入侵检测系统及实例剖析

韩东海　王　超　李　群　编著

清 华 大 学 出 版 社

(京)新登字 158 号

内 容 简 介

本书是一本系统介绍入侵检测系统理论与实际应用的中高级参考用书。全书分为原理篇、使用篇和分析篇三大部分。原理篇介绍了入侵检测的基本原理，主要包括面对的威胁、分类检测的方法及其关键技术。使用篇选取常用的开放源代码系统——Snort 和 AAFID 系统，介绍了系统的总体框架和主要设计思想，分析篇是本书的重点，结合具体的应用实例对系统的源代码进行逐一剖析，全部源代码完全公开。

本书有助于计算机网络安全从业人员加深对入侵检测的理解，积累技术相关的设计与开发经验，对于广大的程序员提高编程水平也大有裨益，是极佳案头参考用书。同时也适用于各大专院校计算机专业的教师和高年级学生。

图书在版编目（CIP）数据

入侵检测系统及实例剖析/韩东海，王　超，李　群 编著. —北京：清华大学出版社，2002/4/17
ISBN 7-302-05392-8

Ⅰ.入...　Ⅱ.①韩...②王...③李...　Ⅲ.计算机网络－安全技术　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 019512 号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑：陈仕云
印 刷 者：北京市清华园胶印厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　**印张**：18.25　**字数**：418 千字
版　　次：2002 年 5 月第 1 版　2002 年 5 月第 1 次印刷
书　　号：ISBN 7-302-05392-8/TP・3171
印　　数：0001～5000
定　　价：28.00 元

前　言

本书对入侵检测技术的基本原理进行了详细的介绍，并精心挑选了两个较有代表性的开源系统进行详尽的剖析。本书主要分为三大部分进行介绍，首先是原理篇，然后是使用篇，最后则是源代码解析。

本书读者对象

本书预期的读者群为：

- 网络安全产品开发人员
- 网络安全技术研究人员
- 网络管理人员
- 系统集成公司的技术人员
- 广大程序员
- 大学教师
- 大学高年级学生

本书假定读者已具有一定的 C 语言和 Perl 语言（开发环境）基础。

本书优点

网络安全已经成为一个非常热门的话题，而入侵检测则是这一两年来在网络安全领域比较热门的技术，而且会在今后的一段时间内持续发展。但是当前网络安全相关的书籍不是很多，而且基本上以介绍网络安全的基本知识为主，尤其是与入侵检测技术相关的书籍更是少见，并不能满足广大读者的需要。我们希望通过本书的出版，能够让广大读者对入侵检测技术有一个深入的了解，对于入侵检测系统的设计和实现有一个明确的概念。

因此，我们选择了两个非常优秀的开源系统，希望能够给大家提供很好的参考。这两个系统是：

- Snort：一个非常优秀的基于误用的入侵检测系统，在开放源代码软件界非常有名，而且很实用。作为一个轻量级的系统，无论从分析安全系统的角度，还是从学习软件开发的角度，都是一个不可多得的范本。
- AAFID：一个非常优秀的概念验证系统，与它同名的理论对于入侵检测系统的设计有着很好的指导作用，而这个验证系统也为理解该理论提供了很好的帮助。这个完全使用 Perl 来实现的小巧系统也对大家加深对 Perl 的理解有很多好处。

我们相信，通过对这些真正优秀的软件进行分析，更能加深对概念的理解，而且能够提高实际的编程水平。

本书的主要内容

本书主要分为三个部分进行，分别介绍入侵检测技术的原理、入侵检测系统的使用以及分析入侵检测系统的源代码。

原理篇

本书的第一篇是入侵检测原理介绍，考虑到本书不是一本网络安全方面的入门书籍，因此我们并没有涉及算法、系统安全等基本的领域，主要是从入侵检测的角度进行介绍。

第 1 章介绍入侵检测的基本概念，包括以下内容：

- 网络安全的基本概念：网络安全的三个基本要素、PDR 模型以及入侵检测在 PDR 模型中的位置和作用
- 我们面对的威胁：谁在攻击，如何攻击
- 什么是入侵检测
- 如何对入侵检测技术进行分类研究

基于第 1 章讨论的分类标准，本书采用了基于异常的入侵检测系统与基于误用的入侵检测系统这种分类方法，第 2 章和第 3 章就分别介绍了这两种系统，内容基本类似，包括：

- 基本原理介绍
- 典型系统类型介绍

在计算机技术领域，标准的重要性是毋庸置疑的。虽然安全领域的标准化进程相对来说比较缓慢，入侵检测技术更是如此，但是标准毕竟是方向，因此在对相关技术进行分析的基础上，第 4 章主要讨论了标准并对主要的入侵检测系统进行简单的介绍。

- 入侵检测的标准化工作
- 主要商用系统简介
- 主要开源系统简介

使用篇

根据第一篇的原理分析，我们选择了两个比较典型的系统进行介绍，其中 Snort 是一个典型的基于误用的入侵检测系统，而 AAFID 则是一个非常灵活的系统，它的基于代理的体系结构使它可以既使用基于异常入侵检测技术，也可以使用基于误用的入侵检测技术。在第二篇中，就主要介绍这两个入侵检测系统的使用。

第 5 章介绍 Snort 的使用，包括：

- 简介，如何获取
- 底层库的安装与配置
- 安装与配置详解（针对不同操作系统）
- 使用详解

作为一个典型的基于误用的入侵检测系统，Snort 的优点和难点就在于规则的使用，因此本书将这部分内容独立出来在第 6 章进行介绍。

- 语法
- 常用攻击手段对应的规则举例
- 如何设计新的规则

Snort 介绍完毕后就开始介绍 AAFID，首先是第 7 章的 AAFID 使用简介：

- 简介，如何获取
- 底层库的安装与配置
- 安装与配置详解
- 使用详解

作为一个基于代理的检测系统，AAFID 与 Snort 具有本质的区别，它没有使用规则来对入侵进行描述，而是使用了非常灵活的代理和过滤机制，在第 8 章就介绍 AAFID 系统的代理和过滤：

- AAFID 的规则：没有规则
- 代理介绍
- 过滤器介绍

分析篇

这一部分是本书的重点：源代码分析，分别对 Snort 和 AAFID 的源代码进行剖析。每个系统分为两章，采用了基本相同的结构来进行分析。

第 9 章和第 11 章分别介绍了两个系统的总体结构，主要是静态的体系结构分析与动态的总体流程分析。

在第 10 章 Snort 关键模块剖析和第 12 章 AAFID 关键模块剖析中，分别按照第 9 章和第 11 章的介绍对两个系统按照模块进行了介绍。需要注意的是，本书采用的模块划分是本书作者使用的，原系统的作者未必同意。在模块的介绍过程中，对于某些不是很重要或者比较简单的内容基本上都是一笔带过，对一些比较重要的模块则进行了比较详细的介绍。

最后，对这两个系统进行了简单的总结，包括优点，也有缺点；在此基础上，本文作者也提出了一个系统的试验性设想。

以上就是本书的主要内容，为了读者阅读方便，我们还提供了以下附录供查阅：

- 附录 A　术语
- 附录 B　函数索引
- 附录 C　参考文献

补充

本书的作者都是安全领域的软件开发人员，在安全领域有一些实际的工作经验。本书从某种程度上可以说是我们的经验总结，难免有不足之处，甚至错误，非常欢迎读者与我们探讨，共同进步，我们的联系地址是：

handonghai@yahoo.com
wangc@nci.al.cn
liqun111@sina.com

目　录

第1篇　入侵检测的原理

第 2 篇 常用入侵检测系统的使用

第3篇 源代码分析

第 1 篇

入侵检测的原理

知己知彼，百战不殆

——— 孙子

第 1 章　入侵检测相关基本概念

本章主要内容：

- 网络安全基本概念
- 我们面对的威胁
- 什么是入侵检测
- 入侵检测的分类方法学

本章主要目的是对入侵检测（Intrusion Detection）技术进行系统的阐述。首先介绍网络安全的基本概念，主要参照 ISO7498-2 的安全体系结构进行；在此基础上，遵循 PDR 模型介绍网络安全保证的各个方面，当然考虑到篇幅的限制和本书的主题，还是把重点留给了入侵检测技术；在本章的最后，将对入侵检测技术进行比较完整的介绍，着重强调入侵检测技术的分类方法，为以后几章的介绍提供依据。

1.1　网络安全基本概念

本节的主要内容包括：

- 网络安全的基本观点
- PDR 模型
- 入侵检测：在 PDR 模型中的位置与作用

1.1.1　网络安全的基本观点

本书中所说的网络安全对应的英文是 Network Security。在很多场合，security 和 safety 的中文译法都为“安全”，但是这两者其实是有区别的，safety 更侧重于物理实体上的安全，因此有人甚至主张将 security 翻译成安全性，在本书中不作这种硬性的区分。

迄今在网络安全领域所进行的研究主要集中在计算机网络，但是随着三网合一趋势的逐渐明朗，网络安全研究的应用领域也逐渐扩大。

网络安全基本上是一个实践性的技术领域，在这里大多数的理论基本上是经验的汇集，因此要给出一个形式化的定义是非常困难的，甚至很难给出一个安全与否的准则。常言道，可以（从实践中）证明有问题，却无法（从理论上）证明是正确的。

在网络安全的范畴内，网络并不是物理的网络，它包含以下三个基本要素：

- 数据：包括在网络上传输的数据与端系统中的数据，从本质上说这些电子意义上的数据都是 01 比特的组合，但是经过特定的程序产生和处理之后，它们就具有了

多种多样的语义学上的意义。

- 关系：网络作为交流的重要手段，涉及到通信各方信赖关系的建立与维护，这也是攻击者比较感兴趣的一个方面，因为信赖关系的窃取就意味着能力和数据访问权力的获取，进而可以转化为物理意义上的财富。
- 能力：包括网络系统的传输能力与端系统的处理能力，前者意味着网络连接能力的充分运用，而后者则意味着数据处理能力和服务提供能力等。

网络安全的意义，就在于为以上三个要素提供保护，保证这三者能够为所应为，为合适的人服务，而且只为合适的人服务。相应地，网络安全也就包含以下三个基本方面：

- 数据保护：包括数据的机密性保护和完整性保护，主要针对数据窃取、数据篡改等攻击，其基本的手段包括加密和访问控制。这方面的理论比较完备（主要是加密体制的建立和加密算法的运用），实现手段也比较完善。
- （信赖）关系保护：包括身份鉴别与安全地建立、维护信赖关系，主要针对网络身份冒充、连接截取等攻击，基本的手段包括加密与协议的安全设计。相对来说这方面的理论也比较完备，但在实现手段上会有一些漏洞。
- 能力保护：包括对网络系统的传输功能与端系统的处理功能的保护，主要针对拒绝服务、远程权力获取等攻击。这方面的理论基本上是实践经验的总结，运用的手段也基本上是试验性的。能力保护相关的工作也是入侵检测系统发挥作用之处。

为了达到以上三个目的，在实践经验和一些理论研究的基础上，提出了一些安全模型，其中比较有代表性的就是 PDR 模型。

1.1.2　PDR 模型

PDR 模型最早由 ISS 公司提出，后来出现了很多变种，包括 ISS 公司自己也将其改换为 PADIMEE，包括策略（Policy）、评估（Assessment）、设计（Design）、执行（Implementation）、管理（Management）、紧急响应（Emergency Response）、教育（Education）等七个方面。经过简单的分析可以看出，这些变化更多的是一种商业策略的反映，其实质内容并没有发生变化，因此在本书中，还是参照 PDR 模型进行介绍。

这里介绍的 PDR 模型可以称为 PPDR 模型，包括策略（Policy）、防护（Protection）、检测（Detection）、响应（Response），它们的关系如图 1-1 所示。

图 1-1　PDR 模型示意图

需要注意的是图 1-1 中虽然是一个平面的循环，但实际上应该是一个螺旋上升的过程。经过了一个 PDR 循环之后，进行防护的水平显然是提高的。

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。因为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。

在制定好策略之后，网络安全的其他几个方面就要围绕着策略进行。以下将按照 PDR 的顺序进行介绍，但这并不意味着必须以这个顺序进行，因为它只是一个正常的顺序而已。

1．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，有别人的，也有自己的。具体包括：

- 安全规章的制定：在安全策略的基础上制定安全细则。
- 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。
- 安全措施的采用：安装防火墙软件或设备、VPN 软件或设备等。

佛家说须弥藏介子，意思是微观可以包含宏观。在防护的步骤里面，实际上也包含了一个小的 PDR 循环。因为在进行安全配置之后，为了证明配置的有效性，必须进行符合性验证、系统脆弱性分析以及漏洞扫描等，再根据结果进行相应的配置改进。这里的 P 是配置和安全措施的采用，D 是系统漏洞扫描，R 是进一步的配置与安全措施。

注：在漏洞扫描方面也有一个非常好的开源软件 —— nessus，有兴趣的读者可以到 www.nessus.org 看看。

2．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完全的保障，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控。

防护相对于攻击来说总是滞后的，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。

3．响应

在发现了攻击企图或者攻击之后，需要系统及时地进行反应，这包括：

- 报告：无论系统的自动化程度多高，都需要让管理员知道是否有入侵发生。
- 记录：必须将所有的情况记录下来，包括入侵的各个细节以及系统的反应。
- 反应：进行相应的处理以阻止进一步的入侵。
- 恢复：清除入侵造成的影响，使系统恢复正常运行。

如果把响应所包含的告知与取证等非技术因素剔除，实际上响应就意味着进一步的防护。

1.1.3　入侵检测：在 PDR 模型中的位置与作用

入侵检测就是 PDR 模型中的检测，它的作用在于承接防护和响应的过程。

入侵检测是 PDR 模型作为一个动态安全模型的关键所在，可以说提出 PDR 模型的原因就是入侵检测技术，这一点可以从 PDR 模型的提出者看出——ISS 正是全球领先的入侵检测系统提供商。

网络安全近几年的热点发展过程基本上是按照以下顺序进行：

- 防火墙技术的研究：在网络边界保卫内部网。
- VPN 技术的研究：连接分散的内部网，完成内部网外延的扩大，与防火墙技术结合比较紧密。
- 认证/PKI 技术的研究：进一步扩大内部网的外延，同时建立广义的信任关系。
- 入侵检测技术的研究。

可以看出，除了入侵检测技术，其他几项都是立足于防。从这个发展趋势可以看出，在不断加强防护的同时，人们已经越来越意识到只有防护是不够的，近两年频繁的网络攻击事件也证明了这种观点。

如果与真实世界相比拟的话，防火墙等技术就像是一个大楼的安防系统，虽然它可能很先进也很完备，但是仍然需要与监视系统结合来进行，仍然需要不断地检查大楼包括安防系统本身。

网络安全也是如此，在设计现有防护系统的时候，只可能考虑到已知的安全威胁与有限范围内的未知安全威胁。防护技术只能做到尽量阻止攻击企图的得逞或者延缓这个过程，而不能阻止各种攻击事件的发生。更何况在安全系统的实现过程中，还有可能留下或多或少的漏洞，这些都需要在运行过程中通过检测手段的引入来加以弥补。

1.2　我们面对的威胁

如果对 PDR 模型进行比较形象的描述，可以认为安全策略代表了需要保护的网络，而防护、检测与响应就代表了管理员为了保证网络安全而进行的种种努力。这个环所要面对的就是来自各方的安全威胁。在 ISO7498-2 的定义中，安全威胁包含潜在的危险以及可能发生或者正在发生的攻击等，在本书中，主要讨论攻击。

1.2.1　攻击来自何方

从一个网络系统的角度出发，可以简单地将相关人群分为两类：授权用户与非法用户。它们作为主体，具备了实施攻击的条件，而攻击的目标则是网络的三个基本要素——数据、

关系与能力。

如果对主体的权力进行一定的量化，并将非法用户的权力设置为零，那么可以简单地将攻击定义为权力的越级实施，包括越级获取数据、获得不应该具有的信任关系以及对系统能力的滥用（包括非法访问服务与干扰服务）。

攻击方法可以是技术性的，也可以是非技术性的。就技术性手段而言，在网络内部发动攻击更加容易。因此，在制定安全策略的时候，最好将内部网划分为不同的安全域，引入安全级别的概念，以防止权力的滥用。

以下对各种攻击进行分类说明。

1.2.2 如何攻击

攻击的分类并没有一个通用的标准，在这里将其大概分为以下六类：

1. 人因攻击

这种类型的攻击方法与人类社会其他领域的偷盗、欺骗行为并无分别，大多是采用如下两种手法：

- 社会工程（Social Engineering）：通过一些日常的交际手段来获取一些本来应该保密的信息，一个电话、一段闲聊、一封邮件都能完成一次攻击。这种攻击手法主要利用网络用户安全意识薄弱的弱点，例如冒充网络管理员打电话给用户，说由于系统维护的需要，要求用户提供自己的密码，非常简单但是在某些情况下却能轻易得逞。
- 盗窃行为：通过一些物理（与电子信息的窃取相对而言）的手段来偷窃保密信息，例如在合法用户登录时偷看密码等。

2. 物理攻击

这种攻击一般来说都是由内部人员发动，危害是最直接的，而且往往能够造成最大的破坏，因为攻击者获得了受保护系统的完全控制权。可以简单地将物理攻击分为两类：

- 物理破坏：对于计算机系统，一杯水可能就足够了。
- 物理访问：如果某个入侵者能够直接接触计算机设备，则基本上可以认为该设备的安全性已经丧失。例如直接用光盘/软盘启动系统，或者 Cisco 的路由器都可以通过一定的操作序列来修改 enable 口令。这种攻击方式与前一种的区别在于攻击的意图是获取信息或者控制系统。当然，如果这种企图失败，恼羞成怒之下，有可能导致“物理破坏”攻击。

以上两种攻击方法能够造成非常大的危害，但它们基本上不是技术性的或者说通过技术手段无法防范的。针对这二者，主要的措施是加强内部用户的安全教育以及采取各种物理安全措施，例如严密看管机房、增加各种物理访问口令（如微机的 CMOS 口令、SUN 的 PROM 口令等，虽然不是百分之百有效，但终归能够起到一定的作用）等，都能或多或少地防范这些攻击手法。

其余几种攻击方法都是技术性的，它们分别针对网络的三个要素发动，下面分别介绍。