# 第7章 入侵检测技术

# 网络安全的构成

- 物理安全性
  - 设备的物理安全：防火、防盗、防破坏等
- 通信网络安全性
  - 防止入侵和信息泄露
- 系统安全性
  - 计算机系统不被入侵和破坏
- 用户访问安全性
  - 通过身份鉴别和访问控制，阻止资源被非法用户访问
- 数据安全性
  - 数据的完整、可用
- 数据保密性
  - 信息的加密存储和传输

# 安全的分层结构和主要技术

# 主要的传统安全技术

- 加密
- 消息摘要、数字签名
- 身份鉴别：口令、鉴别交换协议、生物特征
- 访问控制
- 安全协议： **IPSec、SSL**
- 网络安全产品与技术：防火墙、**VPN**
- 内容控制: 防病毒、内容过滤等

“预防（**prevention**）”和“防护（**protection**）”的思想

# 传统安全技术的局限性

- 传统的安全技术采用严格的访问控制和数据加密策略来防护
  - 在复杂系统中，这些策略是不充分的
  - 这些措施都是以性能损失为代价的
- 大部分损失是由内部引起的
  - 80%以上的损失是内部威胁造成的
  - 传统安全技术难于防内
- 传统的安全技术基本上是一种被动的防护，而如今的攻击和入侵要求我们主动地去检测、发现和排除安全隐患
  - 传统安全措施不能满足这一点

# 7.1 入侵检测系统（IDS）概述

## 入侵检测系统的定义

- 入侵（Intrusion）
  - 企图进入或滥用计算机或网络系统的行为
  - 可能来自于网络内部的合法用户
- 入侵检测（Intrusion Detection）
  - 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
- 入侵检测系统（Intrusion Detection System， IDS）
  - 定义：进行入侵检测的软件与硬件的组合便是入侵检测系统
  - 功能：监控计算机系统或网络系统中发生的事件，根据规则进行安全审计

# 为什么需要入侵检测系统

- 入侵很容易
  - 入侵教程随处可见
  - 各种工具唾手可得
- 防火墙不能保证绝对的安全
  - 网络边界的设备
  - 自身可以被攻破
  - 对某些攻击保护很弱
  - 不是所有的威胁来自防火墙外部
  - 防火墙是锁，入侵检测系统是监视器
- 入侵检测系统IDS
  - 通过对计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象

# 入侵检测的任务

- 检测来自内部的攻击事件和越权访问
  - 80%以上的攻击事件来自于内部的攻击
  - 防火墙只能防外，难于防内
- 入侵检测系统作为传统安全工具的一个有效补充
  - 入侵检测系统可以有效的防范防火墙开放的服务入侵
  - 通过事先发现风险来阻止入侵事件的发生，提前发现试图攻击或滥用网络系统的人员
  - 检测其它安全工具没有发现的网络工具事件
  - 提供有效的审计信息，详细记录黑客的入侵过程，从而帮助管理员发现网络的脆弱性

# 入侵检测相关术语

- **IDS (Intrusion Detection System)**
  - 入侵检测系统
- **Promiscuous**
  - 混杂模式，即IDS网络接口可以看到网段中所有的网络通信量，不管其来源或目的地
- **Signatures**
  - 特征，即攻击的特征
- **Alerts**
  - 警告
- **Anomaly**
  - 异常
- **Console**
  - 控制台
- **Sensor**
  - 传感器，即检测引擎

# 7.2 IDS的类型和策略

- 按照数据来源：
  - 基于主机
    - 系统获取数据的依据是系统运行所在的主机，保护的目标也是系统运行所在的主机
  - 基于网络
    - 系统获取的数据是网络传输的数据包，保护的是网络的运行

# 7.2 IDS的类型和策略

- 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
- 根据时效性
  - 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

# 基于主机的入侵检测系统

- 基于主机的入侵检测系统: **Host-Based IDS(HIDS)**
  - 系统安装在主机上面，对本主机进行安全检测
- 优点
  - 审计内容全面，保护更加周密
  - 视野集中
  - 适用于加密及交换环境
  - 易于用户自定义
  - 对网络流量不敏感
- 缺点
  - 额外产生的安全问题
  - **HIDS**依赖性强
  - 如果主机数目多，代价过大
  - 不能监控网络上的情况

# 基于网络的入侵检测系统

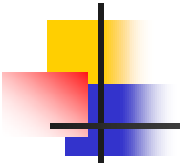
- 基于网络的入侵检测系统：**Network-Based IDS(NIDS)**
  - 系统安装在比较重要的网段内
  - 在共享网段上对通信数据进行侦听采集数据
- 优点
  - 检测范围广，提供对网络通用的保护
  - 无需改变主机配置和性能，安装方便
  - 独立性，操作系统无关性
  - 侦测速度快
  - 隐蔽性好
  - 较少的监测器，占资源少
- 缺点
  - 不能检测不同网段的网络包
  - 很难检测复杂的需要大量计算的攻击
  - 协同工作能力弱
  - 难以处理加密的会话

# 集中式入侵检测系统（CIDS）

- CIDS（Centralized）的各个模块包括数据的收集与分析以及响应都集中在一台主机上运行，这种方式适用于网络环境比较简单的情况。CIDS也可能有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器，审计程序将当地收集到的数据踪迹发送给中央服务器进行分析处理。
- CIDS在系统的可伸缩性、可配置性方面存在致命缺陷。随着网络规模的增大，主机审计程序和服务器之间传送的数据量就会骤增，必将导致网络性能的降低。且一旦中央服务器出现故障，整个系统将会陷入瘫痪。

# 分布式入侵检测系统（DIDS）

- DIDS（Distributed）的各个模块分布在网络中不同的计算机、设备上。一般来说分布性主要体现在数据收集模块上，如果网络环境比较复杂、数据量比较大，那么数据分析模块也会分布在网络的不同计算机设备上，通常是按照层次性的原则进行组织。
- DIDS根据各组件间的关系还可细分为层次式DIDS和协作式DIDS。其中层次式DIDS是一种部分分布控制形式，而协作式DIDS是全分布式控制形式。



# IDS基本结构

- 入侵检测系统包括三个功能部件
  - 信息收集
  - 信息分析
  - 结果处理

# 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

# 信息分析

分析得到的数据，并产生分析结果

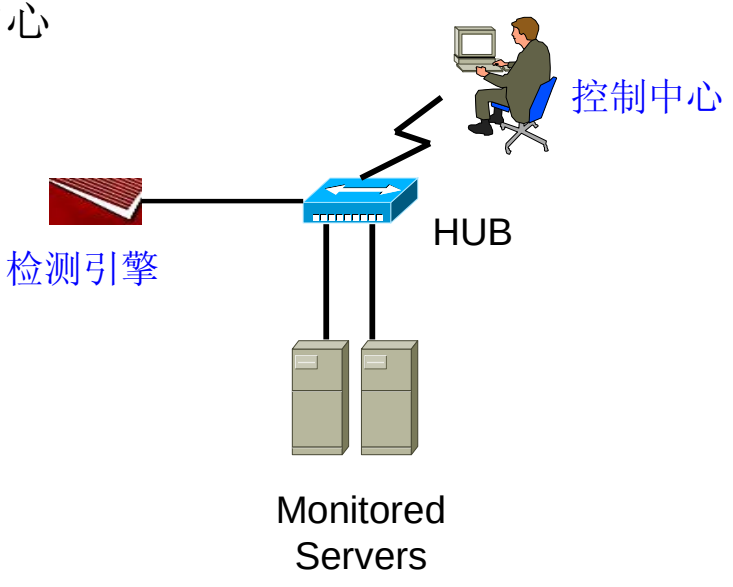
- 模式匹配
  - 将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为
- 统计分析
  - 首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值和偏差将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生
- 完整性分析
  - 事后分析
  - 主要关注某个文件或对象是否被更改
  - 在发现被更改的、被安装木马的应用程序方面特别有效

# 结果处理

- 结果处理，即对分析结果作出反应。
  - 切断连接
  - 改变文件属性
  - 发动对攻击者的反击
  - 报警
  - ……

# IDS的组成

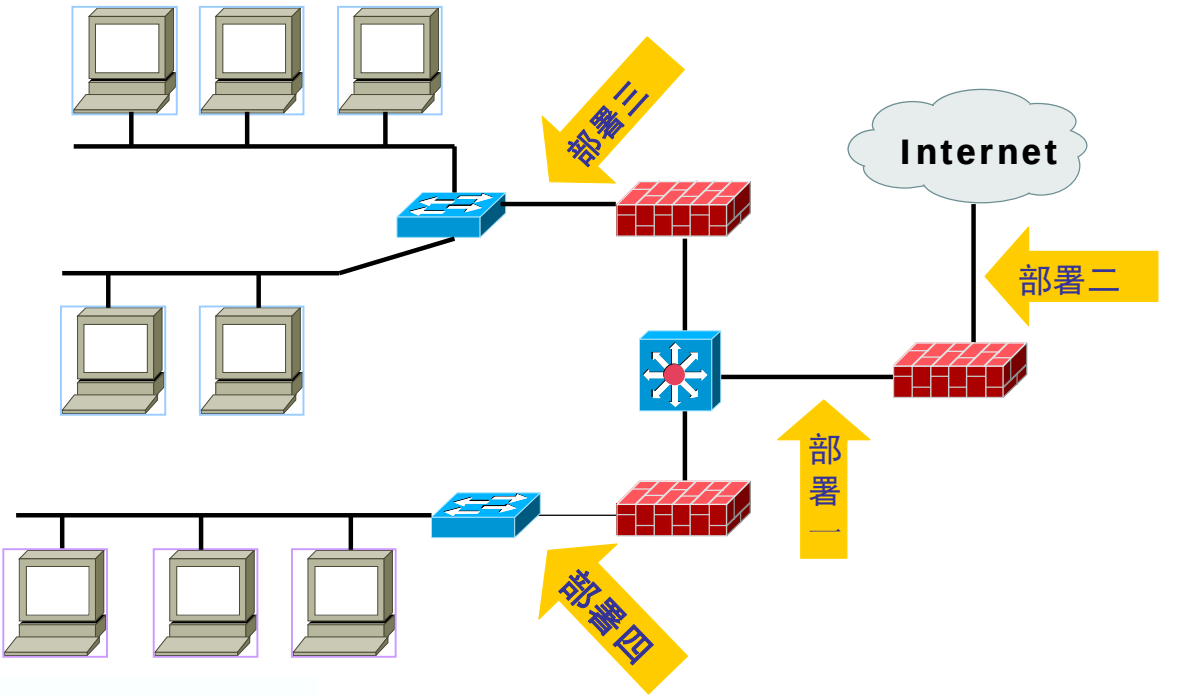
- 检测引擎
- 控制中心



# 检测引擎的部署位置

- 放在边界防火墙之内
- 放在边界防火墙之外
- 放在主要的网络中枢
- 放在一些安全级别需求高的子网

# 检测引擎的部署位置示意图



# 7.3 IDS的检测技术

## 网络入侵技术

- 入侵(Intrusion)是指未经授权蓄意尝试访问信息、篡改信息，使系统不可靠或不能使用的行为
  - 破坏计算机或网络资源的完整性、机密性、可用性、可控性
- 入侵者
  - 可以是一个手工发出命令的人，也可是一个基于入侵脚本或程序的自动发布命令的计算机
  - 入侵者可以被分为两类:
    - 外部的: 网络外面的侵入者
    - 内部的: 合法使用网络的侵入者，包括滥用权力的人和模仿更改权力的人(比如使用别人的终端) 。 80%以上的安全问题同内部人有关

# 侵入系统的主要途径

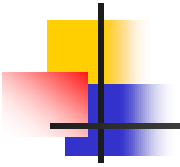
- 物理侵入
  - 侵入者对主机有物理进入权限
  - 方法如移走磁盘等存储介质并在另外的机器读/写
- 系统侵入
  - 侵入者已经拥有系统的较低权限
  - 侵入者可能利用一个知名漏洞获得系统管理员权限的机会
- 远程侵入
  - 入侵者通过网络远程进入系统，侵入者从无特权开始
  - 入侵检测系统主要关心远程侵入

# 网络入侵的一般步骤

- 目标探测和信息收集
- 自身隐藏
- 利用漏洞侵入主机
- 稳固和扩大战果
- 清除日志

# 目标探测和信息收集

- 利用扫描器软件扫描
  - 端口扫描
  - 漏洞扫描
  - 常用扫描器软件：**Linux Kali/BackTrack，SATAN，流光，Nessus，Metasploit**
- 利用**SNMP**了解网络结构
  - 搜集网络管理信息
  - 网络管理软件也成为黑客入侵的一直辅助手段



# 自身隐藏

- 典型的黑客使用“跳板”技术来隐藏IP地址
  - 通过telnet在以前攻克的Unix主机上跳转
  - 通过终端管理器在Windows主机上跳转
  - 配置代理服务器
- 更高级的黑客，精通系统内核，后门技术伪装成普通用户

# 利用漏洞侵入主机

- 已经利用扫描器发现漏洞
  - 例如CGI/IIS漏洞
- 充分掌握系统信息
- 进一步入侵

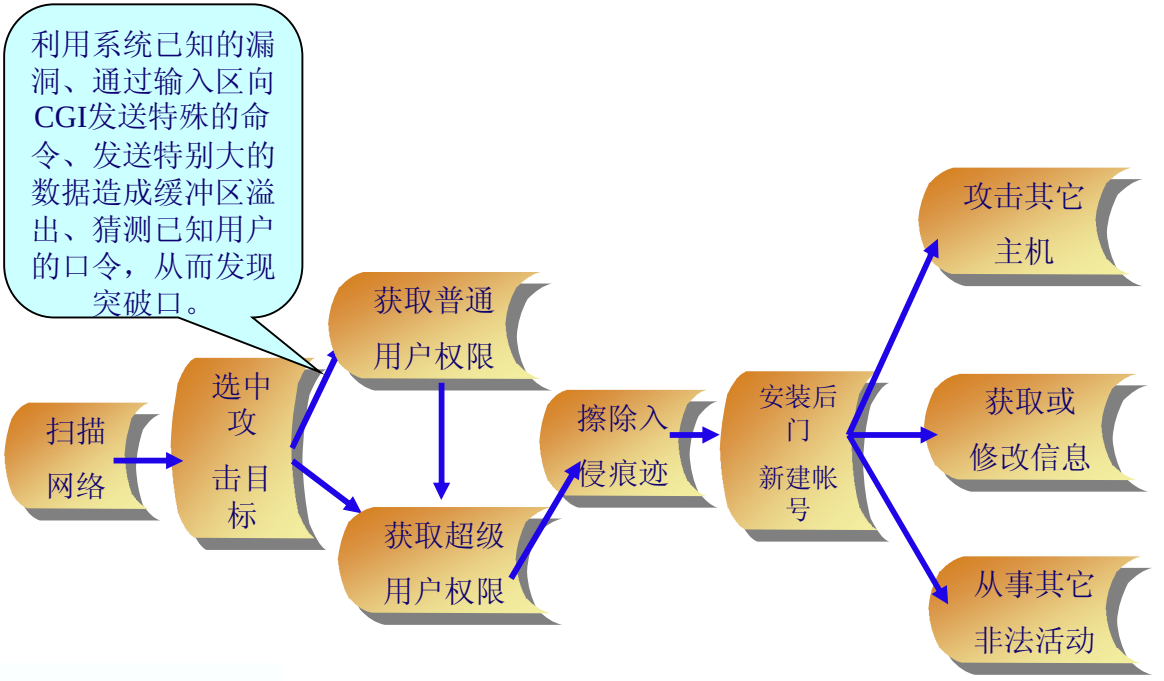
# 稳固和扩大战果

- 安装后门
  - **BO**，冰河
- 添加系统账号
- 添加管理员账号
- 利用**LKM**
  - **Loadable Kernel Modules**
  - 动态加载
  - 无需重新编译内核
- 利用信任主机
  - 控制了主机以后，可以利用该主机对其它邻近和信任主机进行入侵
  - 控制了代理服务器，可以利用该服务器对内部网络进一步入侵

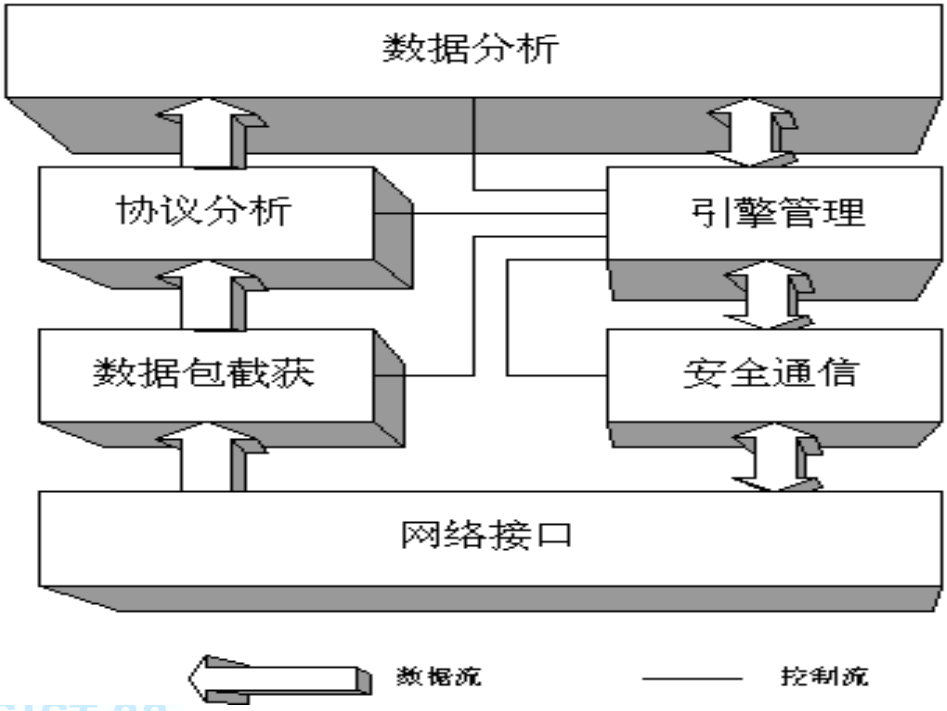
# 清除日志

- 清除入侵日志
  - **Windows**
    - 清除系统日志
    - 清除**IIS**日志
    - 清除**FTP**日志
    - 清除数据库连接日志
  - **Unix**
    - 登陆信息 **/var/log**
    - **/home/user/.bash_history**
    - **lastlog**
- 使管理员无法发现系统已被入侵

# 网络入侵步骤总览


利用系统已知的漏洞、通过输入区向CGI发送特殊的命令、发送特别大的数据造成缓冲区溢出、猜测已知用户的口令，从而发现突破口。
扫描网络
选中攻击目标
获取普通用户权限
获取超级用户权限
擦除入侵痕迹
安装后门
新建帐号
攻击其它主机
获取或修改信息
从事其它非法活动

# 入侵检测引擎工作流程 - 1



# 入侵检测引擎工作流程 - 2

- 监听部分
  - 网络接口混杂模式
  - 根据设置过滤一些数据包
- 协议分析
  - **IP，IPX，PPP，……**
- 数据分析
  - 根据相应的协议调用相应的数据分析函数
  - 一个协议数据有多个数据分析函数处理
  - 数据分析的方法是入侵检测系统的核心
- 引擎管理
  - 协调和配置给模块间工作
  - 数据分析后处理方式
    - **Alert**
    - **Log**
    - **Call Firewall**

# 入侵检测的分析方式

- 异常检测（**Anomaly Detection**）
- 误用检测（**Misuse Detection**）
- 完整性分析

# 异常检测

- 基本原理
  - 正常行为的特征轮廓
  - 检查系统的运行情况
  - 统计模型
- 优点
  - 可以检测到未知的入侵
  - 可以检测冒用他人帐号的行为
  - 具有自适应，自学习功能
  - 不需要系统先验知识
- 缺点
  - 漏报、误报率高
    - 入侵者可以逐渐改变自己的行为模式来逃避检测
    - 合法用户正常行为的突然改变也会造成误警
  - 统计算法的计算量庞大，效率很低
  - 统计点的选取和参考库的建立比较困难

# 误用检测

- 基本原理
  - 提前建立已出现的入侵行为特征
  - 检测当前用户行为特征
  - 模式匹配
- 优点
  - 算法简单
  - 系统开销小
  - 准确率高
  - 效率高
- 缺点
  - 被动
    - 只能检测出已知攻击
    - 新类型的攻击会对系统造成很大的威胁
  - 模式库的建立和维护难
    - 模式库要不断更新
    - 知识依赖于硬件平台、操作系统和系统中运行的应用程序

# 完整性分析

- 基本原理
  - 通过检查系统的当前系统配置，诸如系统文件的内容或者系统表，来检查系统是否已经或者可能会遭到破坏
- 优点
  - 不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其它对象的任何改变，它都能够发现
- 缺点
  - 一般以批处理方式实现，不用于实时响应

# 入侵检测具体方法 - 1

- 基于统计方法的入侵检测技术
  - 审计系统实时地检测用户对系统的使用情况，根据系统内部保持的用户行为的概率统计模型进行监测，当发现有可疑的用户行为发生时，保持跟踪并监测、记录该用户的行为
- 基于神经网络的入侵检测技术
  - 采用神经网络技术，根据实时检测到的信息有效地加以处理作出攻击可能性的判断
- 基于专家系统的入侵检测技术
  - 根据安全专家对可疑行为的分析经验来形成一套推理规则，然后再在此基础之上构成相应的专家系统，并应用于入侵检测
- 基于模型推理的入侵检测技术
  - 为某些行为建立特定的模型，从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本，这种系统就能检测出非法的用户行为
  - 一般为了准确判断，要为不同的攻击者和不同的系统建立特定的攻击脚本

# 入侵检测具体方法 - 2

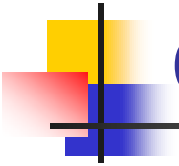
- 基于免疫原理的入侵检测技术
- 基于遗传算法的入侵检测技术
- 基于基于代理检测的入侵检测技术
- 基于数据挖掘的入侵检测技术

# 入侵检测响应机制

- 弹出窗口报警
- **E-mail**通知
- 切断**TCP**连接
- 执行自定义程序
- 与其他安全产品交互
  - **Firewall**
  - **SNMP Trap**

# IDS标准化要求

- 随着网络规模的扩大，网络入侵的方式、类型、特征各不相同，入侵的活动变得复杂而又难以捉摸
- 某些入侵的活动靠单一IDS不能检测出来，如分布式攻击
- 网络管理员常因缺少证据而无法追踪入侵者，入侵者仍然可以进行非法的活动
- 不同的IDS之间没有协作，结果造成缺少某种入侵模式而导致IDS不能发现新的入侵活动
- 目前网络的安全也要求IDS能够与访问控制、应急、入侵追踪等系统交换信息，相互协作，形成一个整体有效的安全保障系统



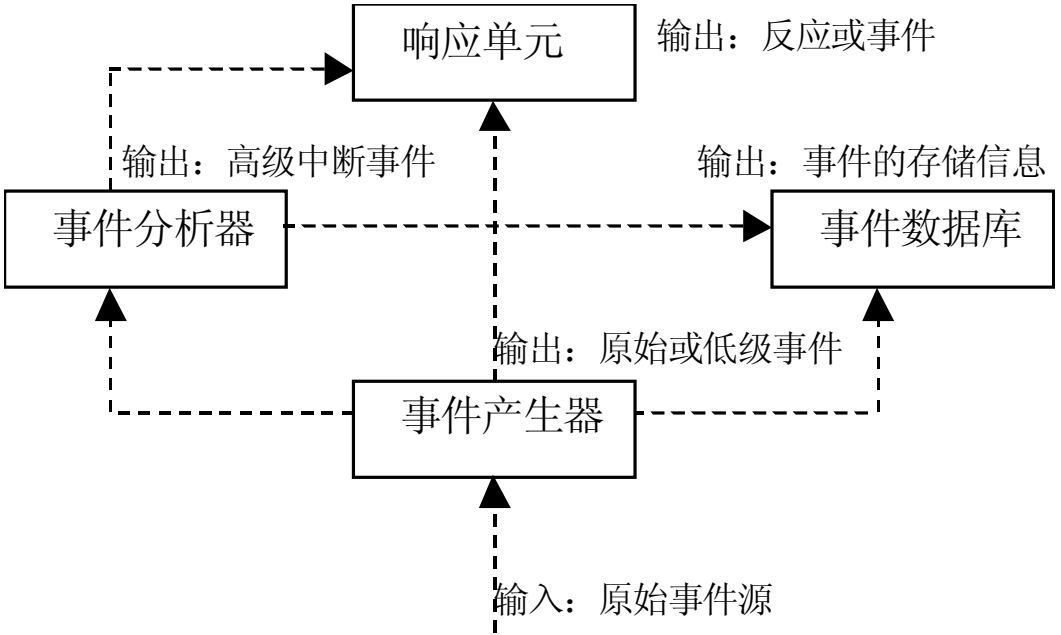
# CIDF

- The Common Intrusion Detection Framework, CIDF
- CIDF是一套规范，它定义了IDS表达检测信息的标准语言以及IDS组件之间的通信协议
- 符合CIDF规范的IDS可以共享检测信息，相互通信，协同工作，还可以与其它系统配合实施统一的配置响应和恢复策略
- CIDF的主要作用在于集成各种IDS使之协同工作，实现各IDS之间的组件重用，所以CIDF也是构建分布式IDS的基础

# CIDF规格文档

- 体系结构
  - 阐述了一个标准的IDS的通用模型
- 规范语言
  - 定义了一个用来描述各种检测信息的标准语言
- 内部通讯
  - 定义了IDS组件之间进行通信的标准协议
- 程序接口
  - 提供了一整套标准的应用程序接口

# CIDF的体系结构示意图



# CIDF的体系结构

- 事件产生器
  - 信息收集，即从整个计算环境中获得事件，并向系统的其他部分提供此事件
- 事件分析器
  - 信息分析，即分析得到的数据，并产生分析结果
- 响应单元
  - 结果处理，即对分析结果作出反应。
    - 切断连接
    - 改变文件属性
    - 发动对攻击者的反击
    - 报警
    - ……
- 事件数据库是存放各种中间和最终数据的地方的统称
  - 可以是复杂的数据库，也可以是简单的文本文件

# 入侵防御系统 IPS

- 入侵防御系统(Intrusion Prevention System 简称IPS)。它不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，大幅度地提高了检测和阻止网络攻击的效率，是今后网络安全架构的一种发展趋势。
- 原理在于IPS拥有大量的过滤器，针对不同的攻击行为，IPS 需要不同的过滤器，每种过滤器都设有相应的过滤规则。
- 当新的攻击手段被发现之后， IPS 就会创建一个新的过滤器。IPS 数据包处理引擎可以深层检查数据包的内容。如果有攻击者利用从数据链路层到应用层的漏洞发起攻击， IPS能够从数据流中检查出这些攻击并加以阻止。
- 基于主机的IPS (HIPS) 、 基于网络的IPS (NIPS)

# 7.4 IDS的实际应用

- IDS在越来越多的企业重视安全时候被提出，针对目前市场上的硬件IDS入侵检测系统来说都是非常昂贵的，比如联想的IDS，金山IDS等设备，如果你有钱也可以考虑cisco IDS，当然，你完全可以使用IDS软件来架设属于自己的ids服务器来确保网络的安全。
- 思科入侵检测系统（IDS）
  - Cisco IPS 4200系列传感器
  - Cisco 入侵检测系统服务模块(IDSM-2)

# 热门入侵检测排行榜

| | | |
|---|---|---|
| 1 | 启明星辰天清NIPS-3060 | ￥61.86万 |
| 2 | 华为NIP 2100D | ￥11.86万 |
| 3 | 启明星辰天阗NS100 | ￥8.58万 |
| 4 | 网御星云Power V6000-P23GQ | ￥13.8万 |
| 5 | 华为NIP 2100 | ￥19.8万 |
| 6 | 启明星辰天清NIPS-2060 | ￥40.86万 |
| 7 | 启明星辰天阗NS2200 | ￥48.86万 |
| 8 | 网御星云TD3000-GS35GX-EC | ￥22.5万 |
| 9 | 网御星云TS-SC104G-EC | ￥24.3万 |
| 10 | 启明星辰天阗NS500 | ￥21.86万 |

# Snort

- 这是一个几乎人人都喜爱的开源IDS，它采用灵活的基于规则的语言来描述通信，将签名、协议和不正常行为的检测方法结合起来。其更新速度极快，成为全球部署最为广泛的入侵检测技术，并成为防御技术的标准。通过协议分析、内容查找和各种各样的预处理程序，Snort可以检测成千上万的蠕虫、漏洞利用企图、端口扫描和各种可疑行为。需要免费的BASE来分析Snort的警告
- BASE：又称基本的分析和安全引擎，BASE是一个基于PHP的分析引擎，它可以搜索、处理由各种各样的IDS、防火墙、网络监视工具所生成的安全事件数据。其特性包括一个查询生成器并查找接口，这种接口能够发现不同匹配模式的警告,还包括一个数据包查看器/解码器，基于时间、签名、协议、IP地址的统计图表等。

# Snort

- 在1998年，Martin Roesch用C语言开发了开放源代码(Open Source)的入侵检测系统Snort。直至今天，Snort已发展成为一个多平台(Multi-Platform),实时(Real-Time)流量分析，网络IP数据包(Pocket)记录等特性的强大的网络入侵检测/防御系统(Network Intrusion Detection/Prevention System),即NIDS/NIPS。Snort符合通用公共许可(GPL——GNU General Pubic License),在网上可以通过免费下载获得Snort,并且只需要几分钟就可以安装并开始使用它。Snort基于libpcap。

# Snort

- **Snort**有三种工作模式：嗅探器、数据包记录器、网络入侵检测系统。
- 嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。
- 数据包记录器模式把数据包记录到硬盘上。
- 网络入侵检测模式是最复杂的，而且是可配置的。用户定义的一些规则可以让**Snort**分析网络数据流，并根据检测结果采取一定的动作。

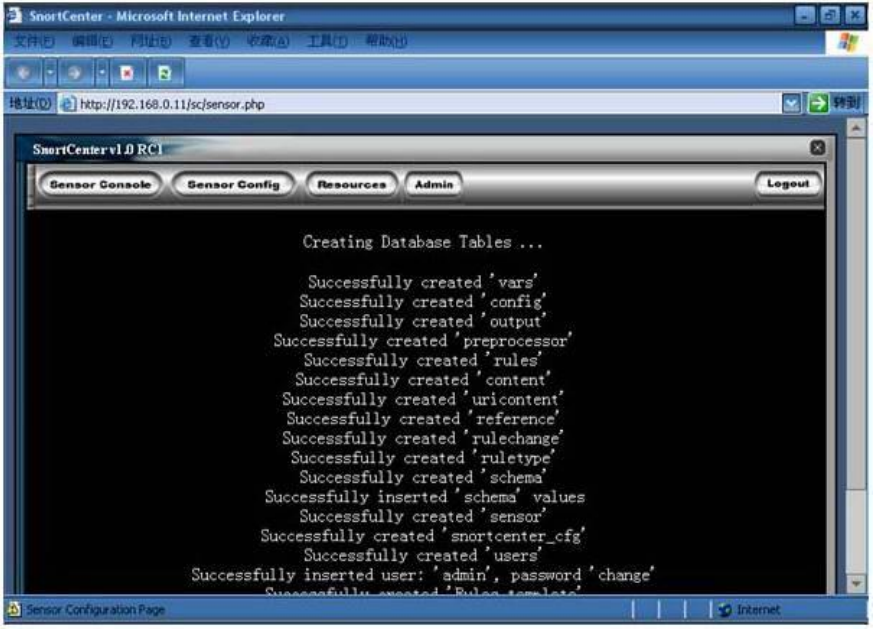
# Snort

- Snort通过在网络TCP/IP的5层结构的数据链路层进行抓取网络数据包，抓包时需将网卡设置为混杂模式，根据操作系统的不同采用libpcap或winpcap函数从网络中捕获数据包；然后将捕获的数据包送到包解码器进行解码。网络中的数据包有可能是以太网包、令牌环包、TCP/IP包、802.11包等格式。在这一过程包解码器将其解码成Snort认识的统一的格式；之后就将数据包送到预处理器进行处理
- 预处理包括能分片的数据包进行重新组装，处理一些明显的错误等问题。预处理的过程主要是通过插件来完成，比如Http预处理器完成对Http请求解码的规格化，Frag2事务处理器完成数据包的组装，Stream4预处理器用来使Snort状态化，端口扫描预处理器能检测端口扫描的能力等；对数据包进行了解码，过滤，预处理后，进入了Snort的最重要一环，进行规则的建立及根据规则进行检测。
- 规则检测是Snort中最重要的部分，作用是检测数据包中是否包含有入侵行为。例如规则alert tcp any any ->202.12.1.0/24 80（msg：”misc large tcp packet”；dsize：>3000；）这条规则的意思是，当一个流入202.12.1.0这个网段的TCP包长度超过3000B时就发出警报。规则语法涉及到协议的类型、内容、长度、报头等各种要素。

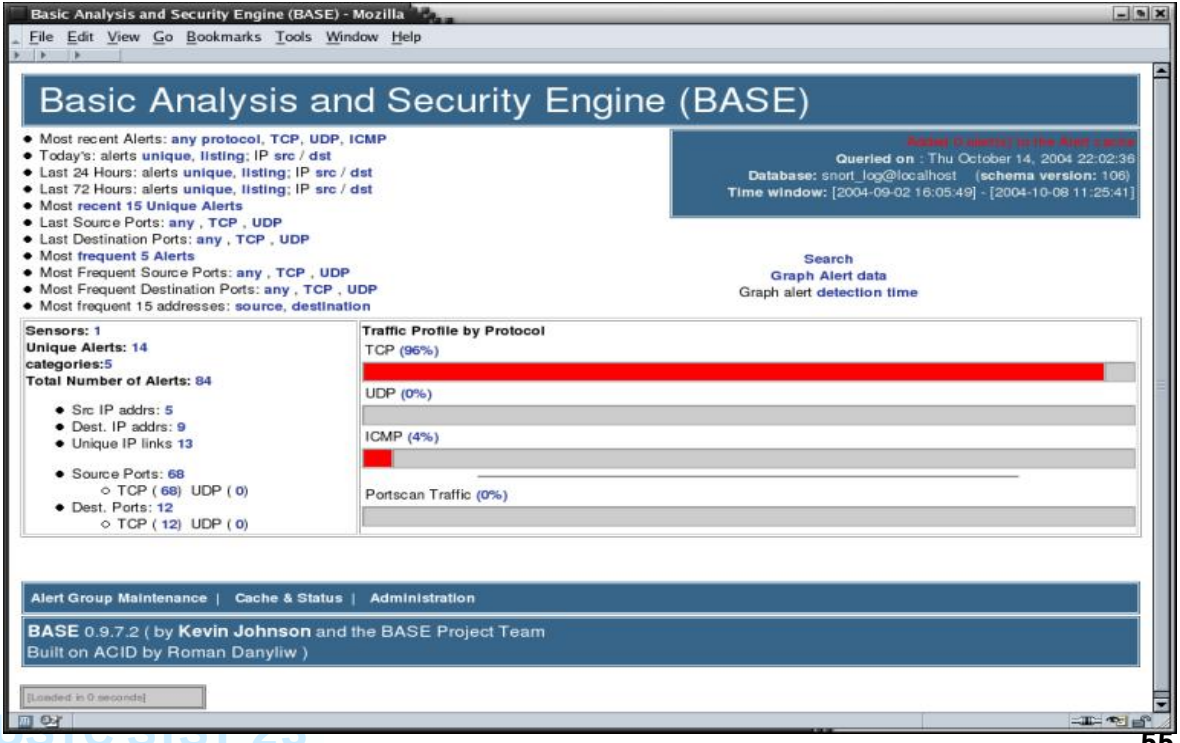
# Snort

- 处理规则文件的时候，用三维链表来存规则信息以便和后面的数据包进行匹配，三维链表一旦构建好了，就通过某种方法查找三维链表并进行匹配和发生响应。规则检测的处理能力需要根据规则的数量，运行Snort机器的性能，网络负载等因素决定；最后一步就是输出模块，经过检测后的数据包需要以各种形式将结果进行输出，输出形式可以是输出到alert文件、其它日志文件、数据库UNIX域或Socket等。
- Snort入侵检测系统适应多种平台，源代码开放，使用免费，受众多用户喜爱，但也有不少缺点。
  - 轻量型-功能还不够完善，比如与其它产品产生联动等方面还有待改进；Snort由各功能插件协同工作，安装复杂，各软件插件有时会因版本等问题影响程序运行；Snort对所有流量的数据根据规则进行匹配，有时会产生很多合法程序的误报。

# Snort

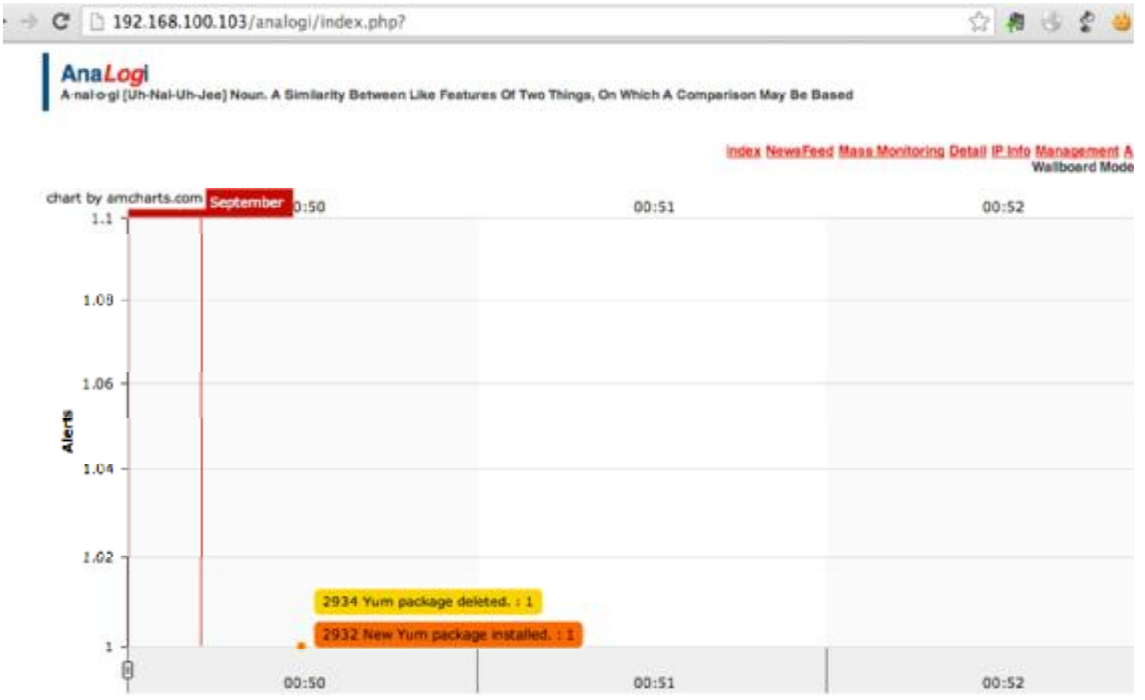

SnortCenter - Microsoft Internet Explorer
http://192.168.0.11/sc/sensor.php
SnortCenter v1.0 RC1
Sensor Console
Sensor Config
Resources
Admin
Logout
Creating Database Tables ...
Successfully created 'vars'
Successfully created 'config'
Successfully created 'output'
Successfully created 'preprocessor'
Successfully created 'rules'
Successfully created 'content'
Successfully created 'uricontent'
Successfully created 'reference'
Successfully created 'rulechange'
Successfully created 'ruletype'
Successfully created 'schema'
Successfully inserted 'schema' values
Successfully created 'sensor'
Successfully created 'snortcenter_cfg'
Successfully created 'users'
Successfully inserted user: 'admin', password 'change'
Sensor Configuration Page
Internet

# BASE


Basic Analysis and Security Engine (BASE) - Mozilla
File Edit View Go Bookmarks Tools Window Help
Basic Analysis and Security Engine (BASE)
Most recent Alerts: any protocol, TCP, UDP, ICMP
Today's: alerts unique, listing; IP src / dst
Last 24 Hours: alerts unique, listing; IP src / dst
Last 72 Hours: alerts unique, listing; IP src / dst
Most recent 15 Unique Alerts
Last Source Ports: any , TCP , UDP
Last Destination Ports: any , TCP , UDP
Most frequent 5 Alerts
Most Frequent Source Ports: any , TCP , UDP
Most Frequent Destination Ports: any , TCP , UDP
Most frequent 15 addresses: source, destination
Queried on : Thu October 14, 2004 22:02:36
Database: snort_log@localhost (schema version: 106)
Time window: [2004-09-02 16:05:49] - [2004-10-08 11:25:41]
Search
Graph Alert data
Graph alert detection time
Sensors: 1
Unique Alerts: 14
categories:5
Total Number of Alerts: 84
Src IP addrs: 5
Dest. IP addrs: 9
Unique IP links 13
Source Ports: 68
TCP ( 68) UDP ( 0)
Dest. Ports: 12
TCP ( 12) UDP ( 0)
Traffic Profile by Protocol
TCP (96%)
UDP (0%)
ICMP (4%)
Portscan Traffic (0%)
Alert Group Maintenance | Cache & Status | Administration
BASE 0.9.7.2 ( by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw )
[Loaded in 0 seconds]

# OSSEC HIDS

- OSSEC是一款开源的基于主机的入侵检测系统HIDS。它具备日志分析，文件完整性检查，策略监控，rootkit检测，实时报警以及联动响应等功能。它支持多种操作系统：Linux、Windows、MacOS、Solaris、OpenBSD/FreeBSD、 HP-UX、AIX。作为一款HIDS，OSSEC应该被安装在一台实施监控的 系统中。如果有多台电脑都安装了OSSEC，可以采用客户端/服务器模式来运行。客户机通过客户端程序 将数据发回到服务器端进行分析。在一台电脑上对多个系统进行监控对于企业或者家庭用户来说都是相当经济实用的。OSSEC的手册上说OSSEC目前还不支持Windows系统下root-kit检测，估计是正在开发中。


192.168.100.103/analogi/index.php?
AnaLogi
A·nal·o·gi [Uh-Nal-Uh-Jee] Noun. A Similarity Between Like Features Of Two Things, On Which A Comparison May Be Based
Index NewsFeed Mass Monitoring Detail IP Info Management A
Wallboard Mode
chart by amcharts.com
September
00:50
00:51
00:52
1.1
1.08
1.06
1.04
1.02
1
Alerts
2934 Yum package deleted. : 1
2932 New Yum package installed. : 1
00:50
00:51
00:52