**入侵检测技术综述**  
胡征兵1 Shirochin V.P.2乌克兰国立科技大学

摘要 Internet蓬勃发展到今天，计算机系统已经从独立的主机发展到复杂、互连的开放式系统，这给人们在信息利用和资源共享上带来了很大的便利。由Internet来传递和处理各种生活信息，早已成为人们重要的沟通方式之一，随之而来的各种攻击事件与入侵手法更是层出不穷，引发了一系列安全问题。本文介绍现今热门的网络安全技术-入侵检测技术，本文先讲述入侵检测的概念、模型及分类，并分析了其检测方法和不足之处，最后说描述了它的发展趋势及主要的IDS公司和产品。

关键词 入侵检测 入侵检测系统 网络安全 防火墙

1 引言

随着个人、企业和政府机构日益依赖于Internet进行通讯，协作及销售。对安全解决方案的需求急剧增长。这些安全解决方案应该能够阻止入侵者同时又能保证客户及合作伙伴的安全访问。虽然防火墙及强大的身份验证能够保护系统不受未经授权访问的侵扰，但是它们对专业黑客或恶意的经授权用户却无能为力。企业经常在防火墙系统上投入大量的资金，在Internet入口处部署防火墙系统来保证安全， 依赖防火墙建立网络的组织往往是“外紧内松”，无法阻止内部人员所做的攻击,对信息流的控制缺乏灵活性，从外面看似非常安全，但内部缺乏必要的安全措施。据统计，全球80%以上的入侵来自于内部。由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于企业内部人员所做的攻击，防火墙形同虚设。

入侵检测是对防火墙及其有益的补充，入侵检测系统能使在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中，能减少入侵攻击所造成的损失。在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加入知识库内，增强系统的防范能力，避免系统再次受到入侵。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时保护,大大提高了网络的安全性[1]。

2 入侵检测的概念、模型

入侵检测（Intrusion Detection，ID）, 顾名思义，是对入侵行为的检测。它通过收集和分析计算机网络或计算机系统中若干关键点的信息，检查网络或系统中是否存在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（Intrusion Detection System,IDS）。

入侵检测的研究最早可以追溯到詹姆斯·安德森[1]在1980年为美国空军做的题为《计算机安全威胁监控与监视》的技术报告，第一次详细阐述了入侵检测的概念。他提出了一种对计算机系统风险和威胁的分类方法，并将威胁分为外部渗透、内部渗透和不法行为三种，还提出了利用审计跟踪数据监视入侵活动的思想。他的理论成为入侵检测系统设计及开发的基础 , 他的工作成为基于主机的入侵检测系统和其它入侵检测系统的出发点。

Denning[2]在1987年所发表的论文中，首先对入侵检测系统模式做出定义：一般而言，入侵检测通过网络封包或信息的收集，检测可能的入侵行为，并且能在入侵行为造成危害前及时发出报警通知系统管理员并进行相关的处理措施。为了达成这个目的，入侵检测系统应包含3个必要功能的组件：信息来源、分析引擎和响应组件。

●信息来源（Information Source）：为检测可能的恶意攻击，IDS所检测的网络或系统必须能提供足够的信息给IDS，资料来源收集模组的任务就是要收集这些信息作为IDS分析引擎的资料输入。

●分析引擎（Analysis Engine）：利用统计或规则的方式找出可能的入侵行为并将事件提供给响应组件。

●响应模组（Response Component）：能够根据分析引擎的输出来采取应有的行动。通常具有自动化机制，如主动通知系统管理员、中断入侵者的连接和收集入侵信息等。

3 入侵检测系统的分类

入侵检测系统依照信息来源收集方式的不同，可以分为基于主机（Host-Based IDS）的和基于网络（Network-Based IDS）；另外按其分析方法可分为异常检测（Anomaly Detection,AD）和误用检测（Misuse Detection,MD），其分类架构如图1所示：

入侵检测系统（IDS）

网络型（Network-Based）

误用检测（MD）

异常检测(AD)

主机型(Host-based )

图 1. 入侵检测系统分类架构图

3.1.1主机型入侵检测系统（Host-based Intrusion Detection System,HIDS）

基于主机的入侵检测系统是早期的入侵检测系统结构 , 其检测的目标主要是主机系统和系统本地用户 , 检测原理是根据主机的审计数据和系统日志发现可疑事件。检测系统可以运行在被检测的主机或单独的主机上, 系统结构如图 2所示。

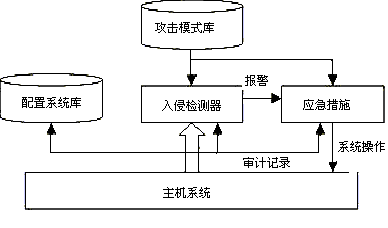


图 2. 基于主机的IDS结构

其优点是：确定攻击是否成功；监测特定主机系统活动；较适合有加密和网络交换器的环境；不需要另外添加设备。其缺点：可能因操作系统平台提供的日志信息格式不同，必须针对不同的操作系统安装个别的入侵检测系统；如果入侵者经其它系统漏洞入侵系统并取得管理者的权限，那将导致主机型入侵检测系统失去效用；可能会因分布式（Denail of Service,DoS）攻击而失去作用；当监控分析时可能会曾加该台主机的系统资源负荷，影响被监测主机的效能，甚至成为入侵者利用的工具而使被监测的主机负荷过重而死机。  
3.1.2 网络型入侵检测系统（Network-based Intrusion Detection System，NIDS）   
 网络入侵检测是通过分析主机之间网线上传输的信息来工作的。它通常利用一个工作在“混杂模式”（Promiscuous Mode）下的网卡来实时监视并分析通过网络的数据流。它的分析模块通常使用模式匹配、统计分析等技术来识别攻击行为。其结构如图 3 所示。



图 3. 基于网络的IDS结构

探测器的功能是按一定的规则从网络上获取与安全事件相关的数据包 , 然后传递给分析引擎进行安全分析判断。分析引擎从探测器上接收到的数据包结合网络安全数据库进行分析 , 把分析的结果传递给配置构造器。配置构造器按分析引擎器的结果构造出探测器所需要的配置规则。一旦检测到了攻击行为，NIDS的响应模块就做出适当的响应，比如报警、切断相关用户的网络连接等。不同入侵检测系统在实现时采用的响应方式也可能不同，但通常都包括通知管理员、切断连接、记录相关的信息以提供必要的法律依据等[3]。

其优点是：成本低；可以检测到主机型检测系统检测不到的攻击行为；入侵者消除入侵证据困难；不影响操作系统的性能；架构网络型入侵检测系统简单。其缺点是：如果网络流速高时可能会丢失许多封包，容易让入侵者有机可乘；无法检测加密的封包；对于直接对主机的入侵无法检测出。

3.1.3 混和入侵检测系统（Hybrid）

主机型和网络型入侵检测系统都有各自的优缺点，混和入侵检测系统是基于主机和基于网络的入侵检测系统的结合 ,许多机构的网络安全解决方案都同时采用了基于主机和基于网络的两种入侵检测系统，因为这两种系统在很大程度上互补，两种技术结合能大幅度提升网络和系统面对攻击和错误使用时的抵抗力，使安全实施更加有效。  
3.2.1误用检测（Misuse Detection）

误用检测(Misuse detection)又称特征检测（Signature-based detection），这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。其难点在于如何设计模式既能够表达“入侵”现象又不会将正常的活动包含进来。

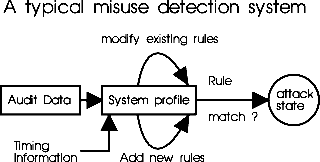


图 4.误用检测系统

设定一些入侵活动的特征（Signature），通过现在的活动是否与这些特征匹配来检测。常用的检测技术为：   
 （l）专家系统：采用一系列的检测规则分析入侵的特征行为。所谓的规则，即是知识，不同的系统与设置具有不同的规则，且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达，是入侵检测专家系统的关键。在系统实现中，将有关入侵的知识转化为if-then结构（也可以是复合结构），条件部分为入侵特征，then部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。  
　　（2）基于模型的入侵检测方法：入侵者在攻击一个系统时往往采用一定的行为序列，如猜测口令的行为序列。这种行为序列构成了具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图。基于模型的入侵检测方法可以仅监测一些主要的审计事件。当这些事件发生后，再开始记录详细的审计，从而减少审计事件处理负荷。这种检测方法的另外一个特点是可以检测组合攻击（coordinate attack）和多层攻击（multi-stage attack）。  
　 （3）简单模式匹配（Pattern Matching）：基于模式匹配的入侵检测方法将已知的入侵特征编码成为与审计记录相符合的模式。当新的审计事件产生时，这一方法将寻找与它相匹配的已知入侵模式。

（4）软计算方法：软计算方法包含了神经网络、遗传算法与模糊技术。

3.2.2 异常检测（Anomaly Detection）

异常检测假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。异常检测的优点之一为具有抽象系统正常行为从而检测系统异常行为的能力。这种能力不受系统以前是否知道这种入侵与否的限制，所以能够检测新的入侵行为。大多数的正常行为的模型使用一种矩阵的数学模型，矩阵的数量来自于系统的各种指标。比如CPU使用率、内存使用率、登录的时间和次数、网络活动、文件的改动等。异常检测的缺点是：若入侵者了解到检测规律，就可以小心的避免系统指标的突变，而使用逐渐改变系统指标的方法逃避检测。另外检测效率也不高，检测时间比较长。最重要的这是一种“事后”的检测，当检测到入侵行为时，破坏早已经发生了。

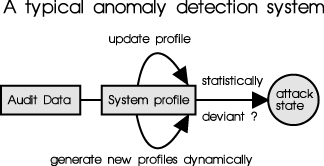


图 5:  异常检测系统

统计方法是当前产品化的入侵检测系统中常用的方法，它是一种成熟的入侵检测方法，它使入侵检测系统能够学习主体的日常行为，将那些与正常活动之间存在较大统计偏差的活动标识成为异常活动。常用的入侵检测统计模型为：

(1)操作模型，该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到，举例来说，在短时间内的多次失败的登录很有可能是口令尝试攻击；

(2)方差，计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常；

(3)多元模型，操作模型的扩展，通过同时分析多个参数实现检测；

(4)马尔柯夫过程模型，将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，或状态矩阵该转移的概率较小则可能是异常事件；

(5) 时间序列分析，将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

统计方法的最大优点是它可以“学习”用户的使用习惯，从而具有较高检出率与可用性。但是它的“学习”能力也给入侵者以机会通过逐步“训练”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。

4 入侵检测技术发展方向

无论从规模与方法上入侵技术近年来都发生了变化。入侵的手段与技术也有了“进步与发展”。入侵技术的发展与演化主要反映在下列几个方面：

入侵或攻击的综合化与复杂化。入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功几率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

入侵主体对象的间接化。通过一定的技术，可以掩盖攻击主体的源地址及主机位置。即使用了隐蔽技术后，对于被攻击对象攻击的主体是无法直接确定的。

入侵或攻击的规模扩大。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击都不可相提并论。

入侵或攻击技术的分布化。以往常用的入侵与攻击行为往往由单机执行。由于防范技术的发展使得此类行为不能奏效。分布式攻击（DDoS）是近期最常用的攻击手段,它能在很短时间内造成被攻击主机的瘫痪,且此类分布式攻击的单机信息模式与正常通信无差异，往往在攻击发动的初期不易被确认。

攻击对象的转移。入侵与攻击常以网络为侵犯的主体，但近期来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统。现已有专门针对IDS作攻击的报道,攻击者详细地分析了IDS的审计方式、特征描述、通信模式找出IDS的弱点，然后加以攻击。

今后的入侵检测技术大致可朝下述三个方向发展：

1）分布式入侵检测：第一层含义，即针对分布式网络攻击的检测方法；第二层含义即使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。

2）智能化入侵检测：即使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。

3）全面的安全防御方案：即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位全面对所关注的网络作全面的评估，然后提出可行的全面解决方案。

5 主要的IDS公司和及其产品

目前国内外已有很多公司开发入侵检测系统，有的作为独立的产品，有的作为防火墙的一部分，其结构和功能也不尽相同。非商业化的产品如 Snort 这一类的自由软件；优秀的商业产品有如：ISS公司的RealSecure是分布式的入侵检测系统，Cisco公司的NetRanger、NAI公司的 CyberCop是基于网络的入侵检测系统，Trusted Information System公司的Stalkers是基于主机的检测系统。下面主要介绍一下ISS公司的RealSecure和Cisco公司的NetRanger

5.1 RealSecure

RealSecure 是目前使用范围最广的商用入侵检测系统 , 它分为两部分 , 引擎和控制台。引擎也就是我们所说的检测器。 ISS 提供的引擎有两个版本 , Windows NT和 UNIX , 控制台则是运行在 Windows NT 系统上。安装好之后 , 策略由分析员来制定 ,RealSecure 重新定义完策略后不需重新启动引擎 , 它的默认设置就能够检测到大量的有用信息 , 报告也相当不错 , 是目前最直观、界面最友好的入侵检测系统。

5.2 NetRanger

NetRanger 包括检测器和分析工作站 , 这些组件之间通过特殊的协议进行通信 , 它的检测器被设计成可以检测 Cisco 路由器的系统纪录和数据包 , 这是所有商业版本中能力最强的一种 , 而且还支持数据包的装配功能 , 这样即使攻击在不同的分段中也能检测出来。但是也有不利因素如系统成本较高。

6 结束语

入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，这从国外入侵检测产品市场的蓬勃发展就可以看出。在国内，随着上网的关键部门、关键业务越来越多，迫切需要具有自主版权的入侵检测产品。但现状是入侵检测仅仅停留在研究和实验样品阶段，或者是防火墙中集成较为初级的入侵检测模块。可见，入侵检测产品仍具有较大的发展空间，从技术途径来讲，我们认为，除了完善常规的、传统的技术（模式识别和完整性检测）外，应重点加强统计分析的相关技术研究。

**参考文献**

[1] J.P Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.   
[2] D.E Denning, “An Intrusion Detection Model ”,IEEE Transaction on Software Engineering, Vol. SE-13,No.2,1987,pp.222-232.   
[3] 张颖,王辉 .一种与入侵检测互动的 Internet安全防范系统 . 计算机工程与应用2003