网络安全 – 入侵检测技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

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

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

入侵检测技术概述 – 章节分解

1. 防火墙技术的不足
2. 入侵检测技术 – 缘起
3. 入侵检测技术 – 定义
4. 入侵检测技术 – 相关术语
5. 入侵检测技术 – 介绍
6. 入侵检测技术的特点
7. 入侵检测技术的细节

防火墙技术的不足

防火墙是所有保护网络的方法中最能普遍接受的方法，能阻挡外部入侵者，但对内部攻击无能为力。

同时，防火墙绝对不是坚不可摧的，即使是某些防火墙本身也会引起一些安全问题。

防火墙不能防止通向站点的后门，不提供对内部的保护，无法防范数据驱动型的攻击，不能防止用户由Internet上下载被病毒感染的计算机程序或将该类程序附在电子邮件上传输。

入侵检测是防火墙的合理补充，它帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。

入侵检测技术 - 缘起 1

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

入侵检测技术 - 缘起 2

1980年JamesP.Anderson在给一个保密客户写的一份题为《计算机安全威胁监控与监视》的技术报告中指出，审计记录可以用于识别计算机误用，他给威胁进行了分类，第一次详细阐述了入侵检测的概念。

1984年到1986年乔治敦大学的DorothyDenning和SRI公司计算机科学实验室的PeterNeumann研究出了一个实时入侵检测系统模型-IDES（Intrusion Detection Expert Systems入侵检测专家系统），是第一个在一个应用中运用了统计和基于规则两种技术的系统，是入侵检测研究中最有影响的一个系统。

1989年，加州大学戴维斯分校的ToddHeberlein写了一篇论文《ANetworkSecurityMonitor》，该监控器用于捕获TCP/IP分组，第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机，网络入侵检测从此诞生。

入侵检测技术 - 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。

入侵检测技术 – 相关术语 1

攻击

- 攻击者利用工具，出于某种动机，对目标系统采取的行动，其后果是获取/破坏/篡改目标系统的数据或访问权限

事件

- 在攻击过程中发生的可以识别的行动或行动造成的后果；在入侵检测系统中，事件常常具有一系列属性和详细的描述信息可供用户查看。
- 将入侵检测系统需要分析的数据统称为事件（event）

入侵检测技术 – 相关术语 2

入侵

- 对信息系统的非授权访问及（或）未经许可在信息系统中进行操作

入侵检测

- 对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程

入侵检测系统（IDS）

- 用于辅助进行入侵检测或者独立进行入侵检测的自动化工具

入侵检测技术 – 介绍 1

入侵检测（Intrusion Detection）技术是一种动态的网络检测技术，主要用于识别对计算机和网络资源的恶意使用行为，包括来自外部用户的入侵行为和内部用户的未经授权活动。

一旦发现网络入侵现象，则应当做出适当的反应。对于正在进行的网络攻击，则采取适当的方法来阻断攻击（与防火墙联动），以减少系统损失。对于已发生网络攻击，应通过分析日志记录找到发生攻击的原因和入侵者踪迹，作为增强网络系统安全性和追究入侵者法律责任的依据。

从计算机网络系统中的若干关键点收集信息，并分析这些信息，查看是否有违反安全策略的行为和遭到袭击的迹象。

入侵检测技术 – 介绍 2

入侵检测系统（IDS）由入侵检测的软件与硬件组合而成，被认为是防火墙之后的第二道安全闸门。

在不影响网络性能的情况下能对网络进行监测，提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现：

1. 监视、分析用户及系统活动
2. 系统构造和弱点的审计
3. 识别反映已知进攻的活动模式并向相关人士报警
4. 异常行为模式的统计分析
5. 评估重要系统和数据文件的完整性
6. 操作系统的审计跟踪管理，并识别用户违反安全策略的行为

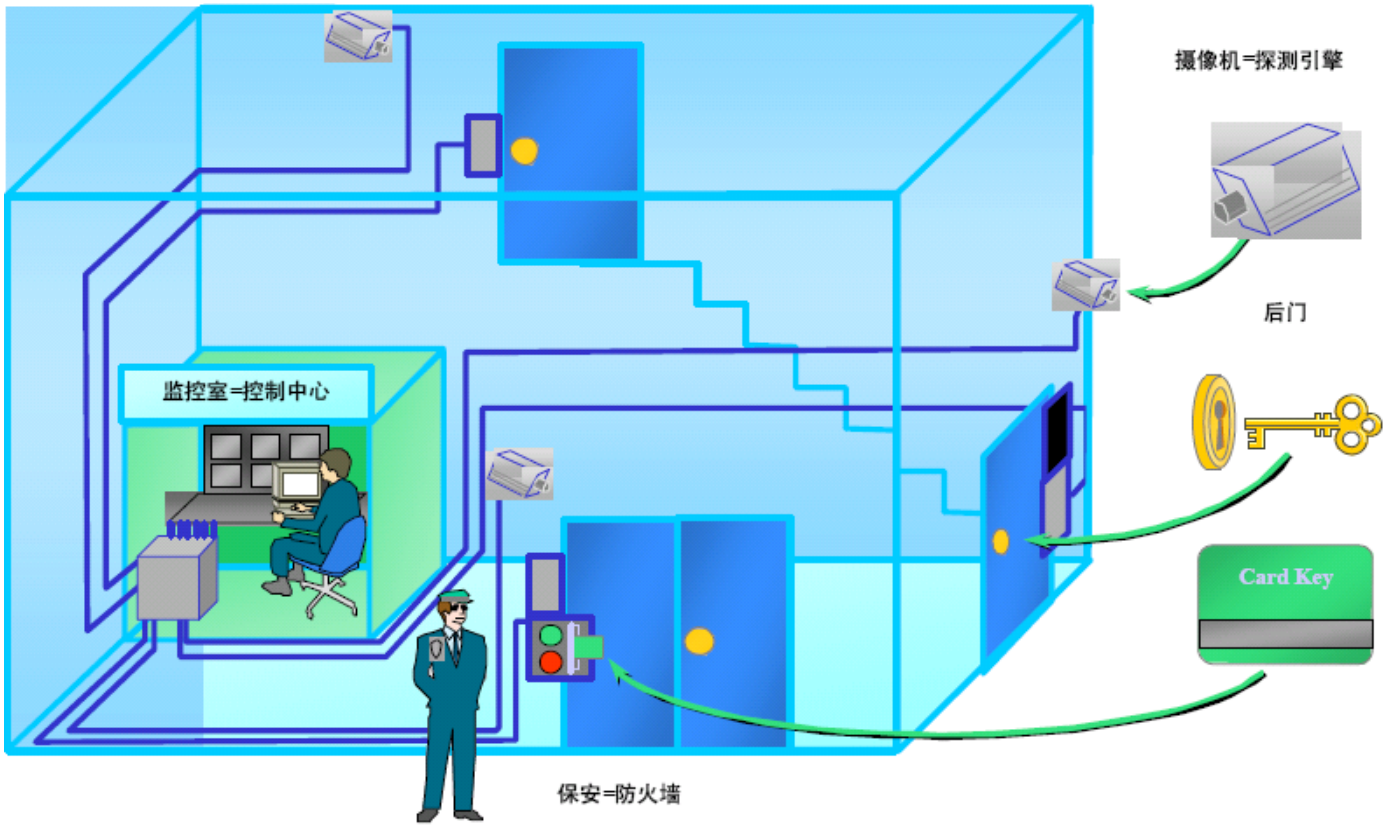
入侵检测技术 – 介绍 3

- 监控网络和系统
- 发现入侵企图或异常现象
- 实时报警
- 主动响应
- 审计跟踪

形象地说，它就是网络摄像机，能够捕获并记录网络上的所有数据，同时它也是智能摄像机，能够分析网络数据并提炼出可疑的、异常的网络数据，它还是X光摄像机，能够穿透一些巧妙的伪装，抓住实际的内容。

它还不仅仅只是摄像机，还包括保安员的摄像机。

入侵检测技术 – 介绍 4



入侵检测技术的特点 - 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

入侵检测技术的特点 - 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。

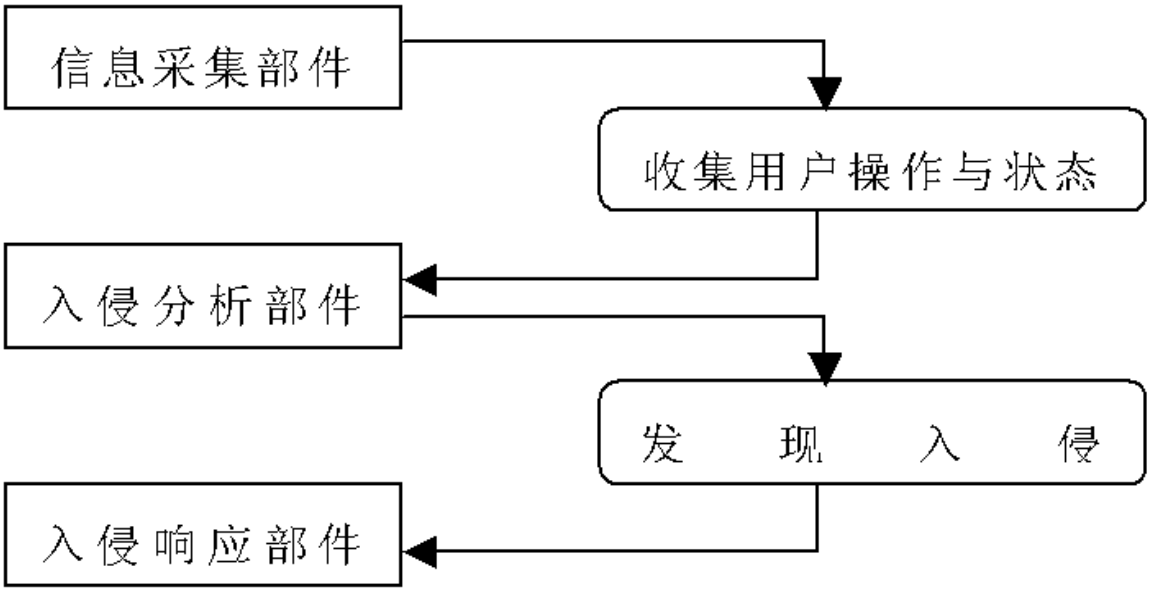
识别反映已知攻击的活动模式。

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

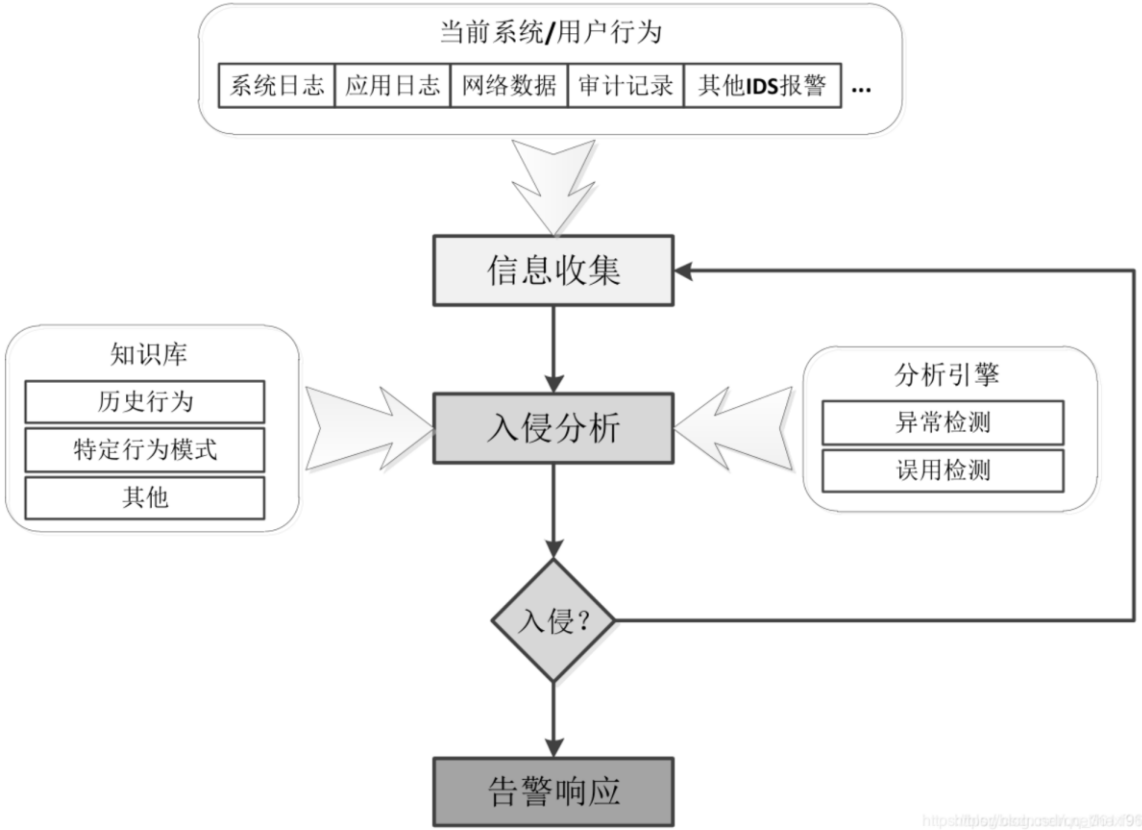
入侵分析部件

- 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

工作机理 - 1


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

工作机理 - 2

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 - 3

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**

入侵检测技术概述

入侵检测分类与评估

入侵检测产品概况

入侵检测分类与评估 – 章节分解

1. 按引擎分类
2. 按实现方式分类
3. 按技术路线分类
4. 按系统各模块的运行方式
5. 按时效性分类
6. IDS评估标准
7. IDS性能指标
8. 入侵防御系统

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）

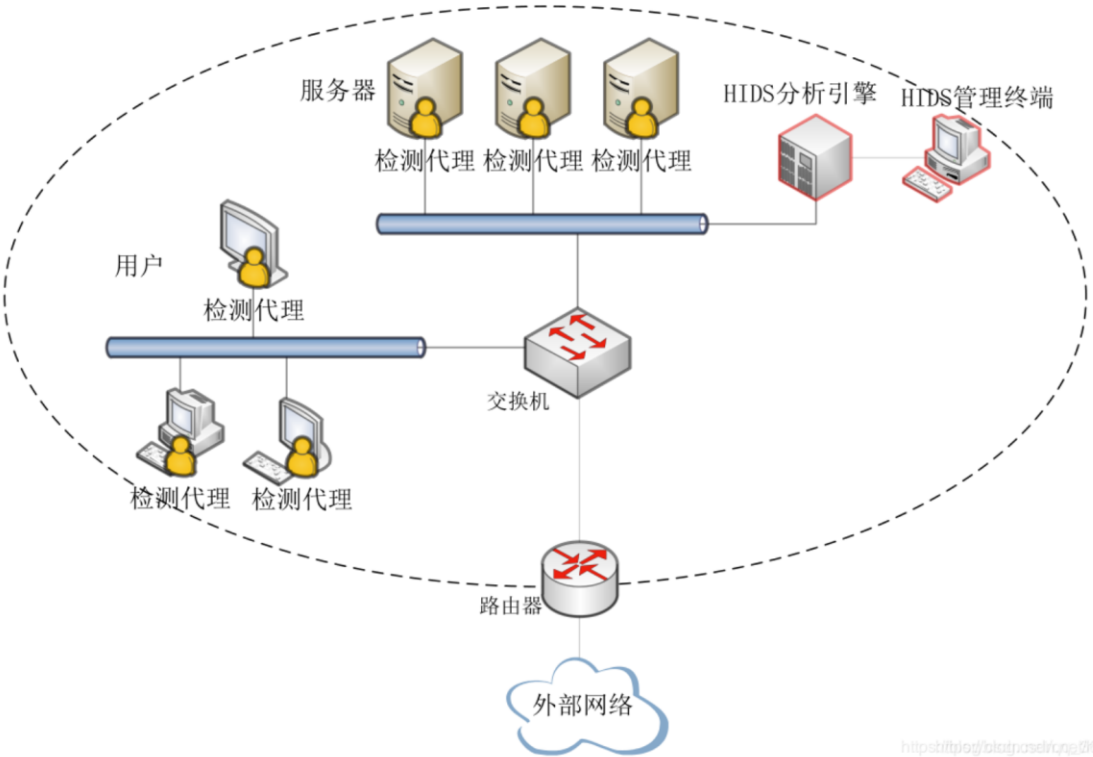
- **安装在被重点检测的主机之上**
- **对该主机的网络实时连接以及系统审计日志进行智能分析和判断**

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**

混合型入侵检测系统（Hybrid IDS）

HIDS示例


服务器
检测代理
检测代理
检测代理
HIDS分析引擎
HIDS管理终端
用户
检测代理
交换机
检测代理
检测代理
路由器
外部网络

HIDS优缺点

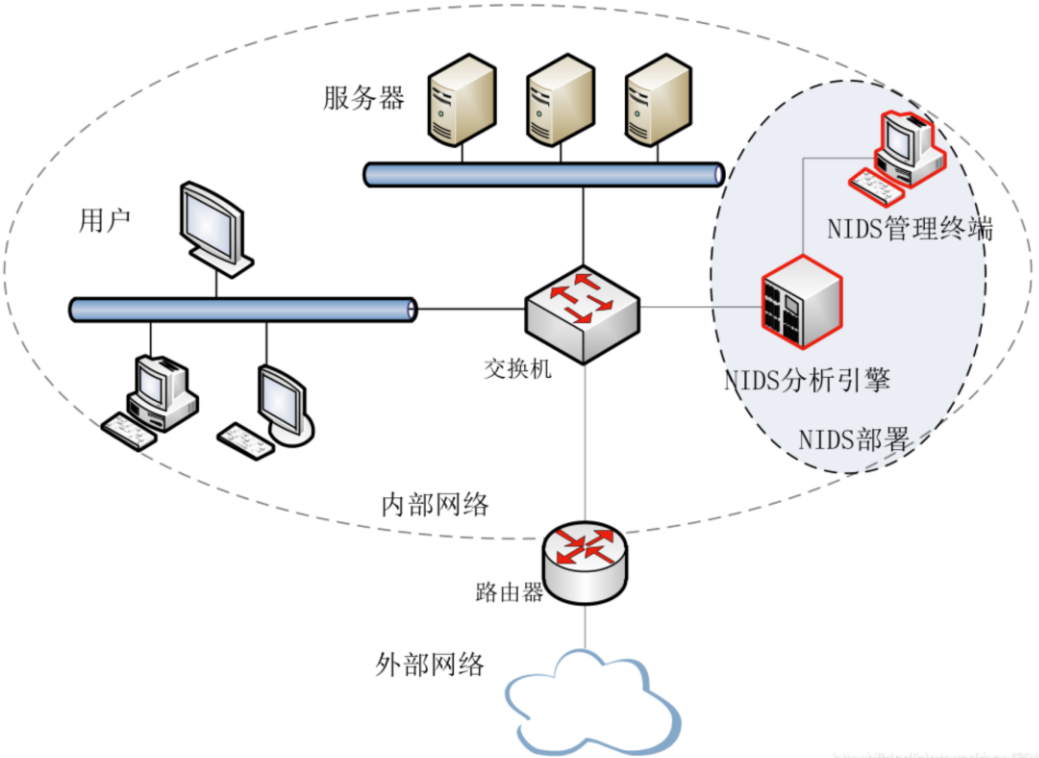
优点

- 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

NIDS示例



NIDS优缺点

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 - 1

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

网络IDS vs 主机IDS对比 - 2

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

网络IDS vs 主机IDS对比 - 3

如果攻击不经过网络基于网络的IDS无法检测到只能通过使用基于主机的IDS来检测。

基于网络的IDS通过检查所有的包头来进行检测，而基于主机的IDS并不查看包头。主机IDS往往不能识别基于IP的拒绝服务攻击和碎片攻击。

基于网络的IDS可以研究数据包的内容，查找特定攻击中使用的命令或语法，这类攻击可以被实时检查包序列的IDS迅速识别；而基于主机的系统无法看到负载，因此也无法识别嵌入式的数据包攻击。

混合型入侵检测系统（Hybrid IDS)

在新一代的入侵检测系统中将把现在的基于网络和基于主机这两种检测技术很好地集成起来，提供集成化的攻击签名检测报告和事件关联功能。

可以深入地研究入侵事件入侵手段本身及被入侵目标的漏洞等。

按技术路线分类 - 基于统计分析

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 - 基于神经网络

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 – 基于专家系统

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 – 基于模型推理

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**

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 - 1

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

IDS评估标准 - 2

完备性 (Completeness): 指IDS能够检测出所有攻击行为的能力。如果存在一个攻击行为，无法被IDS检测出来，那么该IDS就不具有检测完备性。

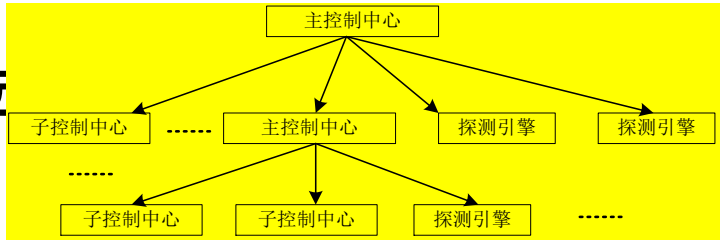
容错性 (Fault Tolerance): 由于IDS是检测入侵的重要手段/所以它也就成为很多入侵者攻击的首选目标。IDS自身必须能够抵御对它自身的攻击，特别是拒绝服务(Denial-of-Service)攻击。

及时性 (Timeliness): 及时性要求IDS必须尽快地分析数据并把分析结果传播出去，以使系统安全管理者能够在入侵攻击尚未造成更大危害以前做出反应，阻止入侵者进一步的破坏活动，和上面的处理性能因素相比，及时性的要求更高。

IDS性能指标 - 1

系统结构

- 好的IDS应能采用分级、迂



事件数量

- 考察IDS系统的一个关键性指标是报警事件的多少
- 一般而言，事件越多，表明IDS系统能够处理的能力越强

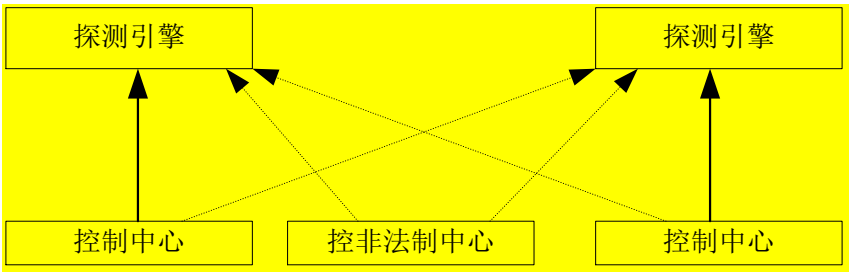
处理带宽

- IDS的处理带宽，即IDS能够处理的网络流量，是IDS的一个重要性能
- 目前的网络IDS系统一般能够处理20～30M网络流量，经过专门定制的系统可以勉强处理40～60M的流量

IDS性能指标 - 2

探测引擎与控制中心的通信

- 作为分布式结构的IDS系统，通信是其自身安全的关键因素。通信安全通过身份认证和数据加密两种方法来实现。
- 身份认证是要保证一个引擎，或者子控制中心只能由固定的上级进行控制，任何非法的控制行为将予以阻止。身份认证采用非对称加密算法，通过拥有对方的公钥，进行加密、解密完成身份认证。



IDS性能指标 - 3

事件的定义

- 事件的可定义性或可定义事件是IDS的一个主要特性。

二次事件

- 对事件进行实时统计分析，并产生新的高级事件能力。

事件响应

- 通过事件上报、事件日志、Email通知、手机短信息、语音报警等方式进行响应。
- 还可通过TCP阻断、防火墙联动等方式主动响应。

IDS性能指标 - 4

自身安全

- 自身安全指的是探测引擎的安全性。要有良好的隐蔽性，一般使用定制的操作系统。

终端安全

- 主要指控制中心的安全性。有多个用户、多个级别的控制中心，不同的用户应该有不同的权限，保证控制中心的安全性。

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

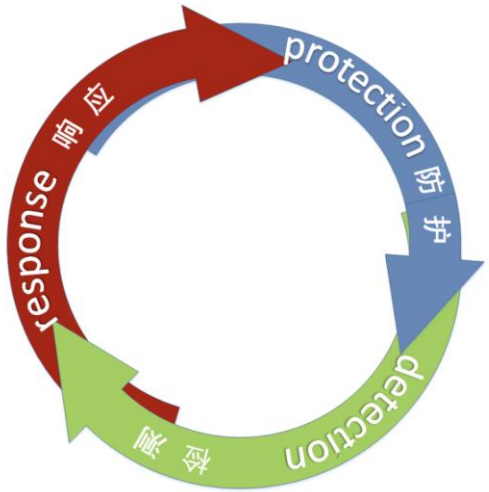
高虚警率，用户处理负担重

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

入侵防御系统 - 1

IDS只能被
之外。因此
保企业网络



威胁阻止在网络
决方案，以确

入侵防御
Detection
能化的入侵
一定的响应
息系统不受

或 Intrusion
IPS是一种智
，而且能通过
实时地保护信
。

IPS在网络中

- Span（接在交换机旁边，作为端口映像）
- Tap（接在交换机与路由器中间，旁路安装，拷贝一份数据到IPS中）
- Inline（接在交换机与路由器中间，在线安装，在线阻断攻击）
- Port-cluster（被动抓包，在线安装）。它在报警的同时，能阻断攻击

入侵防御系统 - 2

串行部署的防火墙可以拦截低层攻击行为，但对应用层的深层攻击行为无能为力。

旁路部署的IDS可以及时发现那些穿透防火墙的深层攻击行为，作为防火墙的有益补充，但很可惜的是无法实时的阻断。

IDS和防火墙联动：通过IDS来发现，通过防火墙来阻断。但由于迄今为止没有统一的接口规范，加上越来越频发的“瞬间攻击”（一个会话就可以达成攻击效果，如SQL注入、溢出攻击等），使得IDS与防火墙联动在实际应用中的效果不显著。

这就是IPS产品的起源：**一种能防御防火墙所不能防御的深层入侵威胁（入侵检测技术）的在线部署（防火墙方式）安全产品。由于用户发现了一些无法控制的入侵威胁行为，这也正是IDS的作用。**

入侵防御系统 - 3

入侵检测系统（IDS）对那些异常的、可能是入侵行为的数据进行检测和报警，告知使用者网络中的实时状况，并提供相应的解决、处理方法，是一种侧重于风险管理的安全产品。

入侵防御系统（IPS）对那些被明确判断为攻击行为，会对网络、数据造成危害的恶意行为进行检测和防御，降低或是减免使用者对异常状况的处理资源开销，是一种侧重于风险控制的安全产品。

这也解释了IDS和IPS的关系，并非取代和互斥，而是相互协作：没有部署IDS的时候，只能是凭感觉判断，应该在什么地方部署什么样的安全产品，通过IDS的广泛部署，了解了网络的当前实时状况，据此状况可进一步判断应该在何处部署何类安全产品（IPS等）。

入侵防御系统 - 4

入侵防护

实时、主动拦截黑客攻击、蠕虫、网络病毒、后门木马、DoS等恶意流量，保护企业信息系统和网络架构免受侵害，防止操作系统和应用程序损坏或宕机。

Web安全

基于互联网Web站点的挂马检测结果，结合URL信誉评价技术，保护用户在访问被植入木马等恶意代码的网站时不受侵害，及时、有效地第一时间拦截Web威胁。

流量控制

阻断一切非授权用户流量，管理合法网络资源的利用，有效保证关键应用全天候畅通无阻，通过保护关键应用带宽来不断提升企业IT产出率和收益率。

上网监管

全面监测和管理IM即时通讯、P2P下载、网络游戏、在线视频，以及在线炒股等网络行为，协助企业辨识和限制非授权网络流量，更好地执行企业的安全策略。

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

产品概况 - 国外产品 1

Cyber Cop IDS： NAI

Realsecure： ISS

Session_wall： Abirnet

NetWare Flight Recorder：Anzen

Internet Emergency Response Service：IBM

Cisco Secure IDS： Cisco

产品概况 - 国外产品 2

Adaptive Intrusion Detection System：布兰登大学

Autonomous Agents For Intrusion Detection：Purdue University

IDES：SRI

Wisdom and Sense：Los Alamos

NSM：加里福利亚大学

产品概况 - 国内产品

RIDS-100：瑞星

曙光GodEye-HIDS：曙光信息产业（北京）

天阗：启明星辰

天眼NPIDS：北京中科网威

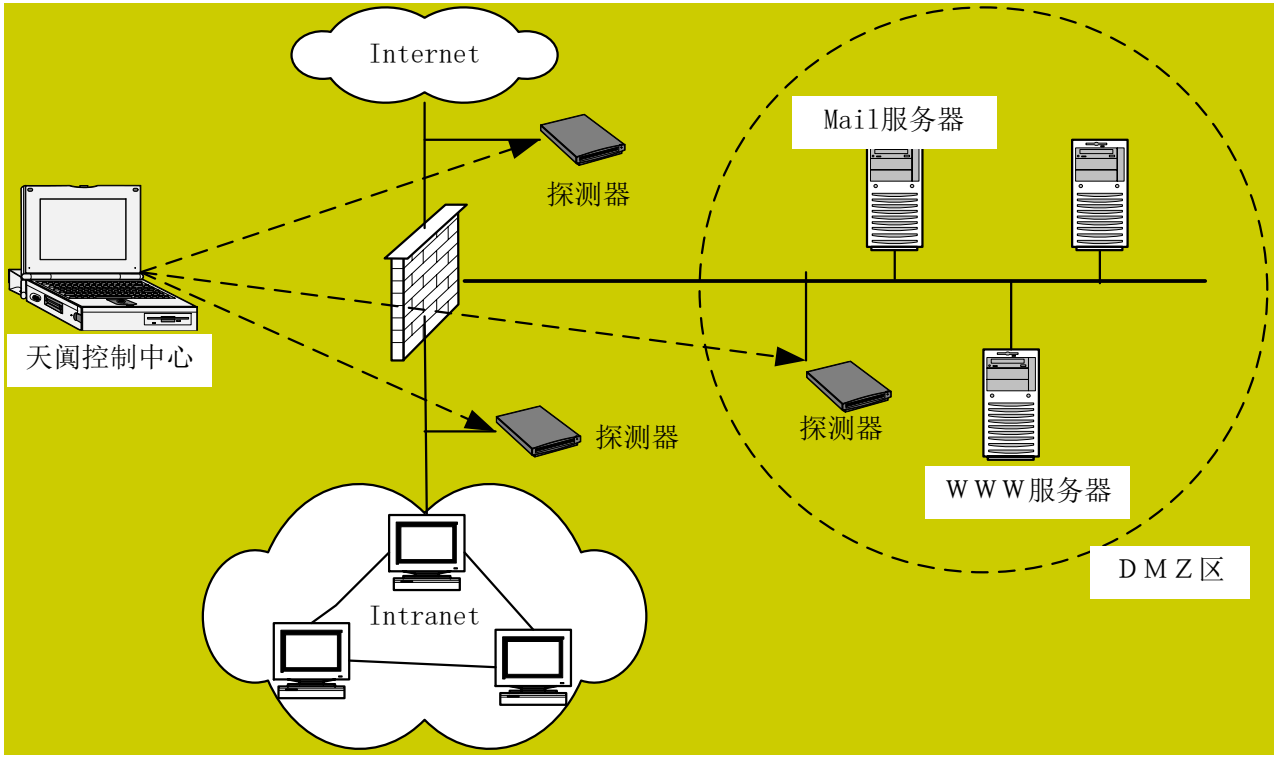
天阗黑客入侵检测与预警系统 - 1

天阗黑客入侵检测与预警系统是一种动态的入侵检测与响应系统。

利用全面流量监控发现异常，结合地理信息显示入侵事件的定位状况，应用入侵和漏洞之间具有的对应关联关系，给出入侵威胁和资产脆弱性之间的风险分析结果，从而有效地管理安全事件并进行及时处理和响应。

实时监控网络传输，自动检测可疑行为，及时发现来自网络外部或内部的攻击。天阗系统可以与防火墙紧密结合，弥补了防火墙的访问控制不严密的问题。

天阗黑客入侵检测与预警系统 - 2



思考题

1. 入侵检测系统按引擎类别分，可以划分为几种类型？这些引擎实现的方法如何？

2. 什么是基于模式匹配的IDS？

3. 什么是基于异常检测的IDS？

4. 某用户平均每天登录3次，但是某日突然登录30次，属于哪种检测技术？

5. 运行程序侯不测试超级用户密码，绑定端口。。。，属于哪种检测技术？

谢谢!