第6章 入侵检测

本章内容

- 6.1 入侵检测概述
- 6.2 入侵检测系统的分类及特点
- 6.3 入侵检测系统结构
- 6.4 入侵检测系统的关键技术

入侵检测系统

- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测概述

- 什么是入侵检测系统
- 为什么需要入侵检测
- 入侵检测系统的作用
- 入侵检测的发展历程
- 入侵检测的相关术语

什么是入侵检测系统

入侵 Intrusion

- 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 Intrusion Detection

- 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

入侵检测概述

- 什么是入侵检测系统
- 为什么需要入侵检测
- 入侵检测系统的作用
- 入侵检测的发展历程
- 入侵检测的相关术语

为什么需要入侵检测系统

入侵行为日益严重

- ✓ 攻击工具唾手可得
- ✓ 入侵教程随处可见

内部的非法访问

- ✓ 内部网的攻击占总的攻击事件的70%以上
- ✓ 没有监测的内部网是内部人员的“自由王国”

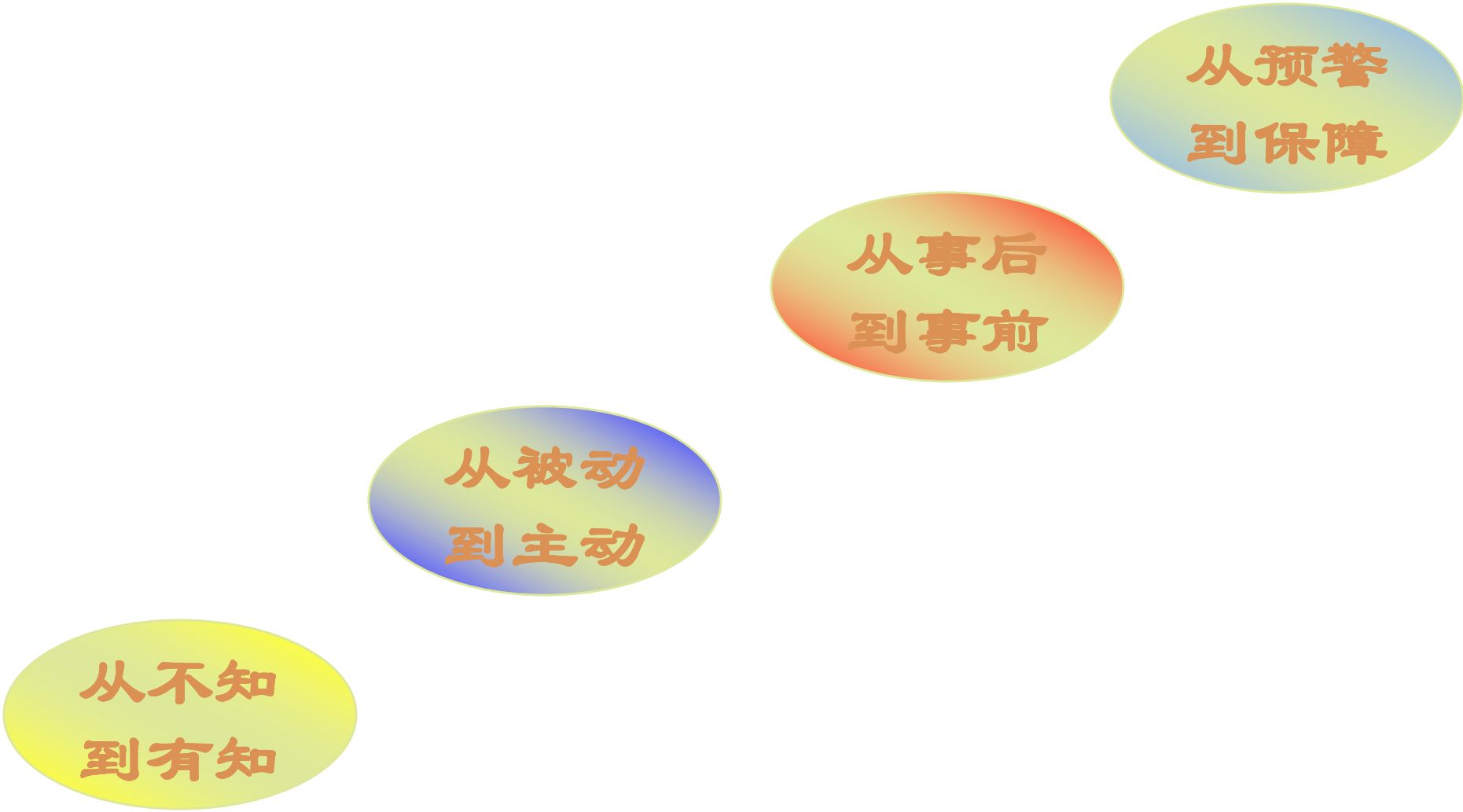
边界防御的局限

- ✓ 防火墙不能防止通向站点的后门。
- ✓ 防火墙一般不提供对内部的保护。
- ✓ 防火墙无法防范数据驱动型的攻击。
- ✓ 防火墙不能防止Internet上下载被病毒感染的程序

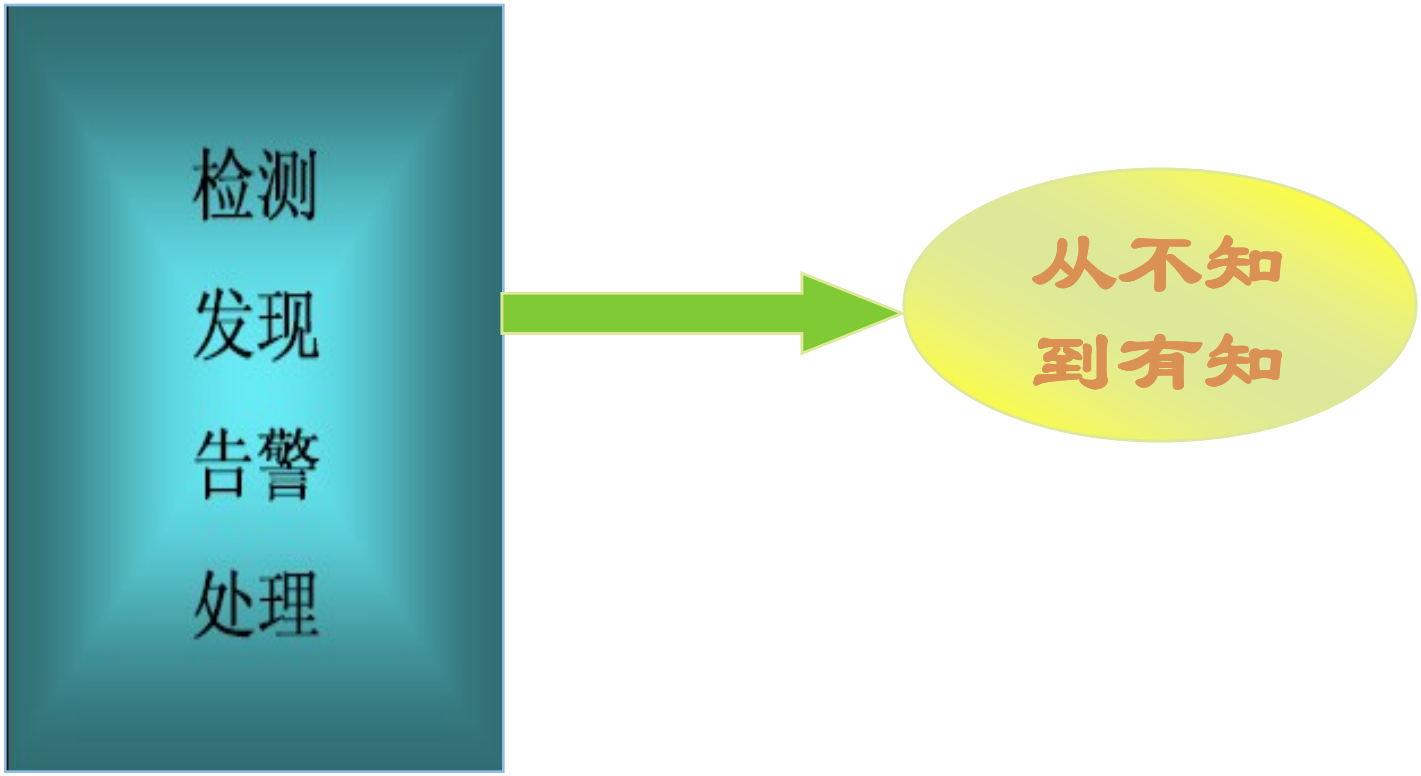
入侵检测概述

- 什么是入侵检测系统
- 为什么需要入侵检测
- 入侵检测系统的作用
- 入侵检测的发展历程
- 入侵检测的相关术语

入侵检测发挥的作用

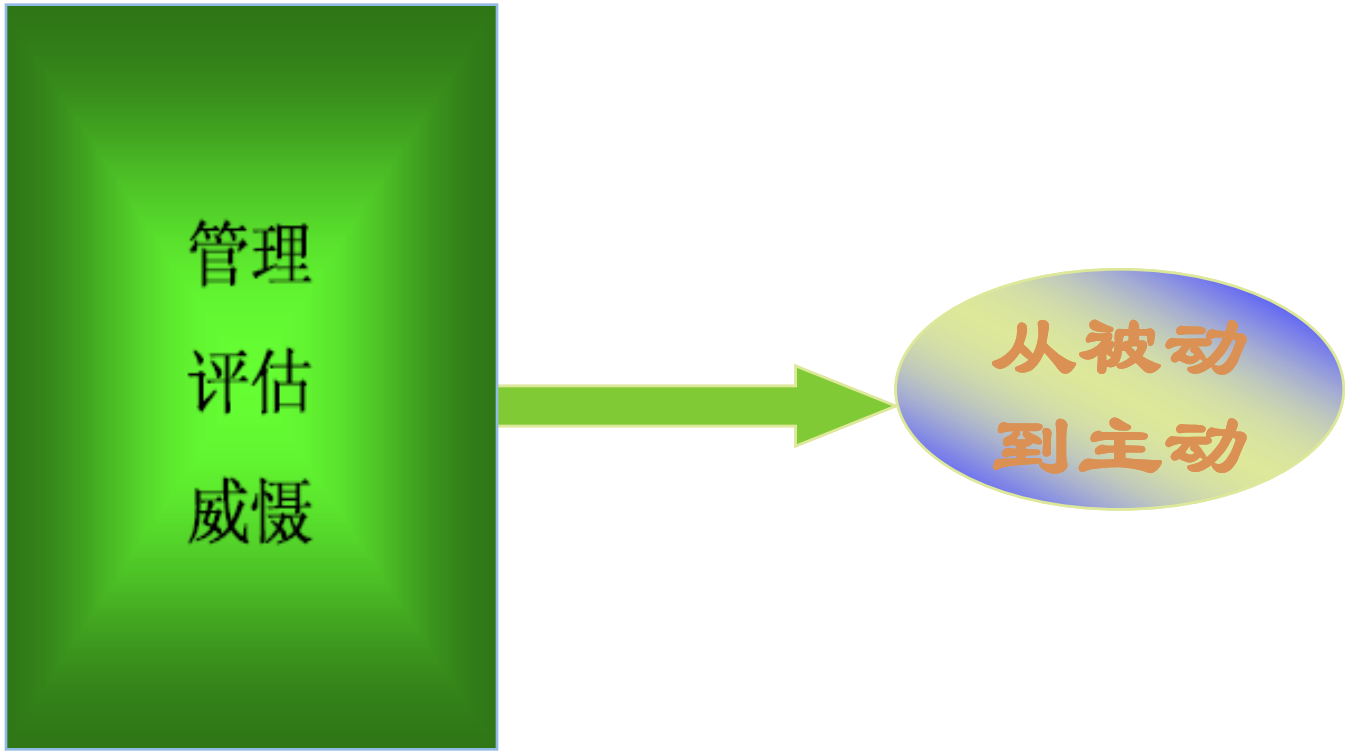


入侵检测发挥的作用



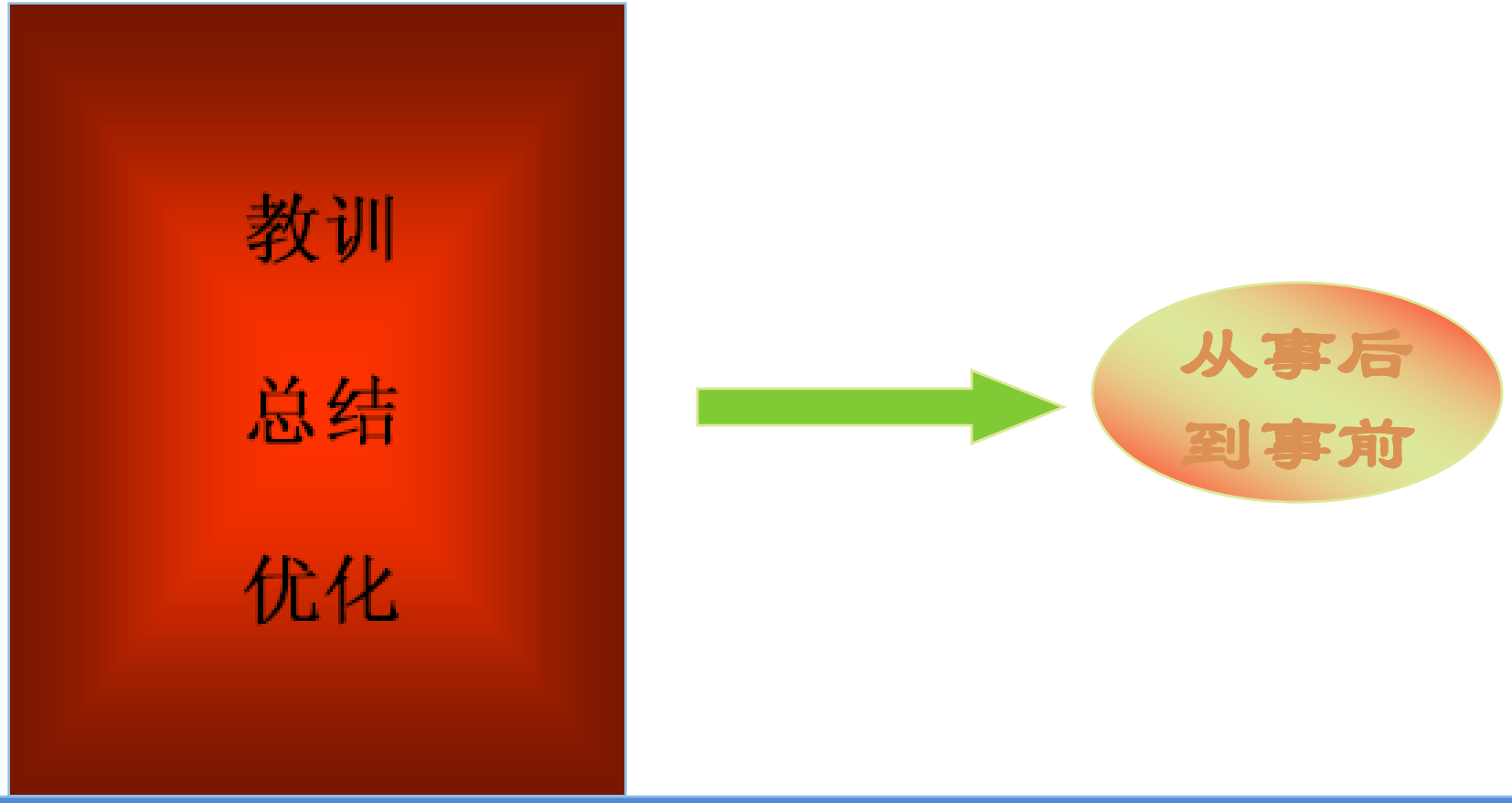
*技术层面：*对具体的安全技术人员，可以利用IDS做为工具来发现安全问题、解决问题。

入侵检测发挥的作用



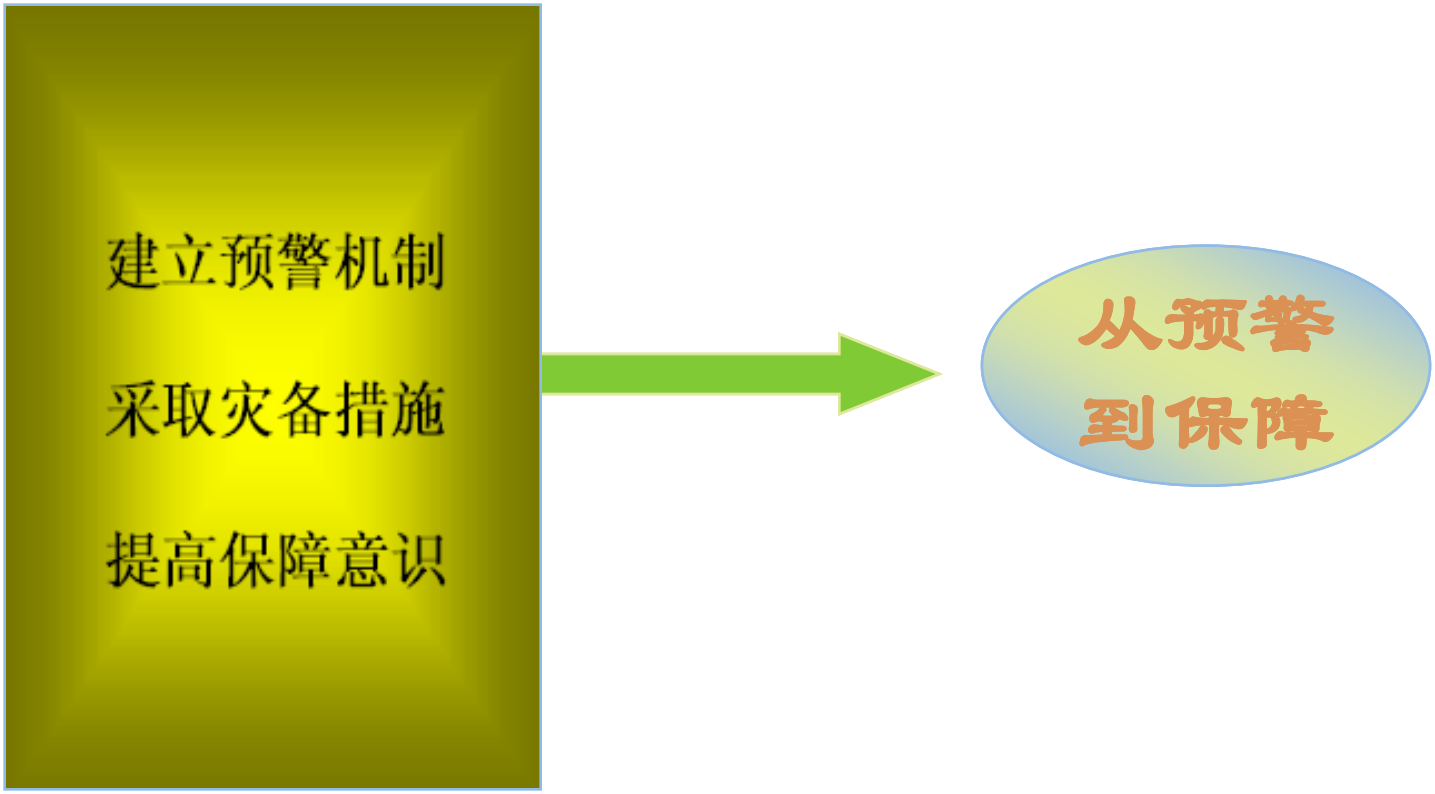
*管理层面：*对安全管理人员来说，是可以把**IDS**做为其日常管理上的有效手段。

入侵检测发挥的作用



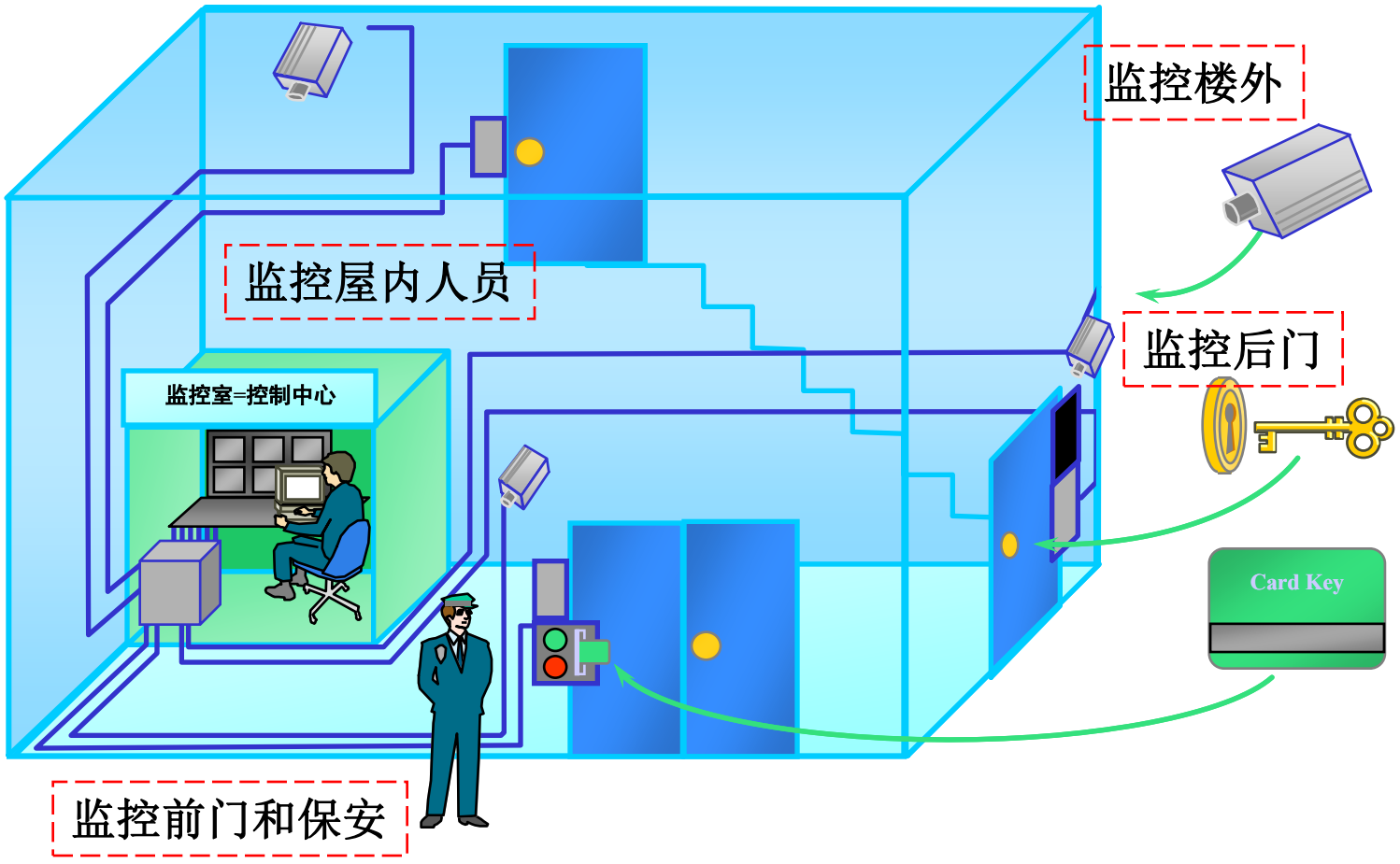
*领导层面：*对安全主管领导来说，是可以把IDS做为把握全局一种有效的方法，目的是提高安全效能。

入侵检测发挥的作用



*意识层面：*对政府或者大的行业来说，是可以通过IDS来建立一套完善的网络预警与响应体系，减小安全风险。

入侵检测系统的作用



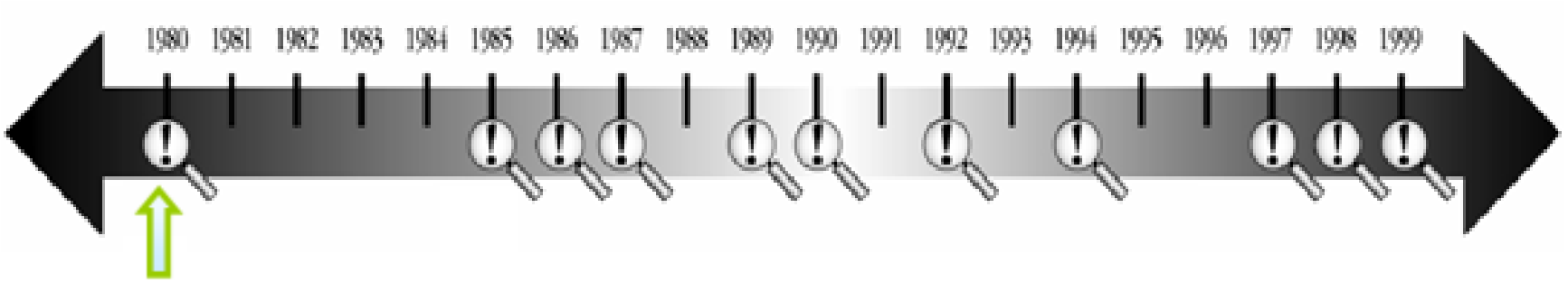
入侵检测系统作用

- 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

入侵检测概述

- 什么是入侵检测系统
- 为什么需要入侵检测
- 入侵检测系统的作用
- 入侵检测的发展历程
- 入侵检测的相关术语

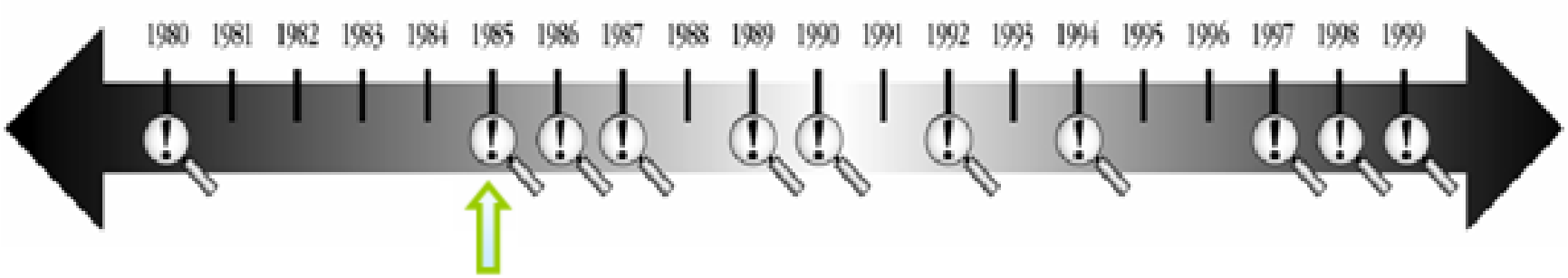
入侵检测系统的历史



1980年James P. Anderson 的《计算机安全威胁监控与监视》

- 第一次详细阐述了入侵检测的概念
- 计算机系统威胁分类：外部渗透、内部渗透和不法行为
- 提出了利用审计跟踪数据监视入侵活动的思想
- 这份报告被公认为是入侵检测的开山之作

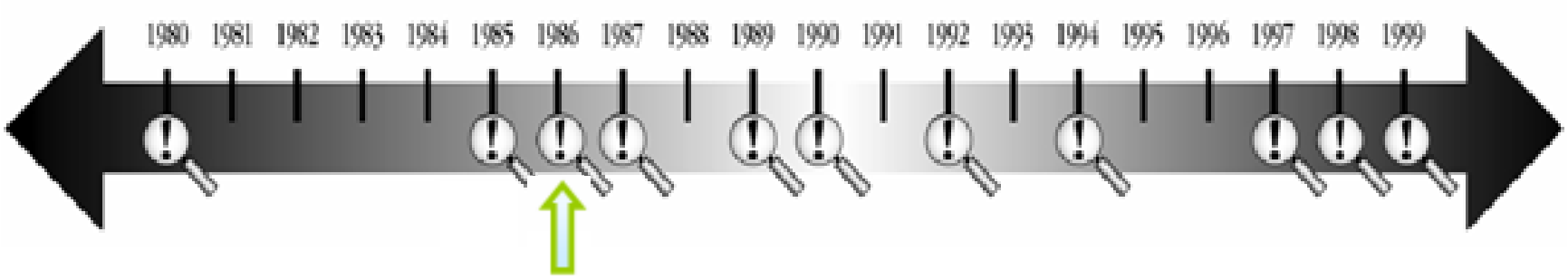
入侵检测系统的历史



1985 年

SRI由美国海军（SPAWAR）资助以建立**Intrusion Detection Expert System(IDES)－入侵检测专家系统（IDES）** 的初步原型。
第一个系统中同时使用了***statistical and rule-based－基于统计和基于规则***的方法。

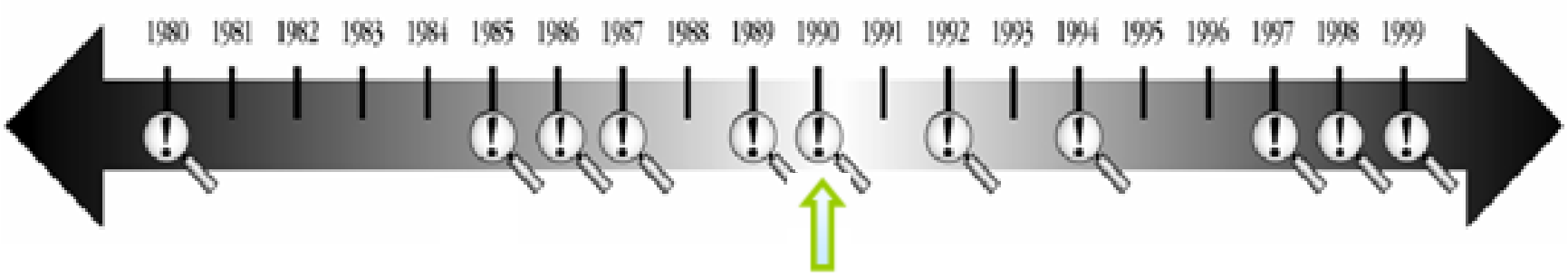
入侵检测系统的历史



1986 年
Dorothy Denning

发表了“***An Intrusion-Detection Model-一个入侵检测的模型***”，入侵检测领域开创性的工作。
基本的行为分析机制。
一些可能的实现系统的方法。

入侵检测系统的历史



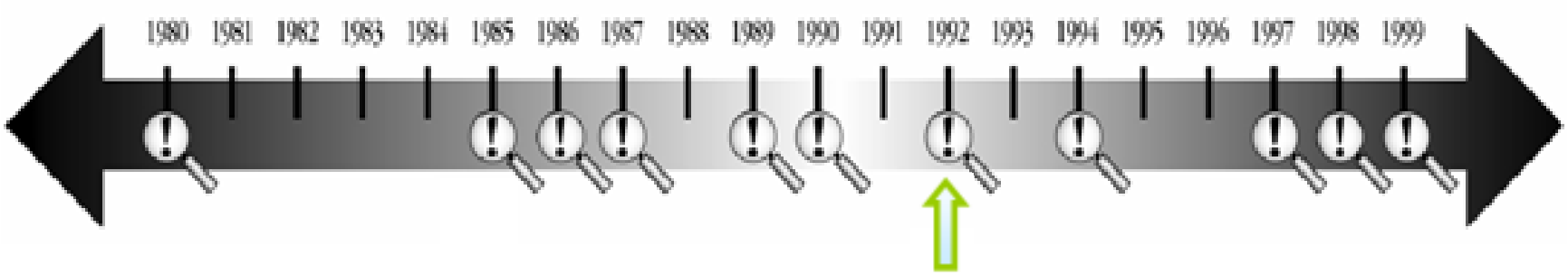
1990 年
Todd Heberlien，California, Davis大学的一个学生

写了***Network Security Monitor(NSM)—网络安全监视器（NSM）***，系统设计用于捕获TCP/IP包并检测异构网络中的异常行动。

网络入侵检测诞生

- **该系统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**
- **入侵检测系统发展史翻开了新的一页，两大阵营正式形成：基于网络的IDS和基于主机的IDS**

入侵检测系统的历史



1992 年

计算机误用检测系统（CMDS）Computer Misuse Detection System(CMDS)

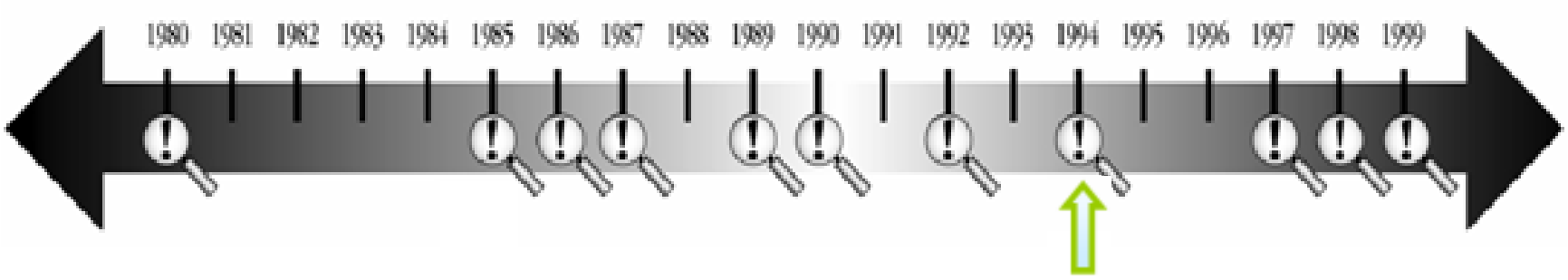
Screen Application International Corporation(SAIC)

基于在海军报告调查中完成的工作

Stalker （ Haystack Labs. ）

基于为空军完成的原Haystack工作，第一个商业化的主机IDS，用于UNIX

入侵检测系统的历史

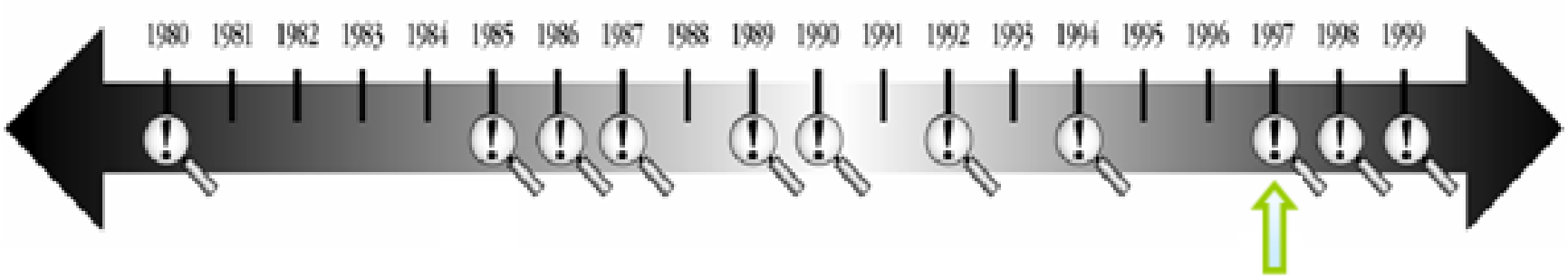


1994 年

A group of researchers at the 空军加密支持中心（Air Force Cryptological Support Center）的一组研究人员创建了鲁棒的网络入侵检测系统，**ASIM**，广泛用于空军。

来自于一家商业化公司 **Wheelgroup**的开发人员开始商业化网络入侵检测技术。

入侵检测系统的历史

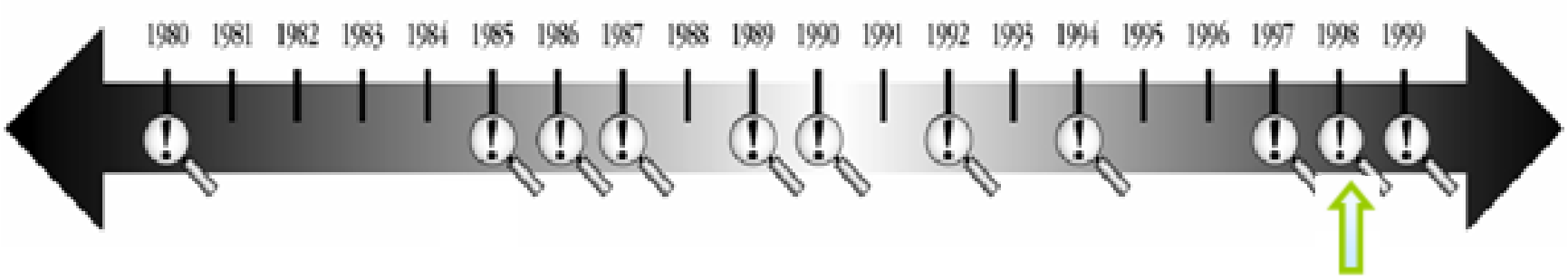


1997 年

Cisco收购了 Wheelgroup并开始将网络入侵检测加入路由器中。

Internet Security Systems发布了 **Realsecure**，Windows NT的网络入侵检测系统。
开始了网络入侵检测的革命。

入侵检测系统的历史



1998 年

Centrax公司发布了 **eNTrax**，用于Windows NT的分布主机入侵检测系统

Centrax是由CMDS的开发人员组成，后来加入了建立Stalker的技术队伍。

入侵检测系统的历史

从20世纪90年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足的进展

入侵检测概述

- 什么是入侵检测系统
- 为什么需要入侵检测
- 入侵检测系统的作用
- 入侵检测的发展历程
- 入侵检测的相关术语

入侵检测相关术语

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。
- CIDF 将入侵检测系统需要分析的数据统称为事件（event）

入侵检测相关术语

false positives（虚警）

- 检测系统在检测时把系统的正常行为判为入侵行为的错误被称为虚警。
- 检测系统在检测过程中出现虚警的概率称为系统的虚警率。

false negatives（漏警）

- 检测系统在检测时把某些入侵行为判为正常行为的错误现象称为漏警。
- 检测系统在检测过程中出现漏警的概率称为系统的漏警率。

这两个参数是体现入侵检测系统性能的最关键的两个参数

入侵检测相关术语

Honeypot（蜜罐）

- 模拟脆弱性主机诱惑攻击者在其上浪费时间
- 延缓对真正目标的攻击

Promiscuous（混杂模式）

- 网卡的一种接收模式
- 在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是 传给它的

- 网卡具有如下的几种工作模式：

1）**广播模式**:物理地址（MAC）地址是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

2）**多播模式**：多播模式地址作为目的物理地址的帧可以被组内的其它主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

3）**直接模式**:工作在直接模式下的网卡只接收目地址是自己Mac地址的帧。

4）**混杂模式**:工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

入侵检测相关术语

CIDF

- 1997年，DARPA(Defense Advanced Research Projects Agency)资助成立了CIDF(Common Intrusion Detection Framework)工作组
- 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
- 为什么需要一套规范？
- 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

入侵检测系统

- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测系统的分类

- ✓ 按数据检测方法分类
- ✓ 按系统结构分类
- ✓ 按时效性分类
- ✓ 按照数据来源分类

入侵检测的分类（一）

- 按照分析方法（检测方法）
  - 误用检测（Misuse Detection）
  - 异常检测（Anomaly Detection ）

入侵检测的分类（一）

- **误用检测思想：**
  - 如果所有的入侵行为和手段（及其变种）都能够表达为一种模式或特征，那么所有已知的入侵方法就可以用匹配的方法来发现。
- **特点：**
  - 与防病毒一样，基于一个特征库
  - 能很准确地检测攻击
  - 只能检测到已知的攻击方式
  - 技术相对成熟，大多数的商业产品基于此技术

入侵检测的分类（一）

- **异常检测思想：**
  - 首先总结正常操作应该具有的特征（如CPU利用率、缓存剩余空间、用户使用计算机的习惯），当用户活动与正常行为有重大偏离时即被认为是入侵。
- **特点：**
  - 统计模型
  - 误报较多
  - 可检测到未知攻击
  - 不太成熟，罕见商业化的产品

入侵检测的分类（二）

按系统结构分类

- 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

入侵检测的分类（三）

- 根据时效性分类
  - 离线入侵检测系统（off-line IDS）
  - 在线入侵检测系统（On-line IDS）

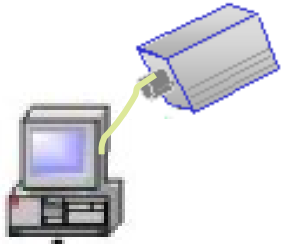
入侵检测系统分类(四)

按数据来源分类

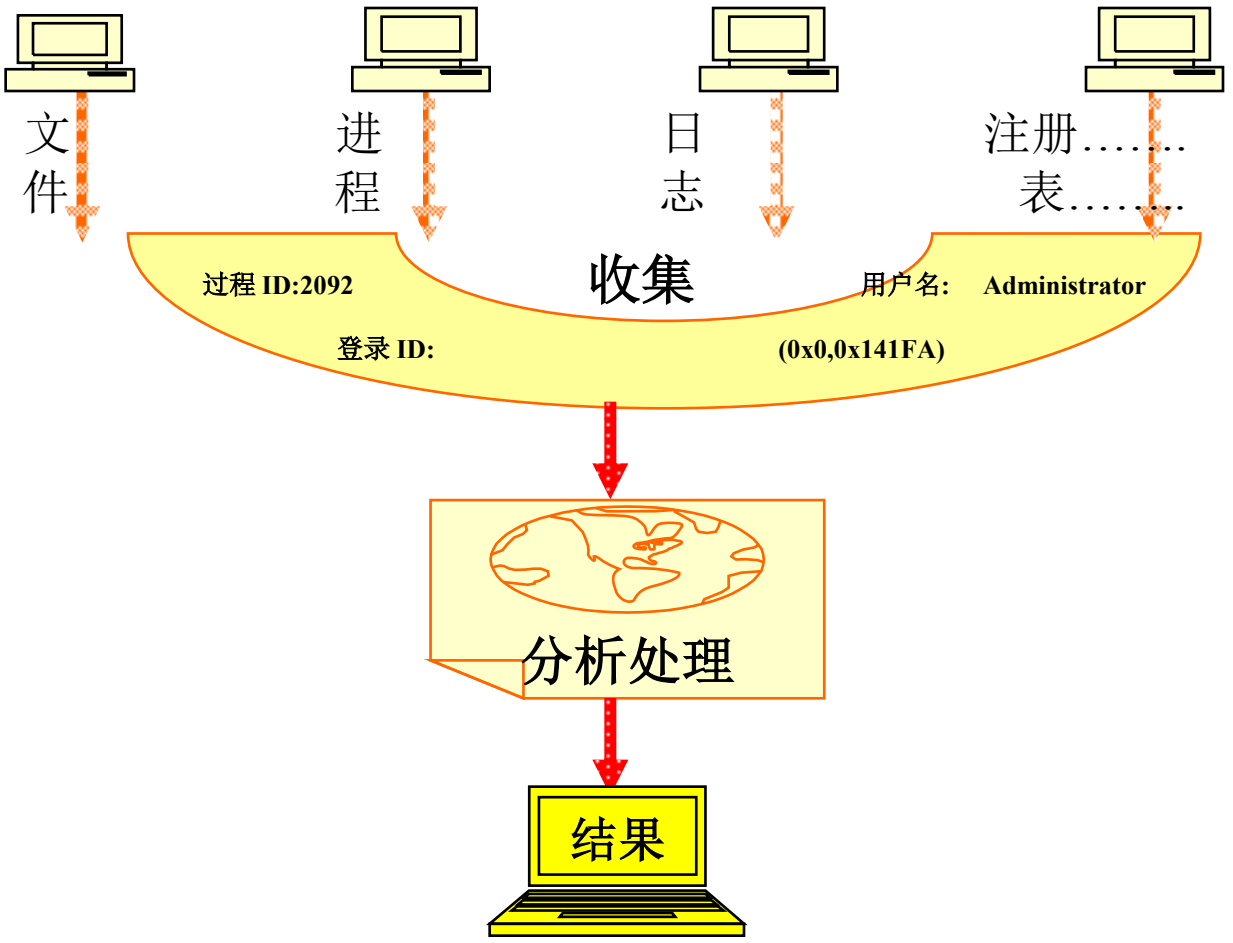
基于主机的入侵检测系统（HIDS）
基于网络的入侵检测系统（NIDS）
混合型入侵检测系统（Hybrid IDS）
网络节点入侵检测系统（NNIDS）

主机IDS

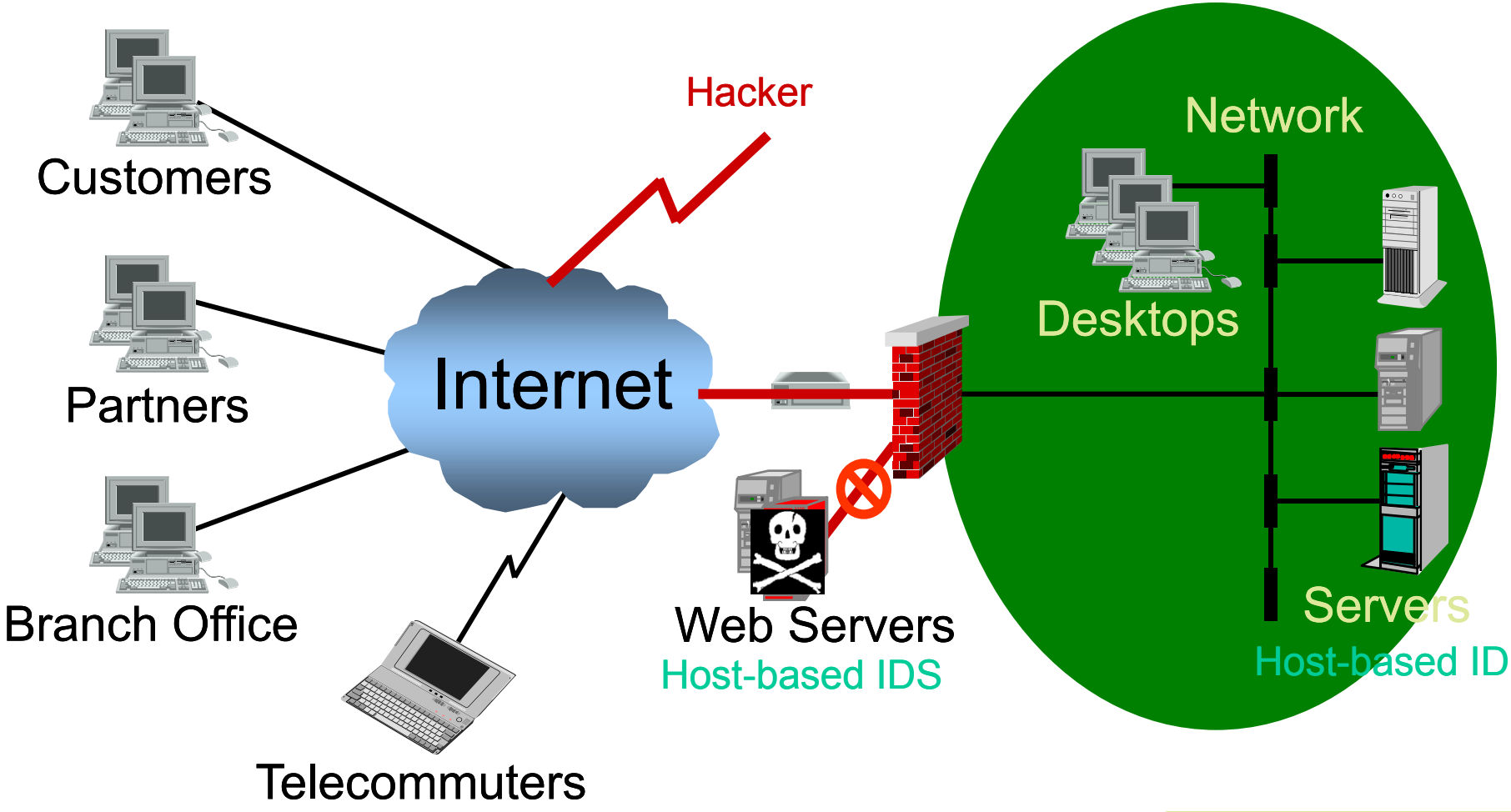
- 定义
  - 运行于被检测的主机之上，通过查询、监听当前系统的各种资源的使用运行状态，发现系统资源被非法使用和修改的事件，进行上报和处理
- 特点
  - 安装于被保护的主机中
    - 系统日志
    - 系统调用
    - 文件完整性检查
  - 主要分析主机内部活动
  - 占用一定的系统资源



主机IDS

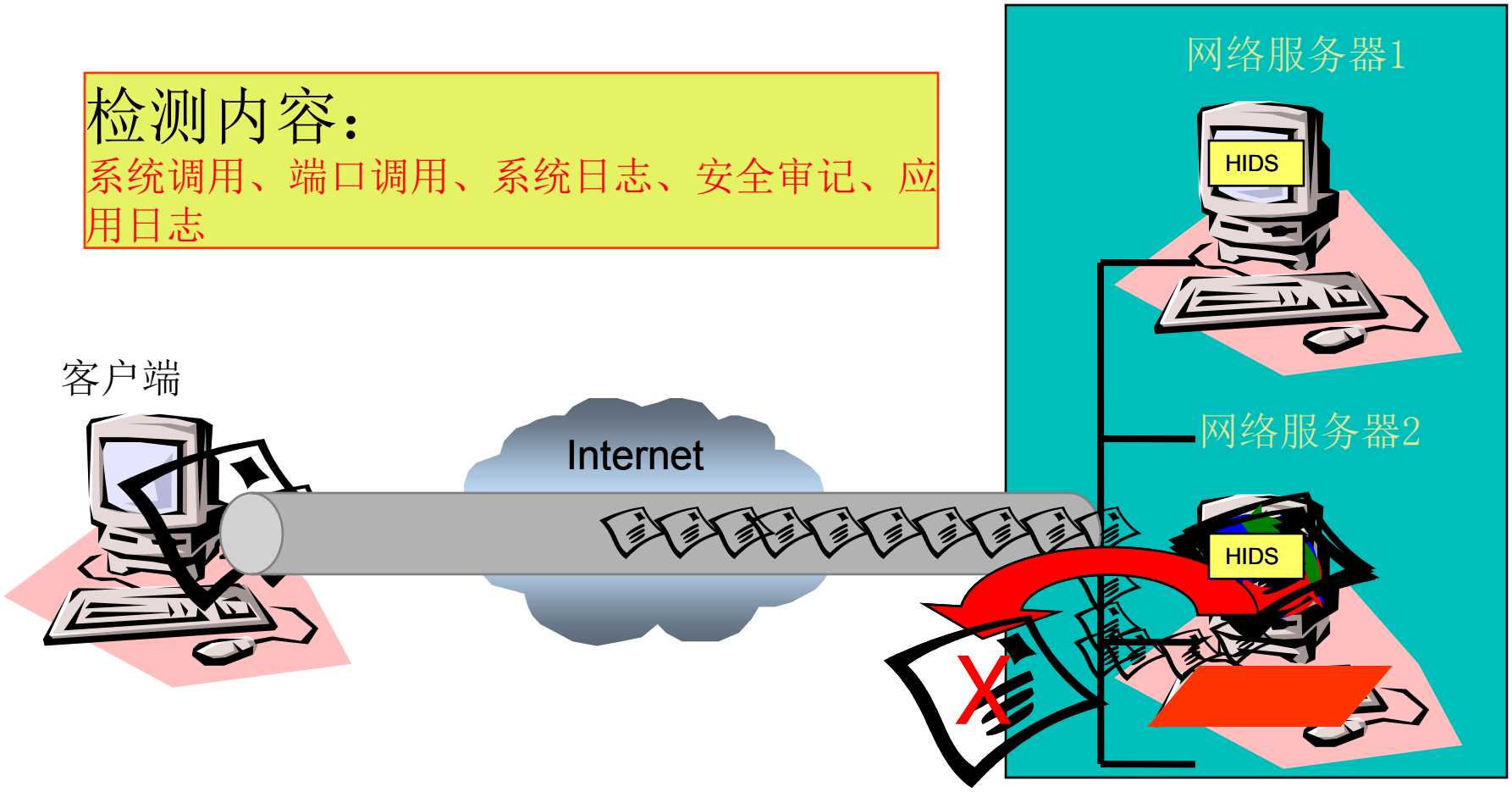

文件
进程
日志
注册……表……
过程 ID:2092
收集
用户名: Administrator
登录 ID:
(0x0,0x141FA)
分析处理
结果

主机IDS


Customers
Partners
Branch Office
Telecommuters
Hacker
Internet
Web Servers
Host-based IDS
Network
Desktops
Servers
Host-based IDS

基于主机入侵检测系统工作原理

检测内容：
系统调用、端口调用、系统日志、安全审记、应用日志



主机IDS

- 按照检测对象的不同，基于主机的入侵检测系统可以分为两类：网络连接检测和主机文件检测。

主机IDS

1.网络连接检测

网络连接检测是对试图进入该主机的数据流进行检测，分析确定是否有入侵行为，避免或减少这些数据流进入主机系统后造成损害。

网络连接检测可以有效地检测出是否存在攻击探测行为，攻击探测几乎是所有攻击行为的前奏。系统管理员可以设置好访问控制表，其中包括容易受到攻击探测的网络服务，并且为它们设置好访问权限。如果入侵检测系统发现有对未开放的服务端口进行网络连接，说明有人在寻找系统漏洞，这些探测行为就会被入侵检测系统记录下来，同时这种未经授权的连接也被拒绝。

主机IDS

2.主机文件检测

通常入侵行为会在主机的各种相关文件中留下痕迹，主机文件检测能够帮助系统管理员发现入侵行为或入侵企图，及时采取补救措施。

主机文件检测的检测对象主要包括以下几种：

（1） 系统日志

系统日志文件中记录了各种类型的信息，包括各用户的行为记录。如果日志文件中存在着异常的记录，就可以认为已经或正在发生网络入侵行为。这些异常包括不正常的反复登录失败记录、未授权用户越权访问重要文件、非正常登录行为等。

主机IDS

（2） 文件系统

恶意的网络攻击者会修改网络主机上包含重要信息的各种数据文件，他们可能会删除或者替换某些文件，或者尽量修改各种日志记录来销毁他们的攻击行为可能留下的痕迹。如果入侵检测系统发现文件系统发生了异常的改变，例如一些受限访问的目录或文件被非正常地创建、修改或删除，就可以怀疑发生了网络入侵行为。

主机IDS

（3） 进程记录

主机系统中运行着各种不同的应用程序，包括各种服务程序。每个执行中的程序都包含了一个或多个进程。每个进程都存在于特定的系统环境中，能够访问有限的系统资源、数据文件等，或者与特定的进程进行通信。黑客可能将程序的进程分解，致使程序中止，或者令程序执行违背系统用户意图的操作。如果入侵检测系统发现某个进程存在着异常的行为，就可以怀疑有网络入侵。

主机IDS优势

(1) 精确地判断攻击行为是否成功。

(2) 监控主机上特定用户活动、系统运行情况

(3) HIDS能够检测到NIDS无法检测的攻击

(4) HIDS适用加密的和交换的环境。

(5) 不需要额外的硬件设备。

主机IDS的劣势

(1) HIDS对被保护主机的影响。

(2) HIDS的安全性受到宿主操作系统的限制。

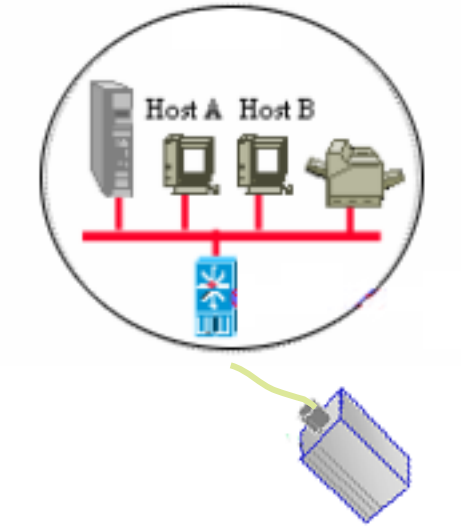
(3) HIDS的数据源受到审计系统限制。

(4) 被木马化的系统内核能够骗过HIDS。

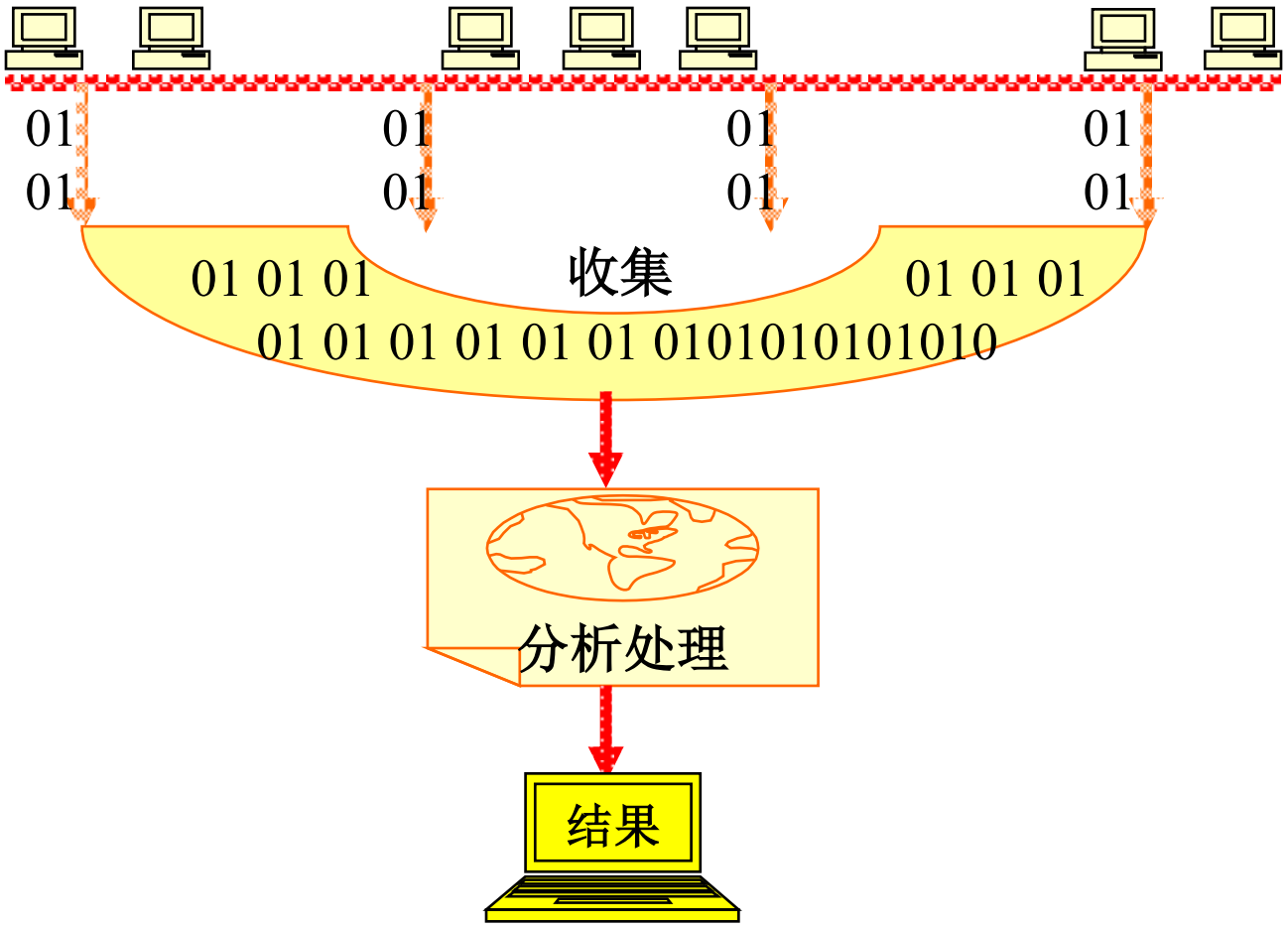
(5) 维护/升级不方便。

网络IDS

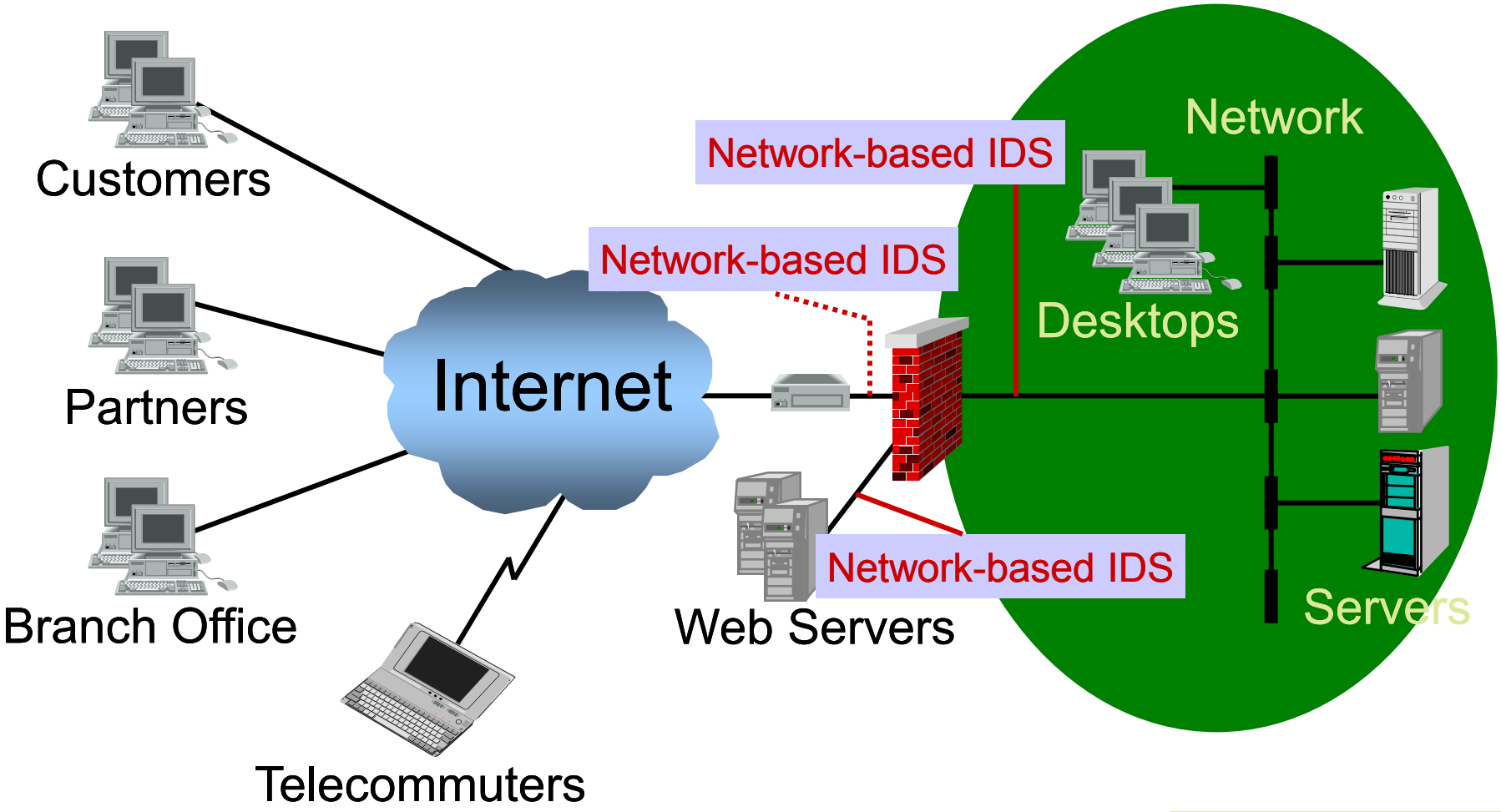
- 定义
  - 通过在共享网段上对通信数据的侦听采集数据，分析可疑现象。这类系统不需要主机提供严格的审计，对主机资源消耗少，并可以提供对网络通用的保护而无需顾及异构主机的不同架构。
- 特点
  - 安装在被保护的网段（通常是共享网
  - 混杂模式监听
  - 分析网段中所有的数据包
  - 实时检测和响应



网络IDS实现

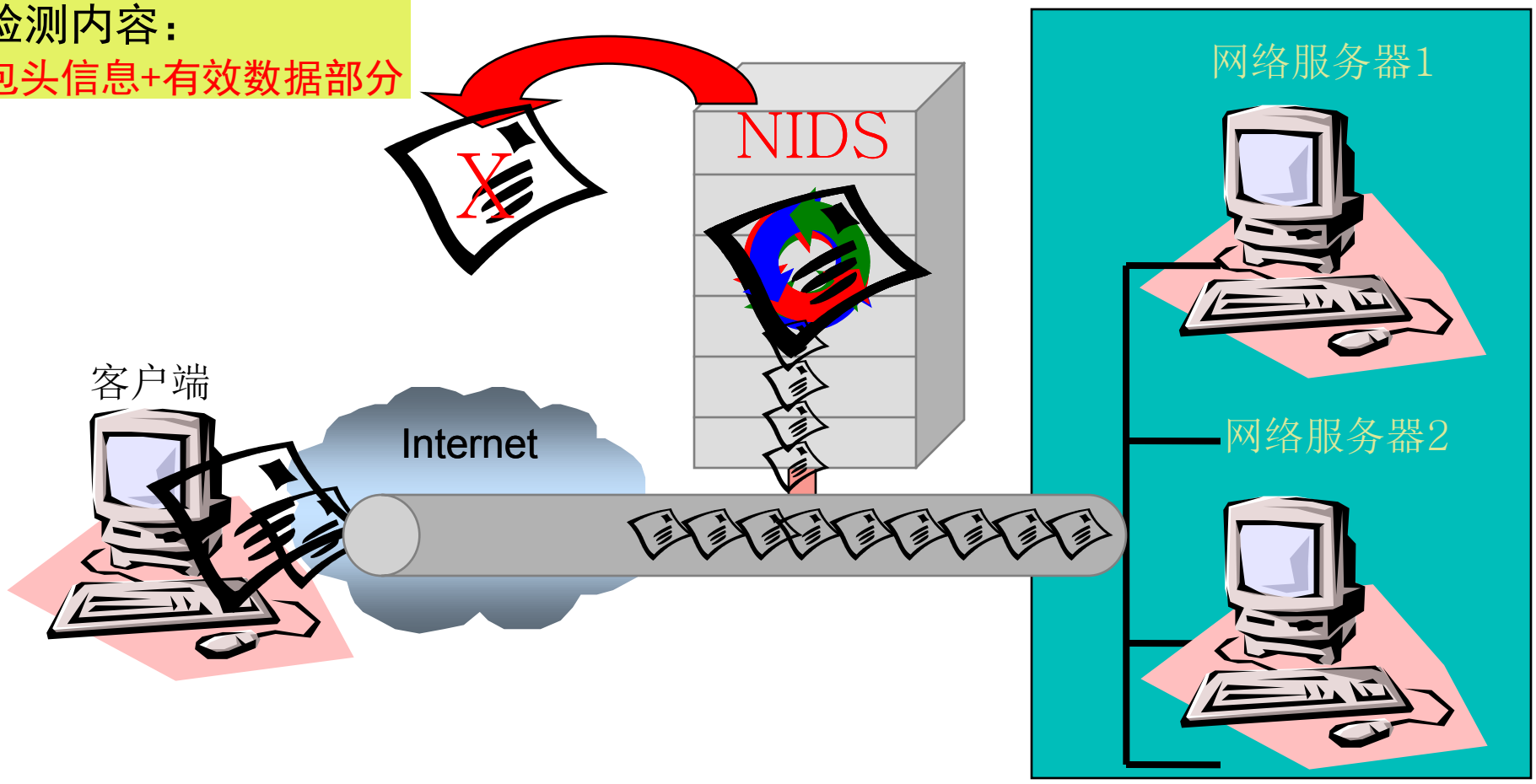

01
01
01
01
01
01
01
01
01 01 01
收集
01 01 01
01 01 01 01 01 01 0101010101010
分析处理
结果

网络IDS


Customers
Partners
Branch Office
Telecommuters
Internet
Network-based IDS
Network-based IDS
Network-based IDS
Web Servers
Network
Desktops
Servers

网络IDS

检测内容：
包头信息+有效数据部分



数据包=包头信息+有效数据部分

网络IDS优势

(1) 实时分析网络数据，检测网络系统的非法行为；

(2) 网络IDS系统单独架设，不占用其它计算机系统的任何资源；

(3) 网络IDS系统是一个独立的网络设备，可以做到对黑客透明，因此其本身的安全性高；

(4) 它既可以用于实时监测系统，也是记录审计系统，可以做到实时保护，事后分析取证；

(5) 通过与防火墙的联动，不但可以对攻击预警，还可以更有效地阻止非法入侵和破坏。

(6)不会增加网络中主机的负担。

网络IDS的劣势

(1)不适合交换环境和高速环境
(2)不能处理加密数据
(3) 资源及处理能力局限
(4) 系统相关的脆弱性

混合型入侵检测系统

- 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。

入侵检测系统

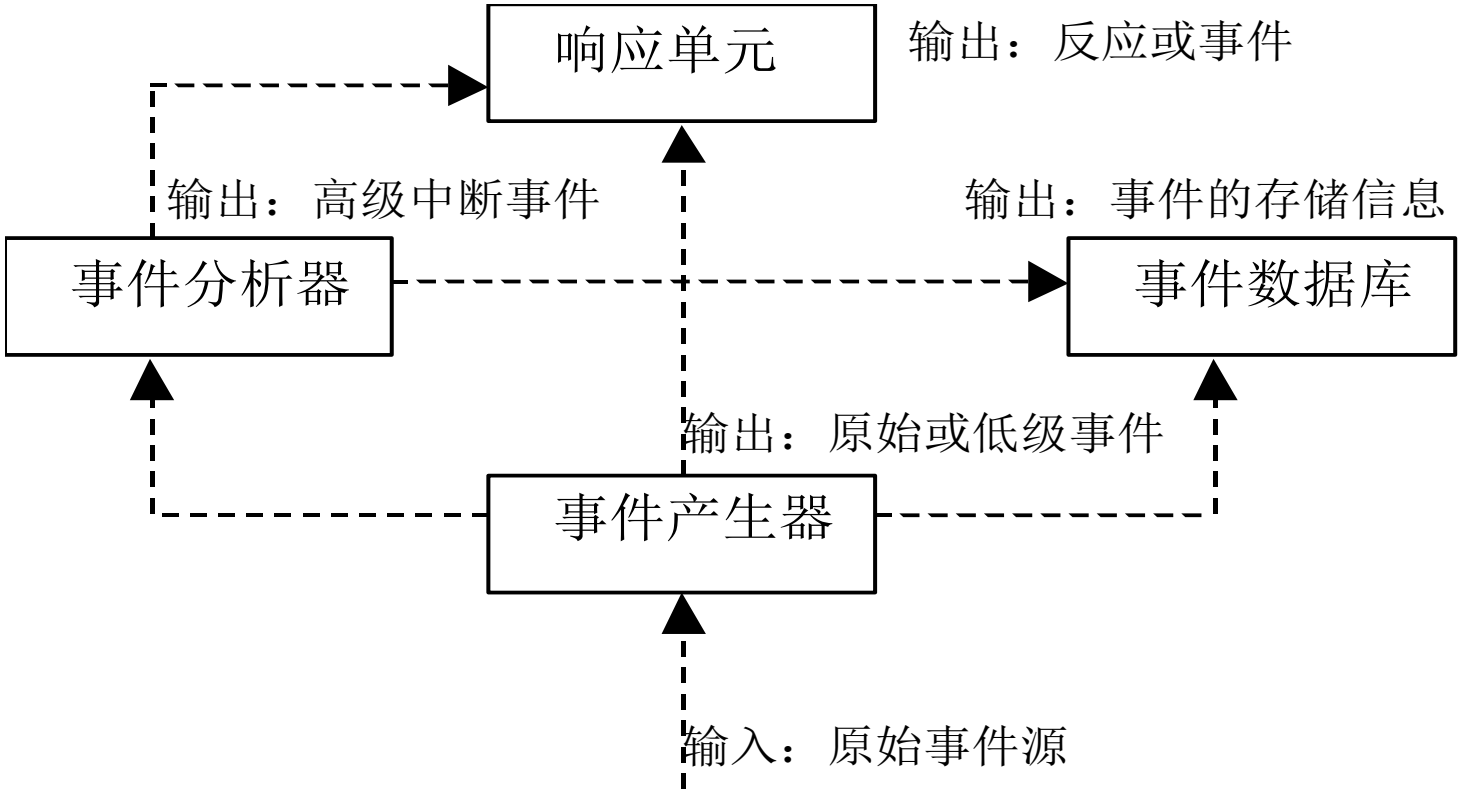
- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测系统结构

Common Intrusion Detection Frame组件

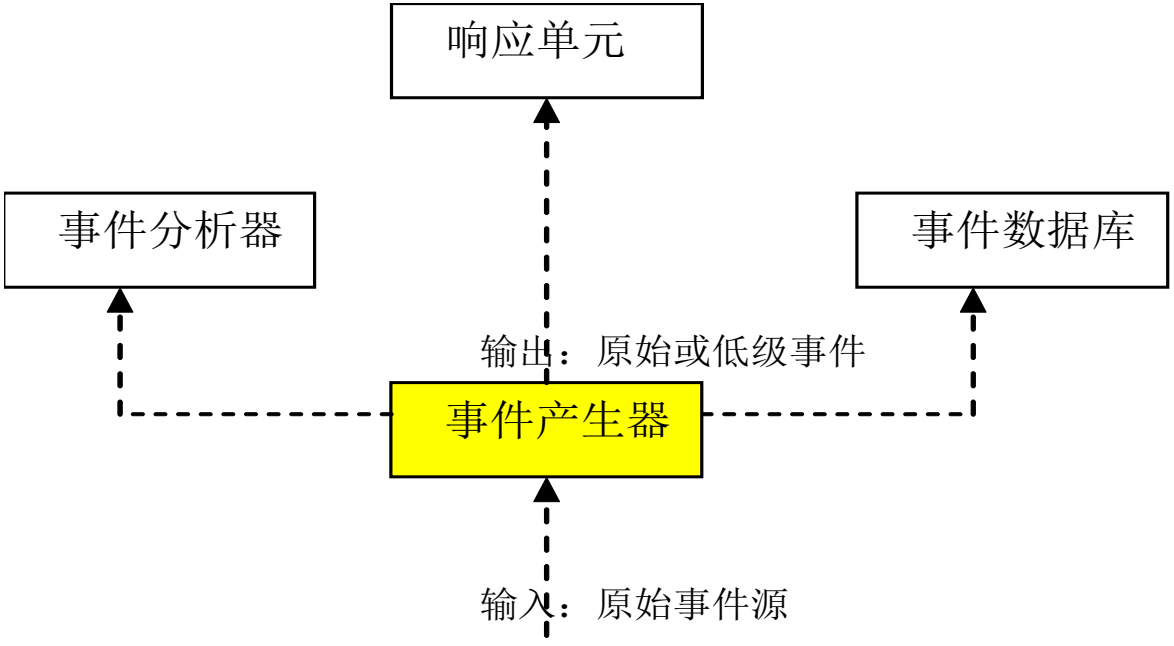
- 事件产生器（Event generators）
- 事件分析器（Event analyzers）
- 响应单元（Response units）
- 事件数据库（Event databases）

CIDF组件


响应单元
输出：反应或事件
输出：高级中断事件
输出：事件的存储信息
事件分析器
事件数据库
输出：原始或低级事件
事件产生器
输入：原始事件源

事件产生器（1）

- 负责原始数据采集，并将收集到的原始数据转换为事件，向系统的其他部分提供此事件。
- 收集内容：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收集信息。

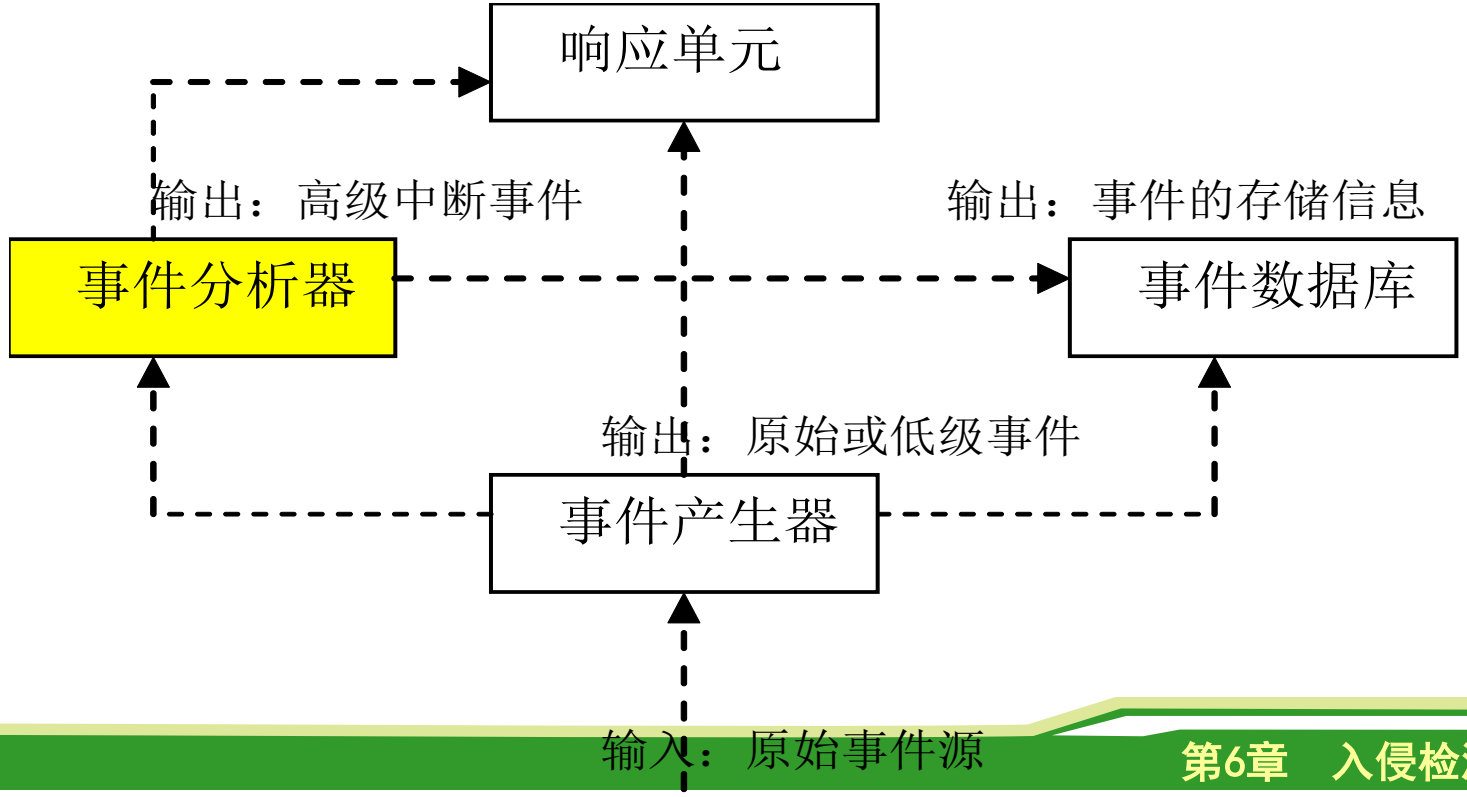


事件产生器（2）

- **注意：**
- **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

事件分析器（1）

- 接收事件信息，对其进行分析，判断是否为入侵行为或异常现象，最后将判断的结果转变为告警信息。



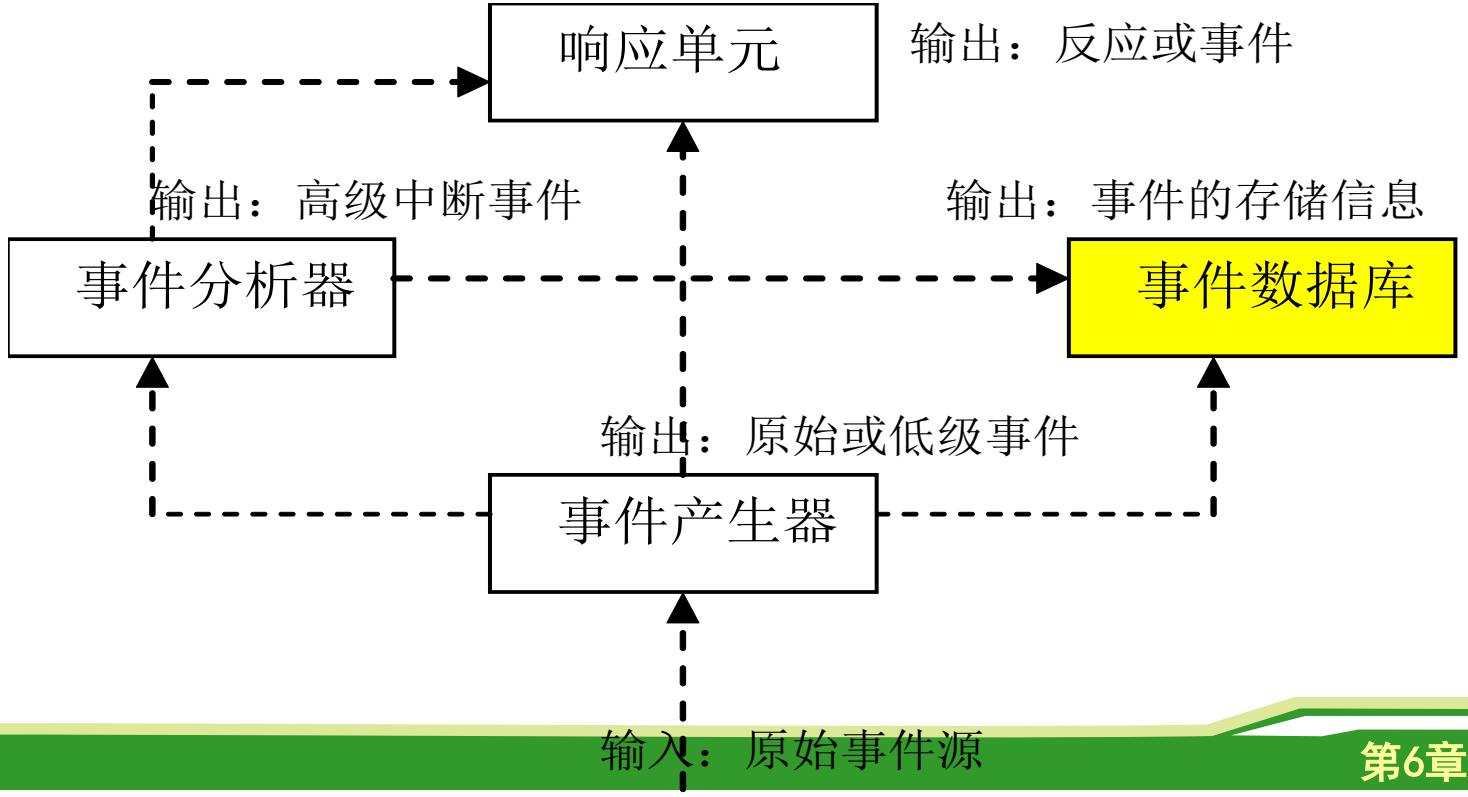
事件分析器（2）

分析方法：

- 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
- 完整性匹配（往往用于事后分析）：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。

事件数据库

- 存放各种中间和最终数据的地方
- 从时间产生器或时间分析器接收数据，一般会将数据进行较长时间的保存。



响应单元

- 根据告警信息作出反应，是IDS中的主动武器
- 可做出：
  - 强烈反应，切断连接、封锁用户账号、改变文件属性等
  - 简单的报警，如控制台显示、电子邮件通知、短信提示等

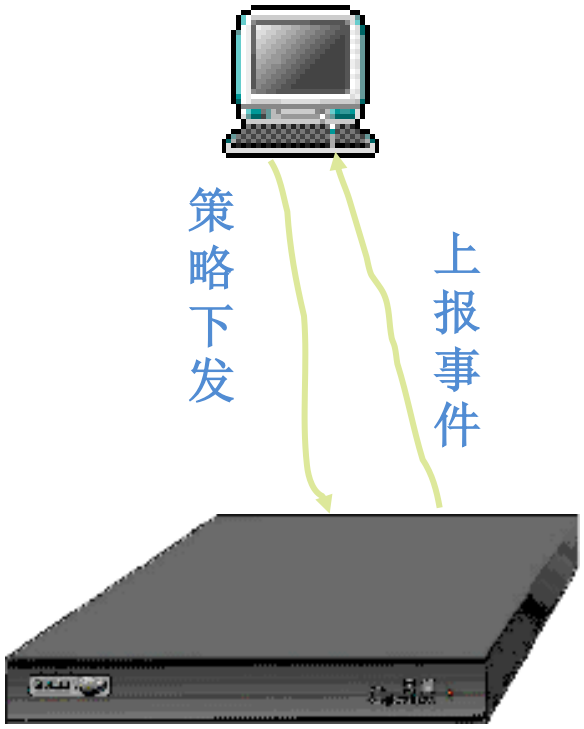
常见产品形态组件

控制中心

- 表现方式：软件
- 功能：
  - ✓接收事件
  - ✓策略下发
  - ✓日志记录与分析
  - ✓事件库升级

探测引擎

- 表现方式：硬件/软件
- 功能：
  - ✓抓包
  - ✓分析数据
  - ✓上报事件



入侵检测系统

- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测系统关键技术

数据采集技术

数据检测技术

数据分析技术

数据采集技术

- 主机信息采集
  - 应用程序日志
  - 审计日志
  - 网络端口的连接状况
  - 系统文件
- 包俘获
  - Libpcap（Packet Capture Libray）数据包捕获函数库：是unix/linux平台下的网络数据包捕获函数包
  - Winpcap是libpcap的Windows版本。
- 高速网络数据采集
  - DMA-based zero copy

入侵检测系统关键技术

数据采集技术

数据检测技术

数据分析技术

数据检测技术

- 基于误用的检测方法

- 基于异常的检测方法

数据检测技术

基于误用的检测方法

- 运用已知攻击方法，根据已定义好的入侵模式，通过判断这些入侵模式是否出现来检测。
- 通过分析入侵过程的特征、条件、排列以及事件间关系能具体描述入侵行为的迹象。
- 也被称为违规检测(Misuse Detection)。
- 检测准确度很高。

数据检测技术

基于误用的检测方法

具体实现

- 专家系统
- 模型匹配检测系统
- 状态转换分析

基于误用的检测方法

专家系统

- 攻击信息使用的输入使用if—then的语法。
- 指示入侵的具体条件放在规则的左边（if侧），当满足这些规则时，规则执行右边（then侧）的动作。

基于误用的检测方法

模式匹配检测

- 根据知识建立攻击脚本库，每一脚本都由一系列攻击行为组成。
- 有关攻击者行为的知识被描述为：攻击者目的，攻击者达到此目的的可能行为步骤，以及对系统的特殊使用等。

基于误用的检测方法

模式匹配检测示例

```
  0  0050 dac6 f2d6 00b0 d04d cbaa 0800 4500   .P.......M....E.
 10  0157 3105 4000 8006 0000 0a0a 0231 d850   .W1.@........1.P
 20  1111 06a3 0050 df62 322e 413a 9cf1 5018   .....P.b2.A:..P.
 30  16d0 f6e5 0000 4745 5420 2f70 726f 6475   ......GET /produ
 40  6374 732f 7769 7265 6c65 7373 2f69 6d61   cts/wireless/ima
 50  6765 732f 686f 6d65 5f63 6f6c 6c61 6765   ges/home_collage
 60  322e 6a70 6720 4854 5450 2f31 2e31 0d0a   2.jpg HTTP/1.1..
 70  4163 6365 7074 3a20 2a2f 2a0d 0a52 6566   Accept: */*..Ref
 80  6572 6572 3a20 6874 7470 3a2f 2f77 7777   erer: http://www
 90  2e61 6d65 7269 7465 6368 2e63 6f6d 2f70   .ameritech.com/p
 a0  726f 6475 6374 732f 7769 7265 6c65 7373   roducts/wireless
 b0  2f73 746f 7265 2f0d 0a41 6363 6570 742d   /store/..Accept-
 c0  4c61 6e67 7561 6765 3a20 656e 2d75 730d   Language: en-us.
 d0  0a41 6363 6570 742d 456e 636f 6469 6e67   .Accept-Encoding
 e0  3a20 677a 6970 2c20 6465 666c 6174 650d   : gzip, deflate.
 f0  0a55 7365 722d 4167 656e 743a 204d 6f7a   .User-Agent: Moz
100  696c 6c61 2f34 2e30 2028 636f 6d70 6174   illa/4.0 (compat
110  6962 6c65 3b20 4d53 4945 2035 2e30 313b   ible; MSIE 5.01;
120  2057 696e 646f 7773 204e 5420 352e 3029    Windows NT 5.0)
130  0d0a 486f 7374 3a20 7777 772e 616d 6572   ..Host: www.amer
140  6974 6563 682e 636f 6d0d 0a43 6f6e 6e65   itech.com..Conne
150  6374 696f 6e3a 204b 6565 702d 416c 6976   ction: Keep-Aliv
160  650d 0a0d 0a                              e....
```

基于误用的检测方法

- 优点
  - 可检测出所有对系统来说是已知的入侵行为
  - 系统安全管理员能够很容易地知道系统遭受到的是那种入侵攻击并采取相应的行动
- 局限：
  - 它只是根据已知的入侵序列和系统缺陷的模式来检测系统中的可疑行为，而不能处理对新的入侵攻击行为以及未知的、潜在的系统缺陷的检测。
  - 系统运行的环境与知识库中关于攻击的知识有关。
  - 对于系统内部攻击者的越权行为，由于他们没有利用系统的缺陷，因而很难检测出来。

数据检测技术

- 基于误用的检测方法
- 基于异常的检测方法

数据检测技术

基于异常的检测方法

基本原理

1. 前提：入侵是异常活动的子集
2. 用户轮廓(Profile)：通常定义为各种行为参数及其阈值的集合，用于描述正常行为范围
3. 过程

监控 → 量化 → 比较 → 判定

↓

修正

4. 指标:漏报率低,误报率高

基于异常的检测方法

具体实现

- 基于统计学方法的异常检测
- 基于神经网络的异常检测
- 基于数据挖掘的异常检测

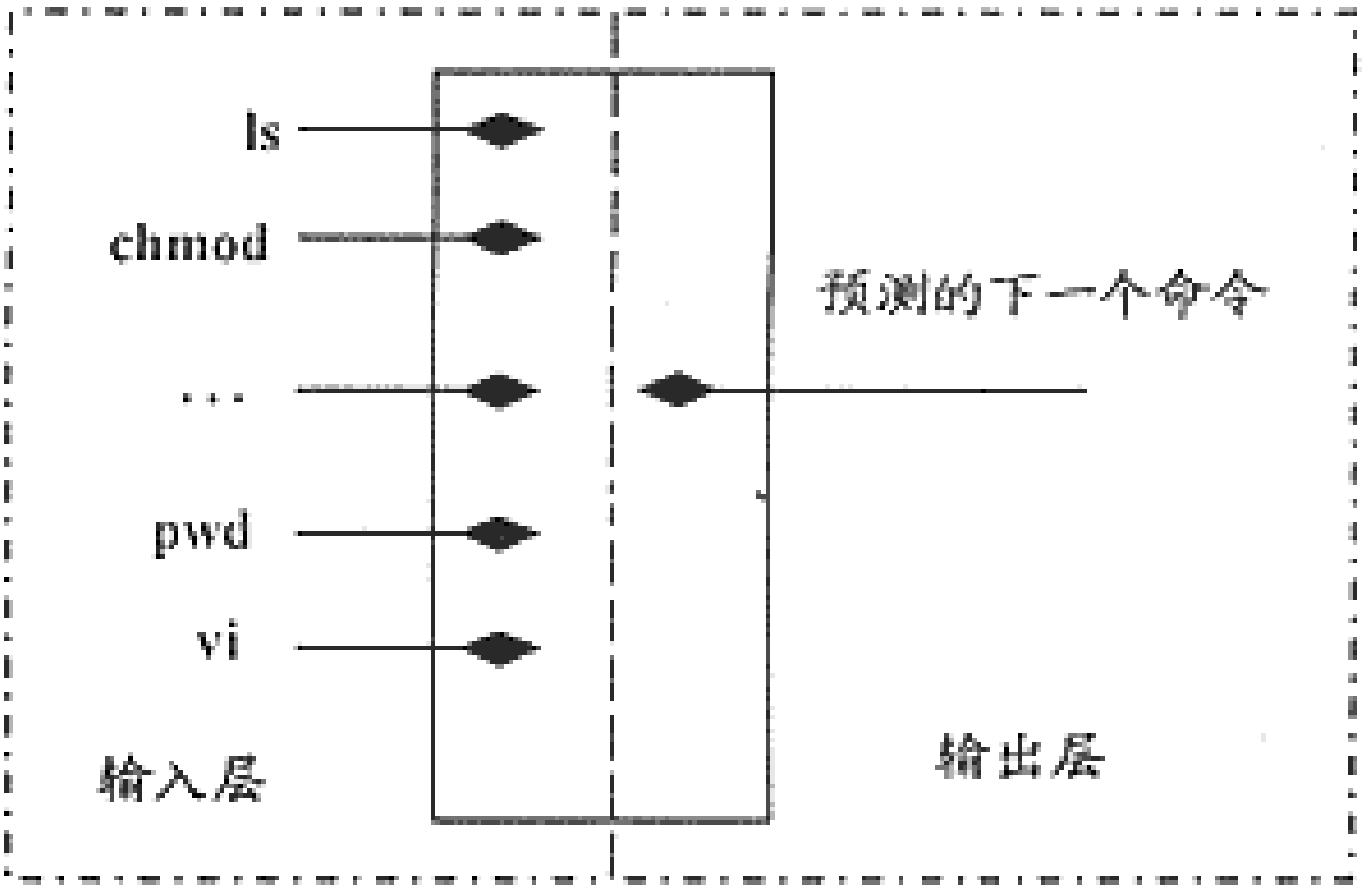
基于异常的检测方法

基于统计学方法

- 记录的具体操作包括：CPU 的使用，I/O 的使用，使用地点及时间，邮件使用，编辑器使用，编译器使用，所创建、删除、访问或改变的目录及文件，网络上活动等。
  - 操作密度
  - 审计记录分布
  - 范畴尺度
  - 数值尺度

基于异常的检测方法

基于神经网络



基于异常的检测方法

- 基于数据挖掘技术的异常检测

- 数据挖掘是指从大量实体数据抽象出模型的处理；
- 目的是要从海量数据中提取对用户有用的数据；
- 这些模型经常在数据中发现对其它检测方式不是很明显的异常。
- 主要方法：聚类分析、连接分析和顺序分析。

基于异常的检测方法

优点

- 不需要操作系统及其安全性缺陷专门知识
- 能有效检测出冒充合法用户的入侵

缺点

- 为用户建立正常行为模式的特征轮廓和对用户活动的异常性报警的门限值的确定都比较困难
- 不是所有入侵者的行为都能够产生明显的异常性
- 有经验的入侵者还可以通过缓慢地改变他的行为，来改变入侵检测系统中的用户正常行为模式，使其入侵行为逐步变为合法。

入侵检测系统关键技术

数据采集技术

数据检测技术

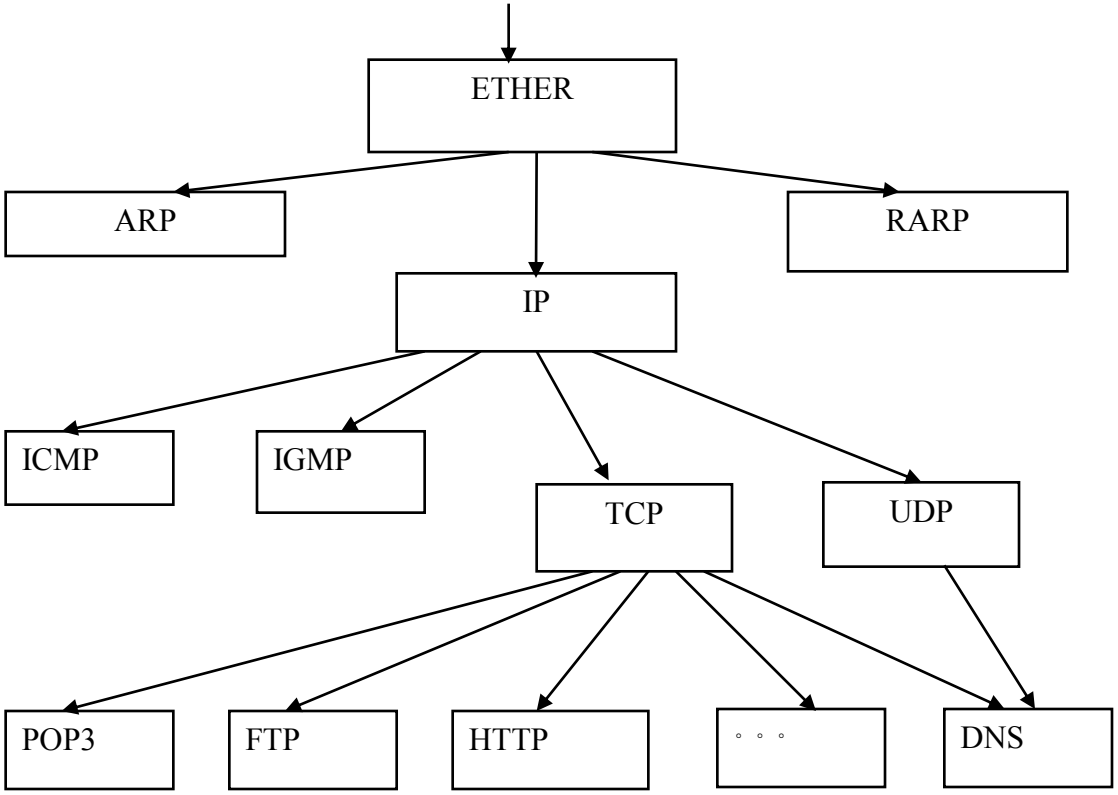
数据分析技术

数据分析技术

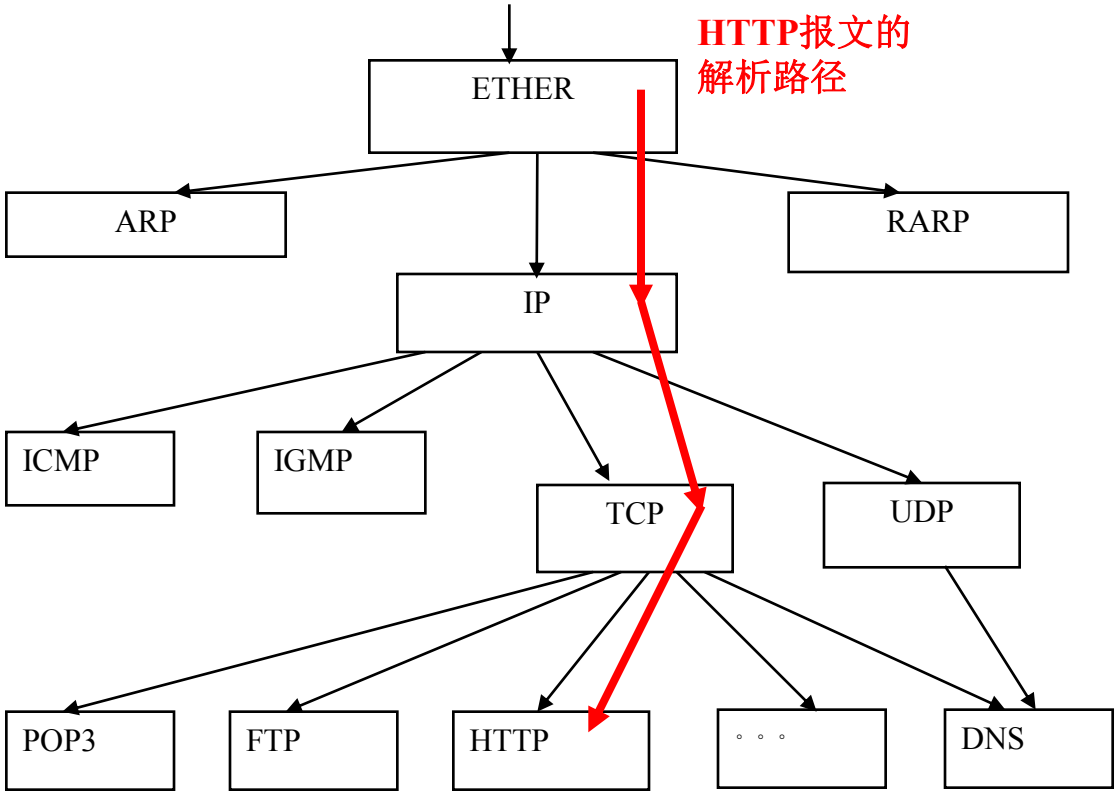
- 协议解析
- 有限状态自动机
- ACBM字符串匹配
- 正则表达式
- 事件规则树
- 完整性分析

数据分析技术

- 协议分析与解码



匹配规则子集



匹配的规则子集

ETHER规则子集

IP规则子集

TCP规则子集

HTTP规则子集

协议分析的优点

- ✓提高了性能
- ✓提高了准确性
- ✓基于状态的分析
- ✓反规避能力
- ✓系统资源开销小

检测实例

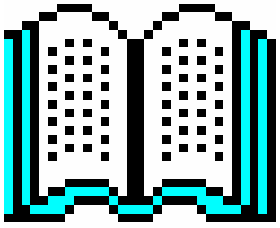
老版本的Sendmail有一个漏洞，telnet到25端口，输入wiz，然后接着输入超过1024Kb的shellcode，就能获得一个rootshell，还有通过debug命令的方式，也能获得root权限，进而控制系统。

```
$ telnet mail.victim.com 25
WIZ
Shell
ecx 0x943a3145 -1808125627
edx 0x408d17fc 1082988540。。。
```

或者

```
DEBUG
#*****
```

直接获得rootshell！



检测实例

简单的匹配

- 检查每个packet是否包含：

  “WIZ”

  “DEBUG”

检测实例

检查端口号

- 缩小匹配范围

```
Port 25:{
    “WIZ”
    |  “DEBUG”
}
```

检测实例

深入决策树

- 只判断客户端发送部分

```
Port 25:{
    Client-sends:  “WIZ”  |
    Client-sends:  “DEBUG”
}
```

检测实例

更加深入

- 状态检测 + 引向异常的分支

```
Port 25:{
    stateful client-sends:  “WIZ”  |
    stateful client-sends:  “DEBUG”
    after stateful  “DATA”  client-sends
          line > 1024 bytes  means
          possible buffer overflow
}
```

入侵检测系统

- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测系统的外围支撑技术

- 联动机制
- 响应机制
- 日志分析
- 事件过滤技术
- 漏洞机理研究

入侵检测系统

- ✓入侵检测概述
- ✓入侵检测系统的分类及特点
- ✓入侵检测系统结构
- ✓入侵检测系统的关键技术
- ✓入侵检测系统的外围支撑技术
- ✓入侵检测系统应用指南
- ✓入侵检测系统的发展趋势

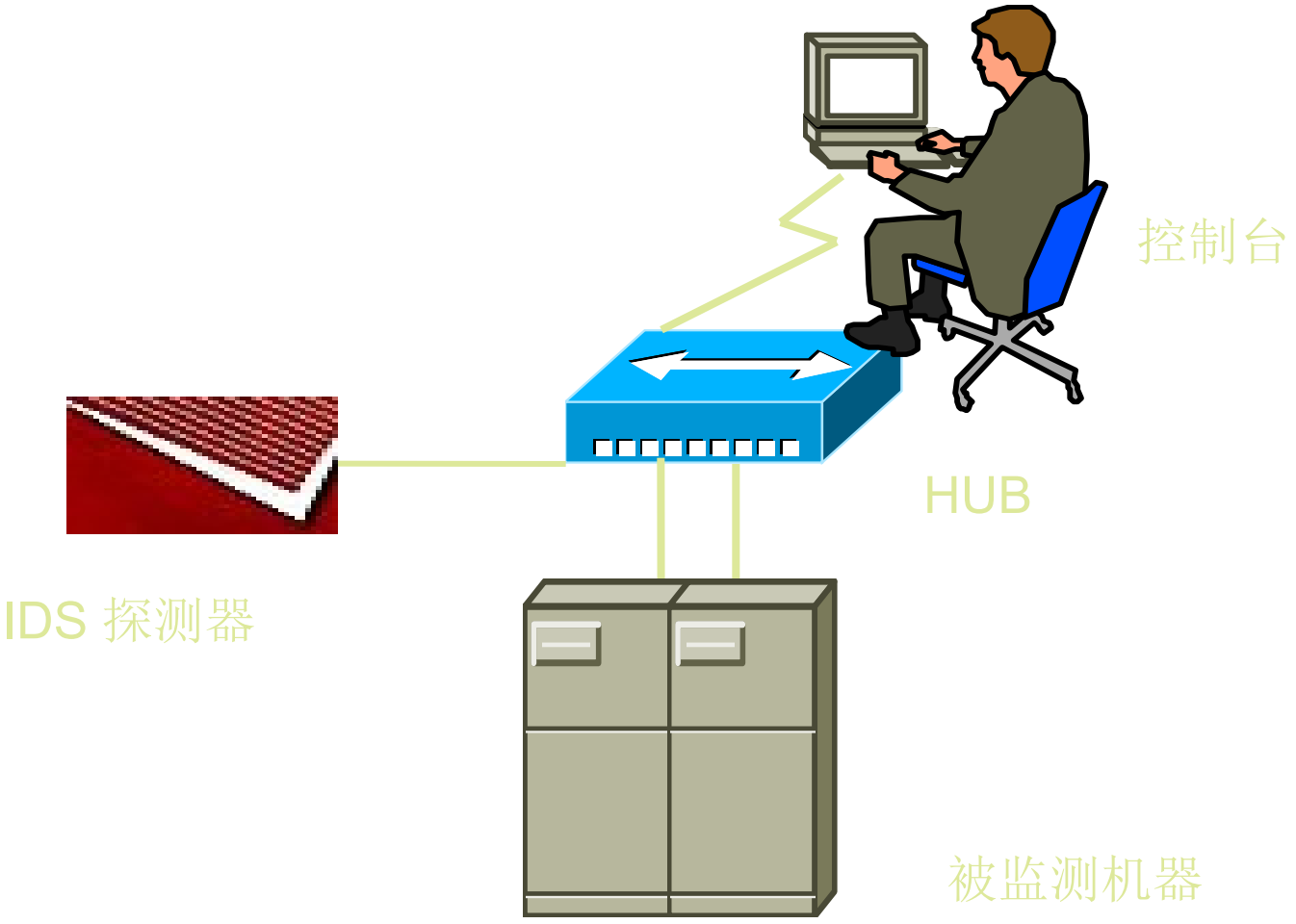
入侵检测系统应用指南

- IDS的部署
- 评价IDS的性能和功能指标
- 典型IDS产品介绍

IDS的部署

- 共享模式
- 隐蔽模式
- 交换模式
- In-line模式
- TAP模式

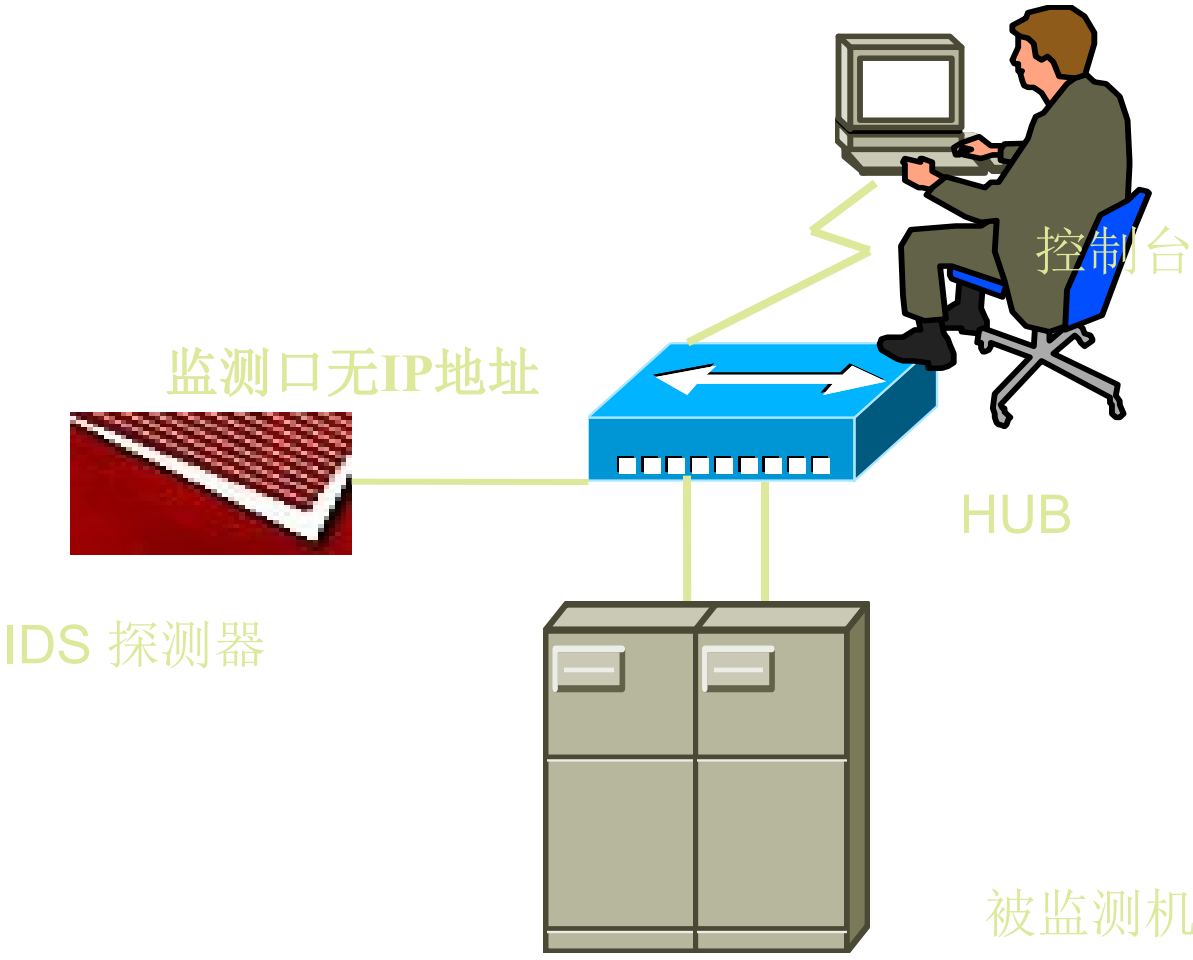
共享环境



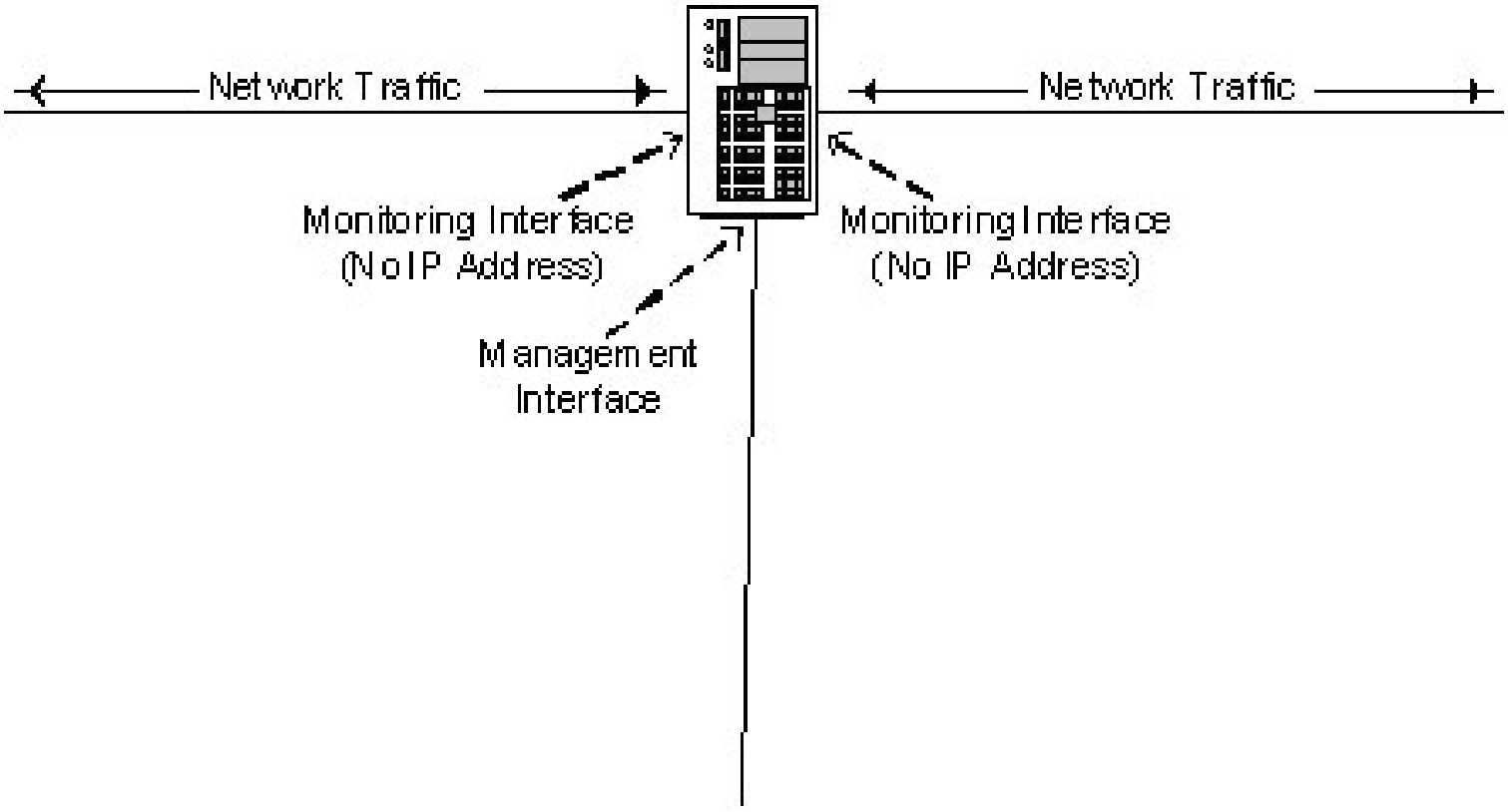
交换环境

通过端口镜像实现

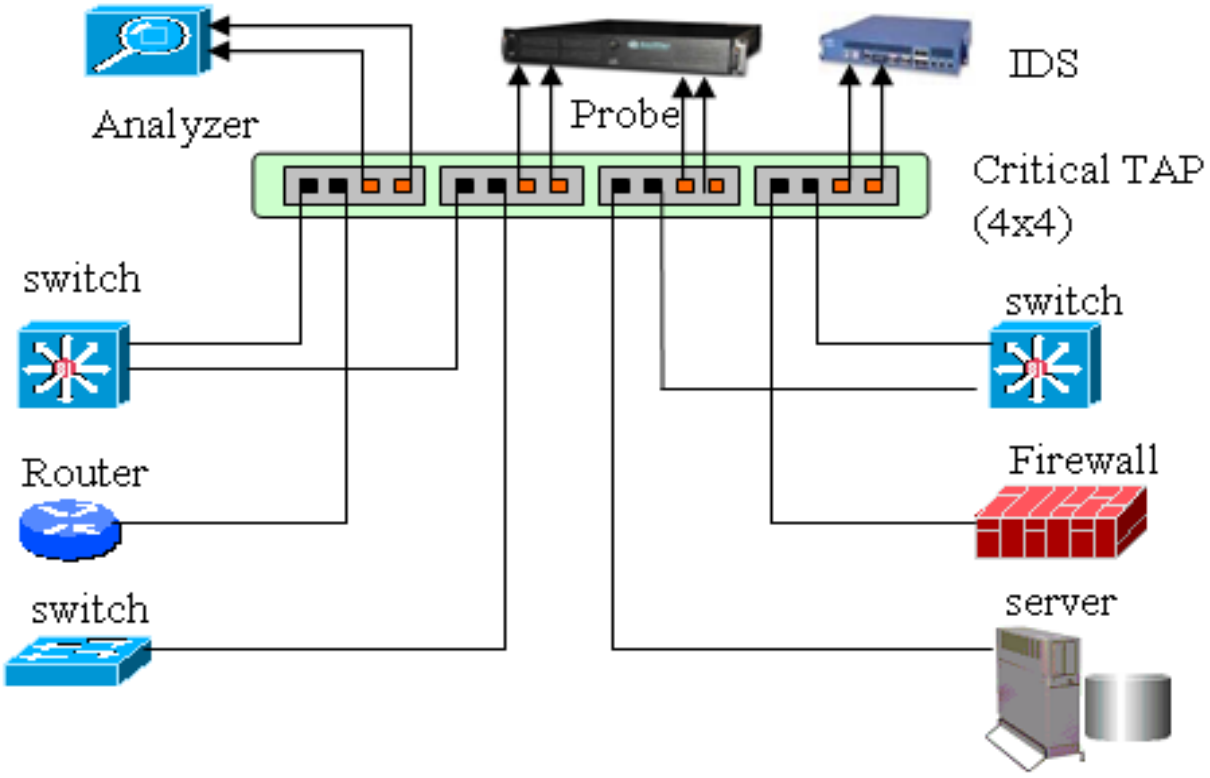
隐蔽模式



In-Line模式


Network Traffic
Network Traffic
Monitoring Interface
(No IP Address)
Monitoring Interface
(No IP Address)
Management
Interface

TAP模式


Analyzer
Probe
IDS
Critical TAP
(4x4)
switch
switch
Router
Firewall
switch
server

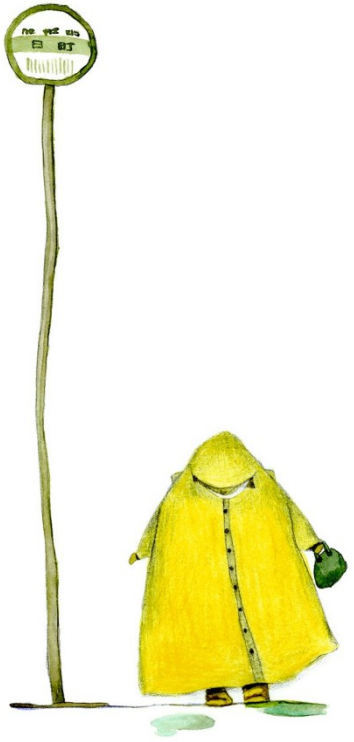
IDS应用指南

- IDS的部署
- 评价IDS的性能和功能指标
- 典型IDS产品介绍

评价IDS的性能指标

- Porras等给出了评价入侵检测系统性能的三个因素：
  - 准确性（Accuracy）
  - 处理性能（Performance）
  - 完备性（Completeness）

- Debar等增加了两个性能评价测度
  - 容错性（Fault Tolerance）
  - 及时性（Timeliness）



评价IDS的性能指标

测试性能

- HIDS：漏报率、误报率、资源占用率；
- NIDS：漏报率、误报率、特征库强度；
- 模拟背景流量

  --硬件：SmartBits，人为构造一定大小的数据报，从64bytes到1518bytes，衡量不同pps（packets per second）下IDS对攻击的检测情况。

  --软件：tcpdump & tcpreplay，对流量的回放。

评价IDS功能指标

结构：

- ✓系统结构
- ✓管理模式
- ✓通讯安全

探测引擎：

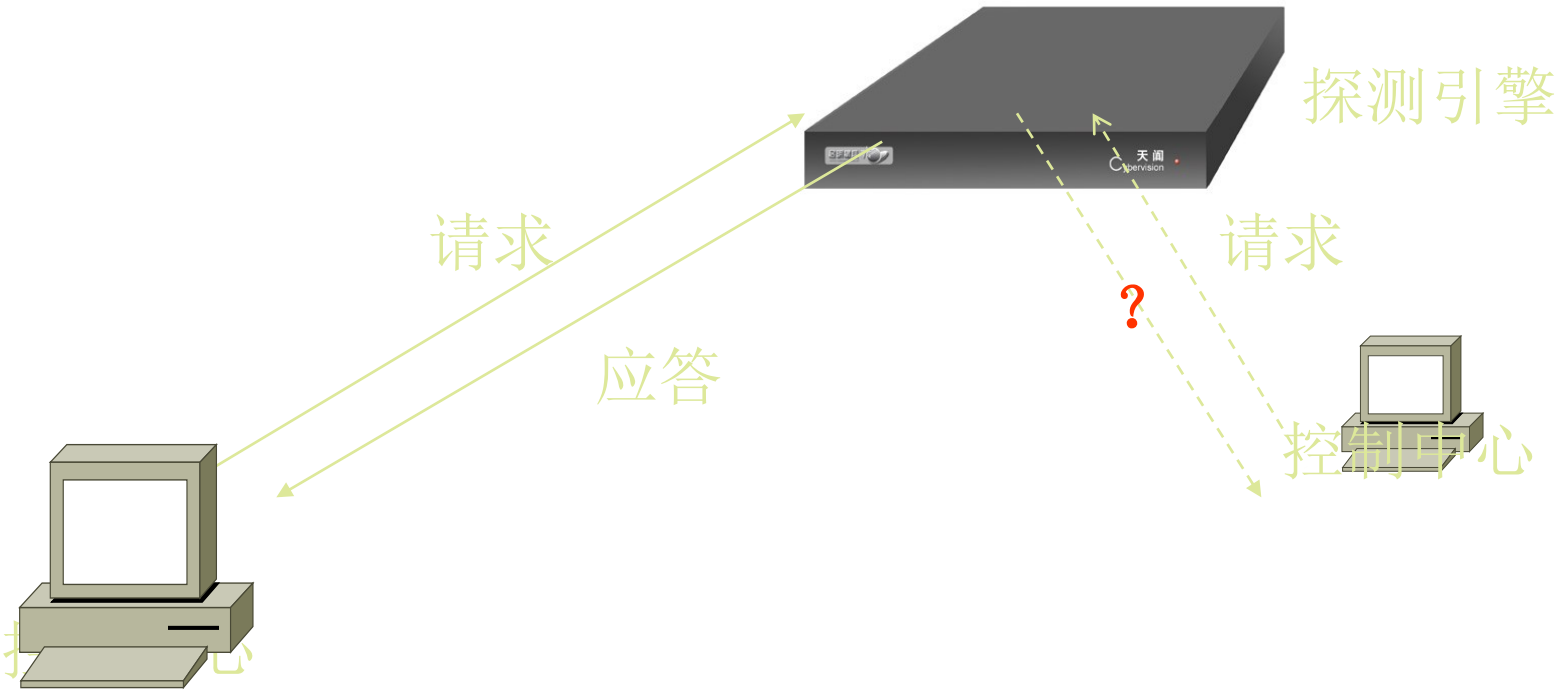
- ✓检测能力
- ✓事件响应
- ✓自身安全

控制台：

- ✓策略灵活性
- ✓自定义事件
- ✓事件库更新
- ✓易用性
- ✓综合分析
- ✓事件数量

评价IDS的功能指标

通讯安全



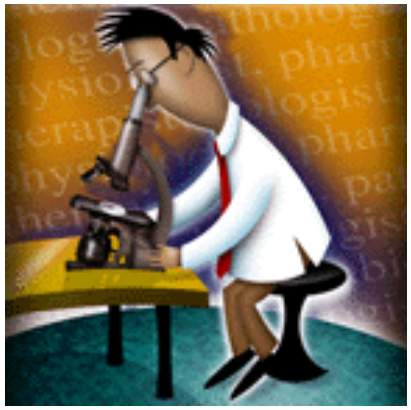
传输数据是明文还是密文？

IDS的功能指标

响应方式

被动

- 屏幕告警
- 邮件告警
- 手机告警
- 声音告警
- SNMP告警
- 自定义告警



主动

-入侵检测系统自身阻断
-与防火墙联动
-与Scanner联动
-与防病毒产品联动
-与交换机联动

IDS功能指标

自身安全

- ✓自身操作系统的安全
- ✓自身程序的安全
- ✓地址透明度
- ✓抗打击能力

IDS的功能指标

日志分析

IDS应用指南

- IDS的部署
- 评价IDS的指标
- 典型IDS产品

典型IDS产品介绍—国外

- ISS RealSecure(WinNT)
- NFR Security NID-100/200
- NAI CyberCop Intrusion Protection
- Cisco NetRanger(Unix)
- snort

典型IDS产品介绍—国内


启明星辰天阗


金诺KIDS


中联绿盟冰之眼

东软Neteye

入侵检测系统

- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

入侵检测系统发展趋势

学术界

- 智能化检测算法
- 数据挖掘

产业界

- 应用层入侵检测的研究
- 入侵检测系统的标准化工作
- 宽带高速网络的实时入侵检测系统
- 入侵追踪、起诉的支持
- IDS→IPS→IMS

总结

- ✓ 安全概述
- ✓ 入侵检测概述
- ✓ 入侵检测系统的分类及特点
- ✓ 入侵检测系统结构
- ✓ 入侵检测系统的关键技术
- ✓ 入侵检测系统的外围支撑技术
- ✓ 入侵检测系统应用指南
- ✓ 入侵检测系统的发展趋势

Thank You!