第 6 章　入侵检测系统

教学目标

通过对本章的学习，学生可以了解入侵检测系统的基础知识和应用环境。熟悉入侵检测系统的工作原理和不足。

能力目标	知识目标	主要教学内容
了解入侵检测系统的基础知识	熟悉入侵检测系统的工作原理	入侵检测系统分类
能部署简单的入侵检测系统	了解入侵检测系统的分类	入侵检测系统的不足

案例引入

在网络安全环境每况愈下的形式下，如果有一款网络安全产品能预测出或者检测出将要到来的网络安全威胁该有多好。入侵检测系统可以辅助防火墙作为威胁行为的预测，这样防火墙就有更准确的查杀能力以及更快的反应速度。

入侵检测系统是 10 年前在全世界入侵检测系统技术大会上提出来的。接下来的许多年，人们都在设法实现这个思想，从可行性上，从技术上，从防护思想上等。那么这款技术针对网络安全环境会起到该有的作用吗？

案例分析

入侵检测系统（IDS）虽然已经投入到了网络安全环境的建设中，但是针对它及其支持技术的争论始终没有停止。那么这是为什么呢？本章就来揭开这个谜题。

案例思考

网络安全部件越来越多，这些部件的引入无疑使得网络安全防护的力量逐步增强，但是也需要考虑：事务都有其两面性，这些安全部件的引入有可能存在哪些问题？

6.1　入侵检测系统基础

针对越来越恶化的网络安全环境，人们启用了很多安全部件。例如，防火墙、防毒墙等。

在一段时期内防火墙始终作为安全的第一道防线有时也是唯一的一道防线。而随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感部门的需要，网络的防卫必须采用一种纵深的、多样的手段。与此同时，当今的网络环境也变得越来越复杂，各式各样的复杂设备，需要不断升级、补漏的系统使得网络管理员的工作不断加重，不经意的疏忽便有可能造成安全的重大隐患。在这种环境下，入侵检测系统成为了网络安全部件的主力，开始在各种不同的环境中发挥作用。

“入侵”（Intrusion）是个广义的概念，不仅包括被发起攻击的人（如恶意的黑客）取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问（DoS）等对计算机系统造成危害的行为。

入侵检测是通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（IDS，Intrusion Detection System）。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全的运行。

6.1.1　入侵检测系统的作用和部署

入侵检测是防火墙的合理补充，协助现有安全系统减少网络安全威胁。IDS 扩展了整体安全系统的安全管理能力（包括安全审计、监视、攻击识别和防护响应），提高了信息安全基础结构的完整性。IDS 从计算机网络系统中的若干关键节点收集信息，并分析这些信息，查找网络中是否有违反安全策略的行为和被攻击的迹象。入侵检测被认为是防火墙之后的第二道安全屏障，因为 IDS 是旁路设备所以其能在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。IDS 可以完成监视、分析用户及系统的活动；针对系统构造和弱点的审计；识别反映已知攻击的运行模式并报警；异常行为模式的统计和分析；评估系统重要数据和数据文件的完整性；针对操作系统的审计跟踪管理，并识别用户违反安全策略的行为等工作。

一款合格的入侵检测系统可使系统管理员时刻了解网络系统（包括用户、文件和传输数据量等）的任何变更，还能给网络安全策略的制订提供帮助。更为重要的是，入侵检测系统能够根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，能及时响应，包括记录相应事件和报警等。

入侵检测的第一步是信息收集，内容包括系统、网络、数据及用户活动的状态和行为。而且，需要在计算机网络系统中的若干不同关键点收集类似信息，因为单一节点的信息可能不足以作为判断网络是否存在安全问题的依据，因为看起来是一个节点产生的数据其实是和其相邻节点有很大的关联，所以从不同的节点获取信息的不一致性是可疑行为或入侵的最好标识。入侵检测很大程度上依赖于收集信息的可靠性和正确性，入侵检测利用的信息一般来

自以下几个方面。

（1）系统和网络日志文件

攻击者经常在系统日志文件中留下他们的踪迹，因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，包括登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容，如图 6-1 所示。

（2）目录和文件中的非授权变化

网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件，经常是攻击者修改或破坏的目标。目录和文件中的非授权变化（例如，修改、创建和删除、运行等）很可能就是一种入侵产生的指示和信号。

（3）系统关键位置的程序运行

网络系统上的程序执行一般包括操作系统、网络服务、用户指定的程序和特定目的的应用，有些程序涉及整个系统的关键位置，比如，类似主机的开机启动部分，服务器的域操作部分等。针对这些关键位置的程序运行也是 IDS 需要得到的信息，因为在关键位置运行的程序可能会改变系统环境的一些原有设置，攻击者的行为也往往涉及此类活动。

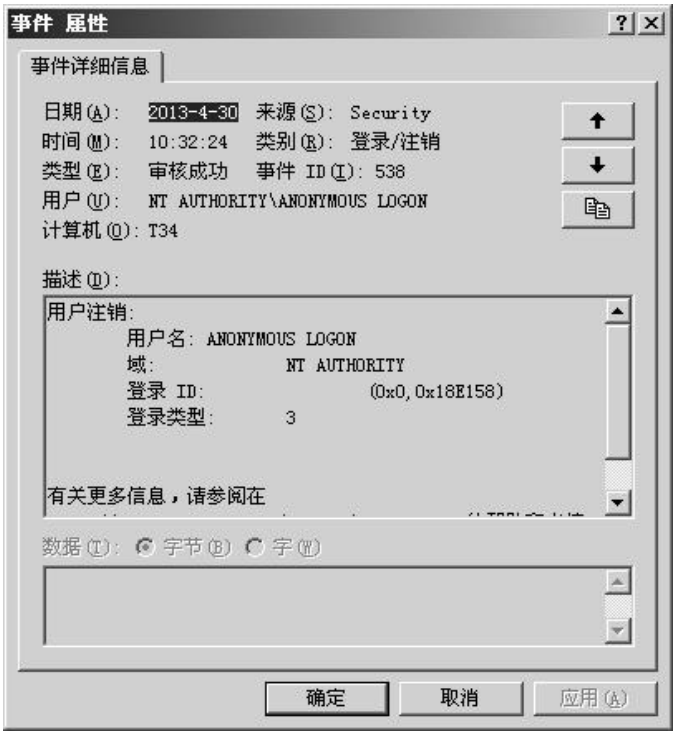

图 6-1　日志系统记录

与防火墙不同，防火墙属于主路设备即必须部署在主干线路上的设备，IDS 是旁路设备，即不用部署在主干线路上的设备，主路设备和旁路设备的区别如图 6-2 所示。IDS 入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流量流经它便可以工作。因此，对 IDS 的部署，唯一的要求是 IDS 应当挂接在所有必要流量都必须流经的链路上。在这里，“必要流量”是指来自不同网络区域的访问流量和需要进行统计、监视的网络报文。在如今的绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，不管什么类别的 IDS 在交换式网络中的位置一般选择在①尽可能靠近攻击源；②尽可能靠近受保护资源。这些位置通常是在服务器区域的交换机上、互联网接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上。

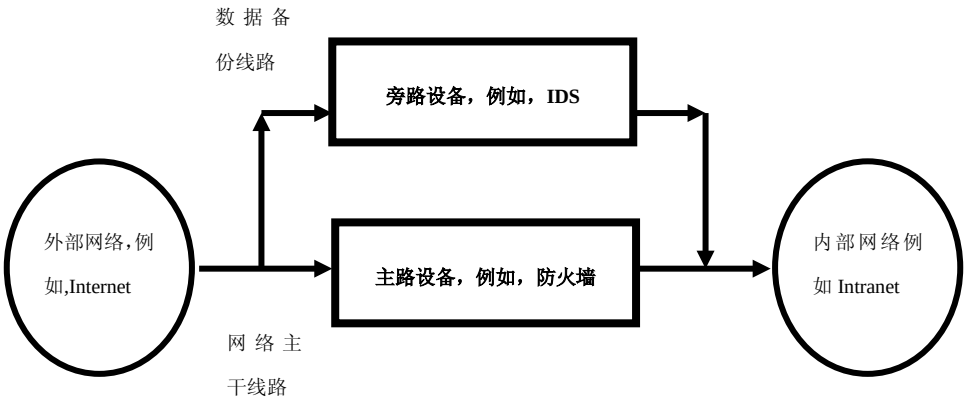

图 6-2　主路设备和旁路设备的区别

入侵系统常被分为基于网络的和基于主机的两种。这两种入侵检测系统在功能，工作原理和部署上还是存在一定的差异。基于网络的入侵检测系统通过监测网络特定部分的所有可能包含恶意流量或有恶意企图的流量来对网络提供保护。基于网络的入侵检测系统的功能是监测该网络流量。基于主机的入侵检测系统是部署在那些具有特定意义的设备上，例如，Web 服务器，数据库服务器和其他主机设备。基于主机的入侵检测系统提供如用户认证，文件修改/删除和其他基于主机的信息。

从入侵检测系统分类的角度来看部署入侵检测系统首先是部署基于网络的入侵检测系统，然后是基于主机的入侵检测系统。这样能够确保网络、主机设备得到保护。

基于网络的入侵检测系统应部署在外部 DMZ (Demilitarized Zone)即俗称的非军事区部分，然后才是 DMZ 部分。这将允许监控所有的外部和 DMZ 的恶意活动。所有的外部网络部分都应该予以监控，包括入站和出站流量。这将确保连接到外部恶意网络的所有设备都受到监控和检查。具体布置拓扑如图 6-3 所示。

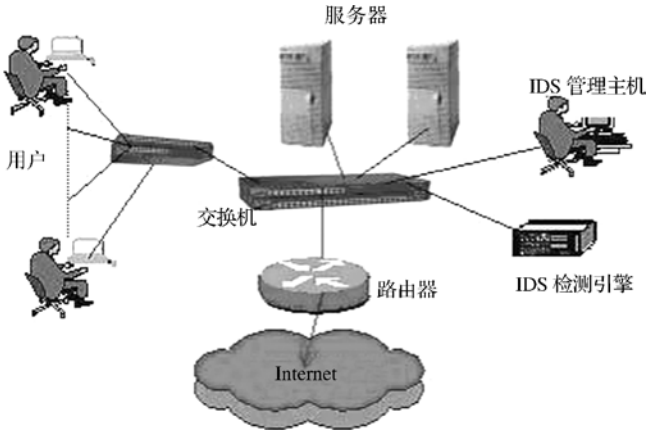

图 6-3　基于网络的IDS的部署

基于主机的入侵检测系统应该部署在 DMZ 内部的所有关键主机设备上。系统内部主机设备都应该拥有一个基于主机的入侵检测系统，以确保这些系统同样也受到保护。基于主机的 IDS 部署应该在基于网络的 IDS 部署之后。这实际上可与基于网络的同时完成，但重点还是应该首先部署基于网络的 IDS。

6.1.2　入侵检测系统的组成和分类

入侵检测系统通常分为 4 个组件：事件产生器（Event generators），事件分析器（Event analyzers），响应单元（Response units），事件数据库（Event databases）。事件产生器的目的是从整个网络环境中获得事件，并向系统的其他部分提供此事件。事件分析器分析得到的数据，并产生分析结果。响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。事件数据库是存放各种中间和最终数据地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。在这个模型中，前三者以程序的形式出现，而最后一个则往往是文件或数据流的形式。 这 4 个组件的工作原理如图 6-4 所示。

入侵检测系统的分类标准很多，有按照检测技术的，有按照发展时间的，有按照具体功能的，还有按照检测对象不同以及按照存在形式的不同很多种分类方法。常见的是按照检测对象的不同和存在形式的不同两种分类方法。

根据检测对象的不同，入侵检测系统可分为主机型和网络型。主机型入侵检测系统往往以系统日志、应用程序日志等作为数据源，当然也可以通过其他手段（如监督系统调用）从所在的主机收集信息进行分析。基于主机的入侵检测系统用于保护关键应用的服务器，实时监视可疑的连接、系统日志、非法访问的闯入等，并且提供对典型应用的监视，如 Web 服务器应用。基于主机的 IDS 通常采用查看针对可疑行为的审计记录来执行。它能够比较新的记录条目与攻击特征，并检查不应该改变的系统文件的校验和，分析系统是否被侵入或者被攻击。

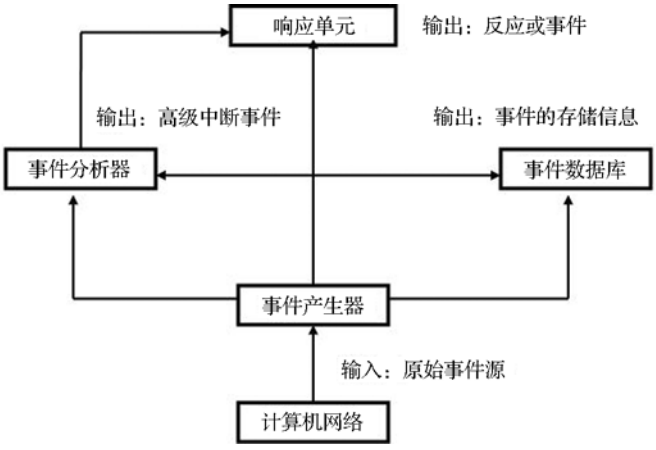

图6-4　组件攻击原理

根据存在形式的不同，入侵检测系统分为软件和硬件两大类。当然无论是软件还是硬件其功能很类似，都是既可以检测主机也可以检测网络。常见的软件入侵检测系统有著名的 SNORT 和 BLACK ICE。SNORT 是一款软件版本的网络入侵检测系统，可以针对网络上各类信息进行收集和检测以发现网络中是否存在入侵的行为或者趋势，常见界面如图 6-5 所示。BLACK ICE 软件版本的一款针对主机的入侵检测系统，当然也具备一定的网络防范能力。BLACK ICE 集成了非常强大的检测和分析引擎，可以识别 200 多种入侵技巧，还能即时监测网络端口和协议，拦截可疑的网络入侵，其灵敏度、准确率和稳定性也相当出色，系统资源占用较少。常见界面如图 6-6 所示。

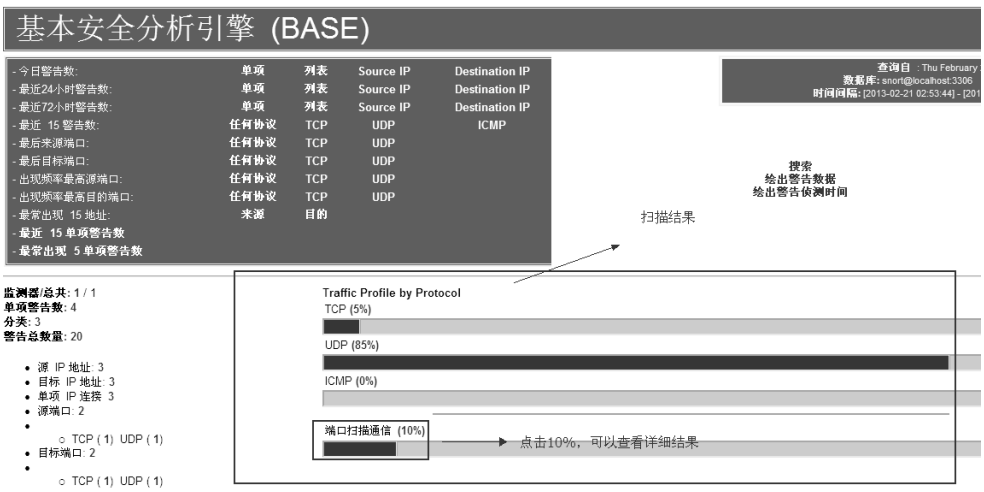

图 6-5　SNORT检测结果界面

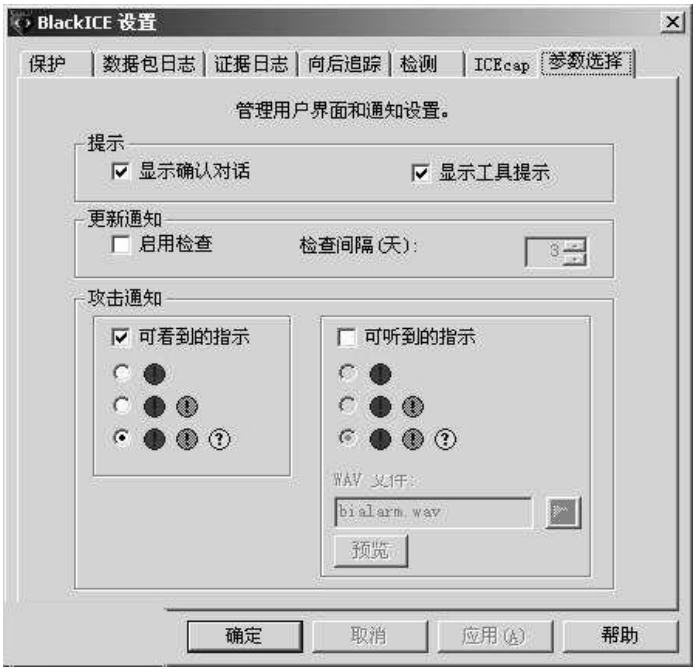

图 6-6 BLACK ICE设置界面

网络型入侵检测系统的数据源则是网络上的数据包。往往将一台计算机的网卡设于混杂模式（promisc mode），监听网段内的数据包并进行判断。 基于网络的 IDS 主要用于实时监控网络关键路径的信息。它可以利用工作在混合模式下的网卡实时监视和分析所有通过共享网络的传输。基于网络的 IDS 一般被放置在比较重要的网段内，有些网络 IDS 也可以利用交换式网络中的端口映射功能来监视特定端口的网络入侵行为。一旦攻击被检测到，响应模块按照配置对攻击作出反应。通常这些反应包括发送电子邮件、寻呼、记录日志、切断网络连接等。

不难看出，网络型 IDS 的优点主要是简便，一个网段上只需安装一个或几个这样的系统，便可以监测整个网段的情况。但由于现在网络的日趋复杂以及高速网络的普及，这种结构正受到越来越大的挑战。由于基于网络的入侵检测系统只能监视经过本网段的活动，并且精确度较差，所以在交换网络环境中难以配置，防入侵欺骗的能力也比较差；但是它可以提供实时网络监视，并且监视力度更细致。

主机型 IDS 存在一些显而易见的缺点，包括必须为不同平台开发不同的程序、增加系统负荷、所需安装数量众多等，但是内在结构却没有任何束缚，同时可以利用操作系统本身提供的功能并结合异常分析，更准确地报告攻击行为。

两种入侵检测系统都具有自己的优点和不足，互相可作为补充。基于主机的入侵检测系统可以精确地判断入侵事件，可对入侵事件立即进行反应，还可针对不同操作系统的特点判断应用层的入侵事件；其缺点是会占用主机的资源。

6.1.3　入侵检测系统的不足和发展

虽然 IDS 作为一款产品已经出现很多年了，但是针对这款产品的争论始终没有停止。这些争论往往集中在 IDS 的功能性是否可靠、IDS 自身的安全性、IDS 的检测技术是否合理等等很多方面。这些争论从这款产品的技术论证就已经开始，有些专家甚至认为 IDS 是一项伪技术，有些专家更倾向于 IPS（入侵防御系统）的开发和部署。虽然争论很多，但是也没有能阻挡 IDS 作为一项安全产品进入网络安全领域，当然从另一角度来看，IDS 也确实存在不少的问题，而且这些问题的解决都是未来 IDS 技术发展的方向。

1）攻击者不断增加的知识，日趋成熟多样自动化工具，以及越来越复杂细致的攻击手法。使得 IDS 的根本检测技术必须不断升级换代。

2）数据加密传输的普及。在当今数据加密、隧道、VPN 等技术都可以针对数据进行加密传输。入侵检测系统通过匹配网络数据包发现攻击行为，IDS 往往假设攻击信息是通过明文传输的，因此，对信息的稍加改变即可骗过 IDS 的检测。这一点是未来 IDS 技术发展所必须要解决的问题。

3）IDS 针对不同网络的适应性必须加强。网络及其中的设备越来越多样化，既存在关键资源如邮件服务器、企业数据库，也存在众多相对不是很重要的 PC。不同企业之间这种情况也往往不尽相同。IDS 要能有所定制以更适应多样的环境要求。

4）不断增大的网络流量。用户往往要求 IDS 尽可能快的报警，因此，需要对获得的数据进行实时分析，这导致对所在系统的要求越来越高。所以提高 IDS 的硬件化和提升 IDS 硬件的性能是未来从硬件环节解决 IDS 存在的问题的方向。

5）IDS 自身存在的安全问题。和其他系统一样，IDS 本身也往往存在安全漏洞。如果对 IDS 攻击成功，则直接导致其报警失灵，入侵者在其后所作的行为将无法被记录。

6）大量的误报和漏报使得发现问题的真正所在非常困难。采用当前的技术及模型，IDS 必须清楚地了解所有操作系统网络协议的运作情况甚至细节，才能准确地进行分析。否则一些问题便无法解决。而不同操作系统之间，甚至同一操作系统的不同版本之间对协议处理的细节的不同，也给 IDS 的工作带来了很多的困难。

7）IDS 增加了网络安全系统的响应时间。系统中增加了 IDS 设备，无疑会增加整体网络安全系统的整体响应时间，其中各网络安全设备的联动性也变得越来越重要，如果缺乏设备之间的联动性，则每一款安全产品的功效将大大降低。

6.2　入侵检测系统的工作原理

6.2.1　入侵检测技术

入侵检测系统的核心功能是对各种事件进行分析，从中发现违反安全策略的行为。从技术上，入侵检测分为两类：一种基于标志（signature-based），另一种基于异常情况

(anomaly-based)。

定义违背安全策略事件的特征是基于标识的检测技术的关键，例如，网络数据包包头的某些信息。入侵检测主要判别这类特征是否在所收集到的数据包头信息中存在。此方法的原理借鉴的是杀毒软件工作原理。

而基于异常的检测技术则是先定义一组系统正常运行时期的数值，如 CPU 利用率、内存利用率、文件校验和等，然后将系统运行时的数值与所定义的正常运行时期的参数进行对比，判断系统是否被攻击。定义正常时期的相关参数是这种检测方式的核心。

实践证明，两种不同的检测技术会得出差异较大的结论。其原因在于基于异常的检测技术的核心是维护一个知识库。对于已知攻击，它可以详细、准确地判断出攻击类型，但是对未知攻击却效果有限。基于异常的检测技术则无法准确判断出攻击的类型，但它可以判断更广范、甚至未发觉的攻击。为了达到更好的检测效果，在允许的环境下可以将两种检测结合起来使用。

6.2.2 入侵检测常见方法

根据常见的入侵检测技术，产生了很多入侵检测方法。这些方法从根本上存在一定的区别，有的入侵检测以数据参数为基础，有的以行为推断为基础，有的以数理运算为基础。大体可以分为以下几类。

（1）基于贝叶斯函数的检测方法

基于贝叶斯推理检测法：通过在任何给定的时刻，测量变量值，推理判断系统是否发生入侵事件。

基于贝叶斯网络检测法：用图形方式表示随机变量之间的关系。通过指定的与相邻节点相关的小的概率集来计算随机变量的联接概率分布。按给定全部节点组合，所有根节点的检验概率和非根节点概率构成这个集。通过测量整体变量的变化趋势来判断是否存在入侵事件。

（2）基于知识库和数据挖掘的检测方法

数据挖掘检测法：数据挖掘的目的是要从海量的数据中提取出有用的数据信息。网络中会有大量的审计记录存在，审计记录大多都是以文件形式存放的。仅靠手工方法来发现记录中的异常现象是远远不够的，所以将数据挖掘技术应用于入侵检测中，可以从审计数据中提取有用的知识，然后用这些知识区别检测异常入侵和已知的入侵。

专家系统法：此方法的思想是把安全专家的知识表示成规则知识库，再用推理算法检测入侵。主要是针对有特征的入侵行为。

（3）基于数据参数的检测方法

基于特征选择检测法：指从一组度量中挑选出能检测入侵的度量，用它来对入侵行为进行预测或分类。

基于模式预测的检测法：事件序列不是随机发生的，而是遵循某种可辨别的模式。这是基于模式预测的异常检测法的假设条件，其特点是考虑到事件序列及相互联系。其最大的优

点是只关心少数相关安全事件，这样可以节省系统资源。

基于统计的异常检测法：是根据用户对象的活动为每个用户都建立一个特征轮廓表，通过对当前特征与以前已经建立的特征进行比较，来判断当前行为的异常性。用户特征轮廓表要根据审计记录情况不断更新，形成衡量指标，这些指标值要根据经验值或一段时间内的统计而得到。

（4）基于行为推断的检测方法

基于应用模式的异常检测法：该方法是根据服务请求类型、服务请求长度、服务请求数据包大小分布计算网络服务的异常值。通过实时计算的异常值和所训练的阈值比较，从而发现异常行为。

模式匹配法：通过把收集到的信息与网络入侵的已知信息进行比较，从而对违背安全策略的行为进行发现。模式匹配法可以显著地减少系统负担，有较高的检测率和准确率。

基于状态转移分析的检测法：该方法的基本思想是将攻击看成一个连续的、分步骤的并且各个步骤之间有一定的关联的过程。在网络中发生入侵时及时阻断入侵行为，防止可能还会进一步发生的类似攻击行为。

6.2.3　入侵检测系统的性能参数和选购

打开一款 IDS 产品的包装，会看到性能参数列表。这份列表可能是厚厚的一本书，其实有些参数是网络安全产品所必须的，并不是 IDS 特有的，还有些是为了进行商业宣传而制定的参数，这些参数不是每款 IDS 所必须的。对于 IDS，往往最关注的参数是每秒能处理的网络数据流量、每秒能监控的网络连接数等指标。但除了上述指标外，还有一些不为一般用户了解的指标也很重要，甚至更重要，例如，每秒抓包数、每秒能够处理的事件数等。

1）每秒数据流量（Mbit/s 或 Gbit/s）：每秒数据流量是指网络上每秒通过某节点的数据量。这个指标是反应网络入侵检测系统性能的重要指标，一般用 Mbit/s 来衡量。例如，10Mbit/s，100Mbit/s 和 1Gbit/s。网络入侵检测系统的基本工作原理是嗅探（Sniffer），它通过将网卡设置为混杂模式，使得网卡可以接收网络接口上的所有数据。如果每秒数据流量超过网络传感器的处理能力，IDS 就可能会丢包，从而不能正常检测攻击。但是 IDS 是否会丢包，主要不是取决于每秒数据流量，而是取决于每秒抓包数。

2）每秒抓包数（pps）：每秒抓包数是反映网络入侵检测系统性能的最重要的指标。因为系统不停地从网络上抓包，对数据包作分析和处理，查找其中的入侵和误用模式。所以，每秒所能处理的数据包的多少，反映了系统的性能。业界不熟悉入侵检测系统的用户往往把每秒网络流量作为判断网络入侵检测系统的决定性指标，这种想法是错误的。每秒网络流量等于每秒抓包数乘以网络数据包的平均大小。当网络数据包的平均大小差异很大时，在相同抓包率的情况下，每秒网络流量的差异也会很大。例如，网络数据包的平均大小为 1024B 左右，系统的性能能够支持 10 000pps 的每秒抓包数，那么系统每秒能够处理的数据流量可达到 78Mbit/s，当数据流量超过 78Mbit/s 时，会因为系统处理不过来而出现丢包现象；如果网络

数据包的平均大小为 512B 左右，则在 10 000pps 的每秒抓包数的性能情况下，系统每秒能够处理的数据流量可达到 40Mbit/s，当数据流量超过 40Mbit/s 时，就会因为系统处理不过来而出现丢包现象。在相同的流量情况下，数据包越小，处理的难度越大。小包处理能力，也是反映防火墙性能的主要指标。

3）每秒能监控的网络连接数：网络入侵检测系统不仅要对单个的数据包作检测，还要将相同网络连接的数据包组合起来作分析。网络连接的跟踪能力和数据包的重组能力是网络入侵检测系统进行协议分析、应用层入侵分析的基础。这种分析延伸出很多网络入侵检测系统的功能，例如，检测利用 HTTP 的攻击、敏感内容检测、邮件检测、Telnet 会话的记录与回放、硬盘共享的监控等。

4）每秒能够处理的事件数：网络入侵检测系统检测到网络攻击和可疑事件后，会生成安全事件或称报警事件，并将事件记录在事件日志中。每秒能够处理的事件数，反映了检测分析引擎的处理能力和事件日志记录的后端处理能力。

目前，市场上的入侵检测产品有很多，性能参数各不一样。但是并不是所有的 IDS 都适合所有的网络，为网络选择合适的 IDS 才是最能起到作用的。在选择 IDS 的过程中应该着重注意以下原则。

（1）产品的攻击检测数量以及产品是否支持升级？

IDS 的主要指标是它能发现的入侵方式的数量，几乎每个星期都有新的漏洞和攻击方法出现，产品的升级方式是否灵活直接影响到它的功能发挥。一个好的实时检测产品应该能经常性升级，并可通过互联网或下载升级包在本地升级。通常这种简单升级还应该是免费的。

（2）最大可处理的流量（PPS）

首先，要分析网络入侵检测系统所部署的网络环境，如果在 512KB 或 2MB 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

（3）产品是否容易被攻击者躲避

有些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。产品在设计时是否考虑到这一点。

（4）能否自定义异常事件

IDS 对特殊的监控需求只能通过用户自己定制监控策略实现。一个优秀的 IDS 产品，必须提供灵活的用户自定义策略能力，包括对服务、访问者、被访问者、端口、关键字以及事件的响应方式等策略。

（5）产品系统结构是否合理

一个成熟的产品，必须是集成了基于百兆网络、千兆网络、基于主机的 3 种技术和系统。传统的 IDS 大多是两层结构，即“控制台→探测器”结构，一些先进的 IDS 产品开始采用多层架构进行部署，即“控制台→事件收集器＋安全数据库→探测器”结构，对于大型网络来说，多层结构更加易于实现分布部署和集中管理，从而提高安全决策的集中性。如果没有远

程管理能力，则对于大型网络基本不具备可用性。

（6）系统本身是否安全

IDS 系统记录了企业最敏感的数据，必须有自我保护机制，防止成为黑客的攻击目标。不要因为引入一款安全产品反而带来了更多的安全问题。

（7）系统是否易用

系统的易用性包括 5 个方面：界面易用——全中文界面，方便易学，操作简便灵活。帮助易用——在监控到异常事件时能够立刻查看报警事件的帮助信息，同时在联机帮助中能够按照多种方式查看产品帮助。策略编辑易用——能否提供单独的策略编辑器，能否同时编辑多个策略，是否提供策略打印功能。日志报告易用——是否提供灵活的报告定制能力。报警事件优化技术——是否针对报警事件进行优化处理，将管理员从海量日志中解放出来。

当然，上述因素是购买 IDS 需要着重考虑的，但是这不是全部的因素。具体购买时还是要根据网络架构的需要、用户的实际情况等相关因素结合考虑。

6.3　本章小结

本章着重从以下几个方面对入侵检测系统进行了讲述。

1）入侵检测系统的工作原理和适用环境。

2）入侵检测系统的分类和部署。

3）入侵检测系统的性能参数和选购。

4）SNORT 系统的部署和使用。

本章的重点是入侵检测系统的分类和部署，难点是 SNORT 系统的使用。

课后练习

1. 填空题

1）入侵检测技术的原理可以分为_____，_____，_____，_____几大类。

2）“入侵”（Intrusion）是个广义的概念，不仅包括_____，也包括收集漏洞信息，造成_____对计算机系统造成危害的行为。

2. 问答

1）入侵检测系统的主要作用是什么？

2）入侵检测系统的部署原则是什么？

3. 实操题

根据实际环境进行入侵检测系统的选择和部署，并进行设置。