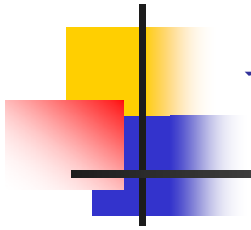
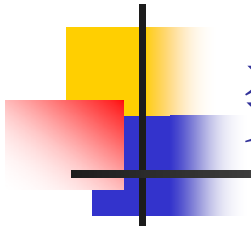


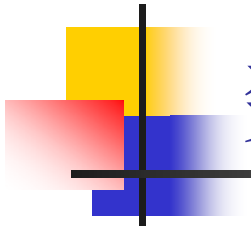
协同

- 目前IDS实现的功能是相对初级的
- IDS也需要充分利用数据信息的相关性
- IDS作为网络安全整体解决方案的重要部分，与其他安全设备之间应该有着紧密的联系
- IDS需要一种新的系统体系来克服自身的不足，并将IDS的各个功能模块与其他安全产品有机地融合起来, 这就需要引入协同的概念



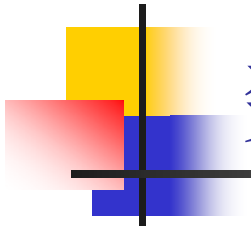
数据采集协同

- 基于网络的IDS需要采集动态数据（网络数据包）
- 基于主机的IDS需要采集静态数据（日志文件等）
- 目前的IDS将网络数据包的采集、分析与日志文件的采集、分析割裂开来，没有在这两类原始数据的相关性上作考虑。
- 在数据采集上进行协同并充分利用各层次的数据，是提高入侵检测能力的首要条件



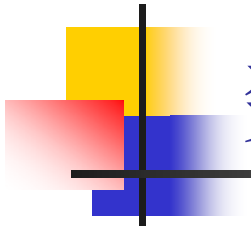
数据分析协同

- 入侵检测不仅需要利用模式匹配和异常检测技术来分析某个检测引擎所采集的数据，以发现一些简单的入侵行为，还需要在此基础上利用数据挖掘技术，分析多个检测引擎提交的审计数据以发现更为复杂的入侵行为。



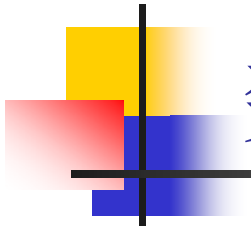
数据分析协同

- 两个层面上进行
  - 1. 单个检测引擎采集的数据：综合使用检测技术，以发现较为常见的、典型的攻击行为<—— 本地引擎
  - 2. 多个检测引擎的审计数据：利用数据挖掘技术进行分析，以发现较为复杂的攻击行为<—— 中心管理控制平台



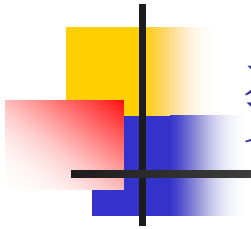
数据挖掘

- 数据挖掘技术是一种决策支持过程，它主要基于AI，机器学习统计等技术，能高度自动化地分析原有数据，做出归纳性推理，从中挖掘出潜在的模式，预测出客户的行为
- 运用关联分析，能够提取入侵行为在时间和空间上的关联，可以进行的关联包括源IP关联、目标IP关联、数据包特征关联、时间周期关联、网络流量关联等；
- 运用序列模式分析可以进行入侵行为的时间序列特征分析；
- 利用以上的分析结构，可以制订入侵行为的分类标准，并进行形式化的描述，通过一定的训练数据集来构造检测模型；
- 运用聚类分析，能优化或完全抛弃既有的模型，对入侵行为重新划分并用显示或隐式的方法进行描述



数据挖掘

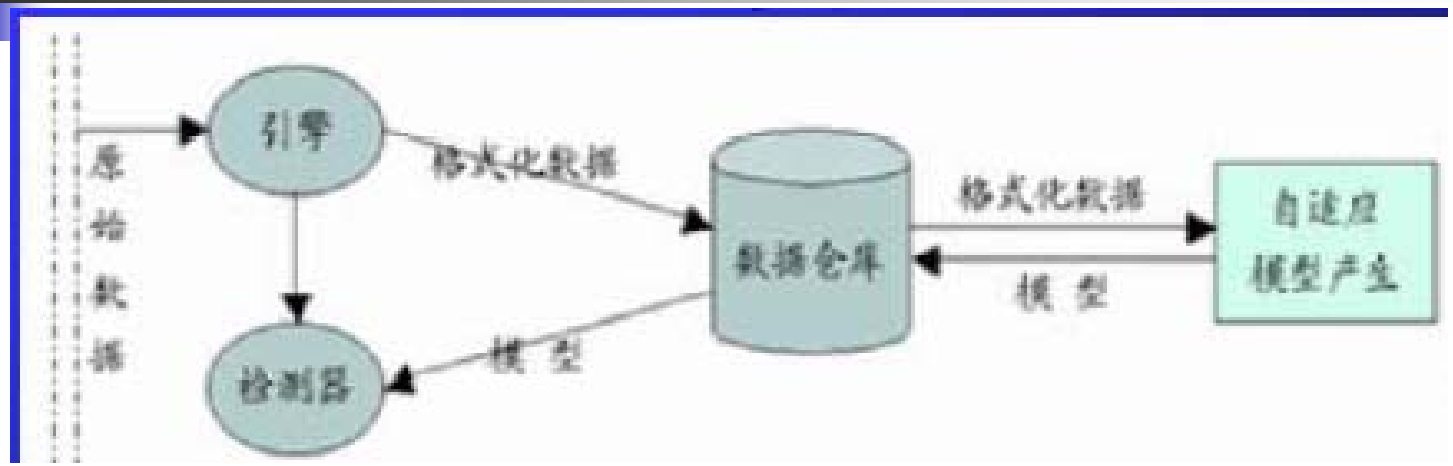
- 数据准备
- 数据清理和集成
- 数据挖掘
- 知识表示
- 模式评估



数据挖掘

- 1. 从审计数据中提取特征，以帮助区分正常数据和攻击行为
- 2. 将这些特征用于模式匹配或异常检测模型
- 3. 描述一种人工异常产生方法，来降低异常检测算法的误报率
- 4. 提供一种结合模式匹配和异常检测模型的方法

数据挖掘



- 1. 引擎观察原始数据并计算用于模型评估的特征
- 2. 检测器获取引擎的数据并利用检测模型来评估它是否是一个攻击
- 3. 数据仓库被用作数据和模型的中心存储地;
- 4. 模型产生的主要目的是为了加快开发以及分发新的入侵检测模型的速度

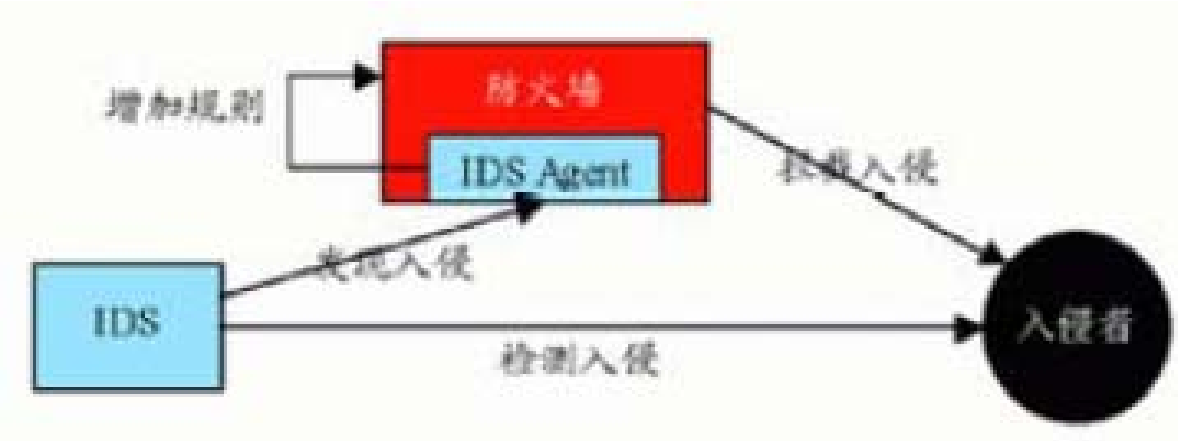
响应协同

- 理想的情况是，建立相关安全产品能够相互通信并协同工作的安全体系，实现防火墙、IDS、病毒防护系统和审计系统等的互通与联动，以实现整体安全防护

- 响应协同：当**IDS**检测到需要阻断的入侵行为时，立即迅速启动联动机制，自动通知防火墙或其他安全控制设备对攻击源进行封堵，达到整体安全控制的效果。
  - IDS与防火墙的联动，可封堵源自外部网络的攻击
  - IDS与网络管理系统的联动，可封堵被利用的网络设备和主机
  - IDS与操作系统的联动，可封堵有恶意的用户账号
  - IDS与内网监控管理系统的联动，可封堵内部网络上恶意的主机

IDS与Firewall联动

- 通过在防火墙中驻留的一个*IDS Agent*对象，以接收来自IDS的控制消息，然后再增加防火墙的过滤规则，最终实现联动



- Cisco CIDF(CISL)
- ISS Checkpoint

其它-报警信息融合

- 虽然目前多种网络入侵检测系统都采用了分布式结构，但对于收到的报警信息，管理器只是进行简单的统计和显示，或只能针对特定类型的事件进行关联分析，但是没有对这些来自不同网络区域的Sensor 的报警信息进行汇总分析或做进一步的融合判断，因而无法检测一些复杂的攻击模式，如分布式攻击等。
- 单一的检测方法或检测系统难以检测各种复杂的攻击，综合多种检测技术和多种检测系统能够有效提高检测的准确性。这就需要对源自不同检测方法或检测系统的检测结果进行融合，得到一个综合的判别结果。
- 为了能够适应攻击者身份识别、计算机和网络的安全态势评估等更高层次的安全需求，同样也需要多个网络检测器、多个入侵检测系统的报警信息进行融合处理。

其它-网络流量异常检测

- 网络流量异常检测是网络入侵检测系统的重要组成部分。DoS、DDoS、网络蠕虫等多种攻击都会引起网络流量的异常变化。
- 以单位时间内的包数作为网络流量特征，使用神经网络检测流量异常的方法；
- 通过对多种异常报文的分析来检测各种DoS 攻击；
- 通过TCP 报文中SYN, FIN 和RST 报文之间的比例关系，使用异常点检测的方法来检测SYN Flooding 攻击；
- 对网络流数目的可视化为管理员判断是否发生网络流量异常提供决策支持；
- 通过建立基于TCP 的连接请求到达模型（Poisson 模型）来检测网络异常
- 研究使用神经网络对会话统计参数如TCP SYN 包数、TCP FIN包数，以及在统计单位时间内建立的TCP 连接数等来检测网络流量异常。

其它-攻击源追踪

- 攻击者可以轻易地获得匿名性，从而逃避惩罚，这是导致网络攻击得以泛滥的一个重要原因。
- 所谓伪造报文攻击，就是攻击者通过伪造报文的源IP 地址，来达到隐藏攻击主机地址的目的。伪造报文攻击主要用于DoS，DDoS等攻击，如SYNFlooding、Smurf、Shaft 等。在端口扫描、TCP 会话劫持、盗取主机机密信息、利用应用程序漏洞获取root 权限等网络攻击中，攻击者需要和目标主机进行交互，必须使用真实的网络地址，这时攻击者就可以采用间接攻击来隐藏自己的真实网络地址。
- 在间接攻击中，攻击者首先连接到一个存在安全漏洞或提供网络代理服务的主机CH1，再从CH1 连接到CH2，从CH2 对目标发动攻击。攻击路线图为攻击者--->CH1--->CH2--->目标。从被攻击的主机只能看到攻击主机CH2，而无法获知攻击源主机。攻击源追踪分为基于主机的攻击源追踪和基于网络的攻击源追踪两部分。

其它-基于主机的攻击源追踪

- DIDS（Distributed Intrusion Detection System）是一个基于主机的分布式入侵检测系统，在域中的每个主机上都有一个监控程序Host Monitor，负责收集本机的日志信息，并对其进行分析，然后将重要的事件比如登录事件等报告给一个中央管理器Director。Director 对各个Host Monitor 报告的信息进行综合分析，就可以构造出用户在各个主机的登录路径，从而获得用户登录的源头。
- Caller ID Caller ID 利用反向攻击来追踪攻击的源头：假设：如果攻击者通过一些中间主机发动攻击，那么极有可能在这些中间主机上存在漏洞，从而使得攻击者可以访问这些主机。当发生攻击时，Caller-ID 可以沿着逆向路径攻击主机，不断获得上一个主机的地址，依次类推，最终获得攻击者的真实地址。

其它-基于网络的攻击源追踪

- 数据指纹技术在间接攻击中，假如攻击者在主机H1，H2，H3，H4 上依次登录，其每次操作都会产生一个从H1 到H2的报文，H2 处理完后，把相应的信息再发送给H3，同样，H3 也会发送报文给H4，命令最后在H4 得以执行。由远程登录的原理可以知道，H1 和H2，H2 和H3，H3 和H4 间传递的报文内容都是相同的。如果可监测到不同主机间的所有通信内容，通过分析就可以得知它们是否属于同一登录链，再由监测到报文的时间就可以确定登录的先后顺序，从而找到登录链的源头。

其它-基于网络的攻击源追踪

- TCP Connection Chain：Kunikazu Yoda 和Hiroaki Etoh 提出了基于TCP 序列号的登录链追踪办法。通过监测记录每个网段上所有TCP 连接发送数据的序列号，就可以判断它们是否属于同一登录链。