入侵检测系统

产品名称	入侵检测系统
公司名称	张家口中科网安科技有限公司
价格	.00/个
规格参数	
公司地址	河北省张家口市桥西区赐儿山街19号
联系电话	0313-5928238 13520132483

产品详情

防火墙好比各单位的门卫，但只有门卫远远不够，我们还需要一些巡逻队或者流动哨。在信息安全领域，我们会在内部部署入侵检测系统（Intrusion Detection System,简称IDS）来提供攻击检测手段。这样万一门卫被突破了，还有进一步的防范措施。

入侵检测工作原理：

入侵检测系统是如何工作的呢？它就像敏锐的铁路警察，能够察言观色发现不法分子的可疑迹象。也就是说，它知道好人什么样（先建立起了系统正常行为的轮廓），一旦与正常相偏离，就认为可能是坏的，这被称为异常检测。

另一种情况时，明确知道坏的是什么样（攻击行为的特征），一旦坏的出现就将其抓住，类似根据公安部发出的通缉令抓捕坏人。

入侵检测的步骤：

第一步：从数据源中搜集数据

第二步：进行分析

第三步：作出响应，如：切断网络连接、记录事件和报警等。

入侵检测系统的分类：

基于主机：部署在主机上，以操作系统的审计、跟踪日志为分析数据源。

基于网络：部署在网络关键节点，以网络数据包为分析数据源。

分布式入侵检测系统：部署在网络关键节点，由多个组件组成，数据源为主机系统的审计日志和来自网

络的数据流。

衡量入侵检测系统的指标：

碰见坏蛋没认出来，称之为漏报；反之，误把好人当坏蛋，那就是误报。如果漏报太多，入侵检测系统也就没发挥作用；如果误报太多，人们就会像听到“ 狼来了 ”那样产生厌烦。所以，这两个指标是衡量入侵检测系统好坏的重要指标。

医学上通常用检测为阴性、阳性来表示是否感染病毒，譬如甲型H1N1流感、艾滋病等。阳性的英文记作positive，表示感染；阴性记作negative，表示未感染。因此，报告未感染病毒但实际上错了就是漏报，英文为false negatives；报告感染病毒而实际上误诊了就是误报，英文为false positives。

—— E N D ——

文字来源：《漫画信息安全保密》