硬件入侵检测系统完全导购(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__E7_A1_AC_E4_BB_B6_E5_85_A5_E4_c101_251043.htm 网络入侵是威胁计算机或网络的安全机制（包括机密性、完整性、可用性）的行为。入侵可能是来自互联网的攻击者对系统的非法访问，也可能是系统的授权用户对未授权的内容进行的非法访问。入侵检测就是对发生在计算机系统或者网络上的事件进行监视、分析是否出现入侵的过程。入侵检测系统（英文称IDS：Intrusion Detection System）是自动进行入侵检测的监视和分析过程的硬件或软件产品。入侵监测系统处于防火墙之后对网络活动进行实时监测。许多情况下，由于可以记录和禁止网络活动，所以入侵监测系统是防火墙的延续。防火墙看起来好像可以满足系统管理员的一切需求。然而，随着基于内部人员的攻击行为和产品自身问题的增多，IDS由于能够在防火墙内部监测非法的活动正变得越来越必要。新的技术同样给防火墙带来了严重的威胁，这些破坏行为也是防火墙无法抵御的。IDS已经成为企业网络安全防护系统的三大重要组成部分之一。 一、入侵检测系统基础原理 1、入侵检测系统的产品分类 根据采集数据源的不同，IDS可分为主机型入侵检测系统（Host-based IDS，简称HIDS）和网络型入侵检测系统（Network-based IDS，简称NIDS）。HIDS从主机/服务器上采集数据，包括操作系统日志、系统进程、文件访问和注册表访问等信息。HIDS的检测引擎被称为主机代理，HIDS的主机代理安装在所保护的主机/服务器上，不同的操作系统平台需要不同的主机代理。NIDS直接从网络中采集原始的数据包

。NIDS的检测引擎被称为网络引擎。NIDS的网络引擎放置在需要保护的网段内，不占用网络资源，可以保护整个网段。主机型入侵检测系统的特点：主机型入侵检测系统通常情况下比网络型入侵检测系统误报率要低，因为检测在主机上运行的命令序列比检测网络流更简单，系统的复杂性也少得多。主机型入侵检测系统安装在我们需要保护的设备上，这会降低应用系统的效率。主机型入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必需重新配置，这将会给运行中的业务系统带来不可预见的性能影响。 网络型入侵检测系统的特点：网络型入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件，从而不会影响这些机器的CPU、I/O与磁盘等资源的使用，不会影响业务系统的性能。网络型入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限。而安装多台网络型入侵检测系统的传感器会使布署整个系统的成本大大增加。 2、入侵检测的主要技术 ●模式匹配 模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，来发现违背安全策略的入侵行为。该过程可以很简单，也可以很复杂。一种进攻模式可以利用一个过程或一个输出来表示。这种检测方法只需收集相关的数据集合就能进行判断，能减少系统占用，并且技术已相当成熟，检测准确率和效率也相当高。但是，该技术需要不断进行升级以对付不断出现的攻击手法，并且不能检测未知攻击手段。 ●异常检测 异常检测首先给系统对象（用户、文件、目录和设备等）创建一个统计描述，包括统计正常使

用时的测量属性，如访问次数、操作失败次数和延时等。测量属性的平均值被用来与网络、系统的行为进行比较，当观察值在正常值范围之外时，IDS就会判断有入侵发生。异常检测的优点是可以检测到未知入侵和复杂的入侵，缺点是误报、漏报率高。 ●协议分析 协议分析是在传统模式匹配技术基础之上发展起来的一种新的入侵检测技术。它充分利用了网络协议的高度有序性，并结合了高速数据包捕捉、协议分析和命令解析，来快速检测某个攻击特征是否存在，这种技术正逐渐进入成熟应用阶段。协议分析大大减少了计算量，即使在高负载的高速网络上，也能逐个分析所有的数据包。 3、入侵检测技术的对比 ●模式匹配技术：预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。对系统资源的消耗较高。 ●异常检测技术：最大优点就是它可以统计用户的网络使用习惯，从而具有较高检测率与可用性。但是它的统计能力也给入侵者以机会通过逐步测试而使入侵事件符合正常操作的统计规律，从而透过入侵检测系统。 ●协议分析技术：充分利用通信协议的已知结构，可以更快更有效地处理信息数据帧和连接。将命令解析技术与协议分析技术相结合，来模拟执行一个命令字符串，可以在通信连接到达操作系统或应用系统之前准确判断该通信是否恶意。对系统资源的极低消耗。 4、入侵检测术语 Alerts（警报） 当一个入侵正在发生或者试图发生时，IDS系统将发布一个alert信息通知系统管理员。如果控制台与IDS系统同在一台机器，alert信息将显示在监视器上，也可能伴随着声音提示。如果是远程控制台，那么alert将通过IDS系统内置方法（通常是加密的）、SNMP（简单网络管理协议，通常不加密）

、email、SMS（短信息）或者以上几种方法的混合方式传递给管理员。 Anomaly（异常） 当有某个事件与一个已知攻击的信号相匹配时，多数IDS都会告警。一个基于anomaly（异常）的IDS会构造一个当时活动的主机或网络的大致轮廓，当有一个在这个轮廓以外的事件发生时，IDS就会告警，例如有人做了以前他没有做过的事情的时候，例如，一个用户突然获取了管理员或根目录的权限。有些IDS厂商将此方法看做启发式功能，但一个启发式的IDS应该在其推理判断方面具有更多的智能。 Attacks（攻击） Attacks可以理解为试图渗透系统或绕过系统的安全策略，以获取信息、修改信息以及破坏目标网络或系统功能的行为。 Enumeration（列举） 经过被动研究和社会工程学的工作后，攻击者就会开始对网络资源进行列举。列举是指攻击者主动探查一个网络以发现其中有什么以及哪些可以被他利用。由于现在的行动不再是被动的，它就有可能被检测出来。当然为了避免被检测到，他们会尽可能地悄悄进行。 Evasion（躲避） Evasion是指发动一次攻击，而又不被IDS成功地检测到。其中的窍门就是让IDS只看到一个方面，而实际攻击的却是另一个目标，所谓明修栈道，暗渡陈仓。Evasion的一种形式是为不同的信息包设置不同的TTL（有效时间）值，这样，经过IDS的信息看起来好像是无害的，而在无害信息位上的TTL比要到达目标主机所需要的TTL要短。一旦经过了IDS并接近目标，无害的部分就会被丢掉，只剩下有害的。 Exploits（漏洞利用） 对于每一个漏洞，都有利用此漏洞进行攻击的机制。为了攻击系统，攻击者编写出漏洞利用代码或脚本。对每个漏洞都会存在利用这个漏洞执行攻击的方式，这个方式就是Exploit。为了攻击系统

，黑客会编写出漏洞利用程序。 False Negatives（漏报） 漏报是指一个攻击事件未被IDS检测到或被分析人员认为是无害的。 False Positives（误报） 误报是指实际无害的事件却被IDS检测为攻击事件。 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