入侵检测系统分析及其在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_ti2020/144/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c103_144488.htm 一、入侵检测系统分析 1.1 什么是入侵检测系统 所谓入侵，是指任何试图危及计算机资源的完整性、机密性或可用性的行为。而入侵检测，顾名思义，便是对入侵行为的发觉。它通过从计算机网络或系统中的若干 关键点收集信息，并对这些信息进行分析，从而发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（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简化管理员的工作，保证网络安全地运行。 1.2 入侵检测系统的分类 按检测所使用数据源的不同可以将IDS分为基于主机的IDS和基于网络的IDS。 基于主机的IDS使用各种审计日志信息（如主机日志、路由器日志、防火墙日志等）作为检测的数据源。通常，基于主机的IDS可监测系统、事件和操作系统下的安全记录以及系统记录。当有文件发生变化时，IDS将新的记录条目与攻击标记相比较，看它们是否匹配。如果匹配，系统就会向管理员报警，以采取措施。 基于网络的入侵检测系统使用原始网络分组数据包作为数据源。基于网络的IDS通常利用一个运行在混杂模式下的网络适配器来实时监视并分析通过网络的所有通信业务。一旦检测到了攻击行为，IDS的响应模块就会对攻击采取相应的反应，如通知管理员、中断连接、终止用户等。 1.3 入侵检测的检测方法 入侵检测技术通过对

入侵行为的过程与特征的研究，使安全系统对入侵事件和入侵过程能做出实时响应，从检测方法上分为两种：误用入侵检测和异常入侵检测。 在误用入侵检测中，假定所有入侵行为和手段都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。误用入侵检测的关键是如何表达入侵的模式，把真正的入侵与正常行为区分开来。其优点是误报少，局限性是它只能发现已知的攻击，对未知的攻击无能为力。 在异常入侵检测中，假定所有入侵行为都是与正常行为不同的，这样，如果建立系统正常行为的轨迹，那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。比如，通过流量统计分析将异常时间的异常网络流量视为可疑。异常入侵检测的局限是并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。 对比这两种检测方法可以发现，异常检测难于定量分析，这种检测方式有一种固有的不确定性。与此不同，误用检测会遵循定义好的模式，能通过对审计记录信息做模式匹配来检测，但仅可检测已知的入侵方式。所以这两类检测机制都不完美。就具体的检测方法来说，现在已经有了很多入侵检测的方法，但任何一种方法都有它的局限性，都不能解决所有问题。因而对于入侵检测方法的研究仍然是当前入侵检测研究的一个重点。