入侵检测技术原理与应用

入侵检测概述
入侵检测技术
入侵检测系统组成与分类
入侵检测系统主要产品与技术指标
入侵检测系统应用

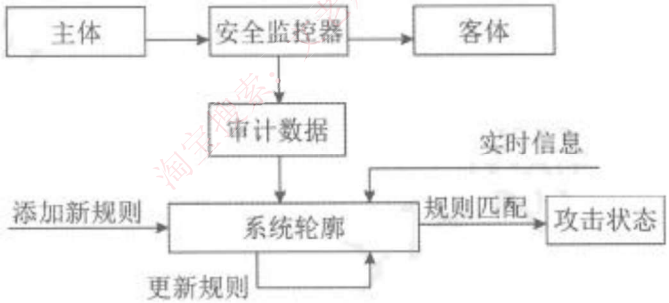
文老师软考教育

入侵检测概述

文老师软考教育

◆入侵检测概念：入侵应与受害目标相关联，该受害目标可以是一个大的系统或单个对象。判断与目标相关的操作是否为入侵的依据是：对目标的操作是否超出了目标的安全策略范围。因此，入侵是指违背访问目标的安全策略的行为。入侵检测通过收集操作系统、系统程序、应用程序、网络包等信息，发现系统中违背安全策略或危及系统安全的行为。具有入侵检测功能的系统称为入侵检测系统，简称为IDS。

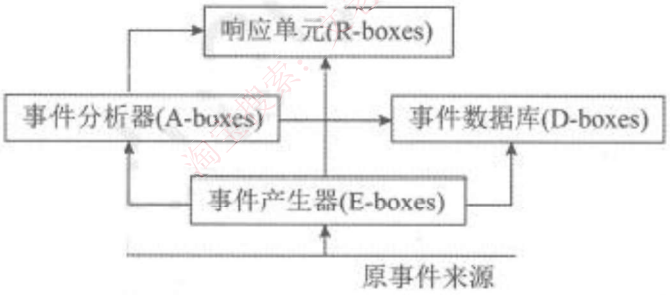
◆入侵检测模型：早期的入侵检测模型主要根据主机系统的审计记录数据，生成有关系统的若干轮廓，并检测轮廓的变化差异，发现系统的入侵行为，如图所示：



入侵检测概述

◆随着入侵行为的种类不断增多，许多攻击是经过长时间准备的。面对这种情况，入侵检测系统的不同功能组件之间，不同IDS之间共享这类攻击信息是十分重要的。于是，一种通用的入侵检测框架模型被提出，简称为CIDF。该模型认为入侵检测系统由事件产生器、事件分析器、响应单元和事件数据库组成，如图所示：

◆ CIDF将入侵检测系统需要分析的数据统称为事件。事件产生器从整个计算环境中获得事件，并向系统的其他部分提供事件。事件分析器分析所得到的数据，并产生分析结果。响应单元对分析结果做出反应。事件数据库存在各种中间和最终数据。



入侵检测概述

文老师软考教育

◆入侵检测作用：

入侵检测系统在网络安全保障过程中扮演类似“预警机”或“安全巡逻人员”的角色，入侵检测系统的直接目的不是阻止入侵事件的发生，而是通过检测技术来发现系统中企图或已经违背安全策略的行为，其作用表现为以下几个方面：

（1）发现受保护系统中的入侵行为或异常行为；

（2）检验安全保护措施的有效性；

（3）分析受保护系统所面临的威胁；

（4）有利于阻止安全事件扩大，及时报警触发网络安全应急响应；

（5）可以为网络安全策略的制定提供重要指导；

（6）报警信息可用作网络犯罪取证。

除此之外，入侵检测技术还常用于网络安全态势感知，以获取网络信息系统的安全状况。网络安全态势感知平台通常汇聚入侵检测系统的报警数据，特别是分布在不同安全区域的报警，然后对其采取数据关联分析、时间序列分析等综合技术手段，给出网络安全状况判断及攻击发展演变趋势。

入侵检测技术

◆基于误用的入侵检测技术：又称为基于特征的入侵检测方法，是指根据已知的入侵模式检测入侵行为。攻击者利用系统和应用软件中的漏洞技术进行攻击，而这些基于漏洞的攻击方法具有某种特征模式。如果入侵者的攻击方法恰好匹配上检测系统中的特征模式，则入侵行为立即被检测到。
◆显然，误用入侵检测依赖于攻击模式库。因此，这种采用误用入侵检测技术的IDS产品的检测能力就取决于攻击模式库的大小以及攻击方法的覆盖面。

◆误用入侵检测的前提条件是，入侵行为能够按某种方式进行特征编码，而入侵检测的过程实际上就是模式匹配的过程，根据入侵特征描述的方式或构造技术，误用检测方法还可以进一步细分为如下几种方法：
（1）基于条件概率的误用检测方法。将入侵方式对应一个事件序列，然后观测事件发生序列，应用贝叶斯定理进行推理，推测入侵行为。

（2）基于状态迁移的误用检测方法。利用状态图表示攻击特征，不同状态刻画了系统某一时刻的特征。初始状态对应入侵开始前的系统状态，危害状态对应已成功入侵时刻的系统状态。初始状态和危害状态之间的迁移可能有一个或多个中间状态。攻击者的操作将导致状态发生迁移，使系统从初始状态迁移到危害状态。通过检查系统的状态变化发现系统中的入侵行为。

入侵检测技术

文老师软考教育

（3）基于键盘监控的误用检测方法。假设入侵行为对应特定的击键序列模式，然后监测用户的击键模式，并将这一模式与入侵模式匹配，从而发现入侵行为。缺点是难以捕获用户击键的可靠方法；此外，也存在多种击键方式表示同一种攻击；如果没有击键语义分析，用户提供别名很容易欺骗这种检测技术；该方法不能检测恶意程序的自动攻击。

（4）基于规则的误用检测方法。将攻击行为或入侵模式表示成一种规则，只要符合规则就认定它是一种入侵行为。优点是检测起来比较简单。缺点是检测受到规则库限制，无法发现新的攻击，并且容易受干扰。Snort是典型应用实例。

◆基于异常的入侵检测技术：是指通过计算机或网络资源统计分析，建立系统正常行为的“轨迹”，定义一组系统正常情况的数值，然后将系统运行时的数值与所定义的“正常”情况相比较，得出是否有被攻击的迹象。
◆异常检测的前提是异常行为包括入侵行为。理想情况下，异常行为集合等同于入侵行为集合，此时，如果IDS能够检测到所有的异常行为，则表明能够检测到所有的入侵行为。但是在现实中，入侵行为集合通常不等同于异常行为集合。事实上，具体的行为有4种状况：行为是入侵行为但不表现异常；行为不是入侵行为但表现异常；行为既不是入侵行为也不表现异常；行为是入侵行为且表现异常。
◆异常检测方法的基本思路是构造异常行为集合，从中发现入侵行为。依赖于异常模型的建立，不同模型构成不同的检测方法，有以下几种常见方法：

入侵检测技术

（1）基于统计的异常检测方法。利用数学统计理论技术，通过构建用户或系统正常行为的特征轮廓。典型的系统主体特征有：系统的登录与注销时间，资源被占用的时间以及处理机、内存和外设的使用情况等。对收集到的数据进行统计处理，并与描述主体正常行为的统计性特征轮廓进行比较，然后根据二者的偏差是否超过指定的门限来进一步判断处理。

（2）基于模式预测的异常检测方法。前提条件是：时间序列不是随机发生的而是服从某种可辨别的模式，其特点是考虑时间序列之间的相互联系。是一种基于时间的推理方法，利用时间规则识别用户正常行为模式的特征。通过归纳学习产生这些规则集，并能动态的修改系统中的这些规则，使之具有较高的预测性、准确性和可信度。如果规则大部分时间是正确的，并能够成功的用于预测所观察到的数据，那么规则就具有较高的可信度。

◆优点：能较好地处理变化多样的用户行为，并具有很强的时序模式；能够集中考察少数几个相关的安全事件，而不是关注可以的整个登录会话过程；容易发现针对检测系统的攻击。

（3）基于文本分类的异常检测方法。是将程序的系统调用视为某个文档中的“字”，而进行运行所产生的系统调用集合就产生一个“文档”。对于每个进程所产生的的“文档”，利用K-最近邻聚类文本分类算法，分析文档的相似性，发现异常的系统调用，从而检测入侵行为。

（4）基于贝叶斯推理的异常检测方法。是指在任意给定的时刻，测量A1, A2, …An变量值，推理判断系统是否发生入侵行为。其中，每个变量Ai表示系统某一方面的特征。

入侵检测技术

◆其他

1. 基于规范的检测方法

基于规范的入侵检测方法（specification-based intrusion detection）介于异常检测和误用检测之间，其基本原理是，用一种策略描述语言 PE-grammars 事先定义系统特权程序有关安全的操作执行序列，每个特权程序都有一组安全操作序列，这些操作序列构成特权程序的安全跟踪策略（trace policy）。若特权程序的操作序列不符合已定义的操作序列，就进行入侵报警。这种方法的优点是，不仅能够发现已知的攻击，而且也能发现未知的攻击。

2. 基于生物免疫的检测方法

基于生物免疫的检测方法，是指模仿生物有机体的免疫系统工作机制，使受保护的系统能够将“非自我（non-self）”的攻击行为与“自我（self）”的合法行为区分开来。该方法综合了异常检测和误用检测两种方法，其关键技术在于构造系统“自我”标志以及标志演变方法。

3. 基于攻击诱骗的检测方法

基于攻击诱骗的检测方法，是指将一些虚假的系统或漏洞信息提供给入侵者，如果入侵者应用这些信息攻击系统，就可以推断系统正在遭受入侵，并且安全管理员还可以诱惑入侵者，进一步跟踪攻击来源。

入侵检测技术

◆其他

4. 基于入侵报警的关联检测方法

基于入侵报警的关联检测方法是通过对原始的 IDS 报警事件的分类及相关性分析来发现复杂攻击行为。其方法可以分为三类：第一类基于报警数据的相似性进行报警关联分析；第二类通过人为设置参数或通过机器学习的方法进行报警关联分析；第三类根据某种攻击的前提条件与结果（preconditions and consequences）进行报警关联分析。基于入侵报警的关联检测方法，有助于在大量报警数据中挖掘出潜在的关联安全事件，消除冗余安全事件，找出报警事件的相关度及关联关系，从而提高入侵判定的准确性。

5. 基于沙箱动态分析的检测方法

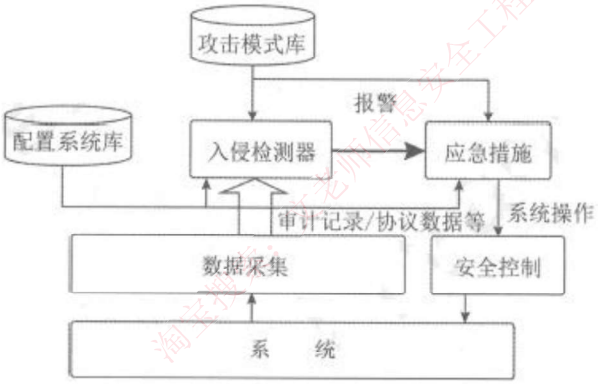
基于沙箱动态分析的检测方法是指通过构建程序运行的受控安全环境，形成程序运行安全沙箱，然后监测可疑恶意文件或程序在安全沙箱的运行状况，获取可疑恶意文件或可疑程序的动态信息，最后检测相关信息是否异常，从而发现入侵行为。

6. 基于大数据分析的检测方法

基于大数据分析的检测方法是指通过汇聚系统日志、IDS 报警日志、防火墙日志、DNS 日志、网络威胁情报、全网流量等多种数据资源，形成网络安全大数据资源池，然后利用人工智能技术，基于网络安全大数据进行机器学习，以发现入侵行为。常见的大数据分析检查技术有数据挖掘、深度学习、数据关联、数据可视化分析等。

入侵检测系统组成与分类

◆入侵检测系统组成：数据采集模块、入侵分析引擎模块、应急处理模块、管理配置模块（提供配置服务，是模块和用户的接口）和相关的辅助模块（为入侵分析引擎模块提供信息）。



◆根据IDS的检测数据来源和它的安全作用范围，可将IDS分成三大类：基于主机的入侵检测系统（简称HIDS，分析主机的信息）；基于网络的入侵检测系统（简称NIDS，扫描网络通信数据包）；分布式入侵检测系统（简称DIDS，多台主机、多个网段采集数据综合分析）。

入侵检测系统组成与分类

◆基于主机的入侵检测系统：即HIDS。通过收集主机系统的日志文件、系统调用以及应用程序的使用、系统资源、网络通信和用户使用等信息，分析这些信息是否包含攻击特征或异常情况，并依次来判断该主机是否收到入侵。CPU利用率、内存利用率、磁盘空间大小、网络端口使用情况、注册表、文件的完整性、进程信息、系统调用等常作为识别入侵事件的依据。

◆ HIDS一般适合检测以下入侵行为：针对主机的端口或漏洞扫描；重复失败的登入尝试；远程口令破解；主机系统的用户账号添加；服务启动或停止；系统重启动；文件的完整性或许可权变化；注册表修改；重要系统启动文件变更；程序的异常调用；拒绝服务攻击。

◆ HIDS中的软件：SWATCH（实施监视日志的程序）；Tripwire（文件和目录完整性检测工具软件包）；网页防篡改系统（防止网页文件被入侵者非法修改）。

入侵检测系统组成与分类

文老师软考教育

基于主机的入侵检测系统的优点：

- 可以检测基于网络的入侵检测系统不能检测的攻击；
- 基于主机的入侵检测系统可以运行在应用加密系统的网络上，只要加密信息在到达被监控的主机时或到达前解密；
- 基于主机的入侵检测系统可以运行在交换网络中。

基于主机的入侵检测系统的缺点：

- 必须在每个被监控的主机上都安装和维护信息收集模块；
- 由于 HIDS 的一部分安装在被攻击的主机上，HIDS 可能受到攻击并被攻击者破坏；
- HIDS 占用受保护的主机系统的系统资源，降低了主机系统的性能；
- 不能有效地检测针对网络中所有主机的网络扫描；
- 不能有效地检测和处理拒绝服务攻击；
- 只能使用它所监控的主机的计算资源。

入侵检测系统组成与分类

◆基于网络的入侵检测系统：简称NIDS。通过侦听网络系统，捕获网络数据包，并依据网络包是否包含攻击特征，或者网络通信流是否异常来识别入侵行为。NIDS通常由一组用途单一的计算机组成，其构成分为两部分：探测器和管理控制器。

◆探测器分布在网络中的不同区域，通过侦听方式获取网络包，探测器将检测到攻击行为形成报警事件，向管理控制器发送报警信息，报告发生入侵行为。
◆管理控制器可监控不同网络区域的探测器，接收来自探测器的报警信息。

◆一般来说，NIDS能够检测以下入侵行为：同步风暴（SYN Flood）、分布式拒绝服务攻击（DDoS）；网络扫描；缓冲区溢出；协议攻击；流量异常；非法网络访问。

入侵检测系统组成与分类

文老师软考教育

基于网络的入侵检测系统的优点：

- 适当的配置可以监控一个大型网络的安全状况；
- 基于网络的入侵检测系统的安装对已有网络影响很小，通常属于被动型的设备，它们只监听网络而不干扰网络的正常运作；
- 基于网络的入侵检测系统可以很好地避免攻击，对于攻击者甚至是不可见的。

基于网络的入侵检测系统的缺点：

- 在高速网络中，NIDS 很难处理所有的网络包，因此有可能出现漏检现象；
- 交换机可以将网络分为许多小单元 VLAN，而多数交换机不提供统一的监测端口，这就减少了基于网络的入侵检测系统的监测范围；
- 如果网络流量被加密，NIDS 中的探测器无法对数据包中的协议进行有效的分析；
- NIDS 仅依靠网络流量无法推知命令的执行结果，从而无法判断攻击是否成功。

入侵检测系统组成与分类

◆分布式入侵检测系统：

网络系统结构的复杂化和大型化，带来许多新的入侵检测问题。

（1）系统的漏洞分散在网络中的各个主机上，这些弱点有可能被攻击者一起用来攻击网络，仅依靠基于主机或网络的 IDS 不会发现入侵行为。

（2）入侵行为不再是单一的行为，而是相互协作的入侵行为。

（3）入侵检测所依靠的数据来源分散化，收集原始的检测数据变得困难。如交换型网络使监听网络数据包受到限制。

（4）网络传输速度加快，网络的流量增大，集中处理原始数据的方式往往造成检测瓶颈，从而导致漏检。

面对这些新的入侵检测问题，分布式入侵检测系统应运而生，它可以跨越多个子网检测攻击行为，特别是大型网络。分布式入侵检测系统可以分成两种类型，即基于主机检测的分布式入侵检测系统和基于网络的分布式入侵检测系统。

入侵检测系统组成与分类

文老师软考教育

◆基于主机检测的分布式入侵检测系统：简称HDIDS，其结构分成两个部分：主机探测器和入侵管理控制器。主机探测器多以安全代理的形式直接安装在每个被保护的主机系统上，并通过网络中的系统管理控制台进行远程控制。

◆基于网络的分布式入侵检测系统：简称NDIDS，其结构分成两个部分：网络探测器和管理控制器。网络探测器部署在重要的区域，用于收集网络通信数据和业务数据并进行分析和报警。NDIDS一般适用于大规模网络或者是地理区域分散的网络，采用这种结构有利于实现网络的分布式安全管理。

图 10-6　基于主机的入侵检测系统典型配置

图 10-7　网络入侵检测系统功能模块的分布式配置及管理

入侵检测系统主要产品与技术指标

◆入侵检测相关产品：

（1）主机入侵检测系统。

（2）网络入侵检测系统。

（3）统一威胁管理。简称UTM，通常会集成入侵检测系统相关的功能模块。UTM是由硬件、软件和网络技术组成的具有专门用途的设备，该设备主要提供一项或多项安全功能，同时将多种安全特性集成于一个硬件设备里，形成标准的统一威胁管理平台，是针对网络及应用系统的安全威胁进行综合防御的网管型设备或系统。通常部署在内部网络和外部网络的边界，对流出和进入内部网络的数据进行保护和控制。其部署方式通常包括透明网桥、路由转发和NAT网关。

（4）高级持续威胁检测。高级持续威胁简称APT，是复杂性攻击技术，通常将恶意代码嵌入word、excel、ppt、pdf文档或电子邮件中，以实现更隐蔽的网络攻击，以逃避普通的网络安全检查。

（5）其他。根据入侵检测应用对象，常见的产品类型有Web IDS、数据库IDS、工控IDS等。其中，Web IDS利用Web网络通信流量或Web访问日志等信息，检测常见的Web攻击；数据库IDS利用数据库网络通信流量或数据库访问日志等信息，对常见的数据库攻击行为进行检测。而工控IDS则通过获取工控设备、工控协议相关信息，根据工控漏洞攻击检测规则、异常报文特征和工控协议安全策略，检测工控系统的攻击行为。

◆入侵检测相关指标：可靠性、可用性、可扩展性、时效性、准确性、安全性。

入侵检测系统应用

◆入侵检测应用场景类型：上网保护、网站入侵检测与保护、网络攻击阻断、主机/终端恶意代码检测、网络安全监测预警与应急处置、网络安全等级保护。

◆入侵检测系统部署方法：

IDS 部署是指将 IDS 安装在网络系统区域中，使之能够检测到网络中的攻击行为。IDS 部署的基本过程包含以下几个步骤：

第一步，根据组织或公司的安全策略要求，确定 IDS 要监测的对象或保护网段；

第二步，在监测对象或保护网段，安装 IDS 探测器，采集网络入侵检测所需要的信息；

第三步，针对监测对象或保护网段的安全需求，制定相应的检测策略；

第四步，依据检测策略，选用合适的 IDS 结构类型；

第五步，在 IDS 上，配置入侵检测规则；

第六步，测试验证 IDS 的安全策略是否正常执行；

第七步，运行和维护 IDS。

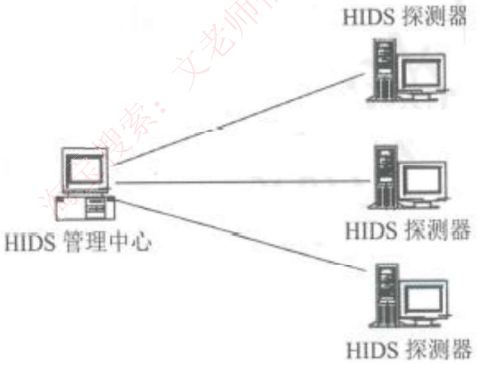
入侵检测系统应用

◆基于HIDS的主机威胁检测：

HIDS 一般用于检测针对单台主机的入侵行为，其主要应用方式如下：

（1）单机应用。在这种应用方式下，把 HIDS 系统直接安装在受监测的主机上即可。

（2）分布式应用。这种应用方式需要安装管理器和多个主机探测器（Sensor）。管理器控制多个主机探测器（Sensor），从而可以远程监控多台主机的安全状况，如图 10-10 所示。

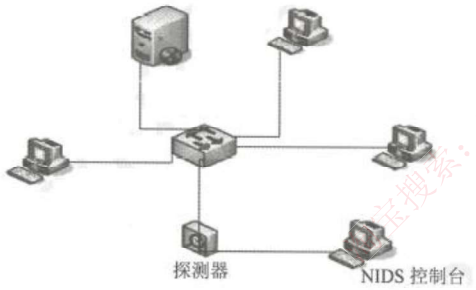


入侵检测系统应用

文老师软考教育

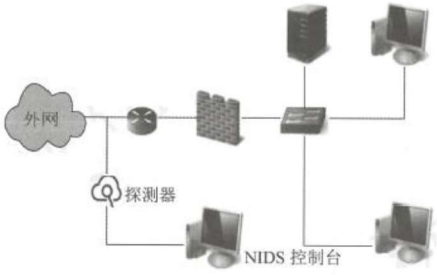
◆基于NIDS的内网威胁检测：

将网络 IDS 的探测器接在内部网的广播式 Hub 或交换机的 Probe 端口，如图 10-11 所示。探测器通过采集内部网络流量数据，然后基于网络流量分析监测内部网的网络活动，从而可以发现内部网络的入侵行为。



◆基于NIDS的网络边界威胁检测：

将 NIDS 的探测器接在网络边界处，采集与内部网进行通信的数据包，然后分析来自外部的入侵行为，如图 10-12 所示。



谢谢！

文老师软考教育