



教育部实用型信息技术人才培养系列教材

边用边学



网络安全技术

杨永川 黄淑华 魏春光 编 著

全国信息技术应用培训教育工程工作组 审 定



机械工业出版社
CHINA MACHINE PRESS



教育部实用型信息技术人才培养系列教材

边用边学网络安全技术

杨永川 黄淑华 魏春光 编著

全国信息技术应用培训教育工程工作组 审定



机械工业出版社

本书是“教育部实用型信息技术人才培养系列教材”之一。本书针对计算机学科的特点,系统、全面地介绍了构建安全网络体系结构所需要掌握的理论和实践基础知识。书中没有过多地讲述原理,而是采用任务驱动的方式撰写,通过实例讲述导出概念、知识点和技术要点,将复杂的网络安全原理及应用技术以清晰和易于接受的方式介绍给读者。

本书共 10 章,主要包括网络安全的概念与性质、典型的网络威胁与攻击、数据加密技术及 PKI、实体安全及访问控制、防火墙技术与配置、VPN 技术与配置、入侵检测技术与产品、恶意代码分析及防范技术、Windows 2000 操作系统安全加固,以及应用服务安全加固等内容。

本书结构清晰、合理,内容丰富、实用、新颖,适合普通高等院校、高等职业学校、高等专科学校、成人高等学校,以及各类计算机培训中心作为教学用书和培训教材,亦可作为读者在今后实践中有效的工具书和参考书。

图书在版编目(CIP)数据

边用边学网络安全技术/杨永川,黄淑华,魏春光编著. —北京:机械工业出版社,2009. 10

(教育部实用型信息技术人才培养系列教材)

ISBN 978 - 7 - 111 - 28187 - 0

I. 边… II. ① 杨… ② 黄… ③ 魏… III. 计算机网络 - 安全技术 - 教材 IV. TP393. 08

中国版本图书馆 CIP 数据核字(2009)第 153615 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

责任编辑:唐德凯

责任印制:李 妍

北京汇林印务有限公司印刷

2010 年 3 月第 1 版·第 1 次印刷

184mm × 260mm · 19.75 印张 · 487 千字

0001 - 3000 册

标准书号: ISBN 978 - 7 - 111 - 28187 - 0

定价: 33.00 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

社服务中心:(010)88361066

门户网:<http://www.cmpbook.com>

销售一部:(010)68326294

教材网:<http://www.cmpedu.com>

销售二部:(010)88379649

读者服务部:(010)68993821

封面无防伪标均为盗版

教育部实用型信息技术人才 培养系列教材编辑委员会

(暨全国 ITAT 教育工程专家组)

主任委员 侯炳辉 (清华大学 教授)

委员 (以姓氏笔划为序)

方美琪 (中国人民大学 教授)

甘仞初 (北京理工大学 教授)

孙立军 (北京电影学院动画学院 院长)

刘 灵 (中国传媒大学广告学院 副院长)

许 平 (中央美术学院设计学院 副院长)

张 骏 (中国传媒大学动画学院 副院长)

陈 明 (中国石油大学 教授)

陈 禹 (中国人民大学 教授)

杨永川 (中国人民公安大学 教授)

彭 澎 (云南财经大学 教授)

蒋宗礼 (北京工业大学 教授)

赖茂生 (北京大学 教授)

执行主编 薛玉梅 (全国信息技术应用培训教育工程负责人
教育部教育管理信息中心开发处处长 高级工程师)

执行副主编 于 泓 (教育部教育管理信息中心)
王彦峰 (教育部教育管理信息中心)

出版说明

信息化是当今世界经济和社会发展的趋势，也是我国产业优化升级和实现工业化、现代化的关键环节。信息产业作为一个新兴的高科技产业，需要大量高素质复合型技术人才。目前，我国信息技术人才的数量和质量远远不能满足经济建设和信息产业发展的需要，人才的缺乏已经成为制约我国信息产业发展和国民经济建设的重要瓶颈。信息技术培训是解决这一问题的有效途径，如何利用现代化教育手段让更多的人接受到信息技术培训是摆在我们面前的一项重大课题。

教育部非常重视我国信息技术人才的培养工作，通过对现有教育体制和课程进行信息化改造、支持高校创办示范性软件学院、推广信息技术培训和认证考试等方式，促进信息技术人才的培养工作。经过多年的努力，培养了一批又一批合格的实用型信息技术人才。

全国信息技术应用培训教育工程（简称 ITAT 教育工程）是教育部于 2000 年 5 月启动的一项面向全社会进行实用型信息技术人才培养的教育工程。“ITAT”教育工程得到了教育部有关领导的肯定，也得到了社会各界人士的关心和支持。通过遍布全国各地的培训基地，ITAT 教育工程建立了覆盖全国的教育培训网络，对我国的信息技术人才培养事业，起到了极大的推动作用。

ITAT 教育工程被专家誉为“有教无类”的平民学校，以就业为导向，以大、中专院校学生为主要培训目标，也可以满足职业培训、社区教育的需要。培训课程能够满足广大公众对信息技术应用技能的需求，对普及信息技术应用起到了积极的作用。据不完全统计，在过去六年中共有五十余万人次参加了 ITAT 教育工程提供的各类信息技术培训，其中有近二十万人次获得了教育部教育管理信息中心颁发的认证证书。工程为普及信息技术、缓解信息化建设中面临的人才短缺问题做出了一定的贡献。

ITAT 教育工程聘请来自清华大学、北京大学、人民大学、中央美术学院、北京电影学院、中国传媒大学等单位的信息技术领域专家组成专家组，规划教学大纲，制定实施方案，指导工程健康、快速地发展。ITAT 教育工程以实用型信息技术培训为主要内容，课程实用性强，覆盖面广，更新速度快。目前工程已开设培训课程二十余类，共计五十余门，并将根据信息技术的发展，继续开设新的课程。

本套系列教材由清华大学出版社、人民邮电出版社、机械工业出版社、北京希望电子出版社等出版发行。根据工程教材出版计划，全套教材共计六十余种，内容将汇集信息技术及应用各方面的知识。今后将根据信息技术的发展不断修改、完善、扩充，始终保持追踪信息技术发展的前沿。

全国 ITAT 教育工程的宗旨是：树立民族 IT 培训品牌，努力使之成为全国规模最大、系统性最强、质量最好，而且最经济实用的国家级信息技术培训工程，培养出千千万万个实用型信息技术人才，为实现我国信息产业的跨越式发展作出贡献。

全国 ITAT 教育工程负责人
系列教材执行主编

薛玉梅

前 言

计算机网络安全是一个随着互联网的发展而不断引起人们关注的课题。发展迅速的互联网广泛应用于金融、电信、能源、交通运输、水供给、国土资源及社会保障等重要领域,成为国家的关键基础设施,同时深入到人们日常生活的各个方面。与此同时,有害信息、黑客入侵、病毒、木马也在网络空间中泛滥……安全问题愈演愈烈。人们已经清醒地认识到,在发展信息网络技术的同时,做好网络安全方面的理论研究与实践应用,是信息化的重要内容。

本书是“教育部实用型信息技术人才培养系列教材”之一。作者在整理、收集网络安全方面各种有关的资料,并结合自身的教学、科研和网络运行管理经验的基础上编写了本书。本书针对计算机学科的特点,系统、全面地介绍了构建安全的网络体系结构所需要掌握的理论和实践基础知识。书中没有过多地讲述原理,而是采用任务驱动方式撰写,通过实例讲述导出概念、知识点和技术要点,将复杂的网络安全原理及应用技术以清晰和易于接受的方式介绍给读者。

本书在内容上分为10章。

第1章网络安全概述,主要介绍了当前网络安全领域发展的现状,网络安全的内涵与外延,网络安全要解决的核心问题,以及网络安全的政策法规与标准。

第2章典型的安全威胁与攻击技术,主要分析了攻击者如何利用各种手段,通过本地或者网络,对目标进行攻击。

第3章密码技术及其应用,主要对构成网络安全基本防护技术的常见加密算法及其应用,如完整性校验、数字签名等进行了说明。

第4章实体安全与容灾备份,主要对计算机设备、设施(含网络)及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施和过程进行阐述,并补充介绍了容灾系统的基本概念及关键技术。

第5章防火墙技术与配置,重点介绍了防火墙技术原理及其结构,并结合实例给出了防火墙的部署。

第6章VPN技术与配置,重点介绍了VPN技术原理及其应用,并结合实例给出了VPN的部署及配置。

第7章入侵检测技术与产品,重点分析了入侵检测技术原理及其结构,并结合实例给出了入侵检测系统的部署及配置。

第8章恶意代码分析与防御技术,首先介绍恶意代码的基本知识,包括定义、分类、起源与发展及其基本特征;然后按类别描述其重要的工作机理;最后总结恶意代码的一般防治方法,并给出网络环境下恶意代码的预警和防范体系。

第9章Windows 2000系统安全加固,重点介绍了增强Windows 2000系统安全性的配置方案。

第10章应用服务安全加固,主要对常用的互联网服务(如Web、FTP及电子邮件服务)的安全增强方案进行介绍。

本书在内容安排上循序渐进，由浅入深地剖析了网络安全面临的威胁和典型攻击实例，并有针对性地给出了防范技术和配置、实施方法。书中给出的范例具有可操作性，读者完全可以参照实例的策略和配置，结合详细的操作步骤和方法，来掌握网络安全的相关基础知识。

本书由全国信息技术应用培训教育工程工作组组编，薛佳和王彦峰对本书进行了审定。在本书的编写和出版过程中，得到了教育部教育管理信息中心、中国人民公安大学信息安全工程系、中国人民公安大学网络中心的大力支持和帮助，在此，向上述单位的有关领导和同志，以及本书引用的有关文献的编著者，表示衷心的感谢。

由于作者水平有限，书中难免存在疏漏和欠妥之处，敬请读者批评指正。

作 者

目 录

出版说明

前言

第1章 网络安全概述	1
1.1 网络安全问题溯源	1
1.1.1 系统的脆弱性	1
1.1.2 网络协议和服务的脆弱性	3
1.1.3 安全管理漏洞	5
1.1.4 黑客攻击	6
1.2 信息安全的概念与内涵	6
1.2.1 信息安全定义	6
1.2.2 信息安全的属性	7
1.2.3 信息安全的作用层次	8
1.3 网络安全总体框架与模型	10
1.3.1 ISO 安全体系结构	10
1.3.2 网络安全模型	12
1.3.3 美国信息保障技术框架	14
1.3.4 网络安全研究总体框架	16
1.4 网络安全关键技术	17
1.5 网络安全的政策法规与标准	20
1.5.1 国际信息安全政策法规	20
1.5.2 国内信息安全政策法规	21
1.5.3 信息安全标准	22
1.6 本章小结	25
1.7 习题	25
1.8 实验	25
第2章 典型的安全威胁与攻击技术	26
2.1 安全威胁与黑客攻击	26
2.1.1 网络中存在的安全威胁	26
2.1.2 网络攻击发展的趋势	27
2.1.3 网络攻击的一般过程	29
2.2 信息收集类攻击	31
2.2.1 信息收集的一般方法	32
2.2.2 利用安全扫描工具收集信息	34
2.2.3 利用网络监听工具收集信息	39
2.3 漏洞类攻击	41

2.3.1	口令攻击	41
2.3.2	缓冲区溢出攻击	46
2.3.3	NetBIOS 漏洞攻击	49
2.4	欺骗类攻击	53
2.4.1	ARP 欺骗	53
2.4.2	IP 欺骗	55
2.4.3	TCP 会话劫持	57
2.4.4	DNS 欺骗	58
2.4.5	DNS 劫持	60
2.4.6	E-mail 欺骗攻击	61
2.4.7	Web 欺骗攻击	62
2.5	拒绝服务类攻击	63
2.5.1	拒绝服务攻击	64
2.5.2	分布式拒绝服务攻击	67
2.5.3	组织一次 DDoS 攻击的过程	71
2.6	本章小结	71
2.7	习题	72
2.8	实验	72
第3章	密码技术及其应用	73
3.1	密码技术基础	73
3.1.1	密码学的发展	73
3.1.2	密码体制	74
3.1.3	古典加密方法	75
3.2	现代加密技术	77
3.2.1	对称加密技术	77
3.2.2	非对称加密技术	81
3.2.3	混合密码体制	84
3.3	密钥管理	85
3.3.1	密钥的类型	85
3.3.2	密钥的分配	86
3.3.3	计算机网络密钥分配方法	87
3.4	完整性校验	88
3.4.1	完整性校验的原理	88
3.4.2	散列函数的特性分析	89
3.4.3	MD5	90
3.4.4	使用 MD5SUM 及 WinMD5 计算文件完整性码	91
3.5	数字签名	92
3.5.1	数字签名的应用和特性	93
3.5.2	用对称加密算法进行数字签名	93

3.5.3	用非对称加密算法进行数字签名和验证	94
3.5.4	实现具有保密性的数字签名	95
3.6	PKI 技术	95
3.6.1	PKI 的基本定义与组成	96
3.6.2	数字证书与 X.509	97
3.6.3	PKI 的核心 CA	101
3.6.4	PKI 的实施	102
3.6.5	配置 Windows 2000 PKI	104
3.7	本章小结	109
3.8	习题	110
3.9	实验	110
第4章	实体安全与容灾备份	111
4.1	计算机实体安全概述	111
4.1.1	实体安全威胁分析	111
4.1.2	实体安全的概念	112
4.1.3	实体安全的内容	112
4.1.4	实体安全的相关标准	113
4.2	环境安全	113
4.2.1	计算机场地安全的环境条件	114
4.2.2	运行环境安全	116
4.3	设备安全	119
4.3.1	设备防盗、防毁	119
4.3.2	设备防水	120
4.3.3	设备防静电	120
4.3.4	设备电磁防护	120
4.4	媒体安全	122
4.4.1	存储媒体的安全管理	122
4.4.2	存储媒体的访问控制技术	123
4.5	容灾备份	124
4.5.1	容灾的基本概念	124
4.5.2	容灾备份关键技术	125
4.5.3	常见的容灾备份方案	129
4.6	本章小结	131
4.7	习题	131
4.8	实验	131
第5章	防火墙技术与配置	132
5.1	防火墙概述	132
5.1.1	防火墙的基本概念	132
5.1.2	防火墙的基本要求	133

5.1.3	防火墙的主要作用	134
5.1.4	防火墙的主要缺点	135
5.1.5	防火墙的常用术语	137
5.2	防火墙的类型	137
5.2.1	从软、硬件形式上区分	138
5.2.2	按照防火墙采用的技术划分	138
5.2.3	按照防火墙结构划分	140
5.2.4	按照防火墙应用部署划分	141
5.2.5	按照防火墙性能划分	141
5.3	防火墙安全体系结构	141
5.3.1	屏蔽主机防火墙	142
5.3.2	屏蔽子网结构	142
5.3.3	双宿主机防火墙	143
5.3.4	混合结构防火墙	144
5.4	防火墙的安全性	145
5.4.1	正确选用、合理配置防火墙	145
5.4.2	正确评价防火墙的失效状态	145
5.4.3	进行动态维护	146
5.4.4	验证防火墙防护功能	146
5.5	实验——配置 Cisco PIX 防火墙	146
5.6	本章小结	150
5.7	习题	150
第6章	VPN 技术与配置	151
6.1	VPN 的基本概念与特性	151
6.1.1	VPN 的基本概念	151
6.1.2	VPN 的基本功能与优势	152
6.1.3	VPN 的组成	152
6.1.4	VPN 关键技术	153
6.1.5	VPN 的分类	153
6.2	VPN 的原理与协议	153
6.2.1	实现 VPN 的隧道技术	154
6.2.2	PPTP 协议	155
6.2.3	L2F 协议	156
6.2.4	L2TP 协议	156
6.2.5	IPSec 协议	156
6.2.6	SSL VPN	157
6.2.7	Windows 2000 的 VPN 技术	158
6.3	VPN 典型应用需求	161
6.3.1	通过 Internet 实现远程用户访问	161

6.3.2	通过 Internet 实现网络互联	162
6.4	构建 VPN 的一般方法	164
6.4.1	VPN 硬件方案	164
6.4.2	VPN 软件方案	164
6.4.3	微软的 VPN 解决方案	165
6.5	在 Windows 操作系统中利用 PPTP 配置 VPN 网络	165
6.5.1	系统组件安装配置	165
6.5.2	VPN 服务器配置	167
6.5.3	路由设置	169
6.5.4	NAT 设置	170
6.5.5	IP 安全设置	170
6.5.6	加密策略设置	171
6.5.7	客户端安全设置	172
6.5.8	Windows 2000 下客户端的设置	173
6.6	实验——在 Windows 中配置 IPSec	175
6.6.1	进入配置界面	175
6.6.2	定制 IPSec 策略	175
6.6.3	指派 IPSec 策略	178
6.6.4	测试配置结果	179
6.7	习题	180
第 7 章	入侵检测技术与产品	181
7.1	入侵检测概述	181
7.1.1	入侵检测与入侵检测系统	181
7.1.2	IDS 的主要功能	182
7.1.3	IDS 的主要分类	183
7.1.4	IDS 的发展过程	184
7.2	入侵检测技术	185
7.2.1	信息收集	185
7.2.2	信号分析	186
7.2.3	入侵检测的功能及其特征	187
7.3	入侵检测体系	188
7.3.1	基于主机的入侵检测	188
7.3.2	基于网络的入侵检测	188
7.3.3	分布式的入侵检测系统	189
7.4	入侵检查系统模型	189
7.4.1	通用入侵检测模型	189
7.4.2	通用入侵检测框架	190
7.5	实验——配置免费的 IDS-Snort 入侵检测系统	191
7.6	本章小结	195

7.7 习题	195
第8章 恶意代码分析与防御技术	196
8.1 恶意代码概述	196
8.1.1 病毒、蠕虫和木马程序的区别与联系	196
8.1.2 恶意代码的表现特征	197
8.1.3 恶意代码的传播形式	198
8.2 病毒	199
8.2.1 定义	199
8.2.2 病毒的起源与发展	200
8.2.3 病毒的特征	201
8.2.4 病毒的分类	203
8.2.5 传统病毒的工作机理	205
8.2.6 宏病毒的工作机理	207
8.2.7 网页病毒的工作机理	208
8.3 蠕虫	209
8.3.1 蠕虫的定义	209
8.3.2 蠕虫的发展史	210
8.3.3 蠕虫的行为特征	212
8.3.4 蠕虫的工作原理	213
8.3.5 蠕虫的防范	215
8.4 木马	215
8.4.1 定义	215
8.4.2 传统木马技术	216
8.4.3 现代木马技术	217
8.4.4 使用“冰河”木马进行远程控制	219
8.5 僵尸网络	220
8.5.1 僵尸网络的定义	221
8.5.2 僵尸网络的发展史	221
8.5.3 僵尸网络的组成方式	222
8.5.4 僵尸程序的感染途径	222
8.5.5 僵尸网络的检测	223
8.6 勒索软件	223
8.6.1 勒索软件的定义	224
8.6.2 勒索软件的特点	224
8.6.3 勒索软件实例介绍	224
8.6.4 勒索软件的应对与防范	225
8.7 恶意代码的防范策略与方法	226
8.7.1 恶意代码的一般防治方法	226
8.7.2 网络环境下恶意代码整体防御策略与方法	227

8.7.3 恶意代码的应急处理和防范管理体系	229
8.8 病毒查杀案例	231
8.8.1 灰鸽子木马手工清除方法	231
8.8.2 熊猫烧香蠕虫病毒手工清除方法	233
8.8.3 ARP 病毒分析与防御	235
8.9 本章小结	236
8.10 习题	236
8.11 实验	237
第9章 Windows 2000 系统安全加固	238
9.1 操作系统安全基础	238
9.1.1 操作系统概述	238
9.1.2 安全操作系统的发展	238
9.1.3 信息系统安全等级	239
9.2 安装系统	241
9.2.1 本地安全策略设置	242
9.2.2 系统配置	252
9.3 系统管理	255
9.3.1 注册表管理	255
9.3.2 Secedit 命令	260
9.3.3 审核系统	262
9.3.4 日志文件	266
9.4 安全配置	268
9.4.1 安全配置与分析	268
9.4.2 安全模板	269
9.5 使用安全配置和分析工具管理 Windows 2000 安全配置	270
9.6 本章小结	274
9.7 习题	275
第10章 应用服务安全加固	276
10.1 应用服务概述	276
10.1.1 应用层协议与服务	276
10.1.2 客户机/服务器模型	276
10.1.3 Internet 的安全	277
10.2 Web 服务的安全加固	281
10.2.1 IIS 安全设置	281
10.2.2 浏览器的安全性	283
10.3 FTP 服务的安全加固	286
10.3.1 服务端口的设置	286
10.3.2 用户验证控制	287
10.3.3 目录安全设置	288

10.4 电子邮件服务的安全加固	289
10.4.1 E-mail 的安全问题	289
10.4.2 E-mail 安全使用的策略	291
10.4.3 SMTP 服务安全	293
10.4.4 Outlook Express 安全	297
10.5 实验——在 Windows 2000 下构建安全的 IIS 服务器	298
10.6 本章小结	299
10.7 习题	299
参考文献	300

第1章 网络安全概述

1969年,互联网的雏形诞生了:连通犹他大学、斯坦福大学、加州大学洛杉矶分校和加州大学巴巴拉分校4个节点的分组交换实验网络互联成功。1972年,第一个互联网络 ARPANet 投入使用。之后,互联网发展迅速,广泛应用于金融、电信、能源、交通运输、水供给、国土资源及社会保障等重要领域,成为国家的关键基础设施,同时深入到人们日常生活的各个方面。然而,伴随着网络的普及,几乎每天都有非法闯入和安全侵犯事件的新闻:有害信息污染严重,黑客入侵和网络攻击频繁发生,计算机病毒蔓延和泛滥,机要信息流失和信息间谍潜入,涉及网络的计算机犯罪案件以指数增加,信息战的阴影也不可忽视……安全问题越来越引起人们的关注。

1.1 网络安全问题溯源

学习目标:

- 了解网络存在安全威胁的根本原因。
- 明确系统脆弱性。
- 理解网络协议和服务的脆弱性。

由于技术发展、工艺水平及设计者的经验等各种条件的限制,网络系统各个部分的设计本身有可能存在导致安全隐患的漏洞。网络中的硬件、软件、系统配置及各种网络协议的设计,其中任何一部分在安全方面的瑕疵都可能造成网络的安全脆弱性。

1.1.1 系统的脆弱性

1. 硬件系统的脆弱性

计算机硬件系统的脆弱性主要来自于以下方面。

- 1) 计算机信息系统的硬件均需要提供满足要求的电源才能正常工作,一旦切断电源,哪怕是极其短暂的一刻,计算机信息系统的工作也会被中断。
- 2) 计算机是利用电信号对数据进行运算和处理的。因此,环境中的电磁干扰能引起处理错误,得出错误的结论,并且所产生的电磁辐射会产生信息泄露。
- 3) 电路板焊点过分密集,极易产生短路而烧毁器件。接插部件多,接触不良的故障时有发生。
- 4) 体积小、重量轻、物理强度差,极易被偷盗或毁坏。
- 5) 电路高度复杂,设计缺陷在所难免,加上有些不怀好意的制造商还故意留有“后门”。

2. 操作系统的脆弱性

任何应用软件均是在操作系统的支持下执行的,操作系统的不安全是计算机信息系统不安全的重要原因。操作系统的脆弱性如图 1-1 所示。

操作系统的脆弱性表现在以下几个方面。

- 1) 操作系统的程序可以动态链接。这种方式虽然为软件开发商进行版本升级提供了方便,但“黑客”也可以利用此法攻击系统或链接计算机病毒程序。
- 2) 操作系统支持网上远程加载程序,这为实施远程攻击提供了技术支持。
- 3) 操作系统通常提供 DEMO 软件。这种软件在 UNIX 和 Windows NT 操作系统上与其他系统核心软件具有同等的权利。借此摧毁操作系统十分便捷。
- 4) 系统提供了 Debug 与 Wizard。它们可以将执行程序进行反汇编,方便追踪执行过程。
- 5) 操作系统的设计缺陷。计算机病毒和“黑客”程序正是利用这些缺陷对操作系统进行致命攻击。

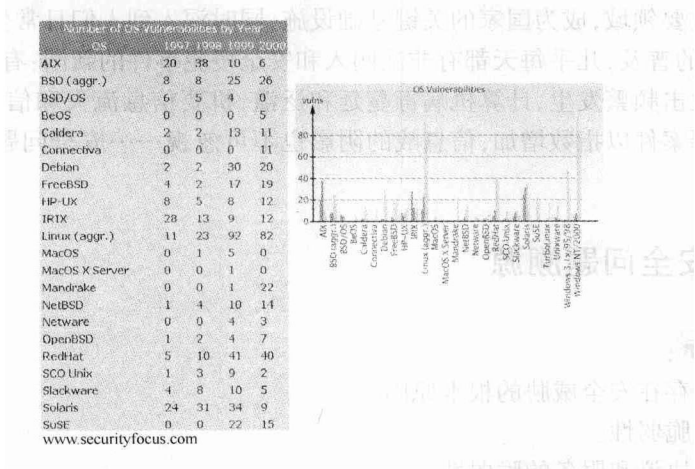


图 1-1 操作系统脆弱性

3. 存储系统的脆弱性

计算机的存储系统分为内存和外存:内存分为 RAM 和 ROM;外存有硬盘、软盘、磁带和光盘等。它们的脆弱性表现在如下几个方面。

- 1) RAM 中存放的信息一旦掉电即刻丢失,并且易于在内嵌入病毒代码。
- 2) 硬盘构成复杂,既有动力装置,也有电子电路及磁介质,任何一部分出现故障均会导致硬盘不能使用,丢失其中的大量软件和数据。
- 3) 软盘及磁带易损坏。它们的长期保存对环境要求高,保存不妥,便会发生霉变现象,导致数据不能读出。此外,盘片极易遭到物理损伤(折叠、划痕、破碎等),从而丢失其中的程序和数据。
- 4) 光盘盘片没有附在一起的保护封套,在进行数据读取和存放的过程中容易因摩擦而产生划痕,引起读取数据失败。此外,盘片在物理上脆性较大,易破碎而损坏,导致磁盘上的数据丢失。
- 5) 各种信息存储媒体的存储密度高,体积小,且重量轻,一旦被盗窃或损坏,损失巨大。
- 6) 存储在各媒体中的数据均具有可访问性,数据信息很容易地被复制而不留任何痕迹。一台远程终端上的用户,可以通过计算机网络连接到你的计算机上,利用一些技术手段,访问到你系统中的所有数据,并按其目的进行复制、删除和破坏。

4. 传输系统的脆弱性

组建计算机网络的出发点是资源共享和数据通信。计算机之间需要借助交换设备和有线