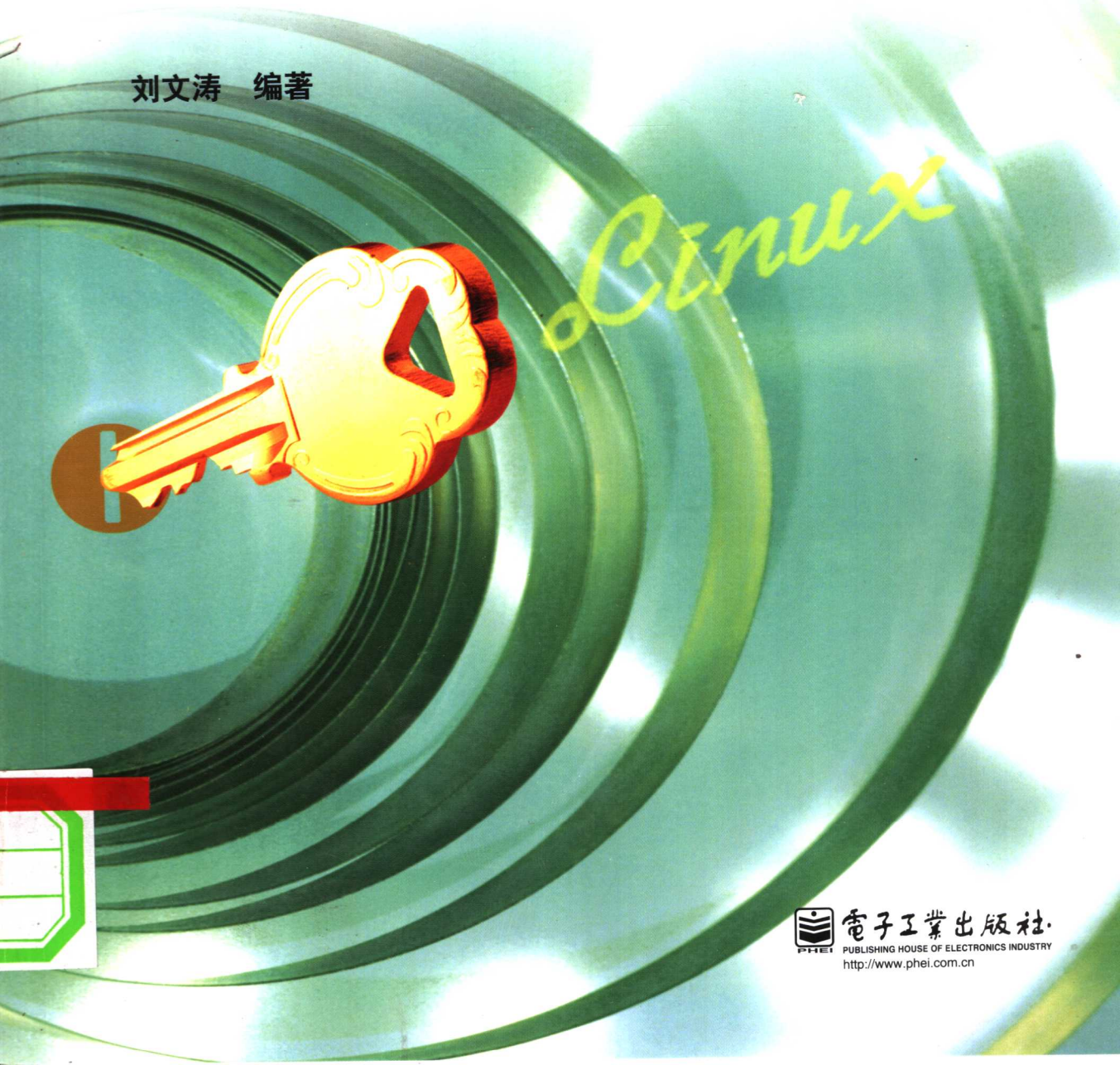
Linux网络入侵检测系统

刘文涛 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Linux 网络入侵检测系统

刘文涛　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书在介绍入侵检测系统的基本概念和原理的基础上，通过在 Linux 下设计一个典型的基于网络的入侵检测系统来更深入地探讨入侵检测技术。本书的一大特色是原理概念的讲述和系统的设计相辅相成，紧密联系。典型系统采用模块化设计思想，分别是网络数据包捕获模块、网络协议分析模块、存储模块、规则解析模块、入侵检测模块、响应模块和界面管理模块七个模块。另外，本书还深入讨论了网络数据包捕获技术、协议分析技术、入侵检测技术、入侵事件描述语言的建立、存储技术、多线程技术、界面设计技术等。

本书适合于计算机专业的本科生和研究生阅读，也可供从事计算机工程与应用的科技工作者或网络安全爱好者参考。

图书在版编目（CIP）数据

Linux 网络入侵检测系统/刘文涛编著. —北京：电子工业出版社，2004.10
ISBN 7-121-00477-1

Ⅰ. L… Ⅱ. 刘… Ⅲ. Linux 操作系统—安全技术 Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字（2004）第 108223 号

责任编辑：竺南直
印　　刷：北京天宇星印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：18　字数：458 千字
印　　次：2004 年 10 月第 1 次印刷
印　　数：4000 册　　定价：25 00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着网络技术的飞速发展，网络安全问题也越来越突出。顺应这一趋势，涌现出了很多的网络安全技术，如网络防火墙、病毒检测、密码技术、身份认证等。但是，即使如此，还是有很多的服务器在不能够及时检测和预防的情况下被攻击，导致了巨大的经济损失。这种被动的防御系统显露出技术上很多的不足，于是，有人提出了主动的网络安全防御体系，这其中的代表者就是网络入侵检测系统。

网络入侵检测系统的根本功能就是实时地检测并分析网络的行为，根据分析的结果做出相应的响应。这样就可以及时地检测出网络的非法攻击，提早做出判断，减少损失。网络入侵检测系统的出发点在于其主动性，它不是被动的防御。主动性是入侵检测系统的一大特色，也是其发展迅速并被人们重视的一个重要原因。

本书介绍了网络入侵检测系统的基本概念和原理，并设计了一个简单又典型的网络入侵检测系统，通过设计与实现本系统可以使读者更好地理解网络入侵检测的相关概念。读者还可以在理解此系统的基础上设计功能更强大的网络入侵检测系统。系统的设计和实现与入侵检测系统相关概念的讲述是紧密联系、相辅相成的。作者在讲述一个概念的同时，将其与设计联系起来，这样有助于更加深入地理解概念的本质。本书中使用的是最新的基于协议分析的网络入侵检测技术，协议分析技术的实现是本书的一大重点。这个典型的入侵检测系统采用模块化设计，包括七个模块，分别为网络数据包捕获模块、网络协议分析模块、存储模块、规则解析模块、入侵事件检测模块、响应模块和界面管理模块。每个模块的设计与实现将分别放在不同的章节里进行详细的讨论。作者将此系统作为一个开发项目，其链接地址为 http://tcpids.cosoft.org.cn。

本书的主要特点

（1）注重基础，重点突出。本书只有一个中心点，就是网络入侵检测系统，本书围绕这个中心展开论述，以便读者对网络入侵检测系统有一个最清楚的认识。包括入侵检测系统的各个方面，如其发展的原因、定义、入侵原理、,入侵检测系统类型、研究发展方向、体系结构等。而本书的重点，就是理解一个完整的入侵检测系统的运行机理，包括它的各个部分，这是通过一个非常典型的系统来进行阐述的。

（2）通过实例进行讲解。本书实现了一个完整的网络入侵检测系统，从最基本的部分开始设计，而这些组成部分几乎是每个大型网络入侵检测系统所具有的。作者深深感觉到，如果想很好地理解网络入侵检测系统的内部运行机理，通过编写实例来理解，是再好不过的，但是这个实例又不能太复杂，它实现了系统的最核心的功能。例如，学习操作系统，如果有一个小的完整的操作系统来进行学习，而且又可以进行裁减，这样学习起来就会理解得更深刻。本书设计的一个入侵检测系统就是为教学和研究所用，它实现了最核心的功能。读者可以根据这个小系统来进行更深入的开发和研究，特别是对于搞入侵检测系统方面开发的人员，有很好的借鉴作用。读者都有这样的体会，讲解一个问题（例如算法），不管你怎样描述，还不如给你一个 DEMO 让你来看，一下子就明白了，并且可以在这个 DEMO 的基础上设计自

己的系统。

（3）程序讲解透彻。通过程序可以很好地描述一个算法和思想，因为程序是无国界的。本书给出了一些最关键的实现程序，并且对程序进行了详细的注解，读者不用担心看不懂程序。通过读本书的程序，可以更好地理解其实现的过程。本书的程序都是模块化的，结构层次都非常清楚。

本书的主要内容

首先我们介绍网络安全问题，讨论了传统的网络安全技术，提出了一种网络安全模型PPDR。然后介绍了入侵检测系统的产生和定义。分析了两种类型的入侵检测系统：主机入侵检测系统和网络入侵检测系统。然后对入侵检测技术进行介绍，包括异常检测技术和误用检测技术。同时介绍入侵检测系统的标准化过程。

接下来介绍 Linux 下基于网络的入侵检测系统的设计原理和整体框架，分别介绍了各个模块的功能，讨论了数据源问题。

在网络数据包捕获模块中，本书详细讨论了数据包捕获机制。在此模块中也详细介绍了编写网络安全程序的函数库 LIBPCAP。LIBPCAP 是一个非常优秀的网络数据包捕获的封装函数库。

在协议分析模块中，本书对 TCP/IP 协议族进行了详细的分析，主要包括以太网协议，ARP/RARP，IP，UDP，TCP，ICMP，DNS，HTTP，DHCP。还对 IPX 协议也进行了分析。对 TCP 协议连接过程进行了详细的分析和实现。

在存储模块中，本书用 MySql 数据库来存储网络信息，详细介绍了 MySql 的使用方法，怎样用 PHPMYADMIN 来管理 MySql 数据库，以及如何实现数据库的链接。介绍了怎样把网络信息存储到数据库中，还实现了对数据库的事后分析过程，实现了一些流量统计功能，着重分析了 HTTP 协议的相关内容，如 HTML 网页内容回放功能的实现。

在规则解析模块中，我们设计了一个入侵事件描述语言，入侵事件描述语言是 IDS 中一个比较重要的组成部分，在这个模块中详细介绍了入侵事件描述语言的设计和实现。对规则的解析过程进行了实现。

在入侵事件检测模块中，对基于协议的入侵检测方法进行了详细的介绍，实现了入侵规则匹配功能。还使用了非规则匹配的方式来检测入侵行为，如网络扫描行为的检测。在这个模块中，我们实现了入侵事件的检测功能。

在响应模块中，本书设计了几种响应方式，包括声音警报、灯光闪烁和被动记录等，还讨论了入侵响应原理、响应类型和响应方法。入侵响应是入侵检测系统中一个必要的组成部分。

在界面管理模块中，本书使用 GTK+技术来实现界面，介绍了 GTK+的相关内容，实现了界面管理模块的设计。在此模块中，还讨论了多线程技术，特别是对界面设计中的多线程技术进行了深入研究，例如界面的动态显示就使用了多线程技术。

由于本人知识有限，书中不免有错误之处，希望广大读者不吝赐教。

在此特别要感谢我的家人和朋友，他们的支持才使我有无穷的创作动力。

刘文涛

于武汉

2004 年 10 月

目　录

第 1 章　网络安全问题及其对策

1.1　网络安全问题

网络的飞速发展是有目共睹的，但是在这个飞速发展的过程中，也出现了种种不安全的因素。网络是一个双刃剑。网络给人类带来了无限好处，但同时也给人类带来了无限困扰。从各大媒体上大家都可以看到很多关于网络遭遇黑客攻击的报道，甚至把黑客的故事都搬上了银屏，这给现实生活中的人们产生了巨大的冲击。现在网络专家们对目前存在的安全隐患深感担忧。据报道，美国国防部已经花费了数十亿美元用以整治网络安全，但是网络安全问题还是不断涌现。现在全世界的公司都面临着网络被攻击的危险。在 2003 年，全球 13 台最重要的母服务器中的 9 台都遭到了黑客袭击。

网络安全问题已经不再是一个新鲜的课题了，也已不再是一个高深的课题了，以前它基本上是跟网络人士打交道，但现在每一个人都可能与它打交道，只要他的电脑连在网络上。特别是随着网络应用范围的不断扩大，例如，政治、军事、文化、经济、教育、卫生、科技、公共服务等等都在普及网络，他们的网络安全问题也越来越突出，特别是在关键应用系统，如金融、电信、民航、电力等系统中。可以预见，随着网络的超常规的发展，网络安全问题会越来越严重，会越来越被人重视，当然网络安全技术也会越来越成熟。在这个过程中，必定会发生网络安全问题，这是不可避免的，但在遭遇网络安全问题的时候，不能够逃避，我们要力求找出应对网络安全问题的策略。

怎样解决网络安全问题，很多人在研究，也在探索。这其中出现了不少可喜的成果，但也有很多不足。随着网络的普及，网络攻击人员的技术也在不断提高，怎样应对这个现象，是一切志在解决网络安全问题的人士必须思考的一个问题。

本书讨论的是网络安全技术中的一个方面，即入侵检测系统。此技术的飞速发展，已经成为现在网络安全技术中的一个热门。本书只是起抛砖引玉的作用，希望能为网络安全的发展作出一点贡献。

1.2　网络安全目标

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的目标主要表现在系统的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。

3. 保密性

保密性是指防止信息泄露给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。

5. 不可抵赖性

不可抵赖性也称做不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

1.3 网络面临的主要威胁

日益严重的网络信息安全问题，不仅使上网企业、机构以及用户蒙受巨大的经济损失，而且使国家的安全与主权面临严重威胁。要避免网络信息安全问题，首先必须搞清楚触发这一问题的原因。总结起来，主要有以下几个方面原因。

1. 黑客的攻击

黑客对于大家来说，不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展，目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了，尤其是现在还缺乏针对网络犯罪很有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，破坏力大，是网络安全的主要威胁。

黑客的攻击方法有很多种，例如口令攻击，一种方法是通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户账号和口令，对局域网安全威胁巨大；二是在知道用户的账号后利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间；三是在获得一个服务器上的

用户口令文件后，用暴力破解程序破解用户口令，此方法在所有方法中危害最大；另外一个攻击方法就是放置特洛伊木马程序。特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在系统启动时悄悄执行的程序。当被植入特洛伊木马程序的机器连上网络时，木马程序就会把机器的信息发给控制端程序，这样控制端程序就会控制中木马的机器了。网络监听又是一个常用的攻击方法。再就是寻找系统的漏洞，其中某些是操作系统或应用软件本身具有的，如 Sendmail 漏洞，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏。黑客的攻击方法多种多样，而且所用技术在不断创新。

2．管理的疏忽

网络系统的管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网络或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。目前，美国 75%～85%的网站都抓不住黑客的攻击，约有 75%的企业网上信息失窃。

3．网络的缺陷

Internet 的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议族缺乏相应的安全机制，而且因特网最初的设计考虑是该网络不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量和带宽等方面存在着不适应性。

4．软件的漏洞

随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器，一些桌面软件，等等，都被发现过存在安全隐患。可以说任何一个软件都可能会因为程序员的一个疏忽，设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

由于漏洞的存在，黑客可以根据漏洞来进行攻击，病毒也可以根据漏洞来进行攻击。现在的病毒已经变得非常智能化，简直是无孔不入。这些病毒再加上黑客的技术就可能产生非常严重的后果。由于病毒传播的速度非常快，如果黑客把入侵代码加入病毒或者做成病毒，这样黑客的攻击范围就会变得非常大。病毒特征和黑客技术相结合的攻击方法会越来越普遍。现在的软件越来越复杂，漏洞就会越来越多，特别是黑客技术在不断提高，他们发现软件漏洞并利用漏洞来进行攻击的时间也会越来越短。

5．网络内部攻击

网络内部用户的误操作、资源滥用和恶意行为。再完善的防火墙也无法抵御来自网络内部的攻击，也无法对网络内部的滥用做出反应。

1.4 传统网络安全技术

传统网络安全技术主要使用以下几种安全机制。

1. 加密机制

加密是一种最基本的安全机制，它能防止信息被非法读取。加密是一种在网络环境中对抗被动攻击的行之有效的安全机制。数据加密是保护数据的最基本的方法。但是，这种方法只能防止第三者获取真实数据，仅解决了安全问题的一个方面。而且，加密机制并不是牢不可破的。

2. 数据签名机制

签名与加密很相似，一般是签名者利用秘密密钥（私钥）对需签名的数据进行加密，验证利用签名者的公开密钥（公钥）对签名数据做解密运算。如果能保证一个签名者的签名只能惟一地从他自己产生，那么当收发双方发生争议的时候，仲裁机构就能够根据消息上的数字签名来裁定这条消息是否是由发送方发出的。

3. 访问控制机制

访问控制机制是按照事先确定的规则决定主体对客体的访问是否合法。当一个主体试图非法使用一个未经授权使用的客体（资源）时，访问控制功能将拒绝这一企图，并可附带报告这一事件给审计跟踪系统，审计跟踪系统产生一个报警或形成部分追踪审计。

4. 数据完整性机制

数据完整性机制可以发现网络上传输的数据已经被非法修改，从而使用户不会被非法数据欺骗。

5. 认证机制

认证是以交换信息的方式来确认实体身份的机制，是进行存取控制所必不可少的条件，因为不知道用户是谁，就无法判断其存取是否合法。

6. 系统脆弱性检测

系统中脆弱性的存在是系统受到各种安全威胁的根源。外部黑客的攻击主要利用了系统提供的网络服务中的脆弱性；内部人员作案则利用了系统内部服务及其配置上的脆弱性；而拒绝服务攻击主要利用资源分配上的脆弱性，长期占用有限资源不释放，使其他用户得不到应有的服务，或者是利用服务处理中的弱点，使该服务崩溃。

7. 防火墙

防火墙系统软件实现将定义好安全策略转换成具体的安全控制操作，它使得内部网络与因特网之间或者与其他外部网络互相隔离，限制网络互访。按照一定的安全策略规则对其检查网络包或服务请求，来决定网络之间的通信是否被允许，其中被保护的网络称为内部网络或私有网络，而与内部网络或私有网络相连的网络称为外部网络或公有网络。防火墙能有效地控制内部网络与外部网络之间的访问及数据传送，从而实现保护内部网络的信息不受外部

非授权用户的访问或者过滤信息的目的。防火墙的实现从层次上大概可以分两种：报文过滤和应用层网关。

1.5　网络安全模型——PPDR

PPDR（Policy Protection Detection Response）的基本思想是：以安全策略为核心，通过一致性检查、流量统计、异常分析、模式匹配以及基于应用、目标、主机、网络的入侵检查等方法进行安全漏洞检测。检测使系统从静态防护转化为动态防护，为系统快速响应提供了依据。当发现系统有异常时，根据系统安全策略快速作出反应，从而达到保护系统安全的目的。PPDR 可适应网络安全模型如图 1-1 所示。

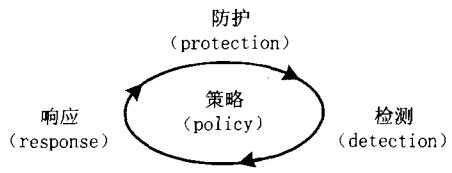


图 1-1　PPDR 网络安全模型

PPDR 模型由 4 个主要部分组成：安全策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）。PPDR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等手段）的同时，利用检测工具（如漏洞评估、入侵检测等系统）了解和评估系统的安全状态，通过适当的响应将系统调整到一个比较安全的状态。防护、检测和响应组成了一个完整的、动态的安全循环。

1．策略

策略是这个模型的核心，在具体的实施过程中，策略意味着网络安全要达到的目标，它决定了各种措施的强度。因此追求安全是要付出代价的，一般会牺牲用户使用的舒适度，还有整个网络系统的运行性能，因此策略的制定要按照需要进行。

2．防护

一般而言，防护是安全的第一步，它的基础是检测与响应的结果。具体包括：

① 安全规章的制定：在安全策略的基础上制定安全细则。

② 系统的安全配置：针对现有网络环境的系统配置，安装各种必要的补丁软件，并对系统进行仔细的配置，以达到安全策略规定的安全级别。

③ 安全措施的采用：安装防火墙软件和设备，VPN 软件和设备等。

3．检测

采取了各种安全防护措施并不意味着网络系统的安全性就得到了安全的保障，网络的状况是动态变化的，而各种软件系统的漏洞层出不穷，都需要采取有效的手段对网络的运行进行监视。

防护相对于攻击者来说总是滞后的，一种漏洞的发现或者攻击手段的发明与相应的防护手段的采用之间，总会有一个时间差，检测就是弥补这个时间差的必要手段。

检测的作用包括：

- 异常监视：发现系统的异常情况如重要文件的修改，不正常的登录等；
- 模式发现：对已知的攻击模式进行发现。

4. 响应

在发现了攻击企图或者攻击之后，需要整个系统及时地作出反应，这包括：

① 报告：就是作出入侵事件响应的报告，通知安全管理员发生了入侵行为，可以利用各种各样的报告方式，如电子邮件、警报甚至手机短信，等等。

② 记录：当有入侵行为发生时，就把所有的系统活动都给记录下来，这样事后就可以进行进一步的分析，以找出系统的弱点和漏洞所在。

③ 反应：反应可以是主动的，例如可以切断当前连接，也可以通过告诉防火墙更改控制策略，等等。其目的就是把损失控制到最低。

④ 恢复：如果入侵行为成功，必然对系统造成一定的破坏，恢复就是修复系统，使系统能够正常运转。

第 2 章　入侵检测系统概述

2.1　入侵检测的产生及其定义

1．入侵检测产生原因

传统的信息安全技术都集中在系统自身的加固和防护上。比如，采用 B 级操作系统和数据库，在网络出口配置防火墙，在信息传输和存储中采用加密技术，使用集中的身份认证产品等。

然而，单纯的防护技术有如下几方面的问题。

（1）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和当前的安全现状；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。

（2）防火墙策略对于防范黑客有其明显的局限性。诸如：

防火墙难于防内。防火墙的安全控制只能作用于外对内或内对外，即：对外可屏蔽内部网的拓扑结构，封锁外部网上的用户连接内部网上的重要站点或某些端口，对内可屏蔽外部危险站点，但它很难解决内部网控制内部人员的安全问题。即防外不防内。而据权威部门统计结果表明，网络上的安全攻击事件有 70%以上来自内部攻击。

防火墙难于管理和配置，易造成安全漏洞。防火墙的管理及配置相当复杂，要想成功地维护防火墙，要求防火墙管理员对网络安全攻击的手段及其与系统配置的关系有相当深刻的了解。防火墙的安全策略无法进行集中管理。一般来说，由多个系统（路由器、过滤器、代理服务器、网关、堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。根据美国财经杂志统计资料表明，30%的入侵发生在有防火墙的情况下。

防火墙的安全控制主要是基于 IP 地址的，难于为用户在防火墙内外提供一致的安全策略。许多防火墙对用户的安全控制主要是基于用户所用机器的 IP 地址而不是用户身份，这样就很难为同一用户在防火墙内外提供一致的安全控制策略，限制了企业网的物理范围。

防火墙只实现了粗粒度的访问控制，且不能与企业内部使用的其他安全机制（如访问控制）集成使用，这样，企业就必须为内部的身份验证和访问控制管理维护单独的数据库。

（3）保证信息系统安全的经典手段是“存取控制”或“访问控制”，这种手段在经典的以及现代的安全理论中都是实行系统安全策略的最重要的手段。但迄今为止，软件工程技术还不可能百分之百地保证任何一个系统（尤其是底层系统）中不存在安全漏洞。

而且，无论在理论上还是在实践中，试图彻底填补一个系统的安全漏洞都是不可能的，也还没有一种切实可行的办法解决合法用户在通过“身份鉴别”或“身份认证”后滥用特权的问题。

针对日益严重的网络安全问题和越来越突出的安全需求，“可适应网络安全模型”和“动态安全模型”应运而生。而入侵检测系统在动态安全模型中占有重要的地位。

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，这从国外入侵检测产品市场的蓬勃发展就可以看出。在国内，随着上网的关键部门、关键业务越来越多，迫切需要具有自主版权的入侵检测产品。但现状是入侵检测还不够成熟，处于发展阶段，或者是防火墙中集成较为初级的入侵检测模块，所以对于入侵检测系统的研究是很重要的。

2. 入侵检测的定义

入侵检测是指在特定的网络环境中发现和识别未经授权的或恶意的攻击和入侵，并对此作出反应的过程。而入侵检测系统 IDS 是一套运用入侵检测技术对计算机或网络资源进行实时检测的系统工具。IDS 一方面检测未经授权的对象对系统的入侵，另一方面还监视授权对象对系统资源的非法操作。

3. 入侵检测系统的作用

入侵检测系统的作用有以下几种：

- 监视、分析用户和系统的运行状况，查找非法用户和合法用户的越权操作；
- 检测系统配置的正确性和安全漏洞，并提示管理员修补漏洞；
- 对用户非正常活动的统计分析，发现攻击行为的规律；
- 检查系统程序和数据的一致性和正确性；
- 能够实时地对检测到的攻击行为进行响应；
- 对操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

2.2 入侵检测系统的分类

入侵检测系统根据检测的对象可分为基于主机的入侵检测系统 HIDS（Host Intrusin Detection System）和基于网络的入侵检测系统 NIDS（Network Intrusion Detection System）。

1. 主机入侵检测系统 HIDS

基于主机的入侵检测是根据主机系统的系统日志和审计记录来进行检测分析，通常在要受保护的主机上有专门的检测代理，通过对系统日志和审计记录不间断的监视和分析来发现攻击。

它的主要目的是在事件发生后提供足够的分析来阻止进一步的攻击。

其优点有：

① 能够监视特定的系统行为，基于主机的 IDS 能够监视所有的用户登录和退出甚至用户所做的所有操作，审计系统在日志里记录的策略改变，监视关键系统文件和可执行文件的改变等。

② HIDS 能够确定攻击是否成功，由于使用含有已发生事件信息，它们可以比 NIDS 更加准确地判断攻击是否成功。

③ 有些攻击在网络的数据流中很难发现，或者根本没有通过网络在本地进行。这时 NIDS 将无能为力，只能借助于 HIDS。