入侵检测基础知识

入侵检测（Intrusion Detection）是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其它网络上可以获得的信息以及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。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。因此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测。入侵检测通过执行以下任务来实现：监视、分析用户及系统活动；系统构造和弱点的审计；识别反映已知进攻的活动模式并向相关人士报警；异常行为模式的统计分析；评估重要系统和数据文件的完整性；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。

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。

对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制订提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员非常容易地获得网络安全。而且，入侵检测的规模还应根据网络威胁、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，会及时作出响应，包括切断网络连接、记录事件和报警等。

入侵检测系统所采用的技术可分为**特征检测**与**异常检测**两种。

特征检测(Signature-based detection) 又称 Misuse 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。

异常检测(Anomaly detection) 的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。异常检测的难题在于如何建立“活动简档”以及如何设计统计算法，从而不把正常的操作视为“入侵”或忽略真正的“入侵”行为。

入侵分类则有基于主机、基于网络和分布式三种：

基于主机：一般主要使用操作系统的审计、跟踪日志作为数据源，某些也会主动与主机系统进行交互以获得不存在于系统日志中的信息以检测入侵。

基于网络：通过被动地监听网络上传输的原始流量，对获取的网络数据进行处理，从中提取有用的信息，再通过与已知攻击特征相匹配或与正常网络行为原型相比较来识别攻击事件。

分布式：这种入侵检测系统一般为分布式结构，由多个部件组成，在关键主机上采用主机入侵检测，在网络关键节点上采用网络入侵检测，同时分析来自主机系统的审计日志和来自网络的数据流，判断被保护系统是否受到攻击。

入侵检测工作过程分为三部分：信息收集、信息分析和结果处理。

（1）信息收集：入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来

收集信息，包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

（2）信息分析：收集到的有关系统、网络、数据及用户活动的状态和行为等信息，被送到检测引擎，检测引擎驻留在传感器中，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。当检测到某种误用模式时，产生一个告警并发送给控制台。

（3）结果处理：控制台按照告警产生预先定义的响应采取相应措施，可以是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的告警。

术语：

1.False Negatives（漏报）：指一个攻击事件未被 IDS 检测到或被分析人员认为是无害的。

2.False Positives（误报）：指实际无害的事件却被 IDS 检测为攻击事件。

3.入侵检测系统（Intrusion-detection system，IDS）是一种网络安全设备或应用软件，可以对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施。它与其他网络安全设备的不同之处便在于，IDS 是一种积极被动的安全防护技术。IDS 最早出现在 1980 年 4 月。1990 年，IDS 分化为基于网络的 N-IDS 和基于主机的 H-IDS。后又出现分布式 D-IDS。