

高等院校信息安全专业规划教材

黑客攻防技术与实践

- 信息收集的常用方法及使用工具
- 常见网络攻击的基本原理与常用工具
- 边界网关（防火墙、VPN）的基本原理及操作实例
- windows 系统安全的基本原理及操作实例
- 病毒与木马的基本常识和防范方法



提供电子教案

李建华 主编

单蓉胜 李 昀 陈 楠 参编



机械工业出版社
CHINA MACHINE PRESS



高等院校信息安全专业规划教材

黑客攻防技术与实践

主编 李建华

参编 单蓉胜 李 昀 陈 楠



机械工业出版社

本书介绍了信息安全攻防技术的基本原理和实现工具。全书共分 18 章,既介绍了网络攻击技术,如信息搜集、拒绝服务攻击、网络嗅探、欺骗与会话劫持、Web 攻击、密码破解、病毒、蠕虫与木马、后门技术和踪迹隐藏等攻击技术,也详细分析了防火墙、入侵检测技术、数据保护、Windows 系统安全、Web 安全等技术,还介绍了攻击技术和防御技术的实践操作实例。

本书既可以作为高等学校信息安全课程的教材,也适合企事业单位的网络管理员、系统管理员等专业技术人员作为工作学习和参考。

图书在版编目(CIP)数据

黑客攻防技术与实践/李建华主编. —北京:机械工业出版社,2009.4
(高等院校信息安全专业规划教材)

ISBN 978-7-111-26785-0

I. 黑… II. 李… 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(2009)第 052447 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:乔 宇

北京双青印刷厂印刷

2009 年 7 月第 1 版·第 1 次印刷

184mm×260mm·23.5 印张·580 千字

0001—3000 册

标准书号:ISBN 978-7-111-26785-0

定价:39.00 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

销售服务热线电话:(010)68326294 68993821

购书热线电话:(010)88379639 88379641 88379643

编辑热线电话:(010)88379753 88379739

封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

主 任 沈昌祥

副主任 王亚弟 王金龙 李建华 马建峰

编 委 王绍棣 薛 质 李生红 谢冬青

肖军模 金晨辉 徐金甫 余昭平

陈性元 张红旗 张来顺

出版说明

信息技术的发展和推广,为人类开辟了一个新的生活空间,它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间,已成为一个迫切需要人们研究、解决的问题。目前,与此相关的新技术、新方法不断涌现,社会也更加需要这类专门人才。为了适应对信息安全人才的需求,我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设,机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者,成立了教材编委会,共同策划了这套面向高校信息安全专业的教材。

本套教材的特色:

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人,具有很高的知名度和权威性,保证了本套教材的水平和质量。
2. 系列性强。整套教材根据信息安全专业的课程设置规划,内容尽量涉及该领域的方方面面。
3. 系统性强。能够满足专业教学需要,内容涵盖该课程的知识体系。
4. 注重理论性和实践性。按照教材的编写模式编写,在注重理论教学的同时注意理论与实践的结合,使学生能在更大范围内、更高层面上掌握技术,学以致用。
5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书,同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前 言

伴随电子商务、电子政务的全面铺开，信息安全行业面对的将是一场前所未有的机遇和挑战。由于信息网络的开放性和复杂性，安全保障的各个状态都处于一种不稳定的快速变化过程中。安全保障各个环节，如风险评估，威胁监测与分析、事件发现、事件控制甚至系统恢复与生存等，都需要具备足够的动态适应能力，以便适应各种变化的状况。然而，如何达到这个要求也面临大量的技术挑战。

黑客攻防技术是伴随着 Internet 的快速延伸而不断发展和完善的技术体系。本书以信息攻防的一对矛盾体为线索为读者逐一展开黑客技术体系的全貌，分为攻击技术、防御技术、攻防实践三个部分，共 18 章。第一部分为黑客攻击技术，涉及九个方面的攻击类型和方法；第二部分为防御技术，包括防火墙、入侵检测系统、数据保护、Microsoft Windows 系统安全、Web 安全等；第三部分为攻防实践，是上述各种技术的实践环节。本书的特色在于：同时涉及攻击与防御技术，将各种攻防技术系统化；配有专门的实践部分，强化了攻防理论与具体实践的结合。本书可用作大专院校计算机、信息安全等专业的本科生、研究生教材，也适合网络安全技术爱好者自学使用。

本书主编是李建华教授，单蓉胜博士参加了第 12~15 章、18 章的编写并负责统稿工作；李昀博士参加了第 1~5 章、16 章的编写工作；陈楠硕士参加了第 6~11 章、17 章的编写工作。

感谢赵旭东博士生对全书的校对。本书的顺利出版，要感谢上海交通大学信息安全工程学院的领导和老师所给予的大力支持和帮助。

本书作为面向 21 世纪高等院校信息安全技术的教材，体现了信息安全技术课程改革的方向之一。本课程建议授课学时为 40 学时，实验学时为 20 学时，并要求先修计算机网络课程。

由于编著水平有限，书中难免存在不妥之处，敬请读者批评指正。

编 者

目 录

出版说明

前言

第 1 章 基础知识	1
1.1 历史上的十大黑客事件	1
1.2 网络安全问题的产生	2
1.3 网络安全成为信息时代人类共同面临的挑战	2
1.4 网络四大攻击方法及发展趋势	3
1.4.1 网络四大攻击方法	3
1.4.2 攻击技术发展趋势	3
1.5 网络安全产品	3
1.5.1 物理隔离	4
1.5.2 逻辑隔离	4
1.5.3 防御来自网络的攻击	4
1.5.4 防止来自网络上的病毒	4
1.5.5 反垃圾邮件	4
1.5.6 身份认证	4
1.5.7 加密通信和虚拟专用网	5
1.5.8 公钥相关软件及服务	5
1.5.9 入侵检测和主动防卫	5
1.5.10 网管、审计和取证	5
1.5.11 其他产品	6
1.6 小结	6
1.7 习题	6
第 2 章 攻击方法概述	7
2.1 与攻击有关的术语	7
2.2 与网络攻防有关的基础知识	7
2.2.1 TCP/IP 连接端及标记	7
2.2.2 TCP 连接的建立	8
2.2.3 IP 地址	8
2.2.4 常用 DOS 命令	9
2.3 攻击的分类	10
2.3.1 主动攻击和被动攻击	10
2.3.2 更常用的分类	11
2.4 黑客常用的攻击方法及完整的入侵步骤	11

2.4.1 黑客常用的攻击方法	11
2.4.2 完整的人侵步骤	13
2.5 小结	15
2.6 习题	16
第3章 信息搜集	17
3.1 信息搜集的意义和步骤	17
3.2 主机信息搜集	17
3.2.1 用 ping 来识别操作系统	17
3.2.2 通过连接端口返回的信息进行识别	18
3.2.3 利用 rusers 和 finger 搜集用户信息	19
3.2.4 用 host 发掘更多信息	20
3.2.5 利用专门的软件来搜集信息	22
3.3 Web 网站信息搜集	23
3.3.1 由域名得到网站的 IP 地址	23
3.3.2 网站基本信息查询	24
3.3.3 网站注册信息及地理位置搜集	24
3.4 网络拓扑结构探测	26
3.4.1 手工探测目标网络结构	27
3.4.2 可视化的网络结构探测集成工具	28
3.5 端口扫描	30
3.5.1 端口扫描器和安全扫描器	30
3.5.2 端口扫描技术	31
3.6 小结	34
3.7 习题	35
第4章 拒绝服务攻击	36
4.1 拒绝服务攻击	36
4.1.1 DoS 攻击的网络基础	36
4.1.2 DoS 攻击的原理	38
4.1.3 典型的 DoS 攻击	38
4.2 分布式拒绝服务攻击	40
4.2.1 分布式拒绝服务攻击的原理	40
4.2.2 DDoS 攻击的危害	42
4.2.3 典型的 DDoS 攻击	42
4.3 分布式反射拒绝服务攻击	43
4.4 小结	45
4.5 习题	45
第5章 嗅探	46
5.1 嗅探器的工作原理	46
5.1.1 嗅探器概述	46

5.1.2 HUB 与网卡的原理	47
5.1.3 Sniffer 工作原理	48
5.1.4 嗅探器造成的危害	49
5.2 黑客如何实施被动嗅探入侵	50
5.3 常用的嗅探器	53
5.3.1 Windows 平台下的 Sniffer	53
5.3.2 UNIX 平台下的 Sniffer	53
5.4 嗅探器的应用	53
5.4.1 Sniffer 的正面应用	53
5.4.2 Sniffer 的反面应用	55
5.5 交换环境下的嗅探方法	55
5.5.1 ARP 欺骗	56
5.5.2 交换机 MAC 地址表溢出	58
5.5.3 MAC 地址伪造	58
5.5.4 ICMP 路由器发现协议欺骗	58
5.5.5 ICMP 重定向攻击	58
5.6 小结	58
5.7 习题	59
第 6 章 欺骗与会话劫持	60
6.1 ARP 的欺骗与会话劫持	60
6.1.1 ARP 的基本概念	60
6.1.2 基于 ARP 的欺骗攻击	60
6.1.3 ARP 欺骗攻击的解决办法	62
6.2 ICMP 重定向	63
6.2.1 ICMP 重定向原理	63
6.2.2 ICMP 重定向攻击	64
6.2.3 ICMP 重定向攻击的防御	64
6.3 源路由欺骗	65
6.3.1 IP 源路由选项介绍	65
6.3.2 源路由欺骗的原理及防御方法	67
6.4 DNS 欺骗	67
6.4.1 DNS 基础概念	67
6.4.2 DNS 域名解析过程	68
6.4.3 DNS 欺骗攻击的原理	69
6.4.4 DNS 欺骗攻击的防御	69
6.5 SSL 会话劫持	70
6.5.1 SSL 协议基础	70
6.5.2 SSL 安全性分析	71
6.6 小结	72

6.7 习题	72
第7章 Web 攻击	73
7.1 SQL 注入攻击	73
7.1.1 Access 注入攻击 (一般为 ASP + Access 型)	74
7.1.2 MSSQL 注入攻击	77
7.1.3 MySQL 注入攻击	83
7.2 跨站脚本攻击	95
7.2.1 什么是跨站脚本攻击	95
7.2.2 来自内部的跨站攻击	95
7.3 旁注攻击	97
7.3.1 确定网站物理路径	97
7.3.2 旁注入侵的工具	97
7.3.3 WEBSHELL	97
7.4 小结	98
7.5 习题	98
第8章 缓冲区溢出攻击	99
8.1 缓冲区溢出攻击简介	99
8.2 缓冲区溢出技术原理	100
8.2.1 Linux x86 平台的 Stack 栈溢出	100
8.2.2 Linux x86 平台的 Shellcode 构造	104
8.2.3 Win32 平台的 Stack 栈溢出	107
8.2.4 Win32 平台的 Shellcode 的构造	107
8.2.5 Linux x86 平台的 Heap 堆溢出	109
8.2.6 Win32 平台的 Heap 堆溢出	112
8.2.7 格式化串溢出	115
8.3 缓冲区溢出漏洞分析	116
8.3.1 Linux x86 平台缓冲区溢出漏洞的分析	116
8.3.2 Win32 平台缓冲区溢出漏洞的分析	117
8.4 缓冲区溢出漏洞的预防	119
8.5 小结	120
8.6 习题	120
第9章 密码破解攻击	121
9.1 Windows 系统的密码猜解	121
9.1.1 Windows 用户账户的密码机制	121
9.1.2 Windows 密码猜解的技术原理	122
9.2 UNIX 系统的密码猜解	125
9.2.1 UNIX 用户账户的密码机制	125
9.2.2 UNIX 密码猜解的技术原理	126
9.3 应用软件的密码破解	127

9.3.1 应用服务软件的密码破解	127
9.3.2 RAR、ZIP、PDF 的密码破解	130
9.3.3 Office 系列文档密码破解	131
9.4 小结	133
9.5 习题	133
第 10 章 病毒、蠕虫与木马	134
10.1 病毒、蠕虫与木马概述	134
10.2 病毒技术	135
10.2.1 常用病毒技术	135
10.2.2 蠕虫病毒技术	140
10.2.3 病毒的隐藏技术	140
10.3 远程控制木马	141
10.3.1 木马概述	141
10.3.2 木马程序的自启动	143
10.3.3 木马程序的进程隐藏	144
10.3.4 木马程序的数据传输隐藏	145
10.3.5 木马程序的控制功能	147
10.4 小结	148
10.5 习题	148
第 11 章 后门技术和踪迹隐藏	149
11.1 系统隐蔽后门——Rootkit 技术	149
11.1.1 基础知识	149
11.1.2 Windows Rootkit——进程隐藏技术	150
11.1.3 Windows Rootkit——端口隐藏技术	155
11.1.4 Windows Rootkit——文件隐藏技术	156
11.1.5 Rootkit 查杀	157
11.2 Web 脚本后门	158
11.2.1 ASP 脚本后门	159
11.2.2 PHP 脚本后门	164
11.2.3 JSP 脚本木马	186
11.2.4 脚本木马的隐藏	186
11.3 日志的清除和伪造	189
11.3.1 Windows 日志的攻防	189
11.3.2 Linux 日志的清除和伪造	192
11.4 小结	193
11.5 习题	194
第 12 章 防火墙技术	195
12.1 防火墙概述	195
12.1.1 定义	195

12.1.2	防火墙的功能	195
12.1.3	防火墙的局限性	196
12.2	防火墙的体系结构	197
12.2.1	分组过滤路由器	197
12.2.2	双宿主机	198
12.2.3	屏蔽主机	199
12.2.4	屏蔽子网	199
12.3	防火墙的实现技术	200
12.3.1	数据包过滤技术	200
12.3.2	代理技术	201
12.3.3	状态检测技术	201
12.3.4	网络地址转换技术	203
12.4	防火墙策略	204
12.4.1	防火墙的基本策略	204
12.4.2	动态安全策略	204
12.4.3	建立规则 and 限制	205
12.5	防火墙技术展望	205
12.5.1	多级过滤技术	205
12.5.2	分布式防火墙技术	206
12.5.3	以防火墙为核心的网络安全体系	207
12.5.4	管理的通用化	208
12.6	防火墙产品介绍	208
12.6.1	主流防火墙产品简介	208
12.6.2	选购防火墙的基本原则	209
12.7	建立防火墙系统实例	210
12.8	小结	211
12.9	习题	212
第 13 章	入侵检测系统	213
13.1	入侵检测系统 (IDS) 概述	213
13.1.1	定义	214
13.1.2	IDS 的部署	214
13.1.3	IDS 的功能	215
13.2	入侵检测模型	217
13.2.1	异常检测原理	217
13.2.2	滥用检测原理	218
13.3	IDS 的分类	219
13.3.1	基于主机的 IDS	219
13.3.2	基于网络的 IDS	220
13.3.3	分布式 IDS	221

13.4 入侵检测方法	222
13.4.1 基于概率统计的检测	222
13.4.2 基于神经网络的检测	222
13.4.3 基于专家系统的检测	222
13.4.4 基于模型推理的检测	223
13.4.5 基于免疫的检测	223
13.5 IDS 的应用和发展	224
13.5.1 免费的 IDS——Snort	224
13.5.2 商业 IDS 产品	225
13.5.3 IDS 产品的选型	226
13.5.4 入侵检测技术的发展方向	226
13.6 小结	228
13.7 习题	229
第 14 章 数据保护	230
14.1 数据备份技术	230
14.1.1 数据备份的作用与意义	230
14.1.2 数据备份的定义	230
14.1.3 数据备份的类型	231
14.1.4 数据备份系统的基本构成	232
14.2 灾难恢复技术	239
14.2.1 灾难恢复的作用与意义	239
14.2.2 灾难恢复的定义	239
14.2.3 灾难恢复策略	240
14.2.4 灾前措施	243
14.2.5 灾难恢复计划	244
14.2.6 常用数据灾难恢复工具简介	245
14.2.7 典型的数据备份和灾难恢复解决方案	246
14.3 安全应急响应	248
14.3.1 安全应急响应概述	248
14.3.2 建立安全应急响应	250
14.3.3 应急响应的运作	253
14.4 小结	254
14.5 习题	255
第 15 章 Windows 系统安全	256
15.1 Windows 家族	256
15.1.1 Windows 95	256
15.1.2 Windows NT 4.0	256
15.1.3 Windows 98	257
15.1.4 Windows ME	257

15.1.5	Windows 2000	258
15.1.6	Windows XP	258
15.1.7	Windows Server 2003	259
15.1.8	Windows Vista	259
15.2	Windows XP 安全	259
15.2.1	Windows XP 安全性分析	259
15.2.2	Windows XP 安全模板	262
15.3	Windows 2000 审计功能	270
15.3.1	Windows 2000 日志文件	271
15.3.2	对日志文件的保护	271
15.3.3	Windows 2000 审核的事件类型	272
15.3.4	审计管理	272
15.3.5	审计账号	272
15.3.6	企业级集成	273
15.4	Windows Server 2003 安全	273
15.4.1	Windows Server 2003 安全强化概览	273
15.4.2	Windows Server 2003 安全策略的制定	277
15.5	Windows Vista 安全	281
15.5.1	Windows Vista 基础结构安全	281
15.5.2	Vista 六大安全功能	282
15.6	小结	283
15.7	习题	283
第 16 章	Web 安全	284
16.1	网站安全保护综述	284
16.1.1	网站的通用保护方法	284
16.1.2	网站的专用保护方法	284
16.1.3	网站保护的缺陷	285
16.2	Windows Internet 服务器安全配置	286
16.2.1	Windows Server 2003 各版本区别	286
16.2.2	Windows Internet 服务器安全配置案例分析	287
16.2.3	IIS 的相关设置	293
16.2.4	ASP 的安全设置	293
16.2.5	PHP 的安全设置	294
16.2.6	MySQL 安全设置	294
16.2.7	数据库服务器的安全设置	294
16.3	Apache 服务器安全	295
16.3.1	Apache 服务器的安全特性	295
16.3.2	Apache 服务器的安全配置	296
16.3.3	Apache Server 基于主机的访问控制	297

16.3.4 Apache Sever 的用户认证与授权	298
16.4 Web 安全工具	299
16.5 小结	300
16.6 习题	300
第 17 章 攻击技术实践	301
17.1 信息搜集技术实践	301
17.2 拒绝服务攻击技术实践	302
17.3 嗅探技术实践	303
17.4 欺骗与会话劫持技术实践	306
17.4.1 基于 ARP 欺骗的工具——Cain & Abel	306
17.4.2 ARP 欺骗工具——xspooof	307
17.4.3 ARP 欺骗防范工具	309
17.5 Web 攻击技术实践	309
17.5.1 SQL 注入工具——Pangolin	309
17.5.2 SQL 注入——手动编写语句	311
17.5.3 跨站脚本攻击	312
17.6 缓冲区溢出攻击技术实践	313
17.6.1 缓冲区溢出	313
17.6.2 缓冲区溢出调试工具	316
17.7 密码破解技术实践	317
17.7.1 Windows 口令破解	317
17.7.2 Linux 口令破解	319
17.8 病毒、蠕虫与木马技术实践	320
17.8.1 典型病毒分析	320
17.8.2 木马查杀工具	324
17.9 后门技术和踪迹隐藏技术实践	328
17.9.1 Rootkit 检测、清除与预防	328
17.9.2 Webshell 的应用	330
17.10 小结	335
17.11 习题	335
第 18 章 防御技术实践	336
18.1 防火墙实践	336
18.1.1 IPFW 防火墙	336
18.1.2 Ipcchains 防火墙	337
18.1.3 Iptables 防火墙	338
18.2 入侵检测系统实践	343
18.2.1 Snort 简介	343
18.2.2 Snort 规则简介	344
18.2.3 Snort 命令介绍	345

18.2.4 Snort 的工作模式	346
18.3 日志和审计技术实践	347
18.3.1 Windows 下对文件操作进行审计	347
18.3.2 对 Windows 用户账户管理进行审计	350
18.4 数据恢复技术实践	351
18.5 Vista 系统安全技术	353
18.6 Web 安全技术实践	354
18.7 小结	357
18.8 习题	357
参考文献	359

第1章 基础知识

1.1 历史上的十大黑客事件

DNA 杂志在印度全国软件和服务企业协会(Nasscom)与孟买警方开展互联网安全周活动,并回顾历史上的十大黑客事件时深刻认识到,即使是那些被认为固若金汤的系统在黑客攻击面前也总是显得不堪一击。

20 世纪 90 年代早期,出现了一位在世界范围内举足轻重的黑客——Kevin Mitnick。诺基亚(Nokia),富士通(Fujitsu),摩托罗拉(Motorola)和 Sun Microsystems 等世界上几大科技和电信公司的电脑系统都曾被他“光顾”过。1995 年他被 FBI 逮捕,于 2000 年获得假释。他从来不把自己的这种入侵行为称为黑客行为,按照他的解释,应为“社会工程(Social Engineering)”。

2002 年 11 月,伦敦人 Gary McKinnon 在英国被指控非法侵入美国军方 90 多个电脑系统。

1995 年,来自俄罗斯的黑客 Vladimir Levin 在互联网上上演了精彩的“偷天换日”。他是历史上第一个通过入侵银行电脑系统来获利的黑客。当年,他侵入美国花旗银行并盗走 1000 万美元。之后,他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。

1990 年,为了获得在洛杉矶地区 kiis-fm 电台第 102 个呼入者的奖励——保时捷 944 s2 跑车,Kevin Poulsen 控制了整个地区的电话系统,以确保他是第 102 个呼入者。最终,他如愿以偿地获得了跑车并为此入狱 3 年。 he 现在是 Wired News 的高级编辑。

1983 年,当 Kevin Poulsen 还是一名学生的时候,他就曾成功入侵 ARPANET(现在使用的 Internet 的前身)。Kevin Poulsen 当时利用了 ARPANET 的一个漏洞,能够暂时控制美国地区的 ARPANET。

1996 年,美国黑客 Timothy Lloyd 曾将一个六行的恶意软件放在了其雇主——Omega 工程公司(美国航天航空局和美国海军最大的供货商)的网络上。整个逻辑炸弹删除了 Omega 工程公司所有负责生产的软件。此事件导致 Omega 工程公司损失 1000 万美金。

1988 年,年仅 23 岁的 Cornell 大学学生 Robert Morris 在 Internet 上释放了世界上首个“蠕虫”程序。Robert Morris 最初仅仅是把他这个 99 行的程序放在互联网上进行试验,可结果却使他的计算机被感染并迅速在互联网上蔓延开,美国等地接入互联网的计算机都受到了影响。Robert Morris 也因此于 1990 年被判入狱。

1999 年,Melissa 病毒是世界上首个具有全球破坏力的病毒。David Smith 在编写此病毒的时候年仅 30 岁。Melissa 病毒使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美金。David Smith 随后被判处 5 年徒刑。

2000 年 2 月 6 ~ 14 日期间,年仅 15 岁的 MafiaBoy(由于年龄太小,因此没有公布其真实身份)成功侵入包括 eBay、Amazon 和 Yahoo 在内的大型网站服务器,他成功阻止了服务器向用户提供服务。同年 MafiaBoy 被捕。

1993 年,自称为骗局大师(MOD)的组织,将目标锁定美国电话系统。这个组织成功入侵