解读IDS入侵检测系统术语 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/460/2021_2022__E8_A7_A3_E8_AF_BBIDS_E5_c98_460945.htm 入侵检测技术07年已经取得了越来越多的应用，很多用户对IDS(入侵检测系统)具体信息并不是十分了解，但随着其快速发展，我们有必要了解IDS，为日后做好准备。与IDS相关的新名词也日新月异，这里按字母顺序罗列了相关的术语，有的可能很普遍了，但是有的却很少见。 警报(Alerts) 警报是IDS向系统操作员发出的有入侵正在发生或者正在尝试的消息。一旦侦测到入侵，IDS会以各种方式向分析员发出警报。如果控制台在本地，IDS警报通常会显示在监视器上。IDS还可以通过声音报警(但在繁忙的IDS上，建议关闭声音)。警报还可以通过厂商的通信手段发送到远程控制台，除此之外，还有利用SNMP协议(安全性有待考虑)、email、SMS/Pager或者这几种方式的组合进行报警。 异常(Anomaly) 大多IDS在检测到与已知攻击特征匹配的事件就会发出警报，而基于异常的IDS会用一段时间建立一个主机或者网络活动的轮廓。在这个轮廓之外的事件会引起IDS警报，也就是说，当有人进行以前从没有过的活动，IDS就会发出警报。比如一个用户突然获得管理员权限(或者root权限)。一些厂商把这种方法称为启发式IDS，但是真正的启发式IDS比这种方法有更高的智能性。 硬件IDS(Appliance ) 现在的IDS做成硬件放到机架上，而不是安装到现有的操作系统中，这样很容易就可以把IDS嵌入网络。这样的IDS产品如CaptIO, Cisco Secure IDS, OpenSnort, Dragon and SecureNetPro。 网络入侵特征数据库(ArachNIDS - Advanced Reference Archive of Current

Heuristics for Network Intrusion Detection Systems) 由白帽子住持Max Vision开发维护的ArachNIDS是一个动态更新的攻击特征数据库，适用于多种基于网络的入侵检测系统。 攻击注册和信息服务(ARIS - Attack Registry &amp. Intelligence Service ) ARIS是SecurityFocus推出的一项安全信息服务，允许用户向SecurityFocus匿名报告网络安全事件。SecurityFocus整理这些数据，并和其它信息综合，形成详细的网络安全统计分析和趋势预测。 攻击(Attacks ) 攻击可以定义为试图渗透系统或者绕过系统安全策略获取信息，更改信息或者中断目标网络或者系统的正常运行的活动。下面是一些IDS可以检测的常见攻击的列表和解释： 拒绝服务攻击(DOS - Denial Of Service attack ) DOS攻击只是使系统无法向其用户提供服务，而不是通过黑客手段渗透系统。拒绝服务攻击的方法从缓冲区溢出到通过洪流耗尽系统资源，不一而足。随着对拒绝服务攻击的认识和防范不断加强，又出现了分布式拒绝服务攻击。 分布式拒绝服务攻击(DDOS - Distributed Denial of Service ) 分布式拒绝服务攻击是一种标准的拒绝服务攻击，通过控制多台分布的远程主机向单一主机发送大量数据，并因此得名。攻Smurf攻击(Smurf ) Smurf攻击是以最初发动这种攻击的程序名Smurf来命名。这种攻击方法通过欺骗方法向“ Smurf放大器 ”的网络发送广播地址的ping，放大器网络向欺骗地址攻击目标系统返回大量的ICMP回复消息，引起目标系统的拒绝服务。 这里有每5分钟更新一次的可用的“ 放大器 ”： http://www.powertech.no/smurf/ (但愿你的网络不在此列…) 特洛伊木马(Trojans ) 特洛伊密码来自于古希腊著名的木马攻击特洛伊城的故事。在计算机术语中最初指的是貌似合法但其

中包含恶意软件的程序。当合法程序执行时，恶意软件在用户毫无察觉的情况下被安装。后来大多数的这类恶意软件都是远程控制工具，特洛伊木马也就专指这类工具，如BackOrifice, SubSeven, NetBus 等。 