入侵检测技术剖析 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c101_251020.htm CNNIC发布的《中国互联网络发展状况统计报告》显示，中国现已有几千万上网用户。因此，越来越多的公司将其核心业务向互联网转移、服务成为当前IT业另一个生长点，但网络安全作为一个无法回避的问题呈现在人们面前。随着计算机网络知识的普及，攻击者越来越多，知识日趋成熟，攻击工具与手法日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要，网络 的防卫必须采用一种纵深的、多样的手段。网络环境也变得越来越复杂，各式各样的复杂的设备，需要不断升级、补漏的系统使得网络管理员的工作不断加重，不经意的疏忽便有可能造成安全的重大隐患。于是，入侵检测系统成为了安全市场上新的热点，不仅愈来愈多的受到人们的关注，而且已经开始在各种不同的环境中发挥其关键作用。 入侵检测系统（IDS） 由于入侵检测系统的市场在近几年中飞速发展，许多公司投入到这一领域上来。Internet Security System（ISS）、思科、赛门铁克等公司都推出了自己的产品。 系统组成 IETF将一个入侵检测系统分为四个组件：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）。 事件产生器的目的是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。事件分析器分析得到的数据，并产生分析结果。响应单元则是对分析结果作出作出反应的功能单元，它可以作出切断连接、改变文件属性等

强烈反应，也可以只是简单的报警。事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。 系统分类 根据检测对象的不同，入侵检测系统可分为主机型和网络型。 基于主机的监测。主机型入侵检测系统就是以系统日志、应用程序日志等作为数据源，当然也可以通过其他手段（如监督系统调用）从所在的主机收集信息进行分析。主机型入侵检测系统保护的一般是所在的系统。这种系统经常运行在被监测的系统之上，用以监测系统上正在运行的进程是否合法。最近出现的一种ID（intrusion detection）：位于操作系统的内核之中并监测系统的最底层行为。所有这些系统最近已经可以被用于多种平台。 网络型入侵检测。它的数据源是网络上的数据包。往往将一台机子的网卡设于混杂模式（promisc mode）,对所有本网段内的数据包并进行信息收集，并进行判断。一般网络型入侵检测系统担负着保护整个网段的任务。 系统通信协议 IDS系统内部各组件之间需要通信，不同厂商的IDS系统之间也需要通信。因此，有必要定义统一的协议。目前，IETF目前有一个专门的小组Intrusion Detection Working Group （idwg）负责定义这种通信格式，称作Intrusion Detection Exchange Format，但还没有统一的标准。 以下是设计通信协议时应考虑的问题：1、系统与控制系统之间传输的信息是非常重要的信息，因此必须要保持数据的真实性和完整性。必须有一定的机制进行通信双方的身份验证和保密传输（同时防止主动和被动攻击）。2. 通信的双方均有可能因异常情况而导致通信中断，IDS系统必须有额外措施保证系统正常工作。 入侵检测技术 对各种事件进行分析，从中发现违反安全策略的行

为是入侵检测系统的核心功能。从技术上，入侵检测分为两类：一种基于标志（signature-based），另一种基于异常情况（anomaly-based）。 对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似杀毒软件。 而基于异常的检测技术则是先定义一组系统“ 正常 ”情况的数值，如CPU利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出），然后将系统运行时的数值与所定义的“ 正常 ”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“ 正常 ”情况。 两种检测技术的方法、所得出的结论有非常大的差异。基于异常的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确的报告出攻击类型，但是对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以（至少在理论上可以）判别更广范、甚至未发觉的攻击。 