架构，设计了一套用于网络管理和安全检测的脚本语言N-Code，可以用来创建入侵检测的检测特征库
- ISS公司的RealSecure
  - 工作组管理器
    - 控制台
    - 企业数据库
    - 事件收集器
  - 传感器
    - 网络传感器
    - 操作系统传感器
    - 服务器传感器
- NAI公司的CyberCopMonitor
  - 混合型入侵检测系统，通过单一控制台提供基于网络和主机的入侵检测功能。两个主要组件
    - 控制台
    - 代理
- Cisco公司的CiscoSecureIDS
  - 传统的网络入侵检测系统，通常与硬件平台捆绑销售。包括三个基本组件
    - 传感器
    - 控制台
    - 入侵检测系统模块