IDS

薛静锋　宁宇鹏　阎　慧　编著

入侵检测技术

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

入侵检测技术

薛静锋　宁宇鹏　阎　慧　编著

机械工业出版社

本书作为国家信息化安全教育认证(ISEC)系列教材中的一本,全面介绍了入侵检测技术,包括入侵检测基础知识,入侵检测系统,入侵检测技术,入侵检测系统的性能指标和评估标准,主要入侵检测系统分析及入侵检测的标准化工作,入侵检测系统的实现,Snort 分析以及入侵检测技术的发展趋势。

本书不仅适合大专院校相关专业作为教材,对从事信息和网络安全方面的管理人员和技术人员也有参考价值。

图书在版编目(CIP)数据

入侵检测技术/薛静锋等编著.—北京:机械工业出版社,2004.4
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14166-0

Ⅰ.入… Ⅱ.薛… Ⅲ.计算机网络—安全技术—资格考核—教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2004)第 019303 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑:李馨馨
责任印制:施 红

北京铭成印刷有限公司印刷·新华书店北京发行所发行

2004 年 4 月第 1 版·第 1 次印刷
787mm × 1092mm $^{1}/_{16}$·11 印张·270 千字
0 001—5 000 册
定价:20.00 元

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
井乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

如今，网络安全问题越来越受到人们的关注，也逐渐成为各相关科研机构研究的热点。传统的网络安全技术以防护为主，即采用以防火墙为主体的安全防护措施。但是，面对网络大规模化和入侵复杂化的发展趋势，以防火墙技术为主的被动防御技术越来越力不从心，由此产生了以入侵检测技术为主的主动保护技术。

入侵检测技术是网络安全的核心技术之一，它通过从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，从而发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象。利用入侵检测技术，不但能够检测到外部攻击，而且能够检测到内部攻击或误操作。但是入侵检测技术毕竟还是一门新技术，还处在不断发展的过程中。本书以国家信息化安全教育认证(ISEC)考试大纲为依据，重点讲解了入侵检测的有关理论知识、技术原理和应用案例。全书包括 8 章内容，第 1 章主要介绍入侵检测的相关基础知识。包括入侵检测的产生与发展历程、入侵检测的基本概念、作用以及研究入侵检测的必要性。第 2 章主要介绍关于入侵检测系统的相关知识。包括入侵检测系统的基本模型、入侵检测系统的工作模式和分类方法、入侵检测系统的数据源以及入侵检测系统的部署方式。第 3 章主要介绍入侵检测技术。包括入侵检测的过程、入侵分析的概念和入侵分析的模型、入侵分析的方法，并且分析了入侵检测中的各种告警与响应方式，此外还对入侵追踪进行了比较详细的介绍。第 4 章介绍入侵检测系统的性能指标和评估标准。包括影响入侵检测性能的参数、评价检测算法性能的测度和评价入侵检测系统性能的标准，在此基础上，介绍了关于网络入侵检测系统的测试评估、测试环境和测试软件，另外还对入侵检测评估现状进行了分析。第 5 章介绍主要的入侵检测系统以及入侵检测的标准化工作。首先对国外主要入侵检测系统进行了介绍和分析；接着对入侵检测的标准化工作进行了详细介绍，主要是 CIDF 的标准化工作和 IDWG 的标准化工作。第 6 章以一个基于 Agent 的分布式入侵检测系统的设计与实现为例，介绍入侵检测系统的实现过程。第 7 章对开放源代码的入侵检测软件 Snort 进行了详细的分析。第 8 章对入侵检测的发展趋势进行了简要分析。分析了入侵检测技术的现状，目前的技术趋势，未来的安全趋势，以及入侵检测的前景。

本书由北京理工大学薛静锋、宁宇鹏、阎慧执笔完成，其中第 1、5、6 章由薛静锋编写，第 4、7、8 章由宁宇鹏编写，第 2、3 章由阎慧编写。本书在写作过程中得到了王勇博士、王伟博士、李志强老师以及北京正阳天马信息技术有限公司刘旸先生、马志谦先生的热情帮助，在此一并表示感谢。

编　者

2004 年 3 月

目　录

第 1 章　入侵检测基础知识

本章导读：

本章主要介绍入侵检测的基础知识。首先介绍了入侵检测的产生与发展，包括入侵检测的早期研究、基于主机与基于网络的入侵检测的研究以及两者的集成；接着介绍了入侵检测的基本概念，包括入侵检测的概念、作用以及研究入侵检测的必要性。

“美国八大著名网站被黑、克林顿总统亲自召集网络安全会议并拨款 20 亿美元”这一消息，使各国政府、IT 厂商和业界同仁在感到震惊的同时，也开始思考网络安全问题，并采取了必要的行动。其实，网络安全的警钟早已鸣响，而且还要警钟长鸣。

根据美国 FBI 的调查，美国每年因为网络安全造成的经济损失超过 170 亿美元。75% 的公司报告财政损失是由于计算机系统的安全问题造成的。但只有 17% 的公司愿意报告黑客入侵，大部分公司由于担心负面影响而不愿声张。在所有的损失中虽然只有 59% 可以定量估算，但每个组织的平均损失已达 40 万美元之多。

对于企业网络来说，入侵的来源可能是企业内部心怀不满的员工、网络入侵者，甚至是竞争对手。攻击者可以窃听网络上的信息，窃取用户的口令、数据库的信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，攻击者可以删除数据库的内容，摧毁网络节点，释放计算机病毒，致使整个企业网络陷入瘫痪。

那么网络在被动保护自己不受侵犯的同时，能否采取某些技术，主动保护自身的安全呢？入侵检测技术就是主动保护自己免受攻击的一种网络安全技术，而入侵检测系统（Intrusion Detection System，IDS）就是能够实施入侵检测的系统。入侵检测技术是网络安全体系的一种防范措施。

1.1　入侵检测的产生与发展

20 世纪 70 年代，随着计算机的速度、数量的增长以及体积的减小，对计算机安全的要求显著增加。面对这样的形势，在 1977 年和 1978 年，美国国家标准局召开了有政府和商业组织代表参加的会议，就当时的安全、审计和控制状况提出报告。

与此同时，军用系统中计算机的使用范围迅速扩大，出于对安全问题的考虑，美国国防部提高了计算机审计的详细程度并以此作为一项安全机制。这个项目由 James Anderson 负责。

1.1.1　早期研究

1980 年，James Anderson 在写给一个保密客户的技术报告中指出，审计记录可以用于识别计算机误用。他提出了入侵尝试（intrusion attempt）或威胁（threat）的概念，并将其定义为：潜在、有预谋且未经授权而访问信息、操作信息，致使系统不可靠或无法使用的企图。同时，他给威胁进行了分类，并对审计子系统提出了改进意见，以使该系统可以检测误用。他认为审计记录分析可

以监视入侵行为，并对入侵进行分类，还提出对不同用户的不同渗透方法。如表 1-1 所示。

表 1-1 不同用户的不同渗透方法

	授 权	非授权
外部用户		外部渗透
内部用户	不当行为	内部渗透

James Anderson 主要工作对象是重要的分级客户，这些客户在主机环境中处理敏感数据，其特点是有严格的安全管理控制。客户有审计所有计算机活动的需求，并由安全部门职员手工检查审计跟踪并调查在审计跟踪中未发现的问题以支持该策略。随着计算量的增加，手工检查和调查工作变得繁重不堪。

James Anderson 在一段时间内致力于解决“伪装者”的问题，“伪装者”指那些用盗窃来的用户名和密码访问系统的人。对系统而言，“伪装者”似乎是合法用户。James Anderson 建议一些针对某些用户行为的统计分析应当具备识别系统不正常使用模式的能力，这是发现“伪装者”的一种方法。

1983 年，SRI(Stanford Research Institute)用统计方法分析 IBM 大型机的 SMF(System Management Facility)记录，这也是早期对入侵检测的研究。

由于 20 世纪 80 年代初期网络还没有像今天这样普遍和复杂，网络之间也没有完全互联，因此关于入侵检测的研究主要是基于主机的事件日志分析。而且由于入侵行为在当时是相当少见的，因此入侵检测在早期并没有受到人们的重视。

1.1.2 主机 IDS 研究

1986 年，SRI 的 Dorothy E.Denning 发表了一篇论文《An Intrusion-Detection Model》，该文深入探讨了入侵检测技术，探索了行为分析的基本机制，首次将入侵检测的概念作为一种计算机系统安全防御措施而提出，并且建立了一个独立于系统、程序应用环境和系统脆弱性的通用入侵检测系统模型，如图 1-1 所示。这篇文章被认为是 IDS 的开山之作，与传统的加密和访问控制相比，IDS 是全新的计算机安全措施。

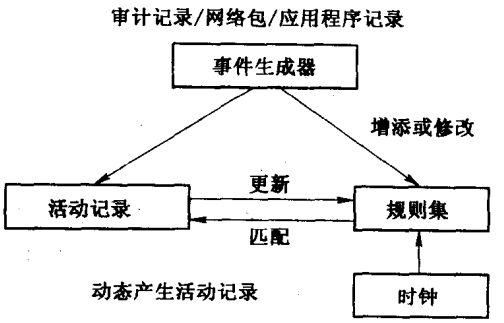

图 1-1 通用入侵检测模型

1988 年，SRI 开始开发 IDES(Intrusion Detection Expert System)原型系统，它是一个实时入侵检测系统。它采用了统计技术来进行异常检测，用专家系统的规则进行误用检测。IDES 在实现双重分析(分析和异常检测)和实时分析两个方面迈出了关键的一步。该系统被认为是

入侵检测研究中最有影响的一个系统，也是第一个在一个应用中运用了统计和基于规则两种技术的系统。

从 1992 年到 1995 年，SRI 对 IDES 在原有基础上加强了优化，在以太网的环境下实现了产品化的 NIDES(Next-Generation Intrusion Detection Expert System)，它具有 IDES 的双重分析特性，采用更为通用、灵活的方法，对于目标系统和审计数据的类型没有限制，采用 C/S 模式。但是在规模化和针对网络环境使用方面还有所欠缺，而且缺少协同工作的能力。由于把用户作为分析的目标(或者说单元)，因此对于多域联合攻击无能为力。

1988 年，针对美国空军计算机系统的多用户环境，Los Alamos 国家实验室的 Tracor Applied Sciences 和 Haystack Laboratories 采用异常检测和基于 Signature 的检测，开发了 Haystack 系统，该系统主要用于检测 Unisys 大型主机。与以往的系统不同，该系统建立了两个模型：为每个用户建立的用户模型和通用用户模型。

同时，出现了为美国国家计算机安全中心 Multics 主机开发的多入侵检测及告警系统(Multics Intrusion Detection and Alerting System，MIDAS)，该系统是在国家计算机安全中心的公共信息系统 Dockmaster 上应用的第一个入侵检测系统。

1989 年，Los Alamos 国家实验室的 Hank Vaccaro 为国家计算机安全中心(National Computer Security Center，NCSC)和能源部(Department of Energy，DOE)开发了 W&S (Widsom and Sence)系统，这是一个基于主机的异常检测系统。W&S 处理一个训练用的数据集，并产生用于描述数据特征的元规则(metarule)，随后当系统应用于新的数据集时，该系统就用这些规则检测异常。W&S 最初被设计用于检测存储核材料的数据记录中的异常，后来被修改为检测 VMS 操作系统的审计记录，以及检测人为的误操作。由于检测到的异常和人为的误操作混合在一起，所以 W&S 永远都不能应用于生产环境中，因为构造、修剪元规则树的方式使得很难解释得到的结果。

同年，PRC(Planning Research Corporation)公司开发了 ISOA(Information Security Officers Assistant)，它由一套统计工具、一个专家系统和一套分级的“利害关系级别(concern levels)”组成。其技术基于一种称为迹象与警告(Indications and Warnings，I&W)的模型，应用该模型可以对即将发生的攻击预先告警。引入的审计数据与一组期望的迹象相比较，并按层次排列以反映利害关系级别。异常是用三类参数来检测的：用户、节点及整个系统。ISOA 后来用在了 PRC 入侵检测系统 PreCis 中。

以上研究虽然有的是在局域网环境下展开的，但是仍然是检测对主机的攻击，对于协同攻击和多域联合攻击没有检测的能力。另外，这方面的研究仍未停止，2001 年 10 月 23 日，SRI 发布了 eXpert-BSMTM for Solaris Version 1.4，据称是当时最先进的基于主机的 IDS。具有可升级、强大的事件分析能力、通用性能好，以及可插的组件等特性。

1.1.3　网络 IDS 研究

1990 年出现的网络安全监视器(Network Security Monitor，NSM)，是 UCD(Carlifornia 大学的 Davis 分校)设计的面向局域网的 IDS，NSM 被设计用来分析来自以太局域网的数据及连接到该网的数据。这个系统的重要贡献是首次使用网络数据包作为审计数据源，提出基于网络的 IDS 的概念。1991 年，NADIR(Network Anomaly Detection and Intrusion Reporter)与

DIDS(Distribute Intrusion Detection System)提出收集和合并来自多个主机的审计信息,来检测针对多个主机的协同攻击。需要指出的是,网络 IDS 的研究方法有两种:一是分析各主机的审计数据,并分析各主机审计数据之间的关系;二是分析网络数据包。

1994 年,美国空军密码支持中心(Cryptological Support Center)的一群研究人员创建了一个健壮的网络入侵检测系统 ASIM,该系统被广泛应用于美国空军,为了将网络入侵检测技术商业化,他们成立了一个商业公司 Wheelgroup。

1996 年,UCD(Carlifornia 大学的 Davis 分校)的计算机安全(Computer Security)实验室,以开发广域网上的入侵检测系统为目的,开发了 GrIDS。目标是使受保护的网络规模达到成千上万,甚至上百万,并且还保护路由器、域名服务器等。

1997 年,Cisco 公司兼并了 Wheelgroup,并开始将网络入侵检测整合到 Cisco 路由器中。同时,Internet 安全系统公司(ISS)发布了 RealSecure,这是一个被广泛使用的、用于 Windows NT 的网络入侵检测系统。从此,网络入侵检测革命的序幕被拉开了。

从 1996 年到 1999 年,SRI 开始 EMERALD(Event Monitoring Enabling Response to Anomalous Live Disturbances)的研究,它是 NIDES 的后继者,具有分布式可升级的特点,用于在大型网络中探测恶意入侵活动(包括对网站的入侵),高度分布,自动响应。并在以下几方面进行了扩展:可以进行基于网络的分析;增强互操作性;使分布式计算环境的集成更容易。根据 SRI 给出的报告,在 1999 年,美国政府发起的网络安全检测系统竞赛上,EMERALD 在 8 项性能测试中有 7 项位列榜首。

1.1.4 主机和网络入侵检测的集成

1990 年以前,大部分入侵检测系统都是基于主机的,它们对于活动性的检查局限于操作系统审计数据及其他以主机为中心的信息源。在 1.1.3 中提到,1990 年出现的 NSM 是面向局域网的 IDS,它把入侵检测扩展到了网络环境中。此时,由于 Internet 的发展及通信和网络带宽的增加,系统的互联性已经有了显著提高,导致人们对计算机安全的关注程度也显著增加。1988 年的 Internet 蠕虫事件使人们对计算机安全的关注达到了令人激动的程度,同时增加了对商业界和学术界的研究资助。分布式入侵检测系统(DIDS)最早试图把基于主机的方法和网络监视方法集成在一起。

DIDS 的开发是一个大规模的合作开发,参与方有美国空军密码支持中心、lawrence、Livermor 国家实验室、加利福尼亚大学 Davis 分校和 Haystack 实验室。这项研究由美国空军、国家安全部和国家能源部资助。它是将主机入侵检测和网络入侵检测的能力集成的第一次尝试,以便于一个集中式的安全管理小组能够跟踪安全侵犯和网络间的入侵。

DIDS 的最初概念是采用集中式控制技术,向 DIDS 中心控制器发送报告。DIDS 的结构如图 1-2 所示。

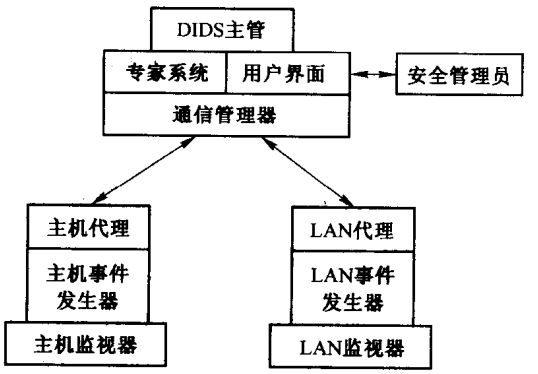

图 1-2 DIDS 结构

DIDS 解决了在大型网络互联中的一个棘手问题，即在网络环境下跟踪网络用户和文件。该项功能非常关键，这是因为：第一，网络入侵者通常会利用不同计算机系统的互联性来隐藏自己的真实身份和地址。实际上，一些入侵者发起的分布式攻击是在每个阶段从不同系统发起攻击的组合结果。第二，对付网络攻击的最有效的方法是发现对攻击负责的人，收集他进行攻击的证据，然后借助执法力量和法律过程来起诉他。系统允许用户在该环境中通过自动跨越被监视的网络跟踪和得到用户身份的相关信息来处理这个问题。DIDS 是第一个具有这个能力的入侵检测系统。

例如，假设攻击者通过“网络跳板”穿越系统，通过一个路由攻击受 DIDS 保护的支付服务器。DIDS 可以通过跟踪攻击者的身份，发现攻击路径节点上的各个用户的身份，例如是主机 1 上的 A、主机 2 上的 B 和主机 3 上的 C。此时，根据 DIDS 的结果，就可以派出调查员调查实际上坐在主机 1 的和 A 相关的终端前的那个人。

DIDS 解决的另一个问题是如何从发生在系统不同抽象层次的事件中发现相关数据或事件。这类信息要求要理解它们对整个网络的影响，DIDS 用一个 6 层的入侵检测模型提取数据相关性，每层代表了对数据的一次变换结果。

此外，还有许多系统，在此不一一赘述了。这些系统的分类如表 1-2 所示。

表 1-2　IDS 简单分类

异　常	自学习	非时间序列	规则模型	W&S
			基于统计	IDES, NIDES, EMERALD, Haystack
		时间序列	ANN	Haperview
	预编程的	描述统计	简单统计	MIDAS, NADIR, Haystack
			基于规则	NSM
			门限	ComputerWatch
		Default deny	状态序列模式	DPEM, JANUS, Bro
特征	预编程的	状态模式	状态转换	USTAT
			Petri 网	IDIOT
		专家系统	NIDES, EMERALD, MIDAS-direct, DIDS, MIDAS	
		字符串匹配	NSM	
		基于规则	NADIR, ASAX, Bro, Haystack	
自动特征	自学习	自动特征选取	Ripper	

1.2　入侵检测的基本概念

上节介绍了入侵检测的诞生及其大致的发展历程，为了使读者对入侵检测有一个清晰的了解，本节将介绍入侵检测的一些基本概念，包括入侵检测的概念、作用以及研究入侵检测的

必要性。

1.2.1 入侵检测的概念

入侵,是指任何试图危及计算机资源的完整性、机密性或可用性的行为。而入侵检测是对入侵行为的发觉。它通过从计算机网络或系统中的若干关键点收集信息,并对这些信息进行分析,从而发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统(简称 IDS)。入侵检测是防火墙的合理补充,帮助系统对付网络攻击,它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。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测,从而提供对内部攻击、外部攻击和误操作的实时保护。

网络入侵检测系统(IDS)是一项很新的网络安全技术,目前已经受到各界的广泛关注,它的出现是对原有安全系统的一个重要补充。入侵检测系统收集计算机系统和网络的信息,并对这些信息加以分析,对保护的系统进行安全审计、监控、攻击识别并作出实时的反应。

1.2.2 入侵检测的作用

形象地说,入侵检测系统就是网络摄像机,能够捕获并记录网络上的所有数据,同时它也是智能摄像机,能够分析网络数据并提炼出可疑的、异常的网络数据,它还是 X 光摄像机,能够穿透一些巧妙的伪装,抓住实际的内容。此外,它还是保安员的摄像机,能够对入侵行为自动地进行反击,如阻断连接。

在网络安全体系中,入侵检测系统是惟一一个通过数据和行为模式判断其是否有效的系统,如图 1-3 所示,防火墙就像一道门,可以阻止一类人群的进入,但无法阻止同一类人群中的破坏分子,也不能阻止内部的破坏分子;访问控制系统可以不让低级权限的人做越权工作,但无法保证高级权限的人做破坏工作,也无法阻止低级权限的人通过非法行为获得高级权限;漏洞扫描系统可以发现系统和网络存在的漏洞,但无法对系统进行实时扫描。

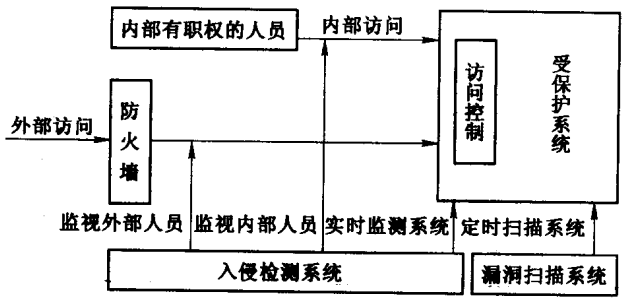

图 1-3 入侵检测的作用

入侵检测系统的作用和功能如下:

- 监控、分析用户和系统的活动。
- 审计系统的配置和弱点。