SAMS 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

网络安全指南

[美] Peter Norton
Mike Stockman 著
潇湘工作室 译

人民邮电出版社
www.pptph.com.cn

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

网络安全指南

Peter Norton
[美] 著
Mike Stockman

潇湘工作室 译

人民邮电出版社

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

网络安全指南

◆ 著　　[美] Peter Norton　Mike Stockman
译　　潇湘工作室
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
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787 × 1092　1/16
印张:11.75
字数:272 千字　　2000 年 11 月第 1 版
印数:1 - 6 000 册　　2000 年 11 月北京第 1 次印刷

著作权合同登记　图字:01 - 1999 - 2553 号
ISBN 7-115-08879-9/TP·1896

定价:22.00 元

内容提要

本书完整地介绍了有关网络安全的基础知识，其主要内容有：各种不同网络的运作方式，网络潜在的安全漏洞的产生方式；查找和修复网络缺陷；各种网络防火墙的应用方式；不危及网络安全的访问网络方式；拨入访问和虚拟专用网的安全使用；添加身份验证，以阻止口令攻击和网络快客入侵。

通过对本书的学习，读者可以解决常见的网络系统和协议的问题，保证系统工作正常和安全；掌握增强网络安全性的工具的使用方法和技巧，如扫描网络漏洞，对快客设置网络服务的圈套。无论读者是网络新手还是富有经验的网络高手，都可以从本书中获得所需要的答案、解释和实例。

本书适用于网络管理员和信息安全管理人员。

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

本书适用于各种级别的网络管理员，其目的是使网络管理员可以对涉及到保持网络安全、防止任何入侵网络的行为（不管这种入侵是发生在网络外部，还是在网络内部）的有关问题和实践有一个总体的认识。自从计算机首次开始相互通信以来，网络安全这个领域已经非常重要了，尤其是在近几年，随着越来越多的计算机配备了网卡和内置网络软件，人们对这个领域的兴趣也随之增长，而网络基础设施（各种线缆、集线器、路由器等）的价格已经直线下跌。

在对已经与 Internet 相连接的网络安全的兴趣背后，是一种更强有力的推动力——Internet 不仅比以往任何时候更可供使用，而且速度变得更快、访问性更好。“随时在线”对线缆调制解调器和 DSL（Digital Subscriber Lines，数字用户线）来说是个巨大的市场卖点，但将用户连到 Internet 上的网络连接，同样也允许其他人经由同一路径进入到用户的网络。本书将向读者展示如何限制对网络的访问，以便尽可能多地控制那些可以看到和修改至关重要的系统和数据的人。

有关为什么要保持网络安全的说法都是很有道理的。快客（恶意的计算机罪犯，相对那些探查并操纵和控制计算机的没有险恶意图的黑客而言）不断地想出新办法，通过利用服务器上的错误、Web 浏览器的缺陷、访问权限的配置不当、口令设置的脆弱性、特洛伊木马程序以及其他各种各样的手段来入侵网络。更糟糕的是新发现的安全上的漏洞很快就被“脚本小孩（script kiddies）”或那些没有经验和能力自己发现这些漏洞，但却似乎有着无限的时间来利用别人发现的网络漏洞的人所利用。

不存在什么绝对安全的服务器、路由器、网络操作系统或其他网络组件。也没有什么不可摧毁的网络，除非计算机根本不连网。对用户来说，最有力的防范方法就是准备充分、信息完整。本书可以帮助读者做好这两方面的起始工作，这样就可以防止大多数的网络入侵，并且，一旦网络受到攻击，就发出通知。本书也可以帮助读者了解有关网络攻击活动的原理，应在何处查出最新的网络缺陷和修正办法以及很多替代方法。

在这场保卫信息和系统的战斗中，用户的同盟是那些网络安全分析专家，如 LOpht Heavy Industries 和 eEye；一些政府和教育部门的网络安全机构，如 CERT 和 CIAC；以及可以增

加到网络中的保护性的网络安全的产品，如防火墙、路由器和入侵检测系统。全书中都提到了这些同盟者，并在附录中列出（只是一部分，并不冗长）。

本书也提到了在这场与网络快客的战斗中如何赢得最基本的同盟者（网络用户）的合作。通过对网络用户的教育，可以防止受到社会工程的攻击（因网络用户受骗而导致的对网络的非法访问）、口令攻击（因为口令太简单而导致的网络漏洞）和一些其他形式的来自网络内部和外部的攻击。如果没有对网络用户的教育和取得他们的合作，本书中提到的解决方案没有一个可以使网络保持长久的安全。

最后，本书讲述了读者可以提供的访问网络的方法，而不是限制访问，但是要以一种在支持网络用户的同时又能保护资源的方式来访问。

本书读者

本书的主要读者是网络管理员（无论管理何种规模的网络，他们关心的是网络系统的安全）和那些想尽可能安全地访问网络的人。如果读者正在管理网络（无论是2台还是2000台计算机）的配置和访问，可能就会用得上本书。使用本书，读者将会理解如何以及在何处会犯下错误，并且减少风险，而不必首先就放弃网络——放弃在计算机用户和资源之间通信。

本书是按照这样一种方式来写作的：要对所有的网络管理员有用，无论读者是从昨天才开始这份工作，还是已经具有好几年管理企业网络的经验。读者应当对在工作中使用的网络操作系统的概念很熟悉，本书对超出这个范围的大多数概念还是讲述得很详细彻底，而没有不必要的，或者说是非常技术性的描述。

本书适用于任何类型计算机网络的网络安全方面的问题，无论是用线缆调制解调器的两台计算机和一台打印机建立的家庭网络，还是管理全球范围内的由数以千计的系统用专线或Internet连接形成的三个站点。

我们将一起花时间讨论 Mac OS、Windows 和 UNIX 这样的操作系统，还有 Windows 网络、UNIX 和 Novell NetWare 服务器。其中每一种都有自己的长处和缺陷，而每一种都需要维护和更新以便尽可能地安全。

如果读者想好好了解网络安全性和可用的解决方案，本书就非常合适。

主要内容

下面是本书中讲到的一些重要的主题：

- 不同类型的网络的运行原理和所产生的潜在的安全漏洞。
- 用户可能会遇到的网络攻击和危险的类型。

- 找出用户自己网络中的缺陷，并且修正它。
- 在网络安全性与使用方便性之间的平衡问题，以及如何达到平衡以使用户获益。
- 在用户网络上采取的安全措施，包括各种防火墙。
- 应在用户网络上的何处采取安全措施以起到最大的保护作用？
- 如何提供网络访问而不危及安全？
- 拨入访问和虚拟专用网（VPN），以及用户如何安全使用它们。
- 口令，为什么口令必须很强健以及如何强化它。
- 提供给网络用户的设置口令的规则。
- 加入认证以阻止口令攻击和网络快客入侵。
- 在建立用户网络之前要提出和回答的几个问题。
- 为什么提供的服务越少越安全，以及如何平衡服务和安全性之间的关系。
- 桌面操作系统(如 Mac OS 和 Windows)的非常有力的网络特征，以及如何确保它们不会损害网络的安全性。
- 网络操作系统(如 Windows NT、Novell NetWare 和 UNIX)的有力特征，以及如何确保它们不会危及网络的安全性。
- 如何知道网络已经被侵袭，以及如何处理。
- 在何处可获得网络安全最新的产品、新闻和安全升级产品。

在防范网络风险之前要先了解网络中的风险，在实施网络安全的解决方案之前则要先理解它。一旦采集了必要的信息，并且建立了一套平衡方便性和安全性的网络安全规划，就可以保证网络安全，防止入侵，让网络按照它的本来设计意图运行，使网络用户的生活更顺利。

目 录

第一部分 识别危险

第 1 章 网络和安全性概述 …… 3

1.1 什么是安全性 …… 3

1.1.1 *安全性与便利性* …… 4

1.1.2 *为什么网络易受攻击* …… 5

1.2 关于局域网 …… 7

1.2.1 *局域网简介* …… 7

1.2.2 *有关局域网的安全主题* …… 8

1.3 关于广域网 …… 8

1.3.1 *广域网简介* …… 8

1.3.2 *有关广域网的安全主题* …… 9

1.4 关于防火墙 …… 9

1.4.1 *防火墙简介* …… 9

1.4.2 *有关防火墙的安全主题* …… 10

1.5 关于万维网和 HTTP …… 10

1.5.1 *万维网* …… 10

1.5.2 *Web 服务器的安全主题* …… 10

1.6 关于虚拟专用网 …… 11

1.6.1 *虚拟专用网简介* …… 11

1.6.2 *虚拟专用网连接的安全主题* …… 11

1.7 关于远程访问和远程控制 …… 11

1.7.1 *远程访问和远程控制* …… 11

1.7.2 *远程访问和远程控制的安全主题* …… 12

1.8 本章小结 …… 12

第 2 章 风险和规划安全性 …… 13

2.1 安全威胁的主要类型和分类 …… 14

2.2 拒绝服务攻击 …… 14
2.2.1 *SYN 湮没* …… 15
2.2.2 *Land 攻击* …… 16
2.2.3 *Smurf 攻击* …… 16
2.2.4 *IP 地址欺骗* …… 16
2.2.5 *Teardrop（和 Bonk/Boink/Nestea/其他）* …… 16
2.2.6 *死亡之 ping* …… 17
2.2.7 *其他拒绝服务攻击* …… 17
2.3 缓冲区溢出 …… 17
2.3.1 *缓冲区的描述* …… 17
2.3.2 *何时缓冲区溢出成为攻击* …… 18
2.3.3 *利用 CGI* …… 18
2.4 特洛伊木马 …… 19
2.5 入侵者和物理安全性 …… 20
2.6 拦截传送 …… 20
2.7 社会工程 …… 21
2.8 缺乏用户支持 …… 22
2.9 本章小结 …… 22

第 3 章 确定网络风险 …… 23

3.1 查找网络的安全漏洞 …… 23
3.1.1 *密切注意新闻* …… 23
3.1.2 *使用端口扫描器* …… 24
3.1.3 *使用网络扫描程序* …… 25
3.1.4 *典型的安全漏洞* …… 27
3.2 使用网络入侵程序 …… 29
3.3 修补安全性漏洞 …… 29
3.3.1 *教育用户* …… 29
3.3.2 *软件更新和补丁程序* …… 32
3.3.3 *更改软件选项* …… 33
3.4 隐蔽的安全性 …… 33
3.5 本章小结 …… 34

第二部分 安全工具

第 4 章 关于防火墙 …… 37

4.1 防火墙的工作方式 …… 38
4.1.1 *包过滤防火墙* …… 38
4.1.2 *有状态（或动态）的包检查防火墙* …… 40

4.1.3 *应用程序代理防火墙* …… 43
4.1.4 *NAT 路由器* …… 44
4.1.5 *个人防火墙* …… 45
4.2 虚拟专用网 …… 47
4.2.1 *优缺点* …… 48
4.2.2 *VPN 服务器的来源* …… 48
4.3 防火墙的设置位置 …… 48
4.4 DMZ 网络 …… 49
4.5 报告网络攻击尝试 …… 49
4.6 阻止未授权的传入访问 …… 50
4.7 阻止未授权的传出访问 …… 50
4.8 本章小结 …… 51

第 5 章 保证用户连接安全 …… 53

5.1 确定用户需求 …… 53
5.1.1 *没有实际连接到网络上时需要的网络服务* …… 54
5.1.2 *需要使用哪种协议* …… 54
5.1.3 *不在现场时使用哪种连接方式* …… 54
5.2 拨入网络服务 …… 55
5.2.1 *优缺点* …… 55
5.2.2 *关于远程访问服务器* …… 56
5.2.3 *建立拨入网络访问* …… 57
5.2.4 *认证* …… 58
5.3 虚拟专用网 …… 61
5.3.1 *优缺点* …… 62
5.3.2 *可用的 VPN 加密方法* …… 62
5.3.3 *建立 VPN 服务器* …… 64
5.4 外部用户的其他 Internet 服务 …… 65
5.4.1 *外壳和文件访问* …… 66
5.4.2 *安全文件传输选项* …… 68
5.5 保护电子邮件 …… 69
5.5.1 *VPN 和拨入网络连接* …… 69
5.5.2 *邮件服务器拨入* …… 70
5.5.3 *防火墙和邮件服务器的安全访问* …… 70
5.6 本章小结 …… 71

第 6 章 认证和口令 …… 73

6.1 创建安全的口令 …… 74
6.1.1 *口令长度* …… 75
6.1.2 *口令的复杂性* …… 76

6.1.3 *更改口令的频率* …… 77
6.1.4 *避免重复的口令* …… 79
6.2 用户守则 …… 79
6.2.1 *守则1：决不要写下口令* …… 80
6.2.2 *守则2：使用一个以上的单词构成口令* …… 80
6.2.3 *守则3：使用短语建立口令* …… 80
6.2.4 *守则4：决不在别人注视键盘或屏幕时输入口令* …… 80
6.2.5 *守则5：经常修改口令（即使系统没有要求）* …… 81
6.2.6 *守则6：如果怀疑口令泄露则立即改变口令* …… 81
6.2.7 *守则7：不要告诉任何人（包括我）你的口令* …… 81
6.3 使用内置的认证 …… 81
6.4 添加额外的或第三方认证 …… 82
6.4.1 *RADIUS 和TACACS+* …… 82
6.4.2 *Kerberos* …… 83
6.4.3 *公开密钥加密方法* …… 84
6.5 智能卡和一次性口令 …… 84
6.5.1 *智能卡* …… 85
6.5.2 *安全令牌* …… 85
6.5.3 *一次性口令* …… 86
6.6 本章小结 …… 87

第三部分 策略与实施

第7章 规划网络 …… 91

7.1 建立网络前要问的问题 …… 91
7.1.1 *网络上应运行何种服务* …… 91
7.1.2 *需要连接哪些实际站点* …… 92
7.1.3 *将要使用何种操作系统* …… 93
7.2 建立服务与禁用不必要的服务 …… 94
7.2.1 *需要运行的协议* …… 94
7.2.2 *不安全的服务及其安全替代措施* …… 96
7.2.3 *扫描网络查找安全漏洞* …… 99
7.3 本章小结 …… 100

第8章 主要网络操作系统概述 …… 101

8.1 确保网络服务器安全的步骤 …… 102
8.2 规划安全性和访问级别 …… 102
8.2.1 *划分安全需要* …… 103
8.2.2 *将用户分成逻辑组* …… 103

8.2.3 *建立维护过程* …… 104
8.2.4 *培训用户* …… 104
8.3 Windows NT 和 Windows 2000 …… 105
8.3.1 *主要安全问题* …… 105
8.3.2 *NT 安全机制的运行方式* …… 106
8.3.3 *使系统更安全* …… 107
8.3.4 *建立安全访问控制列表策略* …… 112
8.4 Novell NetWare 5 …… 115
8.4.1 *NetWare 安全机制的运行方式* …… 115
8.4.2 *使系统更安全* …… 116
8.5 UNIX 操作系统 …… 120
8.5.1 *主要安全问题* …… 120
8.5.2 *UNIX 安全机制的工作方式* …… 121
8.5.3 *使系统更安全* …… 121
8.6 本章小结 …… 126

第 9 章 桌面系统的安全性 …… 129

9.1 用户工作站的问题 …… 130
9.1.1 *共享过多* …… 131
9.1.2 *Web 和 FTP 服务* …… 132
9.1.3 *其他更好的服务* …… 132
9.2 Windows 95/98/NT 工作站 …… 132
9.2.1 *用户连接服务的方式* …… 133
9.2.2 *启用什么和采取的安全预防措施* …… 134
9.2.3 *将 Windows 桌面系统与网络服务相连* …… 136
9.2.4 *NetBEUI 或 IP 上的 Windows 网络* …… 139
9.3 Mac OS …… 141
9.3.1 *用户如何连接服务* …… 141
9.3.2 *启用什么和采取的安全预防措施* …… 142
9.3.3 *Macintosh 桌面系统连接到网络服务* …… 145
9.3.4 *AppleTalk 或 IP 上的 AppleShare* …… 148
9.4 UNIX/Linux …… 149
9.4.1 *UNIX 桌面系统连接到网络服务* …… 149
9.4.2 *其他类 UNIX 的操作系统服务器* …… 150
9.5 总体推荐 …… 150
9.6 本章小结 …… 151

第 10 章 网络被入侵的应对措施 …… 153

10.1 网络入侵检测系统 …… 153
10.1.1 *基于主机的 IDS* …… 154

10.1.2 *基于网络的IDS* …… 154
10.1.3 *IDS如何适应网络* …… 155
10.1.4 *IDS的优缺点* …… 155
10.1.5 *IDS的推荐* …… 156
10.2 关于端口扫描 …… 156
10.2.1 *端口扫描及含义* …… 156
10.2.2 *来自同一网络的重复连接或尝试* …… 157
10.2.3 *何种情况可能已经被端口扫描* …… 158
10.2.4 *已被扫描了端口时应该做什么* …… 159
10.3 关于活动日志 …… 159
10.4 活动警告 …… 159
10.5 如何处理网络入侵 …… 160
10.5.1 *不使用网络通知组织内部* …… 160
10.5.2 *关闭网络漏洞* …… 161
10.5.3 *通知滥用的帐户和系统管理员* …… 161
10.5.4 *备份系统* …… 161
10.6 诱骗快客（引诱上钩） …… 162
10.7 本章小结 …… 162

附录 跟踪安全措施的发展 …… 163

1 政府和学术组织 …… 163
1.1 *CERT（计算机紧急响应小组）* …… 164
1.2 *其他计算机事件和安全性教育站点* …… 164
2 制造商的Web站点 …… 165
3 安全性和黑客组织 …… 165
4 新闻组 …… 166
5 附录小结 …… 167