入侵检测(IDS)及网络安全发展趋势思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c101_644205.htm 作为对防火墙及其有益的补充，IDS(入侵检测系统)能够帮助网络系统快速发现攻击的发生，它扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。 一、入侵检测系统(IDS)诠释 IDS是一种网络安全系统，当有敌人或者恶意用户试图通过Internet进入网络甚至计算机系统时，IDS能够检测出来，并进行报警，通知网络该采取措施进行响应。 在本质上，入侵检测系统是一种典型的“窥探设备”。它不跨接多个物理网段(通常只有一个监听端口)，无须转发任何流量，而只需要在网络上被动地、无声息地收集它所关心的报文即可。 目前，IDS分析及检测入侵阶段一般通过以下几种技术手段进行分析：特征库匹配、基于统计的分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。 二、IDS存在的问题 1、误/漏报率高 IDS常用的检测方法有特征检测、异常检测、状态检测、协议分析等。而这些检测方式都存在缺陷。比如异常检测通常采用统计方法来进行检测，而统计方法中的阈值难以有效确定，太小的值会产生大量的误报，太大的值又会产生大量的漏报。而在协议分析的检测方式中，一般的IDS只简单地处理了常用的如HTTP、FTP、SMTP等，其余大量的协议报文完全可能造成IDS漏报，如果考虑支持尽量多的协议类型分析，网络的成本将无法承受。 2、没有主动防御能力 IDS技术采用了一种预设置式、特征分析式工作原理，所

以检测规则的更新总是落后于攻击手段的更新。 3、缺乏准确定位和处理机制 IDS仅能识别IP地址，无法定位IP地址，不能识别数据来源。IDS系统在发现攻击事件的时候，只能关闭网络出口和服务器等少数端口，但这样关闭同时会影响其他正常用户的使用。因而其缺乏更有效的响应处理机制。 4、性能普遍不足本文来源:百考试题网 现在市场上的IDS产品大多采用的是特征检测技术，这种IDS产品已不能适应交换技术和高带宽环境的发展，在大流量冲击、多IP分片情况下都可能造成IDS的瘫痪或丢包，形成DoS攻击。 思科证书的意义：技术经验的证明 我是主考官：给一位应届毕业生的回信 思科认证考试四个考点难点问题 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