息来实现对用户和系统活动的监控。获取网络数据的方法一般是“抓包”，即将数据流中的所有包都抓下来进行分析，这就对入侵检测系统的效率提出了更高的要求。如果入侵检测系统不能实时地截获数据包并对它们进行分析，那么就会出现漏包或网络阻塞的现象。如果是前一种情况，系统的漏报就会很多；如果是后一种情况，就会影响到入侵检测系统所在主机或网络的数据流速，使得入侵检测系统成为整个系统的瓶颈，这显然是不愿意看到的结果。因此，入侵检测系统不仅要能控制、分析用户和系统的活动，还要使这些操作足够快。

2. 发现入侵企图或异常现象

发现入侵企图或异常现象是入侵检测系统的核心功能，主要包括两方面：一方面是入侵检测系统对进出网络或主机的数据流进行监控，看是否存在对系统的入侵行为；另一方面是评估系统关键资源和数据文件的完整性，看系统是否已经遭受了入侵。前者的作用是在入侵行为发生时及时发现，从而避免系统再次遭受攻击；后者的作用是对攻击者进行追踪，对攻击行为进行取证。

对于网络数据流的监控，可以使用异常检测的方法，也可以使用误用检测的方法。目前有很多新技术被提出来，但多数都还在理论研究阶段，现在的入侵检测产品使用的还主要是模式匹配技术。检测技术的好坏，直接关系到系统能否精确到检测出攻击，因此，对于这方面的研究是入侵检测系统研究领域的主要工作。

3. 记录、报警和响应

入侵检测系统在检测到攻击后，应该采取相应的措施来阻止攻击或响应攻击。作为一种主动防御策略，它必然应该具备此功能。入侵检测系统首先应该记录攻击的基本情况，其次应该能够及时发出报警。合格的入侵检测系统，不仅应该能把相关数据记录在文件中或数据库中，还应该提供报表打印功能。必要时，系统还应该采取响应行为，如拒绝接收所有来自某台计算机的数据、追踪入侵行为等。实现与防火墙等安全部件的响应互动，也是入侵检测系统需要研究和完善的功能之一。

作为一个合格的入侵检测系统，除了具有以上基本功能外，还可以包括其他一些功能，如审计系统的配置和弱点、评估关键系统及数据文件的完整性等。另外，入侵检测系统应该为管理员和用户提供友好、易用的界面，方便管理员设置用户权限、管理数据库、手工设置和修改规则、处理报警和浏览、打印数据等。

三、入侵检测系统的工作原理

在安全体系中，入侵检测系统是唯一一个通过数据和行为模式判断其是否有效的系统。防火墙就像一道门，它可以组织一类人群的进入，但无法只阻止同一类人群中的破坏分子，也不能阻止内部的破坏分子；访问控制系统可以不让低级权限的人做越权工作，但无法保证高级权限的人做破坏工作，也无法保证低级权限的人通过非法行为获得高级权限。

如图 5-9 所示，入侵检测系统在网络连接过程中通过实时监测网络中的各种数据，并与自己的入侵规则库进行匹配判断，一旦发生入侵迹象立即响应和报警，从而完成整个实时监测。入侵检测系统通过安全审计将历史事件一一记录下来，作为证据和为实施数据恢复做准备。如图 5-10 所示为通用网络入侵监测系统模型(NIDS)，主要由以下几个部分组成。

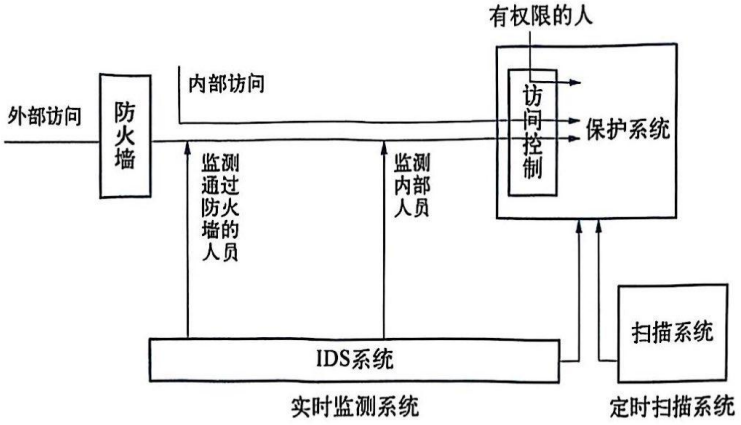

图 5-9 实时监测系统工作原理

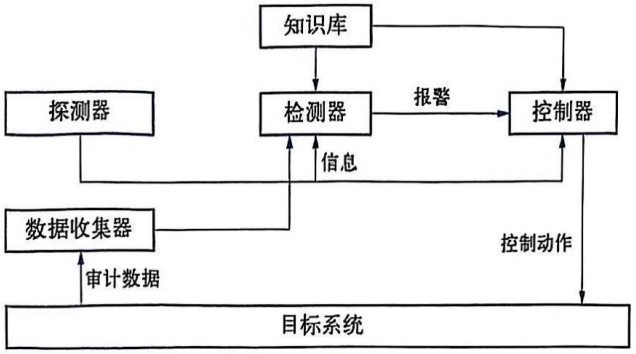

图 5-10 通用网络入侵监测系统模型(NIDS)

数据收集器：主要负责收集数据。

探测器：收集捕获所有可能的和入侵行为有关的信息，包括网络数据包、系统或应用程序的日志和系统调用记录等，探测器将数据收集后，送到检测器进行处理。

检测器：负责分析和监测入侵行为，并发出警报信号。

知识库：提供必要的数据信息支持，如用户的历史活动档案、监测规则集等。

控制器：根据报警信号，人工或自动做出反应动作。

入侵检测的工作流程如下：

第一步，网络数据包的获取(混杂模式)。

第二步，网络数据包的解码(协议分析)。

第三步，网络数据包的检查(规则匹配/误用检测)。

第四步，网络数据包的统计(异常检测)。

第五步，网络数据包的审查(事件生成)。

第六步，网络数据包的处理(报警和响应)。

这六个步骤可以将入侵检测的工作概括成两部分：实时监控和安全审计。实时监控——实时地监视网络中所有的数据报文及系统中的访问行为，识别已知的攻击行为，分

析异常访问行为，发现并实时处理来自内部和外部的攻击事件和越权访问；安全审计——通过对入侵检测系统记录的违反安全策略的用户活动进行统计分析，并得出网络系统的安全状态，并对重要事件进行记录和还原，为事后追查提供必要的证据。

四、入侵检测系统的分类

随着入侵检测技术的发展，出现了很多入侵检测系统，不同的入侵检测系统具有不同的特征。根据不同的分类标准，入侵检测系统可分为不同的类别。对于入侵检测系统，要考虑的因素（分类依据）主要有：信息源、入侵、事件生成、事件处理、检测方法等。下面就不同的分类依据及分类结果分别加以介绍。

1. 按体系结构进行分类

按照体系结构，入侵检测系统可分为集中式和分布式两种。

(1) 集中式入侵检测系统。

引擎和控制中心在一个系统中，不能远距离操作，只能在现场进行操作。优点是结构简单，不会因为通信而影响网络带宽和泄密。

(2) 分布式入侵检测系统。

引擎和控制中心在两个系统中，通过网络通信，可以远距离查看和操作。目前的大多数入侵检测系统都是分布式的，优点是不必在现场操作，可以用一个控制中心管理多个引擎；可以统一进行策略编辑和下发，统一查看和集中分析上报的事件；可以通过分开时间显示和查看的功能提高处理速度等。

2. 按检测原理进行分类

传统的观点是根据入侵行为的属性分为误用和异常两种，然后分别对其建立误用检测模型和异常检测模型。误用入侵检测是指利用已知系统和应用软件的弱点攻击模式来检测入侵方法。异常入侵检测是指能够根据异常行为和使用计算机的资源情况检测出入侵的方法。它试图用定量的方式描述可以接受的行为特征，以区分非正常的、潜在的入侵行为。入侵行为可分为外部闯入、内部渗透和不当行为。外部闯入是指未经授权的计算机系统用户的入侵；内部渗透是指已授权的计算机系统用户访问未经授权的数据；不当行为是指用户虽然授权，但对授权数据和资源的使用不合法或滥用授权。综上所述，可根据系统所采用的检测模型，将入侵检测分为两类：误用检测和异常检测。

(1) 误用检测（misuse detection）。

误用检测运用已知攻击方法，根据已定义好的入侵模式，通过判断这些入侵模式是否出现来检测。因为很大一部分的入侵是利用了系统的脆弱性，通过分析入侵过程的特征、条件、排列及事件间关系能具体描述入侵行为的迹象。因为它匹配的是入侵行为特征，所以又存在以下几个特点：

- 如果入侵特征与正常的用户行为匹配，则系统会发生误报。
- 如果没有特征能与某种新的攻击行为匹配，则系统会发生漏报。
- 攻击特征的细微变化，会使得误用检测无能为力。

误用检测模型误报率低，漏报率高。对于已知的攻击，它可以详细、准确地报告出攻