Addison Wesley

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书

网络安全实施方法

[美] Thomas A. Wadlow 著
潇湘工作室 译
屈延文 审校

人民邮电出版社
www.pptph.com.cn

网络安全实施方法
Addison Wesley

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

网络安全实施方法

[美] Thomas A. Wadlow 著

潇湘工作室 译

屈延文 审校

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

网络安全实施方法/（美）沃德洛（Wadlow.T.A.）著；潇湘工作室译.—北京：人民邮电出版社，2000.10

（信息与网络安全丛书）

ISBN 7-115-08761-X

I. 网… II. ①沃…②潇… 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（2000）第 75316 号

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

网络安全实施方法

◆ 著 ［美］ Thomas A.Wadlow

译 潇湘工作室

审 校 屈延文

责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@ pptph.com.cn

网址 http://www.pptph.com.cn

北京汉魂图文设计有限公司制作

北京朝阳隆昌印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：787×1092 1/16

印张：12

字数：282 千字 2000 年 10 月第 1 版

印数：1－6 000 册 2000 年 10 月北京第 1 次印刷

著作权合同登记 图字：01－2000－0657 号

ISBN 7-115-08761-X/TP·1807

定价：21.00 元

内容提要

本书揭示了有效地保护网络安全的方法、技术和最佳应用惯例。本书的主要内容有：网络攻击和攻击者的特点，建立安全目标，进行网络安全的设计，建立团队，网络安全防御组件，实施物理和个人安全性，监视网络，发现和处理攻击行为，处理法律授权问题。本书的重点在于标准的操作过程以及日常的操作和维护，其中有许多避免网络安全中潜在的漏洞和威胁的内幕、观察方法内幕及忠告，从整个系统的角度（包括机器、人和过程）指出了如何分析、实现、评估和维护网络安全。

本书适合负责计算机/网络安全的管理人员和技术人员阅读。

信息与网络安全丛书 审定委员会

名誉主任：朱恩涛

主　　任：谢模乾

副 主 任：杜肤生

顾建国

徐修存

委　　员：（以下以姓氏笔划为序）

王亚明　冯登国　刘凤昌　吕晓春　杨智慧　屈延文

赵世强　赵战生　卿斯汉　高新宇　崔书昆　缪道期

丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999 年好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从 CIH 噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这些给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行、各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全；在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

由于本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局及部分计算机安全专家组成的审定委员会对图书进行了审阅，从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。

我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

版权声明

前 言

一天，一个朋友告诉我，他想回到原来的 Internet 上。在那时，人们按照需要正常地工作。每个人都是友善的。你可以向从没有见过的朋友发邮件，并且通常能够收到友善的回应。人们能够访问分布在全球的各种计算机，这些计算机能够提供或多或少的自由，以便你能登录上这些计算机，并查看当月的完成情况，或者只是与朋友交谈。如果需要做一些事情，一批聪明人会聚集在一起来完成此项工作，没有太多的忙乱或者是打扰。在很大程度上，它是一个友善的地方。

可是，这只是一种愿望，他的生活依赖于使用今天的 Internet，以及对明天的 Internet 的展望。他从 CNN 的网站和计算机界特定的站点（例如 Slashdot 和 Freshment）获得大量新闻。我已经想不起他上一次没带笔记本电脑的旅行是什么时候，不管他走到哪里，你都可以给他发电子邮件，并且（如果你通过了他的过滤软件）他会从东京、新加坡或者巴黎给予回答。Internet 可能是通过人类竞争创建的最复杂的事情，然而却是（当然是相对而言）容易使用的，并且其中具有你想要去的每个地方的信息。

但我理解他的观点。Internet 不再是过去那个友好的地方。原来，Internet 曾经是个小城，有着友好的邻居，不用锁门就可以离开家。现在，Internet 就是世界上最大（虚拟）的社区，并且每天都在逐渐增大。正如在地球上的其他城市一样，在城中有黑暗的地方，有强盗、小偷和骗子。你不可能被人狠打，但却可能被掠去时间或是钱财。

尽管如此，在现存的相同大小的所有社区中，Internet 可能是最安全的一个，但这不意味着轻松舒适。我这样说的原因是，我和同行不时地被邀请去查看 Internet 站点的安全性。我知道 Internet 在大多数时候是安全的，因为大多数的门仍旧不能打开，并且没有发生重大的事故。正因为如此，Internet 上的大多数人好像都不是坏家伙。但是，情况并不是这样的。

当然，在任何时候情况都可能发生改变。实际上改变已经开始。在 20 世纪 90 年代，越来越多的人在系统地捕获计算机的弱点。这些人并不是想去攻击特定的站点，他们只是在探听、查看他们能够获取什么。90 年代后期，开始出现了出于政治原因的 Internet 攻击。在编写本书的时候，由于发生了几起敌对的事件，并且很多非官方的通信都是通过 Internet 发出的，新闻媒体将科索沃冲突称为“第一次 Internet 战争”。

Internet 正在成为危险的地方。正确地看待这一点是重要的。任何大社区都有其不好的邻居、抢劫犯、蠢人和动荡的地方，但这并不意味着不能在那里安全地生活和工作。窍门是保持警惕，采取一些合理的预防措施，并且不要愚蠢地行动。同样的原则也适用于 Internet。

但在今天，计算机安全的意义远远超过一个人防止 Internet 上出现的危险的能力。它是一件自我保护的事情。实际上，对于保护成百上千甚至上万的计算机而言，这是非常不同的事情。

本书面向那些面临艰难挑战的人，以及那些竭力付出援助的人们。它不是关于如何成为黑客的教科书，也不是如何运行大型计算机网络的技术手册。已经有许多资料覆盖了这些主题。在此，我的目标是赋予负责管理大型公司的网络安全的个人一种工具，这种工具能帮助其理解网络和计算机安全的语言和实现。本书还提供了节省时间和防止节点受损的一些提示。如同任何大型工程一样，有很多方法可以解决这些问题。我没有说本书是综述了所有可能方法的唯一读物，然而它包括了很多好的方法、提示和窍门。

那么我是谁呢？我是经过培训的电子工程师，但我在上高中和大学时，就被计算机科学所吸引。我第一次使用 Internet 是在 20 世纪 70 年代后期，当时我发现能通过 ARPANET 从我念书的卡内基梅隆大学（CMU）连接到英国伦敦的一台计算机上。当时 ARPANET 才刚刚出现。如同在 CMU 的很多人一样，我在大学的计算机中心工作。和我在那里的同事不同的是，我一直从事大致相同的工作，在 Lawrence Livermore 实验室，Schlumberger 的 Palo Alto 研究中心，Xerox 的 Palo Alto 研究中心，ParcPlace Systems 和 Sun Microsystems 实验室里运行越来越大的计算机集合体和网络连接。通过这些经历，我已经学会了一些保证计算机巨大集合体“健壮”的一些知识，以及驱逐坏人、保证好人正常工作的一些知识。现在，我本人是 Pilot Network Services 公司的首席技术官（CTO）和安全副总裁，我帮助建立了这家公司，它的作用是为用户处理 Internet 的安全性，他们是地球上流动性最强和最有趣的（也是最大的）公司的一些分散分支的集合体。我们在商业安全方面运行的一些原则能在本书中找到。编写本书来说明我们如何工作可能会使你感到奇怪，因为它能使人们通过使用我们的原则来与我们竞争。好吧，请继续读下去。如果你仍然认为本书的内容是很容易的，请快速阅读。希望你认真读完本书。

Thomas A. Wadlow

目 录

第 1 章 理解安全性 …… 1

1.1 保护的内容 …… 1
1.2 防御考虑的问题 …… 2
1.3 本书的读者 …… 2
1.4 受保护的机构 …… 2
1.5 安全过程 …… 3
1.6 如何知道安全措施有效 …… 6
1.7 趋势分析 …… 7

第 2 章 编写安全策略 …… 9

2.1 陷阱 …… 10
2.2 实施意外活动 …… 10
2.3 策略的内容 …… 11

第 3 章 谁在攻击 …… 15

3.1 攻击者的种类 …… 16
3.2 将安全性作为不断发展的策略 …… 20

第 4 章 安全性设计过程 …… 23

4.1 安全性考虑因素 …… 23
4.2 安全原则 …… 25
4.3 防御形式 …… 34
4.3.1 机构的网络 …… 34
4.3.2 被动的外部防御 …… 35
4.3.3 主动的内部防御 …… 35
4.3.4 被动监视 …… 35
4.3.5 主动监视 …… 36

4.4 安全机构的形式 …… 36
4.4.1 反应团队 …… 37
4.4.2 诊断团队 …… 37
4.4.3 监察团队 …… 37
4.4.4 员工培训 …… 37

第 5 章 建立安全团队 …… 39

5.1 员工的品质 …… 39
5.2 安全团队的工作职能 …… 40
5.3 训练与交叉训练 …… 42
5.4 面试安全防卫的候选人 …… 43
5.5 背景调查 …… 43
5.6 聘用 …… 44
5.7 解聘 …… 45

第 6 章 加强网络组件 …… 47

6.1 什么是网络组件 …… 47
6.2 组件类型 …… 48
6.3 选择组件 …… 49
6.4 组件分类 …… 52
6.5 加强组件 …… 53
6.5.1 定制新组件 …… 55
6.5.2 升级旧组件 …… 56
6.6 系统加强 …… 57
6.6.1 配置操作系统 …… 58
6.6.2 应用补丁程序 …… 59
6.6.3 删除不必要的服务 …… 59
6.6.4 限制必要的服务 …… 60
6.6.5 禁用和删除不必要的软件 …… 60
6.6.6 结论 …… 61

第 7 章 个人安全 …… 63

7.1 管理层问题 …… 63
7.2 聘用过程 …… 64
7.2.1 面试过程 …… 64
7.2.2 试用期 …… 65
7.3 员工的问题 …… 65
7.4 解聘过程 …… 66
7.5 辞职过程 …… 66
7.6 承包商 …… 66

第 8 章　物理安全 …… 67

8.1　什么是威胁 …… 67
8.2　物理安全要素 …… 68
8.3　过份追求 …… 73
8.4　备份 …… 73
8.5　拒绝服务 …… 74
8.6　电源 …… 74
8.7　电话 …… 76
8.8　访问控制和日志分析 …… 77

第 9 章　监视网络 …… 79

9.1　记录系统的形式 …… 80
9.2　日志内容 …… 82
9.3　记录机制 …… 82
9.4　时间 …… 86
9.5　检测器 …… 87
9.6　记录系统设计 …… 87
9.7　日志管理 …… 89
9.8　日志分析 …… 91

第 10 章　网络审核 …… 93

10.1　审核的原因 …… 93
10.2　审核的种类 …… 94
10.3　审核的内容 …… 97
10.4　审核的人员 …… 98
10.5　期望 …… 100
10.5.1　应该期望从审核员那里得到什么 …… 100
10.5.2　审核员应该期望从你这里得到什么 …… 101
10.5.3　审核应该如何进行 …… 101
10.5.4　应该如何处理审核结果 …… 102

第 11 章　量化安全值 …… 103

11.1　对值的理解 …… 105
11.2　解释安全问题的过程 …… 108
11.3　测量 …… 109

第 12 章　准备处理攻击 …… 111

12.1　开始 …… 111
12.2　战争游戏 …… 112

12.3 事后分析 …… 115
12.4 建立反应计划 …… 116
12.5 人员 …… 119
12.6 安全设备 …… 120
12.7 生存包内容 …… 121
12.8 选择隐藏地点 …… 122
12.9 设置自己的章程 …… 123

第 13 章 处理攻击 …… 125

13.1 令人激动但并不有趣 …… 126
13.2 从反常的角度思考 …… 126
13.3 关于攻击 …… 130
13.4 能做的事情 …… 133
13.5 不应做的事情 …… 135
13.6 反应团队 …… 136
13.7 攻击期间的优先权 …… 138

第 14 章 诊断 …… 143

14.1 开始 …… 144
14.2 调查的艺术 …… 148
14.3 洁净室 …… 150
14.4 分析被感染的文件系统 …… 152
14.5 分析工具 …… 153
14.6 应该寻找什么 …… 155

第 15 章 日志分析 …… 159

15.1 一致性检查 …… 161
15.2 日志分析 …… 163
15.3 搜索 …… 164
15.4 建立理论 …… 165
15.5 合法性 …… 166

第 16 章 损害控制 …… 167

16.1 优先次序 …… 167
16.2 事先准备 …… 168
16.3 事后分析 …… 169

附录 术语表 …… 171

第1章 理解安全性

本章主要内容：

- 保护的对象。
- 防御考虑的问题。
- 本书的读者。
- 受保护的机构。
- 安全过程。
- 如何知道安全措施有效。
- 趋势分析。

本书的内容不是关于“安全”本身的。对于刚刚购买或者正翻阅本书，在考虑是否购买本书的读者，可能会认为这种说法很奇怪。但如果考虑词义本身，就能开始明白这样说的原因。一本有关锻炼的书、有关饮食或者治疗的书可能不是关于“健康”的，但都是介绍如何走向“健康”的过程。“健康”是你从来不能完全达到的理想境界之一。作为一种可达到的状态，“健康”是相对的。你或许足够健康，或者很健康，或者比我更健康，但你永远不会达到一种完美的状态。完美的“健康”状态永远也不能达到。但改善网络和 Internet 安全性的过程，也就是本书所讨论的内容，是值得人们掌握和理解的。

有时，为了理解一个概念，追溯到一些基本原理是很有帮助的。确切地说，要保障某些事物的安全到底意味着什么？为了找到这个问题的答案，首先要定义你正在保护的是什么。

1.1 保护的内容

有很多不同种类的安全，它们的要害是在保护的事务上面。核武器需要一种安全，摇滚音乐会需要另一种安全。破坏一种安全可能会终结世界，而破坏另一种安全可能仅仅听起来像是世界末日来临。

就本书而言，我们将不保护任何一种极端情况。本书的任务是讨论一个机构的安全，也就是某类企业，通常而言是商业企业的安全。我们将要讨论的一些主题适用于任何规模的机构。其他主题需要大型公司的资源，可能不适合较小或者较贫穷的实体。

我已经参与了很多机构网络的防御工作，其中有大型的也有小型的网络。通过多年的实践，我已经积累了一些经验。我认为的要点是这样的：

安全应该与正在保护的事物的价值相称。其中一部分价值是实际价值，一部分价值是

重建所需要做的工作，而另一部分更微妙的价值是再次信任网络所需要做的工作。

很多书介绍单一类型机器的安全，或者是关于特定软件配置的高技术问题。本书是理性的讨论，而不是一本技术教程。有关保护大型复杂网络的大多数问题并不是技术问题，而是防御者如何考虑其网络的内容的问题。

1.2 防御考虑的问题

安全不是技术。技术能够解决物理和工程的难题。它们是可重复的过程，足够小心的测量、深思熟虑的设计以及彻底的测试足以排除错误，使得它完全可靠。

在安全工程学中，人是其中的一个组成部分，他们可能是一些淘气的、邪恶的和聪明的人，他们可能会撒谎、欺骗和偷盗。他们也可能是诚实的、值得信赖的和乐于助人的人，他们聪明伶俐并且工作努力，但有时会感觉疲倦，并且不能理解他们所见事情的隐含意义。当你努力使一个过程自动化时，基本上是将人移出系统，以避免这些变化因素。你想要使来自工厂的钢材在工人心情差时与心情好时质量一样，利用自动过程便可以实现。

但在某些情况下，将永远不能使安全系统自动化，因为要考虑所有的变化因素。在循环中总有人作为攻击者，所以必须在此循环中有防御者。

1.3 本书的读者

本书面向具有一定规模的大型机构的计算机/网络安全管理员，稍后我们将讨论这样的机构。这样的管理员负责保证他所在机构的网络免受攻击。这样的机构比较大，需要有几个人组成一个团队与安全管理员共同工作。团队成员可能负责，也可能不负责这些计算机的日常系统管理，即使如此，他们也应当具备中等水平的技术来控制计算机。他们是能够阅读和理解程序的合格的程序员，能够从 Internet 上安装源代码包，并且熟悉他们使用的操作系统的大多数功能。

本书的部分内容针对安全小组中的领导者，他们具有同样的技术经验，并且实际上可能在此领域有更多的经历。这样的人是安全小组和他所在机构的管理层之间的桥梁。

这里谈到的安全团队是负责日常网络安全的唯一团队，这意味着这是一个中等规模的机构。

1.4 受保护的机构

如果你工作在具有 5 个人的房地产办公室，所有装有 Windows 98 的计算机都独立拨号连接 Internet，那么本书并不适合于你。本书针对中型到大型机构的安全保护工作，该机构正在使用几十台到几千台利用 TCP/IP 协议的计算机，并且通过一个或更多的专用高速链路连接到 Internet。该机构每天、每分钟的商业行为都要依赖它的网络。如果网络一小时不能

使用，就会是严重的事件。很多计算机是不同类型的台式计算机，但此网络上的一些计算机是在商业上起重要作用的计算机，并且持续保证它们的安全是机构管理的主要重点。

网络和在商业上起重要作用的计算机的操作是由机构中的其他团队负责的，这不是安全团队的责任。如果磁盘驱动器发生错误，或者文件必须从备份磁带上进行恢复，会有其他人去解决。安全团队负责与网络安全有关的所有设备的管理和运行。

1.5 安全过程

我们已经说过，安全不是技术。人们不能买到保证网络安全的万能设备，也不能买到或者编写一段保证计算机安全的程序。上面陈述的谬误之处在于，它们暗示安全是你能达到的一种状态。但你却不能。安全是前进的方向，但实际上你永远也不能到达目的地。你能做的和本书要做的事情，是管理人们能够接受的危险级别。

安全不是静态的，这是安全的另一个重要因素。在很多方面，Internet 安全行业的工作就像正在攀登一个不停下降的升降机。你能急剧上升几步，然后为了呼吸而停下来，而当你休息时，会发现升降机已经将你向下移回或越过原处。为了停留在原处，你必须连续不断地努力。为了取得进步、变得更安全，必须一直进行更多的努力。正如一个升降机一样，它不只是你进行努力的程度，而且努力应按照正确的方向进行。

本书最重要的概念是：

安全是一个过程。你应当能将该过程一次又一次地应用于网络和支持它的机构，并且通过这样的操作，可以提高系统的安全性。如果停止应用该过程，或者还没有开始应用，由于新的攻击和手法不断出现，安全性就会变得越来越差。

安全过程是什么？在很多方面，它与古希腊三位一体的概念很相似，如图 1-1 所示。

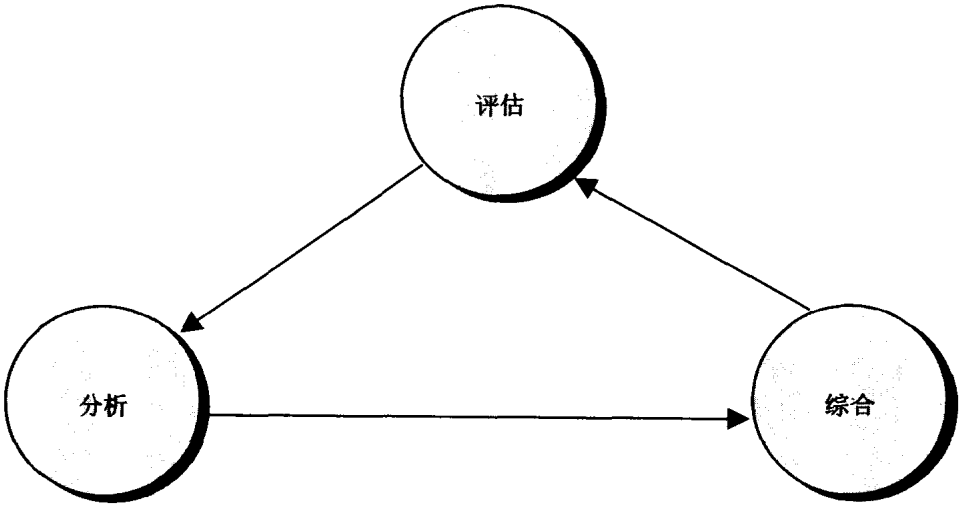

图 1-1 希腊的三位一体图

根据所知道的事情**分析**面对的问题。