Windows2003 2入门IDS构建过程 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_Windows200_c100_460853.htm IDS的技术手段其实并不很神秘，接下来本文会用一种“ 顺藤摸瓜 ”的脉络，给大家介绍一个较简单的IDS入门级构架。从市场分布、入手难易的角度来看，选择NIDS作为范例进行部署，比较地恰当。本文以完全的Windows平台来贯穿整个入侵检测流程，由于篇幅所限，以定性分析角度来陈述。 预备知识 IDS：Intrusion Detection System（入侵检测系统），通过收集网络系统信息来进行入侵检测分析的软件与硬件的智能组合。 对IDS进行标准化工作的两个组织：作为国际互联网标准的制定者IETF的Intrusion Detection working Group（IDWG，入侵检测工作组）和Common Intrusion Detection Framework（CIDF，通用入侵检测框架）。 IDS分类：Network IDS（基于网络）、Host-based IDS（基于主机）、Hybrid IDS（混合式）、Consoles IDS（控制台）、File Integrity Checkers（文件完整性检查器）、Honeypots（蜜罐）。事件产生系统 根据CIDF阐述入侵检测系统（IDS）的通用模型思想，具备所有要素、最简单的入侵检测组件如图所示。根据CIDF规范，将IDS需要分析的数据统称为Event（事件），Event既可能是网络中的Data Packets（数据包），也可能是从System Log等其他方式得到的Information（信息）。 没有数据流进（或数据被采集），IDS就是无根之木，完全无用武之地。 作为IDS的基层组织，事件产生系统大可施展拳脚，它收集被定义的所有事件，然后一股脑地传到其它组件里。在Windows环境下，目前

比较基本的做法是使用Winpcap和WinDump. 大家知道，对于事件产生和事件分析系统来说，眼下流行采用Linux和Unix平台的软件和程序；其实在Windows平台中，也有类似Libpcap（是Unix或Linux从内核捕获网络数据包的必备软件）的工具即Winpcap. Winpcap是一套免费的， 基于Windows的网络接口API，把网卡设置为“ 混杂 ”模式，然后循环处理网络捕获的数据包。其技术实现简单，可移植性强，与网卡无关，但效率不高，适合在100 Mbps以下的网络 相应的基于Windows的网络嗅探工具是WinDump（是Linux/Unix平台的Tcpdump在Windows上的移植版），这个软件必须基于Winpcap接口（这里有人形象地称Winpcap为：数据嗅探驱动程序）。使用WinDump，它能把匹配规则的数据包的包头给显示出来。你能使用这个工具去查找网络问题或者去监视网络上的状况，可以在一定程度上有效监控来自网络上的安全和不安全的行为。 这两个软件在网上都可以免费地找到，读者还可以查看相关软件使用教程。 下面大略介绍一下建立事件探测及采集的步骤 1、装配软件和硬件系统。根据网络繁忙程度决定是否采用普通兼容机或性能较高的专用服务器；安装NT核心的Windows操作系统，推荐使用Windows Server 2003企业版，如果条件不满足也可使用Windows 2000 Advanced Server.分区格式建议为NTFS格式。 2、服务器的空间划分要合理有效，执行程序的安装、数据日志的存储，两者空间最好分别放置在不同分区。 3、Winpcap的简单实现。首先安装它的驱动程序，可以到它的主页或镜像站点下载WinPcap auto-installer（Driver DLLs），直接安装。 注：如果用Winpcap做开发，还需要下载 Developers pack. WinPcap 包括三个模块：第一个

模块NPF（Netgroup Packet Filter），是一个VxD（虚拟设备驱动程序）文件。其功能是过滤数据包，并把这些包完好无损地传给用户态模块。第二个模块packet.dll为Win32平台提供了一个公共接口，架构在packet.dll之上，提供了更方便、更直接的编程方法。第三个模块 Wpcap.dll不依赖于任何操作系统，是底层的动态链接库，提供了高层、抽象的函数。具体使用说明在各大网站上都有涉及，如何更好利用Winpcap需要较强的C环境编程能力。 4、WinDump的创建。安装后，在Windows命令提示符模式下运行，用户自己可以查看网络状态，恕不赘述。 如果没有软件兼容性问题、安装和配置正确的话，事件探测及采集已能实现。 