入侵检测系统

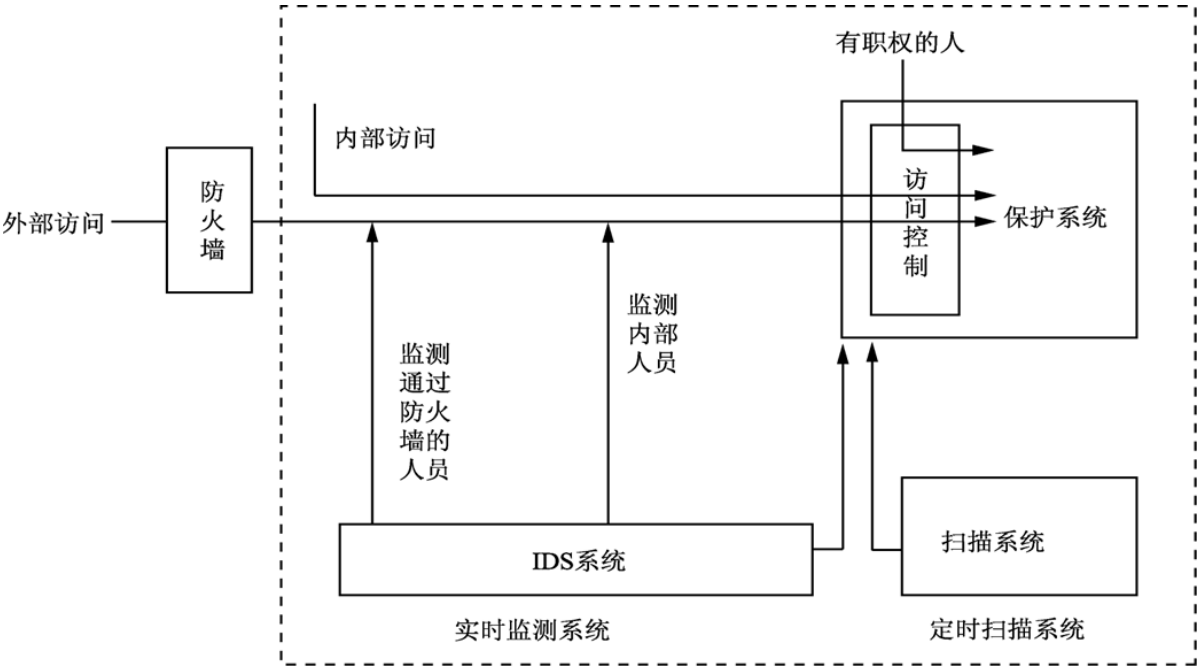
产生的原因

- 防火墙所提供的服务方式是或都拒绝或都通过，不能检查出经过它的合法流量中是否包含着恶意的入侵代码
- 防火墙不能安全过滤应用层的非法攻击，如unicode攻击
- 入侵者易于找到防火墙的漏洞，绕过防火墙进行攻击
- 防火墙对不通过它的连接无能为力，如内网攻击等
- 防火墙采用静态安全策略技术，因此自身无法动态防御新的非法攻击

相关概念

入侵检测（Intrusion Detection）：通过从计算机网络或系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到入侵的迹象的一种安全技术；

入侵检测系统（Intrusion Detection System）：作为防火墙的合理补充，入侵检测技术能够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、攻击识别和响应），提高了信息安全基础结构的完整性，是安全防御体系的一个重要组成部分。



P2DR

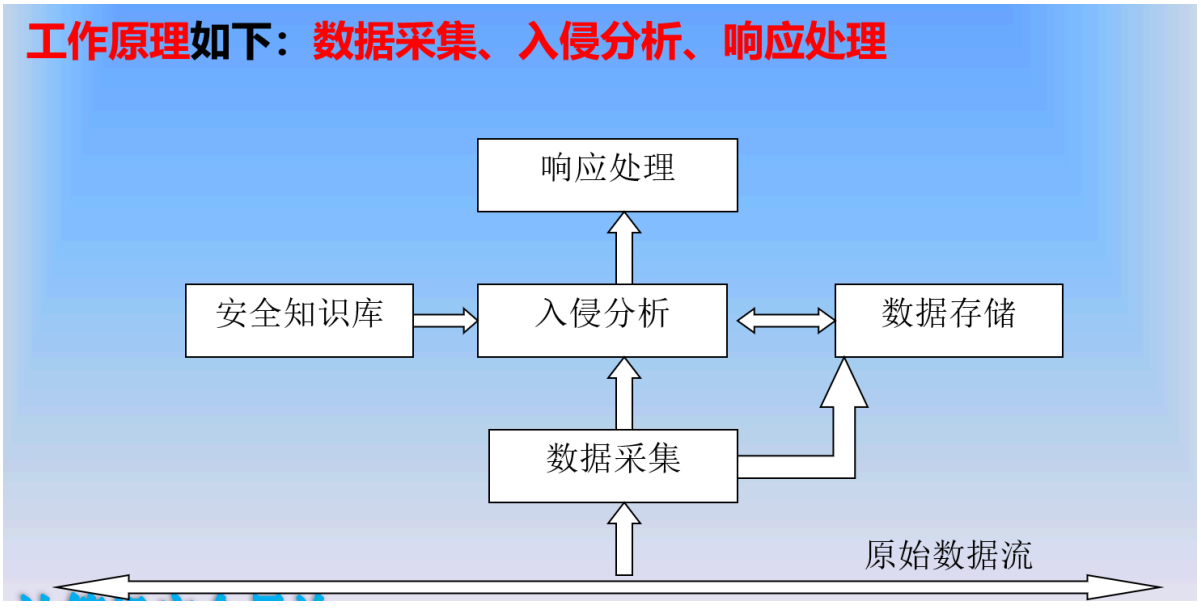
P2DR是Policy(安全策略)、Protection(防护)、Detection(检测)、Response(响应)的缩写。入侵检测技术就是实现P2DR模型中“Detection”部分的主要技术手段。

入侵检测的功能

入侵检测的主要功能包括以下几个方面：

- 对网络流量的跟踪与分析功能
- 对已知攻击特征的识别功能
- 对异常行为的分析、统计与响应功能
- 特征库的在线和离线升级功能
- 数据文件的完整性检查功能
- 自定义的响应功能
- 系统漏洞的预报警功能
- IDS探测器集中管理功能

入侵检测工作原理



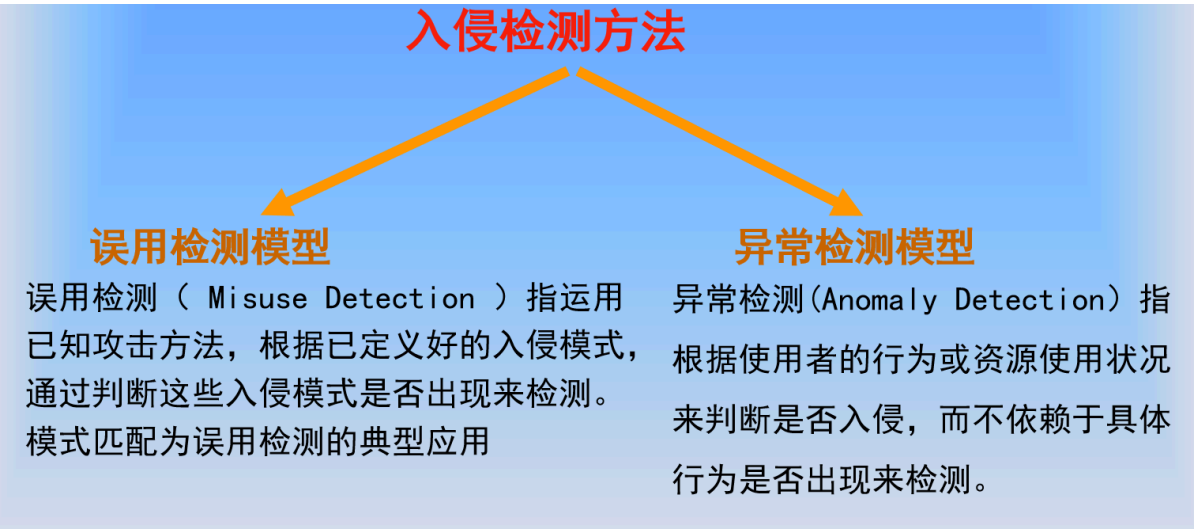
- 数据采集：入侵检测的第一步是数据采集，采集内容包括系统、网络、数据及用户活动的状态和行为。需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息。入侵检测的效果很大程度上依赖于收集信息的可靠性和正确性。要保证入侵检测系统软件本身的完整性，防止被篡改而收集到错误的信息。
- 入侵分析：模式匹配、统计分析和完整性分析
- 响应处理：简单报警、切断连接、封锁用户、改变文件属性、回击攻击者

性能参数

- 误报(false positive)：如果系统错误地将异常活动定义为入侵
- 漏报(false negative)：如果系统未能检测出真正的入侵行为

入侵检测系统分类（重点）

对比项	HIDS	NIDS
部署成本与部署风险	高	低
自身安全性	弱	强
实时性	强	强
主机OS依赖性	高	无
是否影响业务系统的性能	高	无
误报率	低	低
监视系统行为	强	弱
监视网络行为	无	强



对比项	误用检测	异常检测
检测准确性	高	低
误报率	低	高
未知攻击检测能力	弱	强
系统相关性	高	无
新攻击方法检测能力	无	具有

入侵检测技术

蜜罐（了解）

- 定义：一种伪装成真实的目标系统诱骗攻击者攻击或损害的网络安全工具
- 目标：蜜罐的主要目标是容忍攻击者入侵，记录并学习攻击者的攻击工具手段动机目的等行为信息，尤其是未知攻击行为信息，从而调整网络安全策略，提高系统安全性能。同时蜜罐还具有转移攻击者注意力，消耗其攻击资源意志，间接保护真实目标系统的作用

入侵检测工作的特点

事前警告 、事中防护 、事后取证

入侵检测产品

Snort

- Snort是基于C语言的开放源代码的入侵检测系统，有数据包嗅探，数据包分析，数据包检测，响应处理等多种功能，每个模块实现不同的功能，各模块都是用插件的方式和Snort相结合，功能扩展方便。
- **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。我们可以让snort分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。
- Snort工作过程：

①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；

②然后将捕获的数据包送到包解码器进行解码；

③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；

④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。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。

⑤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。