高等学校信息安全系列教材

入侵检测技术

李 剑 编著
曹元大 审

高等教育出版社
Higher Education Press

人像色调技术

高等学校信息安全系列教材

入侵检测技术

李 剑 编著
曹元大 审

高等教育出版社
Higher Education Press

内容提要

本书作为信息安全系列教材，全面系统地介绍了信息安全领域主要内容之一的入侵检测技术。全书内容共分为14章，分别介绍了入侵检测概述、常见的入侵方法与手段、入侵检测系统模型、误用与异常入侵检测系统、模式串匹配与入侵检测、基于主机的入侵检测系统、基于网络的入侵检测系统、典型的入侵检测技术、基于主体的分布式的入侵检测系统、入侵检测系统的相关标准与评估、典型的入侵检测系统、典型的入侵检测产品、使用Snort进行入侵检测以及入侵检测技术的发展。附录A列出了常用入侵检测术语及其释义；附录B是一个实验，介绍如何在Windows下使用Snort来配置一个网络入侵检测系统。

本书可以作为大学本科相关专业的教材，也可以作为计算机、通信、信息安全等领域研究人员和技术开发人员的参考书。

图书在版编目(CIP)数据

入侵检测技术/李剑编著.—北京：高等教育出版社，2008.6

ISBN 978-7-04-024267-6

Ⅰ.入… Ⅱ.李… Ⅲ.信息系统-安全技术-教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2008)第067976号

策划编辑 武林晓 **责任编辑** 郭福生 **封面设计** 于文燕 **责任绘图** 朱 静
版式设计 张 岚 **责任校对** 刘 莉 **责任印制** 毛斯璐

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京北苑印刷有限责任公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2008年6月第1版
印 张	15.5	**印 次**	2008年6月第1次印刷
字 数	340 000	**定 价**	19.70元

物料号 24267-00

前　言

由于计算机病毒的泛滥，全世界平均不到20分钟就会产生一个新的病毒。这些病毒通过Internet传向世界各个角落，这意味着连入Internet的计算机平均每20分钟就有可能被感染一次计算机病毒。据统计，在我国企事业单位的网络系统中，有90%的计算机都曾受到过病毒的感染。60%以上的计算机都曾因病毒而丢失过文件、数据等。1998年到2003年，各种信息安全事件增加了大约33倍。在这种情况下，网络与信息的安全问题就越来越引起人们的注意，研究信息安全的防御技术就显得非常重要了。

传统的网络安全技术以被动防护为主，通常采用以防火墙为主的防护措施。但是面对网络的大规模化、入侵的复杂化及内网的安全等问题，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防护技术。

作为网络与信息安全领域的一项重要技术，入侵检测是整个信息安全防护体系的重要组成部分。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，并对这些信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，从而对这些攻击采取相应的措施。利用入侵检测技术，不但能检测到外部攻击，还能检测到内部攻击或误操作，这一点防火墙是做不到的。

作为信息安全专业的本科阶段的教材，本书详细地介绍了入侵检测领域的理论与应用。全书共分14章。第1章，“入侵检测概述”，介绍入侵检测的定义、历史与作用，入侵检测在信息安全中的地位，入侵检测系统的基本原理与工作模式，入侵检测的分类，常用的入侵检测方法等。第2章，“常见的入侵方法与手段”，介绍攻击的概念、攻击的一般流程、典型的攻击技术与方法等。第3章，“入侵检测系统模型”，介绍入侵检测信息收集、信息分析、报警与响应等。第4章，“误用与异常入侵检测系统”，介绍误用入侵检测技术与异常入侵检测技术。第5章，“模式串匹配与入侵检测”，介绍串匹配算法、串匹配技术在入侵检测中的应用、精确模式串匹配算法、不同串匹配算法的性能对比及串匹配算法的一些改进等。第6章，“基于主机的入侵检测系统”，介绍基于主机的入侵检测信息源的获取、基于主机的入侵检测分析方法、基于主机的入侵检测的优缺点等。第7章，“基于网络的入侵检测系统”，介绍基于网络的入侵检测信息源、基于网络的入侵检测技术、基于主机的入侵检测优缺点等。第8章，“典型的入侵检测技术”，介绍基于神经网络的入侵检测系统模型、基于遗传算法的入侵检测技术、基于数据挖掘的入侵检测技术、基于数据融合的入侵检测技术、基于免疫的入侵检测技术及基于协议分析的入侵检测技术等。第9章，“基于主体的分布式入侵检测系统”，介绍基于主体的分布式入侵检测系统的结构、系统中主体的实现技术、主体之间的通信以及系统实现中的一些问题等。第10章，“入侵检测系统的相关

标准与评估”,介绍入侵检测系统的标准化工作、入侵检测系统的性能指标、入侵检测系统的测试与评估等。第 11 章,“典型的入侵检测系统”,介绍世界上已经有的一些典型的入侵检测系统,包括 DIDS、CSM、EMERALD、AAFID、NetSTAT、GrIDS、IDA、MAIDS 等,并对这些系统做了评价与分析。第 12 章,“典型的入侵检测产品”,介绍思科公司的 NetRanger、Network Associates 公司的 CyberCop、安氏公司的 LinkTrust、Enterasys Networks 公司的 Dragon Sensor、启明星辰公司的“天阗”、中科网威公司的“天眼”、中联绿盟公司的“冰之眼”等入侵检测系统,并介绍了如何选购入侵检测产品。第 13 章,“使用 Snort 进行入侵检测”,介绍 Snort 的工作模式、特点、结构及规则等。第 14 章,“入侵检测技术的发展”,介绍现有入侵检测系统的局限性、入侵检测技术的发展方向及 IPS 和 IMS 等技术。附录 A 列出了常用入侵检测术语及其释义。附录 B 是一个实验,介绍如何在 Windows 下使用 Snort 来配置一个网络入侵检测系统。

与其他入侵检测技术教材相比,本书具有如下特点:

- 图文并茂,内容丰富,适合于本科阶段的教学。
- 全面介绍了入侵检测系统中所用到的关键技术——串匹配算法。
- 全面介绍了世界上已经有的先进入侵检测系统。
- 本书附录中提供了一个 Snort 入侵检测实验,可以配合课堂教学使用。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授、徐国爱副教授、张茹副教授、崔宝江副教授、谷利泽副教授、李辉副教授、周亚健博士、马兆峰博士、辛阳博士、郑康峰博士、李丽香博士、杨榆博士、张淼博士、黄正权博士、郑世慧博士、王励成博士等,他们对本书的出版提出了宝贵的意见和建议。感谢我的博士导师北京理工大学的曹元大教授,曹教授对于本书的出版给予了极大的支持与帮助。

感谢中国电信北京研究院的赵阳博士、中国移动通信公司的冯运波博士、西门子(中国)有限公司的李明柱博士、中国科学院计算技术研究所的谭建龙博士、北京交通大学的姚正林博士,他们对本书的出版给予了很大的支持。其他参与本书审阅编写等工作的还有景博、白小梅、景绍达、李胜斌、陈彦侠、益德全、李美丽等,这里一并感谢!

本教材也是国家信息产业部重点软课题项目“基于互联网内容安全的关键问题研究”(课题编号:2007 - R - 103)资助的成果。

由于本书作者水平有限,书中疏漏与错误之处在所难免,恳请广大同行和读者批评指正,作者在下一版中改正。

作者的电子邮件地址:lijian@ bupt. edu. cn,电话:(010)86212346。

李 剑

北京邮电大学信息安全中心

目　录

第 1 章　入侵检测概述

入侵检测是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。它监视计算机系统或网络中发生的事件，并对它们进行分析，以寻找危及机密性、完整性、可用性或绕过安全机制的入侵行为。本章将概括介绍入侵检测系统。

1.1　入侵检测简介

1.1.1　入侵的定义

Internet 是全球信息共享的基础设施，是一种开放的、面向所有用户的技术。一方面要保证信息共享的方便与快捷，另一方面要防止垃圾信息与恶意信息的泛滥。

根据中国互联网络信息中心（China Internet Network Information Center，CNNIC）在 2007 年 1 月的第 19 次中国互联网络发展状况统计报告统计，中国网民总人数为 13 700 万人。这其中仅有 8.4% 的网民对于网络内容的健康性非常满意。也就是说有 91.6% 的中国网民（12 550 万人）都或多或少的对于网络的健康性不满意。网上的入侵事件时有发生。

图 1.1 中所示为美国计算机紧急事件响应小组协调中心（Computer Emergency Response Team/Coordination Center，CERT/CC）统计到的近年来信息安全事件分析，1998 年到 2003 年安全事件增加了约 33 倍（1998 年为 3 734 次，2003 年为 127 529 次）。

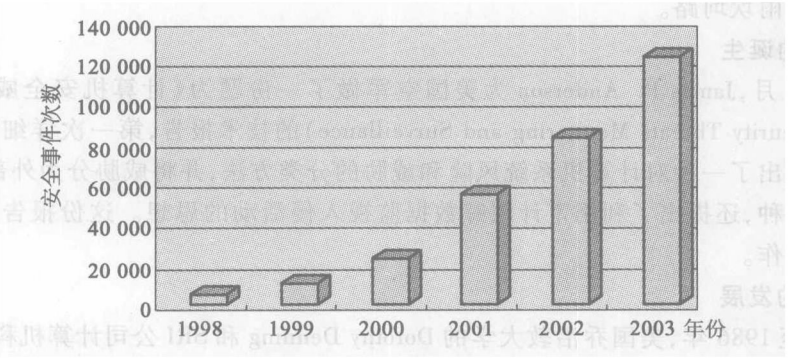

图 1.1　网络入侵事件发展趋势

那么,什么是入侵(intrusion)呢? James P. Anderson 在 1980 年给出了入侵的定义:入侵是指在非授权的情况下,试图存取信息、处理信息或破坏系统以使系统不可靠、不可用的故意行为。

本书中的入侵是个广义的概念,不仅包括发起攻击的人(如恶意的黑客)取得超出合法范围的系统控制权的行为,也包括收集漏洞信息、造成拒绝服务(denial of service)等对计算机系统造成危害的行为。

网络入侵通常是指利用熟练的编写和调试计算机程序的技巧,侵入组织内部网络,来获得非法或未授权的网络或文件访问的行为。早先对计算机的非授权访问称为"破解"(cracking),而 hacking(俗称"黑")则是指那些熟练运用计算机的高手对计算机技术的运用,这些计算机高手称为"黑客"(hacker)。随着个人计算机及网络的出现,"黑客"变成一个贬义词,通常是指那些非法入侵他人计算机的人。

1.1.2 入侵检测的概念

入侵检测(intrusion detection),顾名思义,就是对入侵行为的发觉。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,从中发现网络或系统中是否有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称为入侵检测系统(Intrusion Detection System,IDS)。与其他安全产品不同的是,入侵检测系统需要更多的智能,它必须能够将得到的数据进行分析,并得出有用的结果。一个合格的入侵检测系统能大大地简化了管理员的工作,保证网络的安全运行。

1.1.3 入侵检测的发展历史

从实验室原型研究到推出商业化产品、走向市场并获得广泛认同,入侵检测系统已经走过了二十多年的风雨坎坷路。

1. 概念的诞生

1980 年 4 月,James P. Anderson 为美国空军做了一份题为《计算机安全威胁监控与监视》(Computer Security Threats Monitoring and Surveillance)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 3 种,还提出了利用审计跟踪数据监视入侵活动的思想。这份报告被公认为是入侵检测的开山之作。

2. 模型的发展

1984 年至 1986 年,美国乔治敦大学的 Dorothy Denning 和 SRI 公司计算机科学实验室(CSL)的 Peter Neumann 研究出一种实时入侵检测系统模型,取名为入侵检测专家系统(Intrusion Detection Expert System,IDES)。该模型由 6 个部分组成:主体、对象、审计记录、轮廓特征、异常记录和

活动规则。它独立于特定的系统平台、应用环境、系统弱点及入侵类型，为构建入侵检测系统提供了一个通用的框架。

1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，并成功开发出一个 IDES。该系统包括一个异常检测器和一个专家系统，分别用于统计异常模型的建立和基于规则的特征分析检测，如图 1.2 所示。

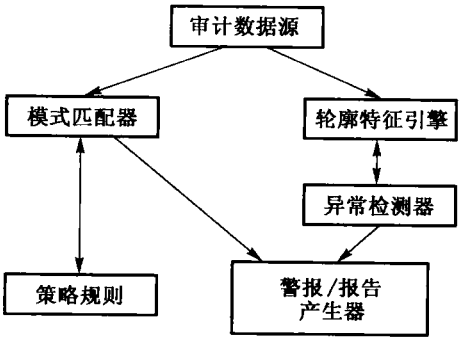

图 1.2 入侵检测专家系统(IDES)模型

3. 百花齐放的春天

1990 年是入侵检测系统发展史上的一个分水岭。这一年，加州大学戴维斯分校的 L. T. Heberlein 等人开发出了网络安全监视器(Network Security Monitor，NSM)。该系统第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机。从此之后，入侵检测系统发展史翻开了新的一页，基于网络的入侵检测系统和基于主机的入侵检测系统两大阵营正式形成。

1988 年的莫里斯蠕虫事件发生之后，网络安全才真正引起了军方、学术界和企业的高度重视。美国空军、国家安全局和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室，开展对分布式入侵检测系统(Distrubuted Intrusion Detection System，DIDS)的研究，将基于主机和基于网络的检测方法集成到一起，其总体结构如图 1.3 所示。

DIDS 是入侵检测系统历史上的一个里程碑式的产品，它的检测模型采用了分层结构，包括数据、事件、主体、上下文、威胁、安全状态等 6 层。

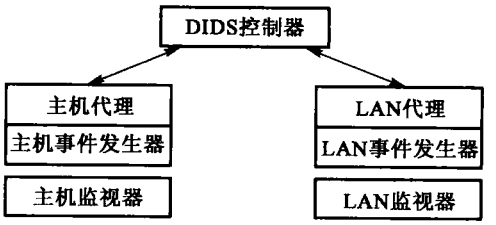

图 1.3 分布式入侵检测系统(DIDS)的结构

从20世纪90年代到现在,入侵检测系统的研发呈现出百家争鸣的繁荣局面,并在智能化和分布式两个方向取得了长足的进展。目前,SRI/CSL、普渡大学、加州大学戴维斯分校、洛斯阿拉莫斯国家实验室、哥伦比亚大学、新墨西哥大学等机构在这些方面的研究代表了当前的最高水平。

1.1.4 入侵检测系统的作用

入侵检测系统作为一种积极主动的安全防护工具,提供了对内部攻击、外部攻击和误操作的实时防护,在计算机网络和系统受到危害之前进行报警、拦截和响应。它具有以下主要作用。

① 通过检测和记录网络中的安全违规行为,惩罚网络犯罪,防止网络入侵事件的发生。

② 检测其他安全措施未能阻止的攻击或安全违规行为。

③ 检测黑客在攻击前的探测行为,预先给管理员发出警报。

④ 报告计算机系统或网络中存在的安全威胁。

⑤ 提供有关攻击的信息,帮助管理员诊断网络中存在的安全弱点,利于其进行修补。

⑥ 在大型、复杂的计算机网络中布置入侵检测系统,可以显著提高网络安全管理的质量。

1.2 入侵检测系统在信息安全中的地位

1.2.1 P^2DR^2 安全模型与入侵检测系统的关系

目前,普遍采用动态网络安全理论来确保网络系统的安全,这种理论就是基于 P^2DR^2 安全模型的动态信息安全理论。P^2DR^2 模型是在整体的安全策略(Policy)的控制和指导下,在综合运用防护工具(Protection,如防火墙、操作系统身份验证、加密等手段)的同时,利用检测工具(Detection,如漏洞评估、入侵检测等系统)了解和评估系统的安全状态,通过适当的响应(Response)将系统调整到"最安全"和"风险最低"的状态。防护、检测和响应组成了一个完整的、动态的安全循环,如图1.4所示。

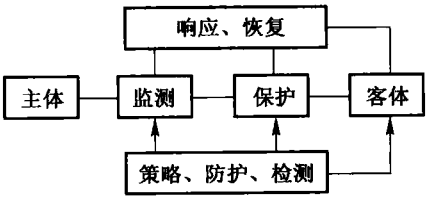

图1.4 P^2DR^2 动态安全模型

根据这个模型,我们可以建立主动的、纵深的动态防御体系,这个体系应包括:建立以入侵检测为核心的安全体系结构;综合采用先进技术和产品构造动态防御体系,包括漏洞扫描系统、防火墙、安全审计等安全技术和产品;建立有效的应急响应机制。

P^2DR^2 的动态信息安全理论模型在1995年开始逐渐形成并得到了迅速发展,学术界先后提

出了 PDR、P^2DR 等多种动态风险模型。随着 Internet 技术的飞速发展，企业网的应用环境千变万化，现有模型存在诸多待发展之处。

一个良好的网络安全模型应在充分了解网络系统安全需求的基础上，通过安全模型表达安全体系架构，通常应具备以下性质：精确、无歧义、简单和抽象，具有一般性，充分体现安全策略。

该理论认为，信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为，还是响应行为等，都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间 t_P；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间——检测时间 t_D；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间——响应时间 t_R。

P^2DR^2 模型可以用一些典型的数学公式来表达安全的要求。

$$t_P > t_D + t_R \tag{1}$$

t_P 代表系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所需花费的时间。t_D 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。t_R 代表从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。针对需要安全保护的目标，如果公式（1）成立，即防护时间大于检测时间加上响应时间，那么在入侵者危害安全目标之前就能被检测到并及时采取防护措施。

$$t_E = t_D + t_R，\text{如果 } t_P = 0 \tag{2}$$

公式的前提是假设防护时间 $t_P = 0$。t_D 代表从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。t_R 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对 Web 服务器被破坏的页面进行恢复。那么，t_D 与 t_R 的和就是该安全目标系统的暴露时间 t_E。针对于需要保护的安全目标，t_E 越小系统就越安全。

通过上面两个公式的描述，实际上给出了“安全”的全新定义：“及时的检测和响应就是安全”，“及时的检测和恢复就是安全”。而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 t_P，降低检测时间 t_D 和响应时间 t_R。

由此安全模型可以看出，入侵检测系统在 P^2DR^2 系统中占有很重要的地位，是该模型的核心。

1.2.2 传统安全技术的局限性

传统的安全技术有许多，如密码技术、防火墙技术、访问控制技术等。但是这些技术都是被动的防御技术，不能主动发现入侵。下面以防火墙为例来介绍传统安全技术的局限性。

防火墙是阻止黑客攻击的一种有效手段，但随着攻击技术的发展，这种单一的防护手段已不能确保网络的安全，它存在以下的弱点和不足。

（1）防火墙无法阻止内部人员所做的攻击

防火墙保护的是网络边界安全,对在网络内部所发生的攻击行为无能为力,而据调查,网络攻击事件有80%以上是由内部人员所为。

(2) 防火墙对信息流的控制缺乏灵活性

防火墙是依据管理员定义的过滤规则对进出网络的信息流进行过滤和控制的。如果规则定义过于严格,则限制了网络的互连互通;如果规则定义过于宽松,则又带来了安全隐患。防火墙自身无法根据情况的变化进行自动调整。

(3) 在攻击发生后,利用防火墙保存的信息难以调查和取证

在攻击发生后,能够进行调查和取证,将罪犯绳之以法,是威慑网络罪犯、确保网络秩序的重要手段。防火墙由于自身的功能所限,难以识别复杂的网络攻击并保存相关的证据信息。

为了确保计算机网络的安全,必须建立一整套的安全防护体系,进行多层次、多手段的检测和防护。入侵检测系统就是安全防护体系中重要的一环,它能够及时识别网络中发生的入侵行为并实时报警。需要说明的是,虽然目前很多防火墙都集成有入侵检测模块,但由于技术和性能上的限制,它们通常只能检测少数几种简单的攻击,无法与专业的入侵检测系统相比。专业入侵检测系统所具有的实时性、动态检测和主动防御等特点,弥补了防火墙等静态防御工具的不足。

入侵检测系统是对防火墙的有益补充。入侵检测系统能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。在入侵攻击之后,能收集入侵攻击的相关信息,作为防范系统的知识添加到知识库中,增强系统的防范能力,避免系统再次受到入侵。入侵检测系统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防护,大大提高了网络的安全性。

对防火墙和入侵检测系统的关系有一个经典的比喻。防火墙相当于一个把门的门卫,对于所有进出大门的人员进行审核:只有符合安全要求的人,即那些有出入许可证的人才可以进、出大门;门卫可以防止小偷进入大楼,但不能保证小偷100%地被拒之门外,而且对于那些本身就在大门内部的以及那些有出入许可证的、以合法身份进入了大门的人,则无法监控,这时候就需要依靠入侵检测系统来进行审计和控制,发现异常情况并发出警报。入侵检测系统能在系统遭受攻击入侵的时候检测到攻击,并利用警报通知系统管理员,或者在攻击已经发生的情况下与其他防护系统合作来驱逐入侵攻击。

1.3 入侵检测系统的基本原理与工作模式

1.3.1 入侵检测系统的基本原理

入侵检测系统(Intrusion Detection System,IDS)的基本原理如图1.5所示。主要分为4个阶