IDS及其Linux下的实现(1) 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_IDS_E5_8F_8A_E5_85_B6L_c101_251038.htm 1、入侵检测系统简介 当越来越多的公司将其核心业务向互联网转移的时候，网络安全作为一个无法回避的问题呈现在人们面前。传统上，公司一般采用防火墙作为安全的第一道防线。而随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，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。与此同时，当今的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。在这种环境下，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。 本文中的"入侵"（Intrusion）是个广义的概念，不仅包括被发起攻击的人（如恶意的黑客）取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问（Denial of Service）等对计算机系统造成危害的行为。 入侵检测（Intrusion Detection），顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中得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被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（Intrusion Detection sys tem,简称IDS）。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。

一个合格的入侵检测系统能大大的简化管理员的工作，保证网络安全的运行。 具体说来，入侵检测系统的主要功能有：A) 监测并分析用户和系统的活动； B) 核查系统配置和漏洞； C) 评估系统关键资源和数据文件的完整性； D) 识别已知的攻击行为； E) 统计分析异常行为； F) 操作系统日志管理，并识别违反安全策略的用户活动。 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。ISS、axent、NFR、cisco等公司都推出了自己相应的产品（国内目前还没有成熟的产品出现）。但就目前而言，入侵检测系统还缺乏相应的标准。目前，试图对IDS进行标准化的工作有两个组织：IETF的Intrusion Detection Working Group (idwg)和Common Intrusion Detection Framework (CIDF)，但进展非常缓慢，尚没有被广泛接收的标准出台。 2、入侵检测系统模型 Common Intrusion Detection Framework (CIDF)（http://www.gidos.org/）阐述了一个入侵检测系统（IDS）的通用模型。它将一个入侵检测系统分为以下组件： 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将IDS需要分析的数据统称为事件（event）,它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。 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

。 在这个模型中，前三者以程序的形式出现，而最后一个则往往是文件或数据流的形式。 在其他文章中，经常用数据采集部分、分析部分和控制台部分来分别代替事件产生器、事件分析器和响应单元这些术语。且常用日志来简单的指代事件数据库。如不特别指明，本文中两套术语意义相同。 3、IDS分类 一般来说，入侵检测系统可分为主机型和网络型。 主机型入侵检测系统往往以系统日志、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。 网络型入侵检测系统的数据源则是网络上的数据包。往往将一台机子的网卡设于混杂模式（promisc mode）,监听所有本网段内的数据包并进行判断。一般网络型入侵检测系统担负着保护整个网段的任务。 不难看出，网络型IDS的优点主要是简便：一个网段上只需安装一个或几个这样的系统，便可以监测整个网段的情况。且由于往往分出单独的计算机做这种应用，不会给运行关键业务的主机带来负载上的增加。但由于现在网络的日趋复杂和高速网络的普及，这种结构正受到越来越大的挑战。一个典型的例子便是交换式以太网。 而尽管主机型IDS的缺点显而易见：必须为不同平台开发不同的程序、增加系统负荷、所需安装数量众多等，但是内在结构却没有任何束缚，同时可以利用操作系统本身提供的功能、并结合异常分析，更准确的报告攻击行为。《Next Generation Intrusion Detection in High-Speed Networks》对此做了描述，感兴趣的读者可参看。 