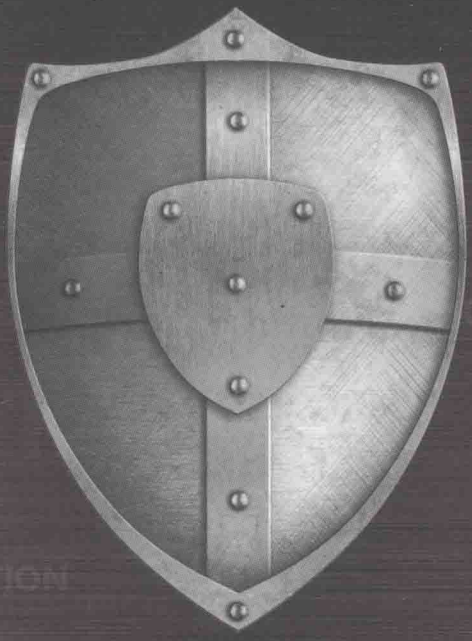
普通高等教育“十一五”国家级规划教材

21世纪高等教育信息安全系列规划教材



入侵检测技术

（第2版）

薛静锋 祝烈煌◎主编

单纯 徐美芳 杨顺民◎副主编

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

21世纪高等教育信息安全系列规划教材

入侵检测技术

（第2版）

薛静锋　祝烈煌　主编

单　纯　徐美芳　杨顺民　副主编

人民邮电出版社

北京

图书在版编目（CIP）数据

入侵检测技术 / 薛静锋，祝烈煌主编. -- 2版. -- 北京 : 人民邮电出版社，2016.1
21世纪高等教育信息安全系列规划教材
ISBN 978-7-115-38908-4

Ⅰ. ①入… Ⅱ. ①薛… ②祝… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第186576号

内 容 提 要

本书全面、系统地介绍了入侵检测的基本概念、基本原理和检测流程，较为详尽地讲述了基于主机的入侵检测技术、基于网络的入侵检测技术、基于存储的入侵检测技术和基于 Hadoop 海量日志的入侵检测技术。在此基础上，本书还介绍了入侵检测系统的标准与评估，并以开源软件 Snort 为例对入侵检测的应用进行了分析。

本书语言通俗，层次分明，理论与实例结合，可以作为高等学校计算机相关专业或信息安全专业本科生高年级的选修课教材，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。

◆ 主　　编　薛静锋　祝烈煌
副 主 编　单　纯　徐美芳　杨顺民
责任编辑　邹文波
责任印制　沈　蓉　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市潮河印业有限公司印刷
◆ 开本：787×1092
印张：14.75　　2016 年 1 月第 2 版
字数：353 千字　　2016 年 1 月河北第 1 次印刷

定价：39.00 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

21世纪高等教育信息安全系列规划教材

编　委　会

主　任：　方滨兴（院士）

副主任：　贾　焰　　马建峰　　李凤华　　杨义先　　张立科

编　委：　马春光　　王丽娜　　王良民　　朱建明　　许　进

孙东红　　李舟军　　李　晖　　李建华　　李欲晓

吴晓平　　邹文波　　邹德清　　张小松　　张红旗

张宏莉　　陈晓桦　　封化民　　胡昌振　　俞能海

姚志强　　翁　健　　谢冬青

第 2 版前言

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。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合性学科。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防御技术显得越来越力不从心，由此产生了入侵检测技术。

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。本书全面介绍了入侵检测技术，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。全书共 9 章，主要内容介绍如下。

第 1 章主要介绍了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和作用、研究入侵检测的必要性以及入侵检测面临的问题和入侵检测技术的发展趋势。

第 2 章主要介绍了常见的入侵方法与手段，包括黑客的入侵模型与原理，以及几种常见的入侵攻击方法。本章的目的是让读者了解黑客入侵的典型方式，这样才有助于部署入侵检测相关设备和工具，查找攻击源，阻击黑客。

第 3 章主要介绍了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以及入侵检测系统的部署方式。本章可以让读者了解入侵检测系统的基本轮廓。

第 4 章主要介绍了入侵检测的基本流程，包括入侵检测的过程、入侵检测的数据源、入侵检测的分析模型和方法以及入侵检测的告警与响应方式。本章可以让读者掌握入侵检测的全过程。

第 5 章主要介绍了基于主机的入侵检测技术，包括审计数据的获取和预处理、各种基于主机的入侵检测方法以及基于主机的入侵检测实例。

第 6 章主要介绍了基于网络的入侵检测技术，包括网络数据包的捕获、检测引擎的设计以及基于网络的入侵检测实例。

第 7 章主要介绍了基于存储的入侵检测技术，包括主动存储设备和块存储设备的数据存取过程以及存储级入侵检测的研究框架，在此基础上介绍了基于数据挖掘的攻击模式自动生成和存储级异常检测方法，并对 IDS 间基于协作的联合防御方法进行了介绍。

第 8 章主要介绍了基于 Hadoop 海量日志的入侵检测技术，主要包括 Hadoop 相关技术、基于 Hadoop 海量日志的入侵检测算法以及基于 Hadoop 海量日志的入侵检测系统的实现。

此为试读，需要完整PDF请访问：www.ertongbook.com

第9章主要介绍了入侵检测系统的标准与评估，包括入侵检测的标准化工作、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。

本书可以作为高等学校计算机相关专业或信息安全专业本科生高年级的选修课教材，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。阅读本书时，读者应学习过计算机网络、操作系统、信息安全基础等方面的基础知识。本书作为教材使用时，建议课时为32学时，各章学时分配如下。

章	学时数	章	学时数
第1章	2	第6章	4
第2章	3	第7章	4
第3章	3	第8章	4
第4章	5	第9章	3
第5章	4		

本书由薛静锋、祝烈煌担任主编，单纯、徐美芳、杨顺民担任副主编。本书在写作过程中得到了北京理工大学王勇副教授以及硕士研究生束罡、张珊珊的热情帮助，在此一并表示感谢。

由于编者水平有限，书中难免存在不足之处，敬请广大读者批评指正。

编者

2015年7月

于北京理工大学

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

▶▶▶ 第 1 章

入侵检测概述

1.1 网络安全基本概念

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合性学科。本节介绍网络安全的基本概念。

1.1.1 网络安全的实质

计算机网络安全问题是随着网络、特别是 Internet 的发展而产生的，目前已经受到普遍关注。计算机网络的连通性和开放性给资源共享和通信带来了很大的便利，但同时也使本不乐观的安全问题雪上加霜。标准化和开放性使许多厂商的产品可以互操作，也使入侵者可以预知系统的行为。

尽管网络安全研究得到越来越多的关注，然而，网络安全问题并没有因此而减少。相反，随着网络规模的飞速扩大、结构的日益复杂和应用领域的不断扩展，出于各种目的，盗用资源、窃取机密、破坏网络的肇事者也越来越多，网络安全事件数量呈迅速增长的趋势，造成的损失也越来越大。

一般认为，计算机网络系统的安全威胁主要来自于黑客（Hacker）的攻击、计算机病毒（Virus）感染和拒绝服务攻击（Denies Of Service，DOS）3 个方面。目前，人们已经开始重视来自网络内部的攻击。黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以针对系统为主的攻击转变到以针对网络为主的攻击。而且随着攻击工具的完善，攻击者不需要专业知识就能够完成复杂的攻击过程。

总之，人们面临的来自计算机网络系统的安全威胁日益严重。安全问题已经成为影响网络发展，特别是商业应用的主要问题，并直接威胁着国家和社会的安全。

网络安全的实质就是要保障系统中的人、设备、设施、软件、数据以及各种供给品等要素免受各种偶然的或人为的破坏或攻击，使它们功能正常，保障系统能安全可靠地工作。因而网络系统的安全应当包含以下内容。

（1）要弄清网络系统受到的威胁及脆弱性，以便人们能注意到网络的这些弱点和它存在的特殊问题。

（2）要告诉人们怎样保护网络系统的各种资源，避免或减少自然或人为的破坏。

（3）要开发和实施卓有成效的安全策略，尽可能减少网络系统所面临的各种风险。

（4）要准备适当的应急计划，使网络系统中的设备、设施、软件和数据在受到破坏和攻击时，能够尽快恢复工作。

（5）要制订完备的安全管理措施，定期检查这些安全措施的实施情况和有效性。

（6）确保信息的安全，就是要保障信息完整、可用和保密的特性。

总之，信息社会的迅速发展离不开网络技术和网络产品的发展，网络的广域化和实用化都对网络系统的安全性提出越来越高的要求。从广义上考虑的网络系统所包含的内容非常丰富，几乎囊括了现代计算机科学和技术的全部成果。为了提高网络安全性，需要从多个层次和环节入手，分别分析应用系统、宿主机、操作系统、数据库管理系统、网络管理系统、子网、分布式计算机系统和全网中的弱点，采取措施加以防范。

1.1.2 网络系统的安全对策与入侵检测

近年来，尽管对计算机安全的研究取得了很大进展，但安全计算机系统的实现和维护仍然非常困难，因为我们无法确保系统的安全性达到某一确定的安全级别。入侵者可以通过利用系统中的安全漏洞侵入系统，而这些安全漏洞主要来源于系统软件、应用软件设计上的缺陷或系统中安全策略规范设计与实现上的缺陷和不足。即使我们能够设计和实现一种极其安全的系统，但由于现有系统中大量的应用程序和数据处理对现有系统的依赖性以及配置新系统所需要的附加投资等多方面的限制，用新系统替代现有系统需付出极大的系统迁移代价，所以这种采用新的安全系统替代现有系统的方案事实上很难得到实施。另一方面，通过增加新功能模块对现有系统进行升级的方案却又不断地引入新的系统安全缺陷。

入侵检测是一种动态的监控、预防或抵御系统入侵行为的安全机制，主要通过监控网络、系统的状态、行为以及系统的使用情况，来检测系统用户的越权使用以及系统外部的入侵者利用系统的安全缺陷对系统进行入侵的企图。和传统的预防性安全机制相比，入侵检测具有智能监控、实时探测、动态响应、易于配置等特点。由于入侵检测所需要的分析数据源仅是记录系统活动轨迹的审计数据，使其几乎适用于所有的计算机系统。入侵检测技术的引入，使得网络、系统的安全性得到进一步的提高（例如，可检测出内部人员偶然或故意提高它们的用户权限的行为，避免系统内部人员对系统的越权使用）。显然，入侵检测是对传统计算机安全机制的一种补充，它的开发应用增大了对网络与系统安全的纵深保护，成为目前动态安全工具的主要研究和开发的方向。许多研发机构和主要的安全厂商都在进行这方面的研究和开发，有的已推出了相应的产品。

实践经验使人们认识到：由于现有的各种安全防御机制都有自己的局限性。例如，防火墙能够通过过滤和访问控制阻止多数对系统的非法访问，但是不能抵御某些入侵攻击，尤其是在防火墙系统存在配置错误、没有定义或没有明确定义系统安全策略时，都会危及到整个系统的安全。另外，由于其主要是部署在网络数据流的关键路径上，通过访问控制来实现系统内部与外部的隔离，从而对于恶意的移动代码（病毒、木马、缓冲区溢出等）攻击、来自内部的攻击等，防火墙将无能为力。因此，针对网络的安全不能只依靠单一的安全防御技术和防御机制。只有通过在对网络安全防御体系和各种网络安全技术和工具研究的基础上，制订具体的系统安全策略，通过设立多道安全防线、集成各种可靠的安全机制（诸如：防火墙、存取控制和认证机制、安全监控工具、漏洞扫描工具、入侵检测系统以及进行有效的安全管理、培训等）、建立完善的多层安全防御体系，才能够有效地抵御来自系统内部和外部的入侵攻击，达到维护网络系统安全的目的。

1.1.3 网络安全的 P^2DR 模型与入侵检测

单纯的防护技术容易导致系统的盲目建设。这种盲目包括两方面：一方面是不了解安全

威胁的严峻，不了解当前的安全现状；另一方面是安全投入过大而又没有真正抓住安全的关键环节，导致不必要的浪费。

由于系统的攻击日趋频繁，安全的概念已经不仅仅局限于信息的保护，人们需要的是对整个信息和网络系统的保护和防御，以确保它们的安全，包括对系统的保护、检测和反应能力等。

总的来说，安全模型已经从以前的被动保护转到了现在的主动防御，强调整个生命周期的防御和恢复。PDR 模型就是最早提出的体现这样一种思想的安全模型。所谓 PDR 模型指的就是基于防护（Protection）、检测（Detection）、响应（Reaction）的安全模型。

20 世纪 90 年代末，美国国际互联网安全系统公司（ISS）提出了自适应网络安全模型（Adaptive Network Security Model，ANSM），并联合其他厂商组成 ANS 联盟，试图在此基础上建立网络安全的标准。该模型是可量化、可由数学证明、基于时间的、以 PDR 为核心的安全模型，亦称为 P^2DR 模型，这里 P^2DR 是 Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）的缩写。其体系框架如图 1.1 所示。其中各部分的含义如下。

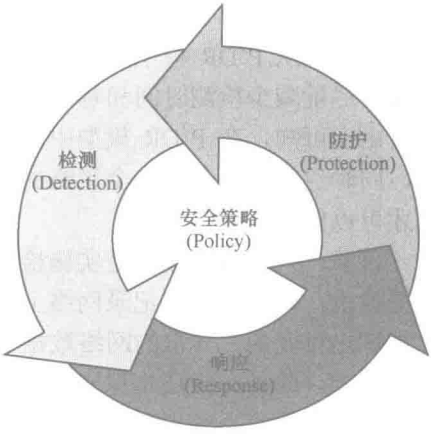


图 1.1 P^2DR 模型的体系框架

（1）Policy（安全策略）：根据风险分析产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。安全策略是 P^2DR 安全模型的核心，所有的防护、检测、响应都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。

（2）Protection（防护）：通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。

（3）Detection（检测）：在 P^2DR 模型中，检测是非常重要的一个环节，检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具。通过不断地检测来监控网络和系统，发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。

（4）Response（响应）：紧急响应在安全系统中占有最重要的地位，是解决潜在安全问题最有效的办法。从某种意义上讲，安全问题就是要解决如何进行紧急响应和异常问题处理。

网络信息系统的安全是基于时间特性的，P^2DR 安全模型的特点就在于动态性和基于时间的特性。下面针对该特性定义几个时间值来进行描述。

（1）攻击时间（Pt）：表示从入侵开始到侵入系统的时间。Pt 的衡量特性包括两个方面。①入侵能力。②系统脆弱性。高水平的入侵及安全薄弱的系统都能增加攻击的有效性，使 Pt 缩短。

（2）检测时间（Dt）：系统安全检测包括发现系统的安全隐患和潜在攻击检测，以利于系统的安全评测。改进检测算法和设计可缩短 Dt，提高对抗攻击的效率。检测系统按计划完成

所有检测的时间为一个检测周期。检测与防护是相互关联的，适当的防护措施可有效缩短检测时间。

（3）响应时间（Rt）：包括检测到系统漏洞或监控到非法攻击到系统启动处理措施的时间。例如，一个监控系统的响应可能包括监视、切换、跟踪、报警、反击等内容。而安全事件的后处理（如恢复、总结等）不纳入事件响应的范畴之内。

（4）系统暴露时间（Et）：系统的暴露时间是指系统处于不安全状况的时间，可以定义为Et=Dt+Rt−Pt。系统的检测时间与响应时间越长，或对系统的攻击时间越短，则系统的暴露时间越长，系统就越不安全。如果Et＜0（即Dt+Rt＜Pt，那么可以基于P^2DR模型，认为该系统是安全的。

可见，从P^2DR模型可以得出这样一个结论：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间。

由上可知，在P^2DR模型中，检测是一个非常重要的环节，是动态响应和加强防护的依据，同时也是强制落实安全策略的有力工具，通过检测，能够不断发现新的威胁和弱点，据此才可以做出有效的响应。

目前，入侵检测技术是实施检测功能的最有效的技术。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。可见，入侵检测系统也具有一定的响应功能。因此，从P^2DR模型来理解，入侵检测系统是一个具有检测功能，同时又兼备防护和响应功能的安全技术产品，是保护网络信息系统安全的强有力的工具。

1.2 入侵检测的产生与发展

20世纪70年代，随着计算机速度、数目的增长以及体积的减小，对计算机安全的需求也显著增加。美国政府意识到传统审计团体在跟踪计算机活动方面具有丰富经验，因此决定获取它们的支持和帮助。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负责主持。

1.2.1 早期研究

1980年，James Anderson在给一个保密客户写的技术报告中指出，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、有预谋的未经授权访问信息、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，以便该系统可以用于检测误用。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，而且提出对不同渗透的相应检测方法，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 工作的主要服务对象是重要的分级客户。该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。客户有要求审计所有计算机活动的策略，并由安全部门职员手工检查审计跟踪和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 建议通过对某些用户行为的一些统计分析应当具备判定系统不正常使用模式的能力，这或许是可以用来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。

总的来说，由于 20 世纪 80 年代初期网络还没有今天这样普遍和复杂，网络之间也没有完全连通，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。

1.2.2 主机入侵检测系统研究

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。这篇文章后来被认为是入侵检测系统（Intrusion Detection System，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。

1988 年，SRI 开始开发入侵检测专家系统（Intrusion Detection Expert System，IDES），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（Signature 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，在 IDES 的基础上，SRI 加强优化 IDES，在以太网的环境下实现了产品化的入侵检测专家系统（Next-Generation Intrusion Detection Expert System，NIDES），它继承了 IDES 的双重分析特性，采用的方法更为通用、灵活，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，并且缺少协同工作的能力。由于用户作为分析的目标（或者说单元），因此对多域联合攻击无能为力。

此为试读，需要完整PDF请访问：www.ertongbook.com