高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

Security Scan

安全扫描技术

张玉清　戴祖锋　谢崇斌　编著

http://www.tup.com.cn

清华大学出版社

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Security Scan

安全扫描技术

张玉清 戴祖锋 谢崇斌 编著

清华大学出版社
北京

内容简介

全书共10章，系统、全面地介绍了网络安全中的扫描技术，对目前主要扫描技术给出了详实的理论讲解和实例分析，以便让读者能够对安全扫描技术有一个深入而全面的了解。本书的主要内容包括：扫描概述、漏洞、端口扫描、认证扫描、代理扫描、操作系统指纹扫描、安全扫描器、反扫描技术以及扫描技术的应用与发展趋势，最后简单介绍了系统安全评估技术。

本书内容丰富，条理清晰，深入浅出，适合作为信息安全、计算机、通信等相关专业本科生、研究生的教材，也可供从事网络与信息安全工作的科研人员以及对网络与信息安全感兴趣的读者参考。

图书在版编目(CIP)数据

安全扫描技术 / 张玉清，戴祖锋，谢崇斌编著. —北京：清华大学出版社，2004.7
(高等院校信息安全专业系列教材)
ISBN 7-302-08419-X

Ⅰ. 安…　Ⅱ. ①张… ②戴… ③谢…　Ⅲ. 扫描－高等学校－教材　Ⅳ. TN27

中国版本图书馆 CIP 数据核字(2004)第 028028 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010 62776969
组稿编辑：张　民
文稿编辑：霍志国
封面设计：孟繁聪
印 装 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：15.5　**字数**：303 千字
版　　次：2004 年 7 月第 1 版　2004 年 7 月第1 次印刷
书　　号：ISBN 7-302-08419-X/TP・6054
印　　数：1～5000
定　　价：24.00 元

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已设立了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业作出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

2003年7月于北京

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，国家对信息安全人才的需求量不断增加，但目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整，结构合理，内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足读者对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养作出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

中国计算机学会教育专业委员会

清华大学出版社

2003 年 7 月

前言

信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入新时代；信息系统的建立已逐渐成为社会各个领域不可或缺的基础设施；信息已成为重要的战略资源，信息化的水平已成为衡量一个国家现代化和综合国力的重要标志。

随着以因特网为代表的信息网络的普及和推广，如何有效地保障信息网络安全和可靠的运转成为目前学术界和产业界探讨的热点和焦点。目前，让黑客有机可乘的安全漏洞越来越多，精心设计的攻击和恶意代码在互联网上肆意流行，可随意下载，已达到可以“傻瓜”使用的程度，加上目前网络入侵检测能力的局限性，以及网络和系统管理配置的复杂性等技术方面的问题，使得网络不可避免地会受到这样或那样的安全攻击。因此如何有效地运用技术手段增强信息网络的健壮性、可靠性和安全性已成为国内外网络与信息安全界业内人士的研究重点。其中，安全扫描技术是一个极为有效的积极预防手段。

安全扫描技术目前应用非常广泛，它是检测远程或本地系统安全脆弱性的一种安全技术。扫描技术把极为烦琐的安全检测，通过程序来自动完成。同时，也可以认为扫描技术是一种网络安全性评估技术。安全扫描是对系统脆弱性的分析和评估，从而能够检查、分析网络范围内的设备、网络服务、操作系统、数据库系统等各类系统的安全性，为提高网络安全的等级提供决策的支持。同时扫描技术也是黑客攻击的常用技术之一，因此也应该了解扫描技术的原理，才能有针对性地采取反扫描技术保护系统。

本书全面介绍了网络安全中的扫描技术，并对目前的主要扫描技术给出了详实的理论讲解和实例分析，以便让读者能够对扫描技术有一个深入和全面的了解。本书作者都是国家计算机网络入侵防范中心从事网络入侵防范研究的科研工作者，以自身对扫描技术的切身体会和科研实践在本书中对安全扫描技术进行了深入的研究和探讨，希望将安全扫描技术的全貌介绍给各

位读者，并为国内信息安全学科的人才培养提供一些帮助。同时，希望用本书来抛砖引玉，并与国内对网络安全有兴趣的人士共同交流和进步。

参加本书编著的人员有张玉清、戴祖锋、谢崇斌、洪宏、翟钰和朱岩等，全书由张玉清统稿。由于时间和能力有限，难以做到尽善尽美，不当之处在所难免，恳请读者批评指正。我们的 E-mail 地址：Zhangyq@nipc.org.cn。

作　者

2004 年 3 月于北京

目录

第 1 章　概述 …… 1

1.1　网络安全概述 …… 1

1.2　安全漏洞概述 …… 2

1.2.1　安全问题的根源 …… 2

1.2.2　漏洞的危害 …… 3

1.2.3　漏洞的防范 …… 4

1.3　安全扫描技术概述 …… 4

1.3.1　基本概念 …… 4

1.3.2　发展历史 …… 5

1.3.3　重要性 …… 5

1.3.4　基本特点 …… 6

1.4　安全扫描器概述 …… 6

1.4.1　功能 …… 6

1.4.2　分类及其结构 …… 7

1.4.3　应用 …… 8

1.5　小结 …… 8

习题 …… 9

第 2 章　漏洞 …… 10

2.1　漏洞概述 …… 10

2.1.1　漏洞的概念 …… 10

2.1.2　漏洞造成的危害 …… 11

2.1.3　漏洞产生的原因 …… 13

2.1.4　漏洞的发现 …… 13

2.2 漏洞的分类分级 …… 14
2.2.1 国外的相关研究 …… 14
2.2.2 漏洞分类 …… 15
2.2.3 漏洞分级 …… 18
2.3 漏洞库及其使用 …… 19
2.3.1 漏洞库概述 …… 19
2.3.2 CVE 漏洞库 …… 19
2.3.3 其他漏洞库 …… 21
2.3.4 漏洞库实例 …… 21
2.3.5 常见漏洞 …… 24
2.4 漏洞的检测与修补 …… 28
2.4.1 漏洞的检测 …… 28
2.4.2 漏洞的修补 …… 31
2.5 小结 …… 32
习题 …… 32

第 3 章 端口扫描 …… 34
3.1 端口扫描的概述 …… 34
3.1.1 TCP/IP 相关知识 …… 34
3.1.2 端口介绍 …… 40
3.1.3 端口扫描的概念 …… 42
3.1.4 端口扫描的分类 …… 43
3.2 常见端口扫描技术 …… 44
3.2.1 TCP connect 扫描 …… 44
3.2.2 TCP SYN 扫描 …… 47
3.2.3 秘密扫描 …… 48
3.3 其他端口扫描技术 …… 51
3.3.1 UDP 扫描 …… 51
3.3.2 IP 头信息 dumb 扫描 …… 52
3.3.3 IP 分段扫描 …… 52
3.3.4 慢速扫描 …… 52
3.3.5 乱序扫描 …… 53
3.4 端口扫描工具 …… 53

3.4.1 常用网络扫描命令 …… 54
3.4.2 Nmap …… 56
3.4.3 其他端口扫描工具 …… 61
3.5 小结 …… 65
习题 …… 65

第 4 章 认证扫描和代理扫描 …… 66
4.1 认证扫描和代理扫描的概念 …… 66
4.2 认证扫描 …… 66
4.2.1 认证协议 …… 67
4.2.2 认证扫描的原理 …… 67
4.2.3 认证扫描的实现 …… 67
4.3 代理扫描 …… 71
4.3.1 FTP 协议 …… 71
4.3.2 代理扫描的原理 …… 78
4.3.3 代理扫描的实现 …… 79
4.4 小结 …… 80
习题 …… 80

第 5 章 操作系统指纹扫描 …… 81
5.1 概述 …… 81
5.1.1 背景知识 …… 81
5.1.2 相关技术及其分类 …… 83
5.2 TCP/IP 栈指纹扫描技术 …… 86
5.2.1 TCP/IP 协议栈的特性 …… 87
5.2.2 TCP/IP 栈指纹扫描实例分析 …… 89
5.3 ICMP 栈指纹扫描技术 …… 94
5.3.1 ICMP 协议 …… 94
5.3.2 ICMP 栈指纹 …… 96
5.3.3 ICMP 栈指纹扫描实例分析 …… 100
5.4 操作系统被动指纹扫描技术 …… 103
5.4.1 实现原理 …… 103
5.4.2 被动指纹扫描实例分析 …… 105

5.5 小结 …… 106
习题 …… 107

第 6 章 安全扫描器 …… 108
6.1 安全扫描器概述 …… 108
6.1.1 安全扫描器的概念 …… 108
6.1.2 安全扫描器的历史 …… 109
6.1.3 安全扫描器的分类 …… 110
6.1.4 安全扫描器的功能 …… 110
6.2 安全扫描器的原理、逻辑结构及相关技术 …… 113
6.2.1 安全扫描器的原理 …… 113
6.2.2 安全扫描器的逻辑结构 …… 115
6.2.3 安全扫描器的相关技术 …… 116
6.3 安全扫描器的设计 …… 118
6.3.1 安全扫描器的需求分析 …… 118
6.3.2 主机型安全扫描器的设计 …… 119
6.3.3 网络型安全扫描器的设计 …… 121
6.4 网络型安全扫描器开发实例 …… 123
6.4.1 系统设计 …… 123
6.4.2 系统实现 …… 127
6.5 小结 …… 130
习题 …… 131

第 7 章 反扫描技术 …… 132
7.1 反扫描概述 …… 132
7.1.1 反扫描技术的原理 …… 132
7.1.2 反扫描技术的组成 …… 133
7.2 防火墙技术 …… 134
7.2.1 防火墙基础知识 …… 134
7.2.2 包过滤技术 …… 135
7.2.3 应用代理技术 …… 137
7.2.4 状态检测技术 …… 139
7.3 入侵检测技术 …… 140

7.3.1 入侵检测系统基本结构 …… 141
7.3.2 入侵检测的标准化 …… 145
7.3.3 入侵检测系统的实现方式 …… 147
7.3.4 入侵检测模型 …… 149
7.4 审计技术 …… 152
7.4.1 审计系统模型 …… 153
7.4.2 审计系统分类 …… 153
7.4.3 安全审计实现方法 …… 154
7.4.4 审计记录标准 …… 155
7.5 访问控制技术 …… 156
7.5.1 自主访问控制模型 …… 157
7.5.2 强制访问控制模型 …… 157
7.5.3 基于角色的访问控制模型 …… 158
7.5.4 基于任务的访问控制模型 …… 160
7.6 其他反扫描技术 …… 160
7.7 小结 …… 162
习题 …… 163

第 8 章 扫描技术的应用 …… 164
8.1 扫描技术应用概述 …… 164
8.1.1 扫描技术概述 …… 164
8.1.2 扫描技术的应用效果 …… 166
8.2 扫描技术应用分类及实例 …… 168
8.2.1 安全扫描器应用分类及实例介绍 …… 168
8.2.2 扫描结果分析与处理 …… 177
8.2.3 安全扫描器的选择 …… 178
8.2.4 应用举例 …… 179
8.3 扫描技术的应用原则 …… 181
8.4 小结 …… 182
习题 …… 183

第 9 章 扫描技术的发展趋势 …… 184
9.1 信息安全的当前研究现状及发展趋势 …… 184

9.2 扫描技术的发展趋势 …… 188
9.2.1 扫描技术 …… 188
9.2.2 扫描器 …… 190
9.2.3 扫描策略 …… 192
9.3 扫描器的评测标准 …… 193
9.4 小结 …… 194
习题 …… 194

第 10 章 系统安全评估技术 …… 195
10.1 安全评估概述 …… 195
10.1.1 安全评估相关概念 …… 195
10.1.2 安全评估的意义 …… 196
10.1.3 安全评估标准发展过程 …… 197
10.2 安全评估的流程、方法和工具 …… 199
10.2.1 安全评估流程 …… 199
10.2.2 安全评估方法 …… 200
10.2.3 安全评估工具 …… 201
10.2.4 国内安全评估权威认证机构 …… 203
10.3 常见安全评估标准 …… 204
10.3.1 BS7799 标准介绍 …… 204
10.3.2 技术安全评估通用标准(CC) …… 205
10.3.3 安全保护等级划分准则 …… 211
10.3.4 标准应用的注意要点 …… 214
10.4 小结 …… 215
习题 …… 215

附录 服务端口列表 …… 216

参考文献 …… 226

第1章 概 述

覆盖全球的因特网，以其自身协议的开放性方便了各种计算机网络的入网互联，这极大地提高了人们的工作效率和生活的便利性。但是，由于早期网络协议对安全问题的忽视，以及在使用和管理上的无序状态，使得网络安全受到严重威胁，安全事故频频发生。

从诸多安全事故中可以看出，大部分的安全事件是由于攻击者利用了网络或者主机的安全漏洞而造成的。安全漏洞在网络安全中越来越受到重视。尽早发现这些存在的漏洞，已经成为网络和主机安全防范的最重要的一步。下面简单介绍网络安全、安全漏洞、安全扫描技术以及安全扫描器等4个方面的基本情况。

1.1 网络安全概述

网络安全是信息安全的引申。信息安全是对信息的保密性、完整性和可用性的保护。网络安全是对网络信息保密性、完整性和网络系统的可用性的保护，目标是为了确保网络系统的信息安全。网络安全包括物理安全、网络系统安全、数据安全、信息内容安全和信息基础设施安全等。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避免各种偶然的或人为的破坏或攻击，使它们发挥正常，保障系统能安全可靠地工作。

网络安全与经济安全、社会安全和国家安全紧密相连，涉及个人利益、企业生存、金融风险防范、社会稳定和国家安全诸方面，是信息化进程中具有重大战略意义的问题。

网络安全风险来源于内部脆弱性和外部威胁。内部脆弱性风险的防范属于主动控制范畴，外部威胁风险的防范属于被动控制范畴。必须全方位解析网络的脆弱性和威胁，才能构建网络安全措施以确保网络安全。

网络安全技术涉及的内容是很广泛的。从广义上讲，网络安全技术主要包括以下几个方面：主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术和黑客跟踪技术等。

为了实现网络安全，当前采用的安全机制主要包括：加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、报文认证、信息流填充机制、路由控制机制和公正

机制等。

一个完整的网络安全解决方案所考虑的问题应当是非常全面的。保证网络安全需要利用一些安全技术，但是，最重要的是要有详细的安全策略和良好的内部管理机制。

在确立网络安全的目标和策略之后，还要确定实施网络安全所应付出的代价，然后选择确实可行的技术方案。方案实施完成后最重要的是加强管理，制定培训计划和网络安全管理措施。一个完整的安全解决方案应该覆盖网络的各个层次，并且与安全管理相结合。

1.2　安全漏洞概述

对网络安全造成威胁的方面很多，包括计算机犯罪、电子故障、人为因素和自然灾害等诸多方面。当前因特网上面临最大的威胁就是计算机犯罪问题，主要体现在一些来自网络外部或者内部的恶意攻击或入侵。通常，攻击者或者入侵者最常利用的就是网络或主机中存在的安全漏洞。下面首先分析安全问题的根源，然后总结安全漏洞的危害和防范。

1.2.1　安全问题的根源

网络中随时都存在着许多的安全威胁与攻击。这些威胁和攻击主要针对网络中存在的安全问题。下面介绍这些安全问题的根源所在，大体上分为物理安全问题、方案设计的缺陷、系统和软件的安全漏洞、TCP/IP 协议的安全以及人的因素等方面。

1. 物理安全问题

主要表现在物理设备本身、设备的位置安全、物理访问限制、物理环境安全以及地域因素等方面。

2. 方案设计的缺陷

主要表现如下：

(1) 某些系统的设计方案中没有考虑整体的安全性，使用的安全产品不少，但没有考虑系统之间的相互补充；

(2) 一些设计方案中只是在系统的局部环节采用了一些安全的产品，但是忽略了其他的环节，此环节如果被突破就可能导致整个系统的突破；

(3) 一些概念对某些系统适用，但并非对所有系统都适用；

(4) 许多系统的安全设计出现“程式化”的趋势，使得黑客容易猜测和类比。

3. 系统和软件的安全漏洞

由于系统规模越来越大、越来越复杂，因此不可避免地出现一些安全漏洞。同时，伴随着各种应用软件的大量应用，许多安全漏洞也出现在这些软件中。

各种新技术（如 CGI、ActiveX、Java Script、VB Script 等）在给用户带来极大便利的同时，也带来了各种安全漏洞。

虽然许多单一技术并不影响网络的安全特性，但是几种技术的组合使用却有可能引入新的安全漏洞。

4. TCP/IP 协议的安全

由于最初的设计基本上没有考虑安全问题，因此 TCP/IP 协议在安全可靠性、服务质量、带宽和方便性等方面存在着不适应性。

TCP/IP 协议中安全问题的根源主要是：一方面，IP 包明文传输，因此容易被偷看和篡改；另一方面，IP 包中没有认证数据，使得伪造和欺骗成为可能。

5. 人的因素

人是信息活动的主体，人的因素其实是网络安全问题中最重要的因素，体现在人为的无意失误、人为的恶意攻击以及管理上的疏忽和错误等方面。

1.2.2 漏洞的危害

上面讲述了安全问题的根源，在这 5 个方面的根源中，有些是很难进行改变的，例如物理安全问题和 TCP/IP 协议的安全问题。在正确的网络安全管理下，更多网络安全攻击事件的发生是由于系统和软件中存在的安全漏洞。那么，安全漏洞到底会造成什么样的危害呢？下面介绍这个问题。

漏洞主要存在于操作系统、应用程序以及脚本中，它使得黑客能够执行特殊的操作，从而获得不应该获得的权限。几乎每天都能在某些程序或操作系统中发现新的漏洞，许多漏洞都能导致攻击者获得 root 权限，从而可以控制系统并且获得机密资料，导致公司或者个人遭受巨大损失。

不同的漏洞其表现形式是不一样的，危害也有大小之分，但是，总的来说，安全漏洞会危害系统的完整性、系统的可用性、系统的机密性、系统的可控性以及系统的可靠性等。

由于安全漏洞而导致安全事件的事例日益增多，造成的损失也呈扩大趋势。由此可以看出，安全漏洞的危害已经达到非常严重的地步，需要我们尽力防范漏洞的出现，防范漏洞被恶意利用。