



- ⊕ 精选近100个攻防示例，帮助读者提升实战能力
- ⊕ 涵盖脚本注入、远程控制、后门、扫描、嗅探、黑客编程、社会工程学等主流的攻防技术
- ⊕ 完整的攻防实战案例：揭秘黑客入侵过程，提供系统加固策略

黑客攻防 实战秘技

⊕ 傅奎 编著



人民邮电出版社
POSTS & TELECOM PRESS



⊕ 傅奎 编著

黑客攻防

人民邮电出版社

北京

图书在版编目 (C I P) 数据

黑客攻防实战秘技 / 傅奎编著. —北京: 人民邮电出版社, 2009. 7
ISBN 978-7-115-20685-5

I. 黑… II. 傅… III. 计算机网络—安全技术 IV.
TP393.08

中国版本图书馆CIP数据核字 (2009) 第050126号

内 容 提 要

本书是指导读者学习如何防御黑客攻击的实战书籍。书中结合当前互联网上主流的防范黑客攻击的技术, 详细地介绍了读者在防范黑客攻击时必须掌握的基本知识、实用工具和技巧, 对读者在防御黑客攻击时经常遇到的问题给予了专业性的解答, 并通过实战案例给读者讲述了多种防范技术的具体应用。

全书分为四篇共 21 章, 主要内容包括, 网络安全基础知识、系统漏洞扫描、搜索引擎信息利用、操作系统本地攻防、网络封锁与代理突破、木马后门防御、网络抓包嗅探、欺骗攻击防御、SQL 注入防御、XSS 跨站脚本攻击防御、缓冲区溢出、防火墙、社会工程学、系统安全加固等知识。

本书采用大量真实案例, 内容新颖, 实例丰富, 语言通俗易懂。书中内容都与当前网络安全现实结合紧密, 既包括有主流的技术, 也探讨了许多前沿知识, 通过本书的学习将会很好地提高读者防范黑客的水平。

本书内容丰富, 实战性和可操作性强, 适合于网络安全技术爱好者、网络系统管理员阅读, 也可作为相关专业学生的学习用书和参考资料。

黑客攻防实战秘技

- ◆ 编 著 傅 奎
责任编辑 屈艳莲
执行编辑 张 涛
- ◆ 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@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
三河市海波印务有限公司印刷
- ◆ 开本: 787×1092 1/16
印张: 21.25
字数: 505 千字
印数: 1—3 500 册
- 2009 年 7 月第 1 版
2009 年 7 月河北第 1 次印刷

ISBN 978-7-115-20685-5/TP

定价: 39.00 元

读者服务热线: (010)67132692 印装质量热线: (010)67129223
反盗版热线: (010)67171154

前言

伴随着网络技术的高速发展,信息安全问题已日益受到人们的关注。信息安全尤其是网络安全,已涉及社会的方方面面,这其中的黑客防范是最值得普及的技术。本书以此为切入点,通过从理论到实践的方式,为读者介绍了当前互联网上流行的各种防范黑客攻击的技术。

本书内容

为了使读者能够逐步掌握全书内容,本书共分4篇:网络安全技术基础篇、木马、嗅探和后门防范技术篇、网络防范技术篇和防范案例实战篇。

网络安全技术基础篇(第1章~第6章)。介绍当前网络安全现状、操作系统安全使用策略、网络协议、常用防范软件、防范黑客编程等。为了提高读者的学习兴趣,讲解上以简单生动的例子介绍一些比较实用的攻防技巧。

木马、嗅探和后门防范技术篇(第7章~第13章)。通过大量的实例,介绍了当前主流的木马、嗅探和后门防范方法。主要内容为,搜索引擎信息获取技术、漏洞扫描、操作系统本地攻防、网络封锁与代理突破、木马与后门防范技术、网络嗅探等。其中搜索引擎信息获取技术是当前网络攻防中热门话题,本篇中做了系统的阐述。

网络防范技术篇(第14章~第19章)。本篇主要介绍网络上最为流行和成熟的防范手段。主要内容为,SQL注入攻击防御、跨站脚本攻击防御、缓冲区溢出、欺骗攻击防御、社会工程学、防火墙技术及综合防范技术运用等。

防范案例实战篇(第20章~第21章)。为了把前面的知识有一个综合的应用,本篇结合个人实战经验,讲述了一个揭秘黑客攻防过程的综合案例,以及一个如何加固系统安全的防御案例,是整本书的知识总结和实战技能提升部分。

本书特点

本书探讨黑客攻防时不仅仅停留在技术上,更多地是倡导学习网络安全技术,增强网络安全意识,提升我国计算机网络安全整体水平。读者在学习的同时,也应遵守职业准则和国家相关的法律法规。

本书的特点主要体现在以下几个方面。

- 本书的编排采用循序渐进的方式,适合初学者由浅入深地学习网络安全知识。通过全书21章的学习,读者可以掌握当前网络上主流的黑客防范技术。
- 本书介绍的各种攻防技术不仅体现在技术实现上,而且从原理角度对技术进行了阐

述。通过本书的学习，读者能够更加深入地理解防范黑客技术的真实原理，如书中提到的 SQL 注入漏洞的具体表现、漏洞产生原理及防范方法。

- 本书注重理论结合实际，相关案例更是贴近真实环境。如书中提到的通过 SSH 加密隧道突破网络封锁登录 QQ、办公室 MSN 聊天加密、构筑铜墙铁壁安全系统等。

- 本书在介绍大量网络安全技术实现原理及具体应用时，均提供了典型的案例和参考图例。读者通过书中提供的真实场景的截图，能够快速学习和掌握各类攻防技术，以便在学习上少走弯路，如书中图文并茂地讲述了开发 Bug 提交系统的安全测试等。

- 本书讲解的内容与当前网络安全现实相结合，既有主流的技术知识，也涉及部分前沿技术，如书中提到的社会工程学等知识。

读者对象

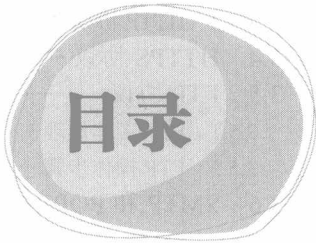
- 网络安全入门者；
- 网络安全爱好者；
- 网络安全管理员。

致谢

本书稿的完成得到了许多人的支持，在此一并致谢。感谢北京的 LXJ 朋友，他给我写作提供了很大的帮助；感谢我的朋友“月亮”，他的多次鼓劲使我能够在面临困境时咬牙向前；感谢融智科技的陈冠军朋友，她的热情帮助和耐心指导一直在鼓舞着我努力写作。

在写作过程中，我力求精益求精，但由于时间所限，书中难免存在一些不足之处，敬请广大读者批评指正。如果您在使用本书时遇到问题，可以发邮件到 zhangtao@ptpress.com.cn 与我们联系。

编者



目录

第一篇 网络安全技术基础篇

第1章 知己知彼,百战不殆——网络安全现状.....2

- 1.1 网络安全现状及发展趋势.....2
 - 1.1.1 认识黑客.....2
 - 1.1.2 互联网安全现状.....2
 - 1.1.3 黑客技术发展.....3
- 1.2 计算机犯罪及相关法律.....4
 - 1.2.1 计算机犯罪相关概念.....4
 - 1.2.2 计算机信息系统安全立法.....4
- 1.3 小结.....4

第2章 千里之行始于足下——认识操作系统及安全策略.....5

- 2.1 Windows 操作系统.....5
 - 2.1.1 认识注册表.....5
 - 2.1.2 注册表和 INI 文件的区别.....6
 - 2.1.3 注册表的结构.....7
 - 2.1.4 注册表的键操作.....8
 - 2.1.5 注册表中键的数据类型.....10
 - 2.1.6 注册表的结构分析.....11
 - 2.1.7 如何打开系统服务.....13
 - 2.1.8 系统服务的作用.....14
 - 2.1.9 FAT32 文件系统.....15
 - 2.1.10 NTFS 文件系统.....16
 - 2.1.11 NTFS 文件系统与 FAT32 系统的比较.....17
 - 2.1.12 NTFS 如何转换为其他文件系统.....19
- 2.2 Windows 安全机制.....20
 - 2.2.1 Windows XP 系统启动密码.....20
 - 2.2.2 Windows XP 权限.....20
- 2.3 Linux 操作系统.....21

- 2.3.1 文件系统.....22
- 2.3.2 目录和文件的基本操作命令.....24
- 2.3.3 Linux 口令安全.....25
- 2.3.4 Linux 配置文件安全.....25
- 2.3.5 使用 Cygwin 模拟 Linux.....26
- 2.4 嵌入式操作系统.....27
 - 2.4.1 嵌入式 Linux.....27
 - 2.4.2 嵌入式 Windows.....28
- 2.5 在线操作系统.....29
 - 2.5.1 JOOCE 在线操作系统.....29
 - 2.5.2 I-Cube 在线操作系统.....30
 - 2.5.3 Ajax Windows 操作系统.....31
 - 2.5.4 千脑在线操作系统.....32
- 2.6 小结.....33

第3章 网络核心基础——网络协议.....34

- 3.1 ISO/OSI 七层模型.....34
 - 3.1.1 OSI 七层模型简介.....34
 - 3.1.2 OSI 七层模型任务.....35
- 3.2 TCP/IP 通信协议.....36
 - 3.2.1 认识 TCP/IP.....36
 - 3.2.2 协议结构及功能.....37
 - 3.2.3 IP 地址的定义.....38
 - 3.2.4 查询主机 IP 地址.....38
 - 3.2.5 IP 地址的分类.....39
 - 3.2.6 计算机端口介绍.....40
 - 3.2.7 计算机端口的种类.....41
 - 3.2.8 查看计算机端口连接的方法.....42
 - 3.2.9 常见计算机端口说明.....43
- 3.3 HTTP 协议.....45
 - 3.3.1 典型的 HTTP 实例.....45
 - 3.3.2 HTTP 协议之 GET 请求.....46

3.3.3 HTTP 协议之 POST 请求	47	安装 Windows XP 操作系统	66
3.4 HTTPS 协议	51	4.5.2 设置虚拟机参数	66
3.5 FTP 协议	51	4.5.3 在虚拟机中安装操作系统	67
3.5.1 FTP 工作原理	51	4.5.4 玩转虚拟机	67
3.5.2 FTP 操作步骤	53	4.6 小结	68
3.6 SMTP 和 POP3 协议	54	第 5 章 自力更生——编程防范	
3.6.1 SMTP 工作原理	54	黑客	69
3.6.2 SMTP 基本命令集	54	5.1 “绿色环保”的批处理	69
3.6.3 命令行下使用 SMTP 发送邮件	54	5.1.1 批处理实例讲解	69
3.6.4 POP3 命令操作原理	55	5.1.2 批处理的几个小技巧	71
3.6.5 POP3 基本总结	56	5.2 功能强大使用方便的 VBS	71
3.6.6 命令行下使用 POP3 收邮件	56	5.2.1 VBS 能做什么	71
3.7 TCP/IP 中的术语和概念	57	5.2.2 VBS 实用小程序	72
3.8 小结	58	5.3 黑客软件开发工具	72
第 4 章 工欲善其事，必先利其器——安全利器	59	5.3.1 编程语言概述	73
4.1 黑软瑞士军刀——NC	59	5.3.2 Visual Basic 编程简介及实例	73
4.1.1 查看 NC 帮助信息	59	5.3.3 Visual C++ 简介及实例	76
4.1.2 使用 NC 监听端口模拟蜜罐	60	5.3.4 Delphi 简介及实例	87
4.1.3 使用 NC 连接远程主机	60	5.4 小结	89
4.2 内核级安全工具——IceSword	61	第 6 章 牛刀小试——防范入侵	
4.2.1 使用 IceSword 查杀隐藏进程	61	实战演练	90
4.2.2 使用 IceSword 超权限操作文件	62	6.1 “秒杀”网吧管理软件	90
4.2.3 使用 IceSword 查看进程模块	62	6.1.1 突破硬盘浏览的限制	90
4.3 软件破解屠龙刀——OllyDBG	63	6.1.2 突破下载限制	91
4.3.1 认识 OllyDBG 操作界面	63	6.1.3 “触类旁通”突破网吧各类限制	91
4.3.2 OllyDBG 的基本调试方法	63	6.2 突破网页鼠标右键功能的限制	92
4.4 文件传输工具——CuteFtp	64	6.2.1 “釜底抽薪”修改源代码	92
4.4.1 使用 CuteFtp 连接服务器	64	6.2.2 Snagit 抓取网页文字	92
4.4.2 使用 CuteFtp 上传文件	65	6.3 揪出网络视频文件的真实下载地址	93
4.4.3 使用 CuteFtp 下载文件	65	6.3.1 抓包获取视频文件真实地址	93
4.5 攻防演练环境搭建软件——虚拟机		6.3.2 抓包获取 MP3 真实地址	94
VMWareWorkStation	65	6.4 小结	94
4.5.1 使用虚拟机 VMWareWorkStation			
第二篇 木马和防木马工具的使用木马、嗅探和后门防范技术篇			
第 7 章 信息仓库——搜索引擎	96	7.1.4 网络中保护好个人隐私	98
7.1 实战搜索引擎	96	7.2 搜索引擎技巧集	99
7.1.1 从一个 QQ 号码开始搜索	96	7.2.1 搜索命令集	99
7.1.2 众里寻她千百度	97	7.2.2 定制关键字	100
7.1.3 我不能，Google 让我能	98	7.2.3 此路不通，还有他路	100
		7.3 小结	100

第 8 章 黑客入侵——主机扫描 101

- 8.1 端口扫描 101
 - 8.1.1 PortScan 使用简介 101
 - 8.1.2 超级扫描器——SuperScan 102
 - 8.1.3 高速端口扫描器——S 扫描器 103
- 8.2 服务及漏洞扫描 104
 - 8.2.1 专业安全评估软件 SSS 104
 - 8.2.2 安全检测软件 Nessus 106
- 8.3 网络共享扫描 108
 - 8.3.1 网络刺客 108
 - 8.3.2 网络刺客主机查找功能 108
 - 8.3.3 网络刺客添加和删除主机 109
 - 8.3.4 网络刺客辅助功能 110
 - 8.3.5 网络刺客猜解机功能 110
 - 8.3.6 超级网上邻居——IPBook 110
- 8.4 弱口令探测 112
 - 8.4.1 优秀漏洞扫描软件 X-scan 112
 - 8.4.2 漏洞扫描软件流光 114
 - 8.4.3 20CN 扫描种植机——扫描
IPC “肉鸡” 116
- 8.5 小结 116

**第 9 章 本土防御——操作系统
安全本地攻防** 117

- 9.1 Windows 操作系统密码攻防 117
 - 9.1.1 Windows 密码破解软件 LC5 118
 - 9.1.2 高速密码破解软件 SAMInside 118
 - 9.1.3 清空系统管理员密码 119
- 9.2 权限的诱惑——从 Guest 到
Administrator 120
 - 9.2.1 偷梁换柱——替换系统文件法 120
 - 9.2.2 暗渡陈仓——利用输入法漏洞 121
 - 9.2.3 都是漏洞惹的祸——本地溢出 122
- 9.3 操作系统安全防护 123
 - 9.3.1 个人计算机系统安全防护 123
 - 9.3.2 企业核心系统的安全防护 124
- 9.4 小结 124

**第 10 章 道高一尺，魔高一丈——
网络封锁与代理突破** 125

- 10.1 网络封锁的现实存在 125
- 10.2 代理服务器软件 125
 - 10.2.1 国产代理服务器软件 CCProxy 126

- 10.2.2 Socks 代理软件 (SocksCap) 128
- 10.2.3 在线代理服务器 129
- 10.3 代理服务器搜索软件 130
 - 10.3.1 代理猎手 (ProxyHunter) 130
 - 10.3.2 代理之狐 (ProxyFox) 132
 - 10.3.3 花刺代理 (ProxyThorn) 133
- 10.4 Foxmail 和 MSN 等网络
工具的代理 134
 - 10.4.1 Foxmail 代理设置 134
 - 10.4.2 MSN 代理设置 135
- 10.5 计算机共享上网实用技巧 135
 - 10.5.1 调制解调器拨号共享上网 135
 - 10.5.2 路由器共享上网 137
 - 10.5.3 用代理服务器软件共享上网 138
 - 10.5.4 ADSL 共享上网 138
- 10.6 突破网络封锁登录 QQ 138
 - 10.6.1 认识 SSH 隧道 139
 - 10.6.2 建立 SSH 隧道 139
 - 10.6.3 使用 SSH 加密隧道登录 QQ 140
- 10.7 小结 141

**第 11 章 揭开木马神秘的面纱——
木马攻防战** 142

- 11.1 特洛伊木马的由来 142
- 11.2 C/S 典型木马——冰河 142
 - 11.2.1 配置冰河木马服务端 143
 - 11.2.2 冰河功能简介 144
 - 11.2.3 冰河口令类命令 144
 - 11.2.4 冰河综合类命令 145
 - 11.2.5 冰河网络类命令 146
 - 11.2.6 冰河其他类命令 146
- 11.3 反弹型木马——“网络神偷” 147
 - 11.3.1 反弹型木马技术剖析 148
 - 11.3.2 配置“网络神偷”客户端程序 148
 - 11.3.3 “神偷谍影”轻而易举 149
- 11.4 精品控制软件——“灰鸽子” 150
 - 11.4.1 “灰鸽子”客户端上线配置 151
 - 11.4.2 实战“灰鸽子”远程控制 152
- 11.5 国外远程控制软件 154
 - 11.5.1 开源远程控制软件 VNC 154
 - 11.5.2 远程管理软件 pcAnywhere 156
 - 11.5.3 远程控制软件 DameWare NT 159
- 11.6 小结 160

第 12 章 关不住的那扇门—— 后门技术剖析.....161

- 12.1 基于命令行的远程控制——
Cmdshell 传奇.....161
 - 12.1.1 独孤剑客的 Winshell.....161
 - 12.1.2 与“狼”共舞的 Wolf 后门.....163
- 12.2 RootKit 与 Anti-RootKit 技术.....165
 - 12.2.1 认识 RootKit 技术.....166
 - 12.2.2 内核级后门 NTRootKit.....166
 - 12.2.3 黑客之门简介.....170
 - 12.2.4 黑客之门配置、安装与卸载.....170
 - 12.2.5 连接黑客之门.....172
 - 12.2.6 防范内核级后门——Anti-RootKit
技术.....175
 - 12.2.7 Rootkit 专用检测工具
Rootkit Unhooker.....176
- 12.3 防范操作系统自带的后门.....177
 - 12.3.1 Windows XP 默认安装的风险.....177
 - 12.3.2 防范内置后门的盗版操作系统.....178
 - 12.3.3 IIS 扩展权限设置不当.....179
- 12.4 脚本后门——Webshell.....180

- 12.4.1 ASP 后门：经典制作 cmd.asp.....180
- 12.4.2 ASP 后门：海阳 ASP 木马.....181
- 12.4.3 ASP 后门：“十三少的 ASP 木马”.....183
- 12.4.4 ASP 后门：ASP 一句话木马.....185
- 12.4.5 PHP 后门：ZaCo 的 php-webshell.....187
- 12.4.6 PHP 后门：C99Shell.....187
- 12.4.7 PHP 后门：PHP 一句话后门.....189
- 12.4.8 CGI、ASPX 和 JSP 后门.....189
- 12.5 小结.....190

第 13 章 这里黎明静悄悄——网络 嗅探攻防实战.....191

- 13.1 局域网嗅探.....191
 - 13.1.1 局域网嗅探原理.....191
 - 13.1.2 HTTP 密码嗅探.....191
 - 13.1.3 FTP 密码嗅探.....193
 - 13.1.4 邮件密码嗅探.....193
- 13.2 您的 MSN 被监听了吗.....195
 - 13.2.1 MSN 聊天内容监听.....195
 - 13.2.2 加密 MSN 通信.....196
- 13.3 小结.....196

第三篇 网络防范技术篇

第 14 章 无孔不入——SQL 注入 攻击剖析与防范.....198

- 14.1 SQL 注入技术理论基础.....198
 - 14.1.1 SQL 注入技术原理.....198
 - 14.1.2 SQL 注入的类型.....199
- 14.2 ASP+Access 环境下注入剖析.....199
 - 14.2.1 ASP+Access 注入语句解析.....200
 - 14.2.2 ASP+Access 入侵网站剖析.....202
 - 14.2.3 破解 md5 加密.....206
- 14.3 ASP+SQL Server 环境下注入
剖析.....207
 - 14.3.1 ASP+SQL Server 注入语句解析.....207
 - 14.3.2 ASP+SQL Server 注入某电影
测试网站剖析.....209
 - 14.3.3 SQL 注入数据库判断.....211
- 14.4 PHP+MySQL 环境下注入剖析.....212
 - 14.4.1 PHP+MySQL 注入语句解析.....212
 - 14.4.2 PHP+MySQL 注入网站剖析.....214
- 14.5 其他形式 Web 注入攻击剖析.....219

- 14.5.1 JSP 和 ASPX 注入剖析.....219
- 14.5.2 HTML 注入剖析.....220
- 14.5.3 Cookie 注入剖析.....220
- 14.6 变形 SQL 注入绕过安全检测.....222
 - 14.6.1 绕过单引号检测继续注入.....222
 - 14.6.2 化整为零突破防注入系统.....223
- 14.7 SQL 注入工具集剖析.....224
 - 14.7.1 注入检测工具 NBSI.....224
 - 14.7.2 注入检测工具.....228
 - 14.7.3 PHP 注入检测工具 CASI.....230
- 14.8 通用防注入系统.....231
 - 14.8.1 通用 ASP 防注入系统.....231
 - 14.8.2 通用 PHP 防注入系统.....232
- 14.9 小结.....233

第 15 章 防不胜防——XSS 跨站脚 本攻击技术剖析与防范.....234

- 15.1 跨站脚本攻击技术剖析.....234
 - 15.1.1 认识跨站脚本攻击.....234
 - 15.1.2 跨站攻击——构造语句艺术.....235

15.2 跨站模拟攻击剖析	237	封锁局域网	258
15.2.1 跨站漏洞测试	237	17.4 DNS 劫持技术剖析与防范	259
15.2.2 精心构造跨站脚本语句	237	17.4.1 DNS 解析原理	259
15.3 小结	240	17.4.2 DNS 劫持技术	259
第 16 章 在内存中跳舞——缓冲区溢出攻击剖析与防范	241	17.4.3 防范 DNS 劫持	260
16.1 缓冲区溢出攻击的概念	241	17.5 小结	260
16.1.1 认识缓冲区溢出攻击	241	第 18 章 无道胜有道——社会工程学	261
16.1.2 缓冲区溢出的历史	241	18.1 认识社会工程学	261
16.2 缓冲区溢出攻击的原理剖析	242	18.1.1 社会工程学的起源	261
16.2.1 缓冲区溢出相关技术术语	242	18.1.2 社会工程学的价值	261
16.2.2 缓冲区溢出漏洞存在的原因	243	18.2 常见社会工程学手段	262
16.2.3 缓冲区溢出攻击的内存模型	244	18.2.1 电话欺骗剖析	262
16.2.4 缓冲区溢出攻击的实现原理	244	18.2.2 身份扮演剖析	262
16.3 缓冲区溢出实例	245	18.2.3 信息收集	263
16.3.1 一个存在漏洞的示例程序	245	18.3 社会工程学典型案例剖析	263
16.3.2 缓冲区溢出简单利用	246	18.3.1 收集信息生成密码字典	264
16.3.3 ShellCode 编写简介	247	18.3.2 社会工程学盗用密码	265
16.4 缓冲区溢出攻击的防护	248	18.3.3 社会工程学破解密码提示问题	267
16.4.1 软件开发阶段的问题避免	248	18.4 防范社会工程学	268
16.4.2 程序编译阶段的问题检查	249	18.4.1 个人用户防范社会工程学	269
16.4.3 软件的安全配置和使用阶段	249	18.4.2 企业或单位防范社会工程学	269
16.5 小结	249	18.5 小结	269
第 17 章 真真假假——防范欺骗攻击	250	第 19 章 防范必备兵器——防火墙技术	270
17.1 眼见为虚——URL 欺骗	250	19.1 防火墙技术原理及功能	270
17.1.1 认识 URL	250	19.1.1 认识防火墙	270
17.1.2 URL 欺骗的实现原理	251	19.1.2 防火墙是网络安全的屏障	270
17.2 Cookies 欺骗	252	19.1.3 强化网络安全策略	271
17.2.1 认识 Cookie 欺骗	252	19.1.4 网络存取和访问监控审计	271
17.2.2 Cookie 欺骗的原理	253	19.1.5 防止内部信息的外泄	271
17.2.3 Cookie 欺骗工具	254	19.1.6 防火墙的历史	271
17.3 局域网中的幽灵——ARP 欺骗与防范	255	19.2 防火墙的分类	272
17.3.1 认识 ARP	255	19.2.1 静态包过滤型防火墙	272
17.3.2 ARP 协议工作原理	256	19.2.2 动态包过滤型防火墙	272
17.3.3 如何查看和清除 ARP 表	256	19.2.3 普通代理型防火墙	272
17.3.4 ARP 数据包分析	256	19.2.4 自适应代理防火墙	273
17.3.5 遭遇 ARP 攻击后的现象	257	19.3 天网恢恢，疏而不漏——防火墙安全策略	273
17.3.6 ARP 欺骗攻击原理	257	19.3.1 用天网防火墙查看网络状况	273
17.3.7 ARP 攻击实例及防护方法	258	19.3.2 用天网防火墙审核访问	274
17.3.8 例说软件“P2P 终结者”		19.3.3 设置应用程序访问规则	274

19.3.4	天网防火墙的 IP 规则	275
19.3.5	用天网防火墙检测入侵及日志	276
19.4	ZoneAlarm 防火墙	276
19.4.1	ZoneAlarm 防火墙简介	277
19.4.2	ZoneAlarm 应用程序访问规则	277
19.4.3	ZoneAlarm 防火墙 IP 规则	278
19.5	费尔个人防火墙	279
19.5.1	费尔防火墙模式设置	279
19.5.2	用费尔防火墙查看网络状态	280

19.5.3	用费尔防火墙监控网络连接	281
19.5.4	费尔防火墙应用规则设置	282
19.5.5	费尔防火墙访问过滤规则	282
19.5.6	用费尔防火墙查看日志	283
19.6	防火墙穿透技术剖析	283
19.6.1	进程插入技术	284
19.6.2	HTTP 隧道通信技术	288
19.7	小结	289

第四篇 防范案例实战篇

第 20 章 完美收官——一次完整的 黑客入侵过程剖析

20.1	信息收集阶段	292
20.1.1	网站基本信息收集	292
20.1.2	网站信息综合分析	294
20.2	跟着感觉走——入侵进行中	295
20.2.1	社会工程学一用	296
20.2.2	通过动网论坛获取 Webshell	297
20.2.3	大权在握——权限提升	298
20.2.4	小小插曲——端口扫描	299
20.2.5	成功入侵	300
20.2.6	得寸进尺——继续渗透扩大战果	301
20.3	做好善后工作	302
20.3.1	清除系统日志信息	302
20.3.2	擦除人为操作信息痕迹	303
20.4	入侵攻击的总结及防范措施	303
20.4.1	成功入侵的总结	303
20.4.2	针对黑客入侵的防范方法	304
20.5	小结	304

第 21 章 构筑铜墙铁壁——系统 安全策略实战技巧

21.1	密码安全策略	305
21.1.1	通过 BIOS 设置开机密码	305
21.1.2	设置操作系统密码	306
21.1.3	使用 syskey 设置操作系统 启动密码	307
21.1.4	永远不使用弱口令	309
21.1.5	制定密码安全策略	309
21.2	修复系统漏洞	310
21.2.1	开启系统自动更新功能	310
21.2.2	在线检测补丁	311

21.2.3	用安全工具修复漏洞	311
21.2.4	为服务器打上安全补丁	312
21.3	“最少服务”换取安全	313
21.3.1	禁用 Windows 自动更新服务	313
21.3.2	禁用打印后台服务程序	314
21.3.3	禁用 NetBIOS	315
21.3.4	禁用其他不必要的服务	315
21.3.5	禁用 Windows 默认共享	315
21.4	访问控制	316
21.4.1	启用 Windows 自带防火墙	316
21.4.2	启用 TCP/IP 筛选	317
21.4.3	灵活使用 IP 安全策略—— 创建筛选器列表	318
21.4.4	灵活使用 IP 安全策略——创建 基于筛选器列表的策略	319
21.4.5	安装防火墙软件	321
21.5	使用防病毒软件	321
21.5.1	国产杀毒软件	321
21.5.2	国外杀毒软件	322
21.6	防范“网页挂马”	323
21.6.1	釜底抽薪——更换浏览器	323
21.6.2	永久免疫上网中毒	324
21.6.3	反浏览器劫持	325
21.6.4	简单屏蔽恶意网站	325
21.7	合理分配权限	326
21.7.1	降低用户权限	326
21.7.2	设置网站文件夹执行权限	327
21.7.3	设置 NTFS 文件访问权限	328
21.8	严防 U 盘病毒	329
21.8.1	启用 U 盘写保护功能	329
21.8.2	“免疫”U 盘病毒	329
21.9	小结	330

第一篇

网络安全技术基础篇

- 第1章 知己知彼，百战不殆——网络安全现状
- 第2章 千里之行始于足下——认识操作系统及安全策略
- 第3章 网络核心基础——网络协议
- 第4章 工欲善其事，必先利其器——安全利器
- 第5章 自力更生——编程防范黑客
- 第6章 牛刀小试——防范入侵实战演练

第1章

知己知彼，百战不殆—— 网络安全现状

本章主要为了配合后面内容的讲解，让读者先对网络安全有一个全面的认识。内容涉及：黑客的由来及其发展现状、国内外网络安全的现状、日益猖獗的互联网犯罪和国家出台的相关法律、法规。

1.1 网络安全现状及发展趋势

我国的互联网起步较晚，虽然经过多年的发展已经有了很大进步，但是仍然存在很多问题，尤其是基础设施较差、核心技术级的关键人员缺乏等。最新统计显示，我国拥有网民两亿多人，位居世界第二。面对如此庞大的用户群，我们不得不去考虑日益严峻的网络信息安全现状。

1.1.1 认识黑客

“用了好几年的QQ号被盗！”

“苦练了50级的传奇游戏账号中的装备一夜之间被卸光！”

“XX媒体报道，重要的网站遭遇黑客入侵！”

“HD-DVD最新加密技术被黑客瞬间破解！”

“熊猫烧香病毒感染我的机器啦！”

.....

上面的场景相信很多人都遇到过。大多数上过网的读者，或多或少地接触过黑客这个词。黑客的英文原名叫“Hacker”，本意是指那些热衷解决问题、克服限制的技术人员。不过由于近年计算机领域的飞速发展，也在不断地创造黑客的传奇，使得黑客常被理解为计算机高手。同时，伴随着互联网犯罪的扩大化，很多人更是将黑客理解为攻击或入侵计算机的人员。

1.1.2 互联网安全现状

当前，计算机病毒、各种有害信息、系统安全漏洞和网络违法犯罪等信息安全问题日渐

突出,这不仅与信息通信业的持续健康发展目标相背,也给用户使用互联网带来了许多负面影响。因此,互联网信息安全状况受到了社会各界的关注和重视。

互联网犯罪是近几年媒体关注的热门话题。从“传奇大盗”到“熊猫烧香”,短短几年的时间,网络犯罪活动越来越猖狂。

网络犯罪其根本原因是,某些人希望通过计算机用非法手段获取利益,如一些虚拟的网络游戏中,黑客们利用非法手段盗取他人账号、密码,再通过一定的渠道将盗来的装备或虚拟货币在市场上兜售非法获利。

另外一方面原因是,一些网民在上网时缺乏防范黑客攻击的安全意识,如果用了盗版的操作系统,而且没有下载修复系统漏洞的各种升级程序,这样“千疮百孔”的计算机一旦连接上网络就很容易被黑客种植木马或病毒,成为黑客手中的“肉鸡”。



提示:“肉鸡”是指那些被植入木马或后门程序后,完全受黑客控制的计算机。形象地比喻为黑客菜板上的“肉鸡”,任人宰割。

一些黑客组织从未放弃对我国计算机网络进行攻击渗透,从CNCERT的统计报告可以看出,每天国内网站被入侵的数目居高不下,如图1.1所示。

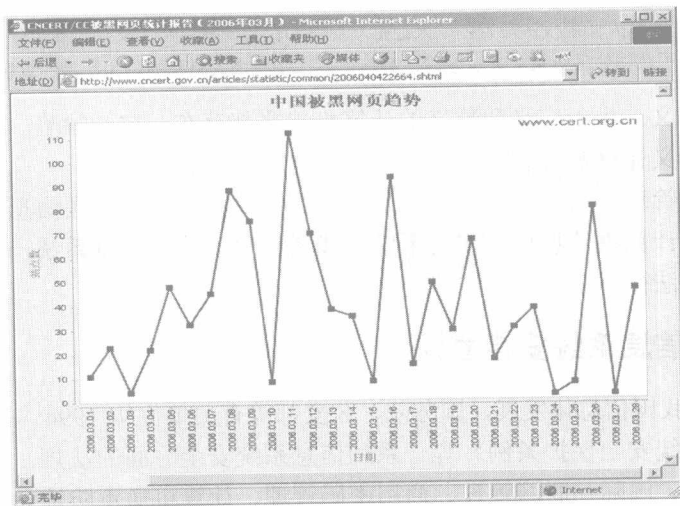


图 1.1 CNCERT 统计的网站被入侵情况

1.1.3 黑客技术发展

当前网络上各种常见的攻击技术包括:漏洞扫描、口令破解、脚本注入、缓冲区溢出、网络嗅探、木马后门、病毒破坏、代理渗透、身份伪造、社会工程学等。

随着黑客工具的傻瓜化,使得很多本身技术并不是很高的人也能很快上手,并能用这些工具制造出一定的破坏。据统计,网络上绝大部分所谓的黑客攻击实际上是那些并没有掌握多少深层技术的“菜鸟黑客”所为,他们常被称为“Tool User”。

由于信息网络的迅速发展,新的黑客攻防技术已经不再是简单入侵和破坏,而是上升到从系统的角度对目标系统造成破坏和保护己方系统稳定运行的高度。

1.2 计算机犯罪及相关法律

本节以计算机犯罪为基础，介绍计算机犯罪相关的概念、特点、防范及国家相关法律、法规。

1.2.1 计算机犯罪相关概念

由于计算机普及率的提高，人们利用计算机从事的各项活动日益增多。那么在计算机中什么样的活动是合法的，什么样的活动是非法的，存在一个法律界限的问题。计算机犯罪作为人类社会的一种新兴犯罪形式，人们对它的认识或多或少存在一定的局限性。

(1) 广义的计算机犯罪定义。在计算机犯罪出现的早期，由于计算机应用面较窄，计算机技术较为神秘，人们把与计算机相关的犯罪都认定为特殊犯罪，均归为计算机犯罪。

(2) 狭义的定义。针对广义的计算机犯罪定义过于宽泛，各国学者和机构都提出了自己冠以计算机犯罪定义的观点。



说明：瑞典的私人保密权法规定：“未经批准建立和保存计算机私人文件，有关侵犯受保护数据的行为，非法存取电子数据处理记录或非法修改、删除记录，侵犯个人隐私的行为都是计算机犯罪”。

(3) 折中的定义。由于广义和狭义的计算机犯罪都存在一定的缺陷，很多人开始寻求一种折中的方式来定义计算机犯罪。

公安部计算机管理监察司给出的定义是：所谓计算犯罪，就是在信息活动领域中，利用计算机信息系统或计算机信息指示作为手段，或者针对计算机信息系统，对国家、团体和个人造成危害，依据法律，应当予以刑罚处罚的行为。

1.2.2 计算机信息系统安全立法

为适应和保障我国信息化发展，国务院、公安部等有关单位从 1994 年起颁发了《中华人民共和国计算机信息系统安全保护条例》等一系列信息系统安全方面的法规。这些法规主要涉及信息系统安全防护、国际互联网管理、商用密码管理、计算机病毒防治和安全产品检测与销售 5 个方面。

1.3 小结

本章通过较短的篇幅为读者介绍了黑客的由来、国内外网络安全现状及发展趋势，同时还介绍了计算机犯罪相关的法律知识。从下一章开始，将介绍相关技术的理论知识，为读者后续学习打下基础。



第2章

千里之行始于足下—— 认识操作系统及安全策略

操作系统（operating system）是所有软件和系统运行的基础，它是一个大的基础平台。软件、系统都是围绕操作系统而发挥作用。网络安全也包括系统安全，因此学习网络安全，认识操作系统是必不可少的一个环节。本章的出发点是，在读者学习网络安全之前，为读者介绍一些必备的操作系统知识。在了解操作系统的各种特性（尤其是安全机制），后期的学习才能更加深入和透彻。

2.1 Windows 操作系统

Windows 操作系统在个人桌面操作系统用户中占有相当高的比率。由于 Windows 操作系统拥有最多的个人用户，Windows 操作系统也是黑客们紧盯的对象。本节将从注册表、系统服务、文件格式、安全机制等方面介绍 Windows 操作系统的相关知识。在后面章节介绍的 Windows 平台下的攻防技术都将会涉及本节的内容。

2.1.1 认识注册表

注册表是 Windows 系统的核心，它控制着 Windows 整个系统的运行。注册表到底是什么？本小节将对这个问题展开全面的讨论，并为读者进一步操作注册表打下基础。

注册表（registry）是 Windows 系统的一个核心数据库，它是辅助 Windows 控制硬件、软件、用户环境和 Windows 界面的一套数据文件。注册表包含系统的所有应用程序和软、硬件的相关信息。从用户的角度看，注册表系统由注册表数据库和注册表编辑器两部分组成。



提示：操作系统 Windows 目录下的 regedit.exe 就是注册表编辑器。在 Windows 早期的版本中（Windows95 以前），这些功能是靠 WIN.INI、SYSTEM.INI 及其他与应用程序有关联的 .INI 文件来实现的。

在 Windows 系列的操作系统中，文件 SYSTEM.INI 和 WIN.INI 包含了操作系统所有的控制功能和应用程序的信息，其中 SYSTEM.INI 负责管理计算机硬件，而 WIN.INI 则管理桌面和应用程序。系统中所有驱动、字体、设置和参数都会保存在 .INI 文件中，任何新程序都会被记录在 .INI 文件中，这些记录可以在程序中被引用。由于受到 WIN.INI 和 SYSTEM.INI

文件大小的限制，一般由程序员添加辅助的 INI 文件以便用来控制更多的应用程序。举例来说，某个软件 SoftX 安装成功后会生成 softx.ini 文件，它包含有选项、设置、默认参数和其他关系到该程序正常运行的信息。在操作系统的 SYSTEM.INI 和 WIN.INI 中只需指出 softx.ini 的路径和文件名即可。

在早期的 Windows 版本中，SYSTEM.INI 和 WIN.INI 控制着所有系统自身和应用程序的特征和存取方法，它在少数的用户和少数应用程序的环境中工作得很好。随着应用程序的数量和复杂性的增加，则需要 INI 文件中添加更多的参数项，这样每当有新的程序安装后操作系统都会去变更 INI 文件。但是，很少有程序在卸载后会清理这个配置文件，导致 SYSTEM.INI 和 WIN.INI 这两个文件会变得越来越大会，增加的内容会导致系统性能越来越慢。而且当应用程序需要升级时将会遇到很多麻烦问题，升级会增加更多的参数项，而对于旧参数则很少修改。由于 INI 文件的大小最多不超过 64kB，因此这会严重影响系统性能。为了解决这个问题，软件提供商一般都会提供自己的 INI 文件，然后指向特定的 INI 文件，如 WIN.INI 和 SYSTEM.INI 文件，这样会使多个 INI 文件影响系统正常的存取级别设置。如果一个应用程序的 INI 文件和 WIN.INI 文件在参数设置上发生冲突，程序往往无法判断其优先级。

注册表是一套控制操作系统外壳和辅助系统响应外来事件工作的文件。这些外来“事件”的范围包括：直接访问硬件设备或者接口，如何响应特定用户，应用程序及运行等。注册表因为其复杂性，被设计为专门向 32 位应用程序提供服务，其文件大小被限制为约 40MB。

2.1.2 注册表和 INI 文件的区别

在 Windows XP 下，注册表和 Windows NT 以前的 INI 文件主要有以下几点不同。

- 注册表采用了二进制形式登录数据。
- 注册表支持子键，每一个子关键字拥有自己的数据。
- 注册表中的键值项可以包含可执行代码，而不是简单的字符串。
- 注册表可以存储系统中多个用户的配置信息。

Windows 系统在安装过程中，安装程序会扫描计算机的硬件配置，并扫描检测系统中硬件的驱动，然后用扫描结果初始化注册表。同时，安装程序在系统盘的根目录下生成 System.1st 文件。如果系统更换了部分硬件，而这些硬件的驱动在注册表中没有存储，那么计算机用户就需要重新安装操作系统。



说明：System.1st 是注册表的原始备份文件。

下面通过对 Windows 系统工作过程的跟踪性描述，揭示操作系统如何使用注册表来启动计算机。

(1) 启动计算机。启动时，Windows 系统自动扫描计算机的硬件配置，并将扫描结果写入注册表，扫描结果包括 CPU 数量，内存容量等配置信息。同时，系统更新每台设备的相关信息，包括设备所使用的资源（DMA 中断和 I/O 地址），然后，Windows 系统利用注册表来配置计算机。



说明：配置过程主要包括初始化设备驱动程序，打开计算机的网络连接，以及启动相关的服务，如任务表等。