入侵检测技术：网络安全的第三种力量 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/166/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c101_166584.htm 网络安全技术发展到今天，除了防火墙和杀毒系统的防护，入侵检测技术也成为抵御黑客攻击的有效方式。尽管入侵检测技术还在不断完善发展之中，但是入侵检测产品的市场已经越来越大，真正掀起了网络安全的第三股热潮。 入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。 入侵检测被认为是防火墙之后的第二道安全闸门。IDS主要用来监视和分析用户及系统的活动，可以识别反映已知进攻的活动模式并向相关人士报警。对异常行为模式，IDS要以报表的形式进行统计分析。产品提供的功能还要评估重要系统和数据文件的完整性。 一个成功的入侵检测系统，不仅可使系统管理员时刻了解网络系统，还能给网络安全策略的制订提供依据。它应该管理配置简单，使非专业人员非常容易地获得网络安全。入侵检测的规模还应根据网络规模、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。IDS分类入侵检测通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程作出实时响应。 IDS产品分类 目前市场上的IDS产品从技术上看，基本可分为两大类:基于网络的产品和基于主机的产品。混合的入侵检测系统可以弥补一些基于网络与基于主机的片面性缺陷。此外，文件的完整性检查工具也可看做是一类入侵

检测产品。 基于网络的入侵检测产品放置在比较重要的网段内，对每一个数据包或可疑的数据包进行特征分析。商品化的产品包括:国外的ISS RealSecure Network Sensor、Cisco Secure IDS、CA e-Trust IDS、Axent的NetProwler，以及国内的金诺网安KIDS、北方计算中心NISDetector、启明星辰天阗黑客入侵检测与预警系统和中科网威“ 天眼 ”网络入侵侦测系统等。基于主机的入侵检测产品主要对主机的网络实时连接以及系统审计日志进行智能分析和判断。基于主机的入侵检测系统有:ISS RealSecure OS Sensor、Emerald expert-BSM、金诺网安KIDS等。 混合式入侵检测系统综合了基于网络和主机的两种结构特点，既可发现网络中的攻击信息，也可从系统日志中发现异常情况。商品化产品有:ISS Server Sensor、NAI CyberCop Monitor、金诺网安KIDS等。 文件完整性检查工具通过检查文件的数字摘要与其他一些属性，判断文件是否被修改，从而检测出可能的入侵。这个领域的产品有半开放源代码的Tripwire。IDS产品形式 绝大多数的入侵检测产品都以纯软件的形式出售，但为了达到性能最佳，往往需要对安装的系统进行优化调整。这样，把产品做成“ 黑盒子 ”的形式可以达到目的，如Cisco公司的Secure IDS和金诺网安KIDS。随着入侵检测产品日益在规模庞大的企业中应用，分布式技术也开始融入到入侵检测产品中来。同时，集中管理多个传感器的中央控制台也在不断地完善。目前，绝大多数的入侵检测产品，尤其是企业级产品都具有分布式结构。 产品重要指标 在入侵检测产品中，有几个重要的性能指标值得重视，比如网络入侵检测系统负载能力，网络入侵检测系统是非常消耗资源的，但很少有厂商公布自己的pps (packet per second)

参数。 网络入侵检测系统可支持的网络类型也是应该考虑的。目前，国内的入侵检测厂商还只是支持以太网和快速以太网。 网络入侵检测系统运行在什么操作系统平台上，网络入侵检测系统的运行平台一般以Unix为主，也有少数使用专有设备或基于Windows平台的入侵检测系统。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com