

 信息安全技术与教材系列丛书

网络安全

黄传河 杜瑞颖 张沪寅 张健 张文涛 傅建明 詹江平 / 编著



全国优秀出版社
武汉大学出版社

内 容 简 介

本书为武汉大学信息安全本科专业教材,按网络攻击技术、网络防御技术、网络安全保障体系三大部分组织编写。书中全面介绍了网络侦察、拒绝服务攻击、缓冲区溢出攻击、程序攻击、欺骗攻击、利用处理程序错误实施攻击等主要攻击技术;介绍了访问控制技术、防火墙技术、入侵检测技术、VPN、网络病毒防治、无线网络安全、安全恢复、取证技术等主要防御技术。对网络安全保障体系做了简要介绍。

本书可作为信息安全专业的本科生教材,也可作为相关领域技术人员的参考资料。

图书在版编目(CIP)数据

网络安全/黄传河等编著. —武汉:武汉大学出版社,2004.10

(信息安全技术与教材系列丛书)

ISBN 7-307-04358-0

I. 网… II. 黄…[等] III. 计算机网络—安全技术—高等学校—教材
IV. TP393.08

中国版本图书馆 CIP 数据核字(2004)第 097467 号

责任编辑:黄金文 责任校对:王 建 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:湖北恒吉印务有限公司

开本:787×980 1/16 印张:30.5 字数:589千字

版次:2004年10月第1版 2004年10月第1次印刷

ISBN 7-307-04358-0/TP·156 定价:45.00元

版权所有,不得翻印;凡购我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。



序 言

21 世纪是信息的时代,信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一,信息技术改变着人们的生活和工作方式,信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前,以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用,正引起社会和经济的深刻变革,为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统,已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命,信息战、网络战成为新的作战形式。

总之,随着计算机在军事、政治、金融、商业等部门的广泛应用,社会对计算机的依赖越来越大,如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此,确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全,事关经济发展,必须采取措施确保信息安全。

发展信息安全技术与产业,人才是关键。培养信息安全领域的专业人才,成为当务之急。2001 年经教育部批准,武汉大学创建了全国第一个信息安全本科专业。到 2003 年,全国设立信息安全本科专业的高等院校增加到 20 多所。2003 年经国务院学位办批准武汉大学建立信息安全博士点。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材,武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域,既可用做本科生的教材,又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际,努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天,这套丛



书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见,以使丛书能够进一步修改完善。

中国工程院院士,武汉大学兼职教授

沈昌祥

2003年7月28日



前言

在信息时代,信息已经成为重要的战略资源。信息安全已经不再只关系到信息本身的安全,还关系到政治、经济、军事等各个领域,甚至整个国家的安全。网络作为信息的主要收集、存储、分配、传输、应用的载体,其安全对整个信息的安全起着至关重要甚至是决定性的作用。

本书是武汉大学“十五”规划信息安全系列教材。全书按网络攻击技术、网络防御技术、网络安全保障体系三大部分组织编写。由于篇幅及系列教材统一规划的原因,一些重要的内容如密码理论与技术、公钥基础设施、网络应用安全等,没有包含在本书中。

本书注重理论联系实际,在介绍原理的同时,尽量给出实例,让读者能够立即学以致用。

本书由黄传河负责规划、统筹和审校。具体分工是:第一、二、五、六、十四、十五、十七章由黄传河编写,第三、十二章由杜瑞颖编写,第四、九章由张沪寅编写,第十、十一章由张健编写,第七、八章由张文涛编写,第十三章由傅建明编写,第十六章由詹江平、黄传河编写。张焕国、郭学理、王丽娜等教授为本书的内容提出了许多建设性的意见。参加资料收集整理的还有周红卫、明沛、殷晓东、李江巍、刘丹丹。

编者收集整理了大量资料,结合自己的研究工作,撰写了本书。由于资料来源的广泛性,书中引用的很多资料没有能够一一注明出处,对此,我们对原作者表示歉意,同时对原作者表示感谢。

由于课时的限制,具体使用本教材时,可对内容进行必要的取舍,例如第十三、十四、十六章,可能独立开课,可以不在本课程中讲授。

网络安全是内容广泛、发展迅速,加之编者水平限制,本书一定存在不少不足之处,诚望读者不吝赐教。

作者

2004年7月

目 录

前 言	1
第一章 网络安全概论	1
1.1 计算机安全	1
1.2 网络面临的安全威胁	1
1.3 网络安全的目标	4
1.4 信息系统安全评估标准	4
1.4.1 TCSEC 标准	4
1.4.2 信息安全管理标准 BS7799 与 ISO17799	5
1.4.3 中国计算机安全等级划分	7
1.5 保证网络安全的途径	7
第二章 网络攻击行径分析	8
2.1 攻击事件	8
2.1.1 攻击事件概述	8
2.1.2 攻击事件分类简介	8
2.2 攻击的目的	14
2.2.1 攻击的动机分析	14
2.2.2 攻击的目的	16
2.3 攻击的步骤	17
2.3.1 攻击的步骤简述	17
2.3.2 攻击的准备阶段	17
2.3.3 攻击的实施阶段	19
2.3.4 攻击的善后阶段	20
2.4 攻击诀窍	22
2.4.1 基本攻击诀窍概述	22
2.4.2 常用攻击工具	26
习 题	29

第三章 网络侦察技术	30
3.1 网络扫描	30
3.1.1 扫描器	30
3.1.2 扫描的类型	30
3.1.3 常用的网络扫描器	35
3.2 网络监听	39
3.2.1 以太网的监听	40
3.3 口令破解	46
3.3.1 字典文件	47
3.3.2 口令攻击类型	47
3.3.3 口令破解器	48
3.3.4 口令破解器的工作过程	49
3.3.5 Windows 口令破解	49
3.3.6 Unix 口令破解	51
习 题	55
第四章 拒绝服务攻击	56
4.1 拒绝服务攻击概述	56
4.1.1 DoS 定义	56
4.1.2 DoS 攻击思想及方法	57
4.2 拒绝服务攻击分类	57
4.2.1 消耗资源	57
4.2.2 破坏或更改配置信息	60
4.2.3 物理破坏或改变网络部件	60
4.2.4 利用服务程序中的处理错误使服务失效	60
4.2.5 拒绝服务攻击分析	61
4.3 服务端口攻击	61
4.3.1 同步包风暴(SYN Flooding)	61
4.3.2 Smurf 攻击	67
4.3.3 利用处理程序错误的拒绝服务攻击	69
4.4 电子邮件轰炸	72
4.5 分布式拒绝服务攻击 DDoS	74
习 题	77
第五章 缓冲区溢出攻击	78
5.1 缓冲区溢出攻击的原理	78

5.2 缓冲区溢出程序的原理及要素	79
5.2.1 缓冲区溢出程序的原理	79
5.2.2 缓冲区溢出程序的要素及执行步骤	82
5.3 攻击 UNIX	84
5.3.1 UNIX 操作系统简介	84
5.3.2 攻击 UNIX 实例分析	90
5.4 攻击 Windows	99
5.4.1 返回地址的控制方法	99
5.4.2 Windows 下 ShellCode 的编写	100
5.4.3 Windows 下缓冲区溢出的实例	103
习 题	106
 第六章 程序攻击	 109
6.1 逻辑炸弹攻击	109
6.2 植入后门	114
6.2.1 UNIX 后门策略	114
6.2.2 Windows 的后门	118
6.2.3 Netcat 介绍	120
6.3 病毒攻击	125
6.3.1 蠕虫病毒	125
6.3.2 蠕虫病毒实例分析	126
6.4 特洛伊木马攻击	129
6.4.1 特洛伊木马概述	129
6.4.2 木马的分类	130
6.4.3 木马的实现技术	140
6.4.4 键盘型木马的挂钩源代码示例	150
6.5 其他程序攻击	153
6.5.1 邮件炸弹与垃圾邮件	153
6.5.2 IE 攻击	153
习 题	154
 第七章 欺骗攻击	 156
7.1 DNS 欺骗攻击	156
7.1.1 DNS 的工作原理	156
7.1.2 DNS 欺骗的原理	158
7.1.3 DNS 欺骗的过程	159



7.2 E-mail 欺骗攻击	161
7.2.1 E-mail 攻击概述	161
7.2.2 E-mail 欺骗攻击的具体描述	162
7.3 Web 欺骗攻击	163
7.3.1 Web 欺骗的原理	163
7.3.2 Web 欺骗的手段和方法	165
7.3.3 Web 欺骗的预防办法	168
7.4 IP 欺骗攻击	169
7.4.1 IP 欺骗的原理	169
7.4.2 IP 欺骗的过程	171
7.4.3 IP 欺骗的例子	172
习 题	175
 第八章 利用处理程序错误攻击	176
8.1 操作系统的漏洞及攻防	176
8.1.1 Windows 系统的常见漏洞分析	176
8.1.2 其他操作系统的安全漏洞	179
8.1.3 系统攻击实例	180
8.2 Web 漏洞及攻防	197
8.2.1 Web 服务器常见漏洞介绍	197
8.2.2 CGI 的安全性	198
8.2.3 ASP 及 IIS 的安全性	200
习 题	206
 第九章 访问控制技术	207
9.1 访问控制技术概述	207
9.2 入网认证	208
9.2.1 身份认证	208
9.2.2 口令认证技术	209
9.3 物理隔离措施	212
9.3.1 物理隔离	212
9.3.2 网络安全隔离卡	215
9.3.3 物理隔离网闸	216
9.4 自主访问控制	218
9.4.1 访问控制矩阵	218
9.4.2 自主访问控制的方法	219



9.4.3 自主访问控制的访问类型	220
9.4.4 自主访问控制小结	220
9.5 强制访问控制	221
9.5.1 防止特洛伊木马的非法入侵	221
9.5.2 Bell-La Padual 模型	222
9.5.3 Biba 模型	224
9.6 新型访问控制技术	225
9.6.1 基于角色的访问控制技术	225
9.6.2 基于任务的访问控制技术	228
9.6.3 基于组机制的访问控制技术	229
习 题	229
第十章 防火墙技术	230
10.1 防火墙技术概述	230
10.1.1 经典安全模型	230
10.1.2 防火墙规则	231
10.1.3 匹配条件	232
10.1.4 防火墙分类	234
10.2 防火墙的结构	238
10.2.1 常见术语	239
10.2.2 防火墙的体系结构	239
10.2.3 其他体系结构	244
10.3 构建防火墙	250
10.3.1 选择体系结构	251
10.3.2 安装外部路由器	253
10.3.3 安装内部路由器	254
10.3.4 安装堡垒主机	254
10.3.5 设置数据包过滤规则	256
10.3.6 设置代理系统	261
10.3.7 检查防火墙运行效果	262
10.3.8 服务过滤规则示例	262
10.4 软件防火墙产品——Checkpoint	266
10.4.1 FireWall- I 使用的技术与体系结构	266
10.4.2 FireWall- I 的管理	268
10.5 硬件防火墙产品——天融信	276
10.5.1 防火墙 3000 组成	276



10.5.2 安全机制	277
10.5.3 功能模块	277
10.5.4 配置和管理	277
习 题	285
第十一章 入侵检测技术	287
11.1 入侵检测技术概述	287
11.1.1 入侵检测定义	287
11.1.2 入侵检测技术原理与系统构成	288
11.1.3 入侵检测系统的基本功能	289
11.2 入侵检测分类与评估	290
11.2.1 IDS 分类	290
11.2.2 分类优劣评估	290
11.3 入侵检测产品情况	291
11.3.1 商业产品的层次与分类	291
11.3.2 产品入侵检测技术分类	292
11.3.3 IDS 的不足	293
11.3.4 产品介绍与综合分析	293
11.4 天阗黑客入侵检测与预警系统	295
11.4.1 天阗产品系列	295
11.4.2 天阗系统组成与安装环境	296
11.4.3 天阗系统设置	298
习 题	303
第十二章 VPN 技术	305
12.1 VPN(Virtual Private Network)概述	305
12.1.1 VPN 的产生	305
12.1.2 VPN 的概念	305
12.1.3 VPN 的组成	306
12.2 VPN 的分类	307
12.2.1 远程访问虚拟网(Access VPN)	307
12.2.2 企业内部虚拟网(Intranet VPN)	308
12.2.3 企业扩展虚拟网(Extranet VPN)	308
12.3 VPN 使用的协议与实现	309
12.3.1 隧道技术基础	310
12.3.2 隧道协议	311



12.4 VPN 应用	319
12.4.1 VPN 网关	319
12.4.2 VPN 解决方案实例	321
习 题	324
 第十三章 网络病毒防治	325
13.1 计算机病毒概述	325
13.1.1 计算机病毒的产生	326
13.1.2 计算机病毒的特征	326
13.1.3 计算机病毒的分类	326
13.1.4 计算机病毒的组成	327
13.2 计算机病毒基本原理	329
13.2.1 DOS 病毒	329
13.2.2 宏病毒	332
13.2.3 脚本病毒	335
13.2.4 PE 病毒	339
13.3 计算机病毒的传播途径	340
13.4 计算机病毒对抗的基本技术	342
13.4.1 特征值检测技术	343
13.4.2 校验和检测技术	343
13.4.3 行为监测技术	344
13.4.4 启发式扫描技术	345
13.4.5 虚拟机技术	346
13.5 病毒的清除	347
13.5.1 引导型病毒的清除	348
13.5.2 宏病毒的清除	349
13.5.3 文件型病毒的清除	349
13.5.4 病毒的去激活	349
13.6 计算机病毒的预防	350
习 题	351
 第十四章 无线网络安全防护	353
14.1 常见攻击与弱点	353
14.1.1 WEP 中存在的弱点	353
14.1.2 搜索	356
14.1.3 窃听和监听	357



14.1.4 欺骗和非授权访问	358
14.1.5 网络接管与篡改	359
14.1.6 拒绝服务 (DoS) 和洪泛攻击	360
14.1.7 其他攻击方式	361
14.2 无线安全对策	362
14.2.1 安全策略	362
14.2.2 实现 WEP	364
14.2.3 利用 ESSID 防止非法无线设备入侵	365
14.2.4 过滤 MAC	366
14.2.5 使用封闭系统	368
14.2.6 分配 IP	369
14.2.7 防范无线网络入侵	369
14.2.8 扩展的移动安全体系结构 (EMSA)	370
14.3 无线通信安全	371
14.3.1 蓝牙安全机制	371
14.3.2 GSM 安全机制	373
14.3.3 GPRS 安全机制	377
14.3.4 3G 安全机制	379
14.4 无线 VPN	383
14.4.1 无线 VPN 介绍	383
14.4.2 无线 VPN 的优势	384
14.4.3 无线 VPN 的缺点	384
14.4.4 使用 VPN 增加保护层	384
习 题	385

第十五章 安全恢复技术	387
15.1 网络灾难	387
15.1.1 灾难定义	387
15.1.2 网络灾难	387
15.1.3 灾难预防	387
15.1.4 安全恢复	388
15.1.5 风险评估	388
15.2 安全恢复的条件	388
15.2.1 备份	389
15.2.2 网络备份	391
15.3 安全恢复的实现	392



15.3.1 安全恢复方法论	392
15.3.2 安全恢复计划	394
15.3.3 实例:Legato Octopus	398
习 题	400
第十六章 取证技术	401
16.1 取证的基本概念	401
16.1.1 计算机取证的定义	401
16.1.2 计算机取证的目的	402
16.1.3 电子证据的概念	403
16.1.4 电子证据的特点	403
16.1.5 电子证据的来源	405
16.2 取证的原则与步骤	406
16.2.1 计算机取证的一般原则	406
16.2.2 计算机取证的一般步骤	410
16.2.3 计算机取证相关技术	411
16.3 蜜罐技术	414
16.3.1 蜜罐概述	414
16.3.2 蜜罐的分类	415
16.3.3 蜜罐的基本配置	420
16.3.4 蜜罐产品	423
16.3.5 Honeynet	426
16.3.6 蜜罐的发展趋势	427
16.4 其他取证工具	428
16.4.1 TCT(The Coroner's Toolkit)	428
16.4.2 NTI公司的产品	429
16.4.3 Encase	431
16.4.4 NetMonitor	434
16.4.5 Forensic ToolKit	435
16.4.6 ForensiX	435
16.5 部分工具使用介绍	436
习 题	439
第十七章 信息系统安全保证体系	440
17.1 认 证	440
17.1.1 认证与鉴别的概念	440



17.1.2 认证方式	441
17.2 授 权	444
17.2.1 授权的基本概念	444
17.2.2 授权技术	444
17.2.3 授权的管理	446
17.2.4 授权的实现	447
17.2.5 分布式授权	448
17.3 密码管理	449
17.3.1 密码的设置选择	449
17.3.2 密码的更改	450
17.3.3 密码的存储	450
17.3.4 密码的使用	451
17.3.5 密码制度	451
17.4 密钥管理	451
17.4.1 密钥的生成	452
17.4.2 密钥的分配	453
17.4.3 密钥托管技术	457
17.4.4 密钥传送检测	458
17.4.5 密钥的使用	458
17.4.6 密钥存储与备份	459
17.4.7 密钥的泄露	459
17.4.8 密钥的生存期	459
17.4.9 密钥的销毁	460
17.5 可信时间戳的管理	460
17.5.1 时间戳概述	460
17.5.2 时间戳技术	462
17.5.3 时间误差的管理控制	463
习 题	464
课外实验	466
参考文献	467



第一章 网络安全概论

网络技术的飞速发展,Internet 的普及,深刻地改变了人类的工作和生活方式。各种各样的不安全因素,对网络的安全运行、信息的安全传递构成了巨大的威胁。本章简要介绍网络面临的安全威胁、信息系统的安全评估标准。

1.1 计算机安全

按照范围和处理方式的不同,通常将信息安全划分为三个级别。第一级为计算机安全,第二级为网络安全,第三级为信息系统安全。

计算机安全是信息安全的基础。计算机安全包括设备安全、操作系统安全、数据库安全、场地安全、介质安全等方面。设备如 CPU、显示器、外设等的安全又是计算机安全的基础。现在已经能够在 200 米之外接收到 CRT 显示器的电磁辐射,能够把对方显示器上的信息完整地接收并显示出来。根据已经公布的信息,一些著名的 CPU、操作系统、数据库管理系统、办公软件、路由器都存在设计上的漏洞和人为留下的后门,随时都有可能在用户毫无察觉的情况下把网络上的信息传送到别处,造成信息泄露。

网络安全是信息安全的核心。网络作为信息的主要收集、存储、分配、传输、应用的载体,其安全对整个信息的安全起着至关重要甚至是决定性的作用。网络安全的基础是需要具有安全的网络体系结构和网络通信协议的。但遗憾的是,今天的 Internet 不论是其体系结构还是通信协议,都具有各种各样的安全漏洞,因此而带来的安全事故层出不穷。当然,任何一种体系结构和通信协议都不可能尽善尽美、没有漏洞,因此利用网络进行的攻击与反攻击、控制与反控制永远不会停止。

信息系统安全是信息安全的目标。对用户而言,安全机制最好是透明的,不需要知道其细节,甚至不需要知道其存在。用户希望的是安全、方便的信息系统。

1.2 网络面临的安全威胁

随着网络的普及,“网上生活”已经成为一种趋势和必然,应运而生了电子政务、电子商务、电子海关、电子银行、电子证券、网上商场、网上拍卖、网上娱乐等一系列依赖网络的新的工作和生活方式。但因种种原因,网络面临着各种各样的安全威胁,其