

电脑硬道理 第9版

黑客攻防

电脑报 编

玩家级
DIY

从菜鸟到大虾 练就黑客终极必杀技能

PC DVD



精彩光盘

- 黑客攻防多媒体视频教程
- 常用密码管理工具软件
- 电脑报专用版杀毒软件
- 系统优化、网络安全工具



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

TP393.08/260D

2008



黑客攻防



电脑报 编



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容简介

在很多人眼里,“黑客”是一群高深莫测的神秘人物,然而,随着网络的普及和病毒木马的泛滥,更多的人意识到“黑客”其实离我们很近,他就在我们的身边。“黑客”不只是代表破坏、攻击,如今,更多的是代表着网络安全,学习黑客知识,捍卫你的电脑安全,做网络安全卫士,你也行!

电脑硬道理之《黑客攻防》共包括以下四大部分:

基础入门篇:为读者讲解了黑客入门的基础知识,包括黑客应具备的基本技能、黑客必知必会的术语、黑客攻击前的扫描技能以及信息筛选方法;

上手实战篇:这一部分为大家安排了初级黑客攻防实例演练,包括QQ攻击与防范方法、局域网内的安全攻防、常见的密码攻防实例、各类账户欺骗实例剖析;

进阶操练篇:这部分主要讲解更深一层的黑客应用与技巧,包括病毒查杀方法、木马攻防实例、远程控制演练、网吧与网络游戏安全防范、系统与网站漏洞攻防;

安全防范篇:了解黑客攻防的实例操作后,这一部分将为大家介绍黑客防范技巧,包括U盘安全防护、P2P安全防范、使用网络代理隐藏IP、如何进行黑客追踪等内容,让读者知己知彼,做一名安全高手。

警告:文中涉及到的黑客攻防相关内容,仅供读者学习之用,如用于非法用途,后果自负!

光盘要目

- 1.电脑报专用版安全工具(2款)
(《木马清除大师》、《FileGee个人同步备份系统》)
- 2.系统与网络安全辅助工具(5款)
- 3.密码管理工具(5款)
- 4.Windows优化工具(4款)
- 5.黑客攻防视频教程(12部)

版权所有 盗版必究
未经许可 不得以任何形式和手段复制和抄袭

书 名: 黑客攻防

编 者: 电脑报

技术编辑: 李 勇

封面设计: 陈鲁豫

出版单位: 电脑报电子音像出版社

地 址: 重庆市双钢路3号科协大厦

邮政编码: 400013

对外合作: (023)63658933

发 行: 电脑报经营有限责任公司

经 销: 各地新华书店、报刊亭

C D 生产: 四川省荃山数码科技有限公司

文本印刷: 重庆市联谊印务有限公司

开本规格: 787mm×1092mm 1/16 23印张 400千字

版 号: ISBN 978-7-900729-72-9

版 次: 2008年5月第1版 2008年5月第1次印刷

定 价: 32.00元(1CD+配套书)

挑战自我，享受DIY的乐趣

在这愈发崇尚自我的时代，

DIY 已不局限于Do it yourself（自己动手）的范畴。

DIY不知不觉进入到2.0时代，它其实代表着一种精神，一种自由。

而创意、时尚、个性、体验、享受、互动，俨然一张张鲜明的DIY 2.0新时代标签。

1996年，DIY的理念由《电脑报》在国内率先提出，并随即在电脑爱好者中迅速流传开来，深受电脑商家和用户的推崇，以致一批又一批电脑玩家乐此不疲。DIY甚至一度成为性价比极高的组装电脑的代名词。

透过电脑应用的发展历程不难看出，正是DIY精神的深入人心，推动了国内个人电脑应用的迅速普及。而今，随着信息技术的不断升级，信息化应用得以广泛而深入地推进，DIY也不断被赋予新的内涵，不知不觉已悄然进入到了彰显个性的DIY 2.0时代，DIY的精神进而得以发扬光大：除传统硬件的选购、组装、改造、升级DIY以外，软件/系统的潜能挖掘、网络应用的按需定制、故障怪象的诊断排除、网络黑客的有效防御、酷炫作品的完美打造……也统统被纳入了DIY的领地。新一代DIY迷们通过自己动手、自学、自助，实现一项项目标应用或任务，努力挑战想象力的极限，充分享受着DIY带来的乐趣与成就。

如果说DIY 1.0的核心在于“创造性性价比”，那么DIY 2.0的核心就是“以人为本”。在DIY 2.0精神的召唤下，不仅电脑应用手段大为丰富，更多产品和服务的需求也被激发了出来。在DIY 2.0时代，可以说只有你想不到的，没有做不到的。

1999年，电脑报组织资深DIY玩家和电脑高手精心编写《电脑硬道理》丛书并适时推出，实际上将当时电脑DIY的经验和精髓结集成册，系统展现给了广大读者。丛书自出版以来，已连续9次再版，累计发行量超过200万册。《电脑硬道理》丛书，事实上成为电脑用户及时了解最新电脑应用的风向标，也是广大电脑爱好者首选的经典电脑实战手册。

由于电脑技术更新换代快，电脑应用也不断翻新，我们广泛听取了众多电脑专家和读者的意见，并顺应目前电脑DIY的趋势和潮流，选取最受广大用户关注的电脑装机、系统操作、故障排查、硬件维修、网管实战、黑客防范等主要应用，重新策划和编写了这套新版的《电脑硬道理2008》丛书。《电脑硬道理2008》丛书延续了历年《电脑硬道理》的风格，始终将通俗、实用放在首位，并结合DIY 2.0的最新潮流，为广大读者提供最新鲜、最全面、最权威的电脑应用资讯和实战技巧，是广大电脑爱好者提升应用水平不容错过的一道饕餮大餐！

电脑报

2008年5月





	入口	目的
基础入门	S 1 黑客入门第一课	常用的黑客手段 黑客必知必会的术语 查看隐藏进程和远程进程
	S 2 黑客攻击前的准备工作	网站信息探测 信息的筛选 扫描与嗅探实例分析
上手实战	S 3 QQ攻击与防范实例	QQ强制视频聊天 “假”密码保护陷阱 QQ聊天记录泄秘 QQ密码本地监听
	S 4 局域网攻防实例	Windows XP安全共享 修改组策略增强共享安全 Windows Vista系统安全共享
	S 5 密码攻防实例	Syskey双重加密与解除 文件和文件夹密码攻防 办公、压缩文档密码攻防
	S 6 账户欺骗实例剖析	管理员账户删除与伪造 识破管理员组的Guest账户 防范假终端管理员 防范邮箱账户欺骗
进阶操练	S 7 病毒查杀与防范实例	防范邮件附件病毒 全面防范网络蠕虫 搭建虚拟机深入理解病毒发作
	S 8 木马攻击与防范实例	木马的攻击过程分析 如何检测木马的存在 防范变幻网页木马 专业工具杀木马
	S 9 远程控制攻防实例	Windows XP自带远程控制工具 Windows Vista远程桌面连接 远程管理主机的利用
	S 10 网游与网吧攻防实例	网络游戏“盗号”揭秘 解读网站充值欺骗术 防范服务器遭遇DoS攻击 网游外挂完全解密
	S 11 系统与网站漏洞攻防实例	系统漏洞检测与修复 扫描局域网内计算机的安全漏洞 网站提权漏洞攻防 网站数据库攻防
安全防范	S 12 网络代理与黑客追踪	用“代理猎手”找代理 组合代理服务器的深入应用 实战IP追踪术
	S 13 网络安全与黑客防范	用安全卫士清理恶意软件 P2P网络安全防护 多功能的黑客工具箱 数字签名揪出可疑文件 影子系统保障系统安全

基础入门篇

第一章 黑客入门第一课

1.1 黑客要具备哪些技能	2	1.3.1 关闭进程和重建进程	20
1.1.1 常用的黑客手段	2	1.3.2 查看进程的发起程序	21
1.1.2 黑客常用的防御工具	4	1.3.3 关闭“杀不了”的进程	21
1.2 黑客必知必会的术语	6	1.3.4 查看隐藏进程和远程进程	22
1.2.1 系统相关术语	6	1.3.5 杀死病毒进程	23
1.2.2 网络术语	14	1.3.6 当心带毒的SVCHOST.EXE	23
1.3 Windows 进程攻防演练	19	1.3.7 判断Explorer.exe进程真假	24

第二章 黑客攻击前的准备工作

2.1 探测操作系统	27	2.3 搜索引擎探测	36
2.1.1 使用X-scan探测	27	2.3.1 搜索特殊的“关键词”	36
2.1.2 使用Ping命令探测	28	2.3.2 使用专用工具搜索	37
2.1.3 通过网站判断	30	2.4 信息的筛选	38
2.2 网站信息探测	31	2.4.1 人工筛选	38
2.2.1 探测域名和IP	31	2.4.2 软件筛选	39
2.2.2 强悍的Nslookup	33	2.4.3 社会工程学	40
2.2.3 获得网站的注册信息	34	2.5 网络监听与嗅探	41
2.2.4 网站其他信息	36	2.5.1 监听的魅力	41

目录 CONTENTS

2.5.2 监听实战·····	44	2.6.2 用流光扫描弱口令·····	51
2.5.3 网络监听防范方法·····	47	2.6.3 命令行下的嗅探器WinDump···	54
2.6 扫描与嗅探实例分析·····	47	2.6.4 经典嗅探器Iris·····	57
2.6.1 Sss扫描器扫描实战·····	47		

上手实战篇

第三章 QQ 攻击与防范实例

3.1 新手最易被攻击的方式·····	60	3.4.4 用QQ申诉信息夺取QQ号·····	68
3.1.1 QQ强制视频聊天·····	60	3.5 警惕“QQ大杀器”盗号·····	69
3.1.2 “假”密码保护·····	61	3.5.1 QQ号盗取剖析·····	69
3.1.3 QQ聊天记录泄秘·····	61	3.5.2 自动生成QQ尾巴·····	70
3.1.4 QQ密码本地监听·····	63	3.5.3 文件捆绑、自动弹出网页·····	70
3.2 防范完美QQ大盗破密码·····	64	3.6 QQ安全防范措施·····	71
3.2.1 初识完美QQ大盗·····	64	3.6.1 防范QQ被盗8项“注意”·····	71
3.2.2 QQ邮件、密保一网打尽·····	64	3.6.2 QQ密码防盗专家·····	71
3.3 防范“啊拉QQ大盗”·····	65	3.6.3 安全卫士“QQKeeper”·····	73
3.3.1 邮箱收信·····	65	3.6.4 噬菌体密码防盗专家·····	73
3.3.2 网站收信·····	66	3.7 全面武装，打造安全QQ·····	74
3.3.3 防范“啊拉QQ大盗”·····	66	3.7.1 用磁盘读写权限封杀QQ广告···	74
3.4 密码保护的克星·····	67	3.7.2 为QQ硬盘设置密码·····	75
3.4.1 木马客户端制作分析·····	67	3.7.3 为QQ通讯录设置密码·····	76
3.4.2 盗取QQ密码解析·····	68	3.7.4 保护Q币·····	76
3.4.3 轻松突破密码保护·····	68		

CONTENTS 目录

第四章 局域网攻防实例

4.1 Windows XP 安全共享	77	4.3.3 修改注册表法	81
4.1.1 禁用简单文件共享	77	4.3.4 停止服务法	81
4.1.2 创建用户账户和用户组	78	4.3.5 卸载“文件和打印机共享”	81
4.1.3 共享文件设置	78	4.4 Vista 系统安全共享	82
4.1.4 设置共享权限	78	4.5 共享漏洞攻防实例演示	83
4.2 修改组策略增强共享安全	79	4.5.1 使用工具	84
4.2.1 指定特定用户可以访问	79	4.5.2 配合IPC\$	84
4.2.2 禁止非法用户访问	79	4.5.3 窃取共享密码	87
4.3 封杀系统默认共享	80	4.6 共享漏洞安全防范	88
4.3.1 “停止共享”法	80	4.6.1 安全策略配置	88
4.3.2 批处理自启动法	80	4.6.2 权限设置与管理	90

第五章 密码攻防实例

5.1 系统密码攻防	96	5.2.2 利用回收站给文件夹加密	113
5.1.1 Syskey双重加密与解除	96	5.2.3 NTFS文件系统加密数据	114
5.1.2 BIOS密码设置与解除	98	5.2.4 与众不同的分时段加密	116
5.1.3 设置系统登录密码	101	5.2.5 图片加密好帮手	117
5.1.4 轻松找回WinXP管理员密码	103	5.2.6 文件分割巧加密	118
5.1.5 用ERD恢复系统密码	105	5.2.7 生成自解密文件的“机器虫”	119
5.1.6 系统其他密码设置	107	5.2.8 WinGuard加密应用程序	120
5.2 文件和文件夹密码攻防	112	5.3 办公文档密码攻防	122
5.2.1 系统文件夹属性简单加密	112	5.3.1 使用WordKey恢复密码	122

目录 CONTENTS

5.3.2 Word密码查看器.....	123	5.4.1 RAR Password Cracker恢复密码	125
5.3.3 轻松查看Excel文档密码	123	5.4.2 多功能密码破解软件.....	126
5.3.4 WPS密码攻防	124	5.4.3 暴力破解压缩文件密码.....	127
5.4 压缩文件密码攻防.....	125		

第六章 账户欺骗实例剖析

6.1 管理员账户删除与伪造	129	6.5 揪出密码大盗的伪装账户	146
6.1.1 更改账户名.....	130	6.5.1 本地破解法.....	146
6.1.2 伪造陷阱账户.....	131	6.5.2 远程破解法.....	147
6.2 识破管理员组的 Guest 账户	133	6.5.3 防范对策.....	147
6.2.1 虚假的管理员账户.....	133	6.6 系统账户克隆探秘	149
6.2.2 识破管理员组的Guest账户	134	6.6.1 Regedit与Regedit32.....	149
6.2.3 Guest账户的安全管理	134	6.6.2 建立隐藏的超级用户.....	150
6.3 防范假终端管理员	136	6.7 防范邮箱账户欺骗	153
6.3.1 初步了解终端服务.....	136	6.7.1 邮箱账户的伪造.....	153
6.3.2 终端服务器的连接.....	136	6.7.2 巧妙隐藏邮箱账户.....	154
6.3.3 非法终端管理员的识别.....	137	6.7.3 垃圾邮件的防范.....	154
6.4 管理员账户破解实例剖析	140	6.7.4 针对重要邮箱的使用防范.....	158
6.4.1 利用默认的Administrator ...	140	6.7.5 查找伪造邮箱账户发件人.....	158
6.4.2 创建密码恢复盘.....	141	6.8 Foxmail 账户破解与防范	158
6.4.3 通过双系统删除SAM文件	143	6.8.1 邮箱口令的安全防范.....	158
6.4.4 借助第三方密码恢复软件.....	144	6.8.2 邮箱账户密码的防范.....	160

进阶操练篇

第七章 病毒查杀与防范实例

- 7.1 计算机病毒及其分类 162
 - 7.1.1 计算机病毒的概念 162
 - 7.1.2 计算机病毒的分类 162
 - 7.1.3 计算机病毒传播途径 162
- 7.2 防范邮件附件病毒 163
 - 7.2.1 什么是邮件附件病毒 163
 - 7.2.2 邮件病毒的“夺命三招” 163
 - 7.2.3 全面阻截邮件病毒 165
- 7.3 全面防范网络蠕虫 167
 - 7.3.1 什么是网络蠕虫 167
 - 7.3.2 网络蠕虫的特性 168
 - 7.3.3 网络蠕虫病毒实例分析和防范 169
 - 7.3.4 网络蠕虫的全面防范 170
- 7.4 真假 Desktop.ini 和 *.htt 文件 172
 - 7.4.1 病毒的入侵 172
 - 7.4.2 病毒资料信息 172
 - 7.4.3 清除病毒 173
 - 7.4.4 加密我的文件夹 173
- 7.5 变型病毒原理分析与识别 175
 - 7.5.1 什么是变型病毒 176
 - 7.5.2 原理及其特征 176
 - 7.5.3 变形引擎的工作原理 177
 - 7.5.4 查杀病毒 178
- 7.6 宏病毒及其防治方法 179
 - 7.6.1 什么是宏病毒 179
 - 7.6.2 宏病毒的判断方法 180
 - 7.6.3 宏病毒的防治和清除 181
- 7.7 深入理解病毒发作 182
 - 7.7.1 了解VMWare Workstation 182
 - 7.7.2 VMWare Workstation的安装 182
 - 7.7.3 打造自己的虚拟计算机 183
 - 7.7.4 文件共享 186
 - 7.7.5 虚拟机中的木马实战 187

目录 CONTENTS

第八章 木马攻击与防范实例

8.1 认识木马.....	189	8.3.1 启动.....	197
8.1.1 木马的分类.....	189	8.3.2 进程.....	199
8.1.2 木马的结构.....	190	8.3.3 使用杀毒软件.....	200
8.1.3 常见木马入侵手法.....	190	8.4 木马攻防实例	200
8.1.4 木马的运行原理.....	191	8.4.1 冰河的反入侵实战.....	200
8.1.5 木马隐形位置.....	192	8.4.2 防范变幻网页木马.....	204
8.2 木马的攻击过程分析	194	8.4.3 探密远程开启视频的木马.....	209
8.2.1 配置木马.....	194	8.4.4 DLL木马追踪防范	211
8.2.2 传播木马.....	194	8.5 专业工具杀木马	214
8.2.3 运行木马.....	195	8.5.1 木马防线查杀木马.....	214
8.2.4 信息泄露.....	196	8.5.2 Windows木马清道夫	216
8.2.5 建立连接.....	196	8.5.3 微点主动防御软件.....	218
8.2.6 远程控制.....	196	8.5.4 超级巡警为木马自动脱壳.....	221
8.3 如何检测木马的存在	197		

第九章 远程控制攻防实例

9.1 Windows XP 自带远程控制 ...	223	9.2.2 允许远程桌面连接.....	225
9.1.1 用好Windows XP的远程协助...	223	9.2.3 发起远程桌面连接.....	226
9.1.2 Windows XP远程关机.....	224	9.2.4 在远程本地桌面间传文件.....	227
9.2 Windows Vista 远程桌面连接	225	9.3 Windows Vista 远程协助	228
9.2.1 什么是远程桌面.....	225	9.3.1 允许远程协助.....	228

CONTENTS 目录

9.3.2 邀请别人帮助.....	228	9.5.2 利用漏洞入侵主机.....	234
9.3.3 帮助别人.....	229	9.5.3 为漏洞主机打补丁.....	236
9.3.4 远程协助与远程桌面的区别...	230	9.5.4 隐藏式网站建立的方法.....	238
9.4 注册表远程连接与安全	231	9.6 远程控制工具演练	242
9.4.1 什么是注册表.....	231	9.6.1 用PcAnywhere远程控制.....	242
9.4.2 开启远程注册表服务.....	232	9.6.2 用灰鸽子进行远程管理.....	245
9.4.3 注册表安全设置实例剖析.....	233	9.6.3 用QuickIP进行多点控制	248
9.5 远程管理主机的利用	234	9.6.4 用WinShell实现远程控制.....	250
9.5.1 远程管理主机的利用思路.....	234	9.6.5 用PsExec远程控制.....	252

第十章 网游与网吧攻防实例

10.1 网络游戏“盗号”揭秘	254	10.4.1 DoS攻击与其局限性.....	261
10.1.1 用木马盗取账号	254	10.4.2 攻击CS服务器解析	261
10.1.2 远程控制方式盗号	255	10.4.3 防范方法	262
10.1.3 利用系统漏洞盗号	255	10.5 用内存补丁破解传奇外挂 ...	262
10.2 解读网站充值欺骗术	256	10.5.1 外挂介绍	262
10.2.1 欺骗原理	256	10.5.2 外挂验证	263
10.2.2 防范方法	256	10.6 透视免费外挂	264
10.2.3 提高防范意识	256	10.6.1 破解的开始	264
10.3 CS 作弊器实例剖析.....	257	10.6.2 防范方法	266
10.3.1 作弊器分类	257	10.7 网游外挂完全解密	268
10.3.2 作弊器开发过程	257	10.7.1 木马式外挂	268
10.3.3 典型作弊程序介绍	257	10.7.2 加速式外挂	270
10.3.4 常见反作弊程序	261	10.7.3 封包式外挂	272
10.4 防范服务器遭遇 DoS 攻击...	261	10.8 警惕局域网监听	274

目录 CONTENTS

10.8.1 了解监听的原理	274	10.10 防范网游盗号木马	276
10.8.2 防范方法	274	10.10.1 哪些程序容易被捆绑木马...	276
10.9 防范本地账户破解	275	10.10.2 木马程序感染途径.....	276
10.9.1 勿用“自动记住密码”	275	10.10.3 哪些网游账号容易被盗.....	276
10.9.2 防范方法	275	10.10.4 盗取WOW账号揭秘	276

第十一章 系统与网站漏洞攻防实例

11.1 认识系统漏洞攻防	278	11.4.1 远程控制实战	292
11.1.1 系统漏洞的基本概念	278	11.4.2 安全管理	295
11.1.2 系统漏洞的自动修补	278	11.5 博客系统攻防	299
11.2 系统漏洞检测与修复	281	11.5.1 博客系统简介	299
11.2.1 DcomRpc漏洞溢出防范.....	281	11.5.2 攻击实战分析	299
11.2.2 系统漏洞检测强大武器MBSA	284	11.6 网站提权漏洞攻防	300
11.2.3 扫描局域网内计算机的安全漏洞	285	11.6.1 提权漏洞实战	300
11.3 FTP 漏洞攻防	288	11.6.2 提权漏洞防范	305
11.3.1 FTP入侵分析.....	288	11.7 网站数据库攻防	307
11.3.2 Serv-U漏洞实战	289	11.7.1 数据库攻防简介	307
11.3.3 FTP攻击防范.....	291	11.7.2 下载数据库	308
11.4 FSO 漏洞攻防	292		

安全防范篇

第十二章 网络代理与黑客追踪

- 12.1 什么是代理服务器312
 - 12.1.1 什么是代理服务器 312
 - 12.1.2 代理服务器的分类 312
 - 12.1.3 如何使用代理服务器 313
- 12.2 用“代理猎手”找代理314
 - 12.2.1 软件的安装 315
 - 12.2.2 基本设置 315
 - 12.2.3 使用方法 316
- 12.3 SocksOnline 代理实战上手 317
 - 12.3.1 SocksOnline的作用..... 317
 - 12.3.2 实际操作过程 317
- 12.4 组合代理服务器的深入应用 318
 - 12.4.1 工具选择 318
 - 12.4.2 安装与设置 319
 - 12.4.3 连通性测试 320
- 12.5 架设超级 Sock5 代理321
 - 12.5.1 原理 321
 - 12.5.2 实际操作过程 321
- 12.6 感受远程跳板式攻击323
 - 12.6.1 扫描选择目标 323
 - 12.6.2 代理的架设 324
- 12.7 实战 IP 追踪术324
 - 12.7.1 网络定位 324
 - 12.7.2 获取好友 IP地址 325
 - 12.7.3 IP追踪 326

第十三章 网络安全与黑客防范

- 13.1 用安全卫士清理恶意软件 ...328
 - 13.1.1 系统漏洞修复 328
 - 13.1.2 查杀恶意软件 328
 - 13.1.3 全面系统诊断与修复 329
 - 13.1.4 免费查杀病毒 329
- 13.2 金山系统清理专家330

目录 CONTENTS

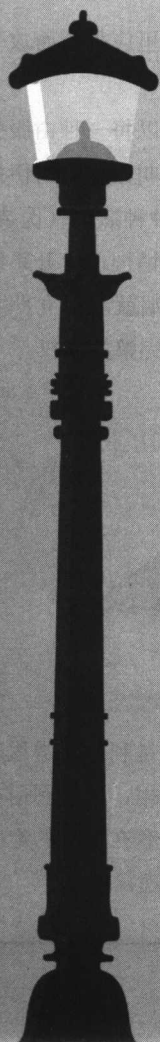
13.2.1 恶意软件查杀	330	13.5.3 PeerGuardian优化设置	339
13.2.2 两种IE修复方式	331	13.6 多功能的黑客工具箱	339
13.2.3 进程和启动项管理	331	13.6.1 文件图标更改、捆绑	339
13.2.4 历史痕迹清理	331	13.6.2 加密解密	340
13.2.5 特色功能	332	13.6.3 强制破解	341
13.3 使用瑞星查杀病毒	332	13.6.4 其他功能	341
13.3.1 全新的虚拟脱壳	333	13.7 全方位管理网络安全	343
13.3.2 开机“抢先”杀毒	333	13.7.1 工具介绍	343
13.3.3 独特的“碎甲”技术	333	13.7.2 进程管理	344
13.3.4 主动漏洞扫描、修补	334	13.7.3 Ping探测	344
13.3.5 易用的文件粉碎功能	334	13.7.4 局域网安全管理	344
13.3.6 嵌入式查杀病毒	334	13.7.5 网络连接管理	345
13.4 “防护盒”为U盘护航	335	13.7.6 地址转换	345
13.4.1 拦截免疫	335	13.8 数字签名揪出可疑文件	346
13.4.2 创建autorun.inf文件实现U盘免疫	336	13.8.1 查看文件的数字签名	346
13.4.3 1000多种常见病毒免疫	336	13.8.2 结合时间找到可疑的病毒文件	347
13.4.4 强大的进程管理	336	13.9 影子系统保障系统安全	348
13.5 P2P 网络安全防护	337	13.9.1 影子系统PowerShadow	348
13.5.1 PeerGuardian安装设置	337	13.9.2 数据保护伞ShadowUser	349
13.5.2 阻止P2P中的可疑连接	338	13.9.3 沙盘Sandboxie影子系统	350

01

基础入门篇

第一章 黑客入门第一课

第二章 黑客攻击前的准备工作



第一章

黑客入门第一课

在许多人眼里,“黑客”(Hacker)是一群高深莫测的神秘人物,他们利用掌握的技术肆意展开各种攻击,他们无往而不利……再加上一些媒体对黑客事件不负责任地夸大报道,使得黑客以及黑客技术对普通的电脑用户而言,无形中就多了几许神秘的色彩!其实,黑客以及黑客技术并不神秘,也并不高深。本章就带领大家认识黑客,学习黑客的入门知识。



1.1 黑客要具备哪些技能

怎样才能做一名黑客呢?黑客都常用哪些“绝招”来进行攻防呢?很多人由于对电脑安全防护和黑客入侵原理缺乏必要的了解,常常被黑客攻击了都还蒙在鼓里。因此,本节将一些常见的黑客攻击手段进行简单的介绍。

1.1.1 常用的黑客手段

在网络不断走向高速化的今天,全球网民的总量天天都在增加,再加上电脑安全配置不尽相同、用户安全意识有高有低,这都给黑客提供了“练兵场”。因而,黑客可以实施的手段各种各样。

1.木马与病毒

木马全称为“特洛伊木马”,其名源于古希腊神话。传说古希腊人围困特洛伊城,久攻不下。后来想出了一个妙计,让一些死士躲进巨大的木马中。大部队假装撤退而将木马遗弃于特洛伊城下,让敌人将其作为战利品拖入城内。夜晚特洛伊人正在觥筹交错、庆祝胜利的时候,木马内的

士兵乘机爬出来,与城外的部队里应外合而攻下了特洛伊城。

在计算机安全领域中,之所以将一种由服务器端和客户端两部分组成的程序叫做“特洛伊木马”,是因为其服务器端在通过种种欺骗(伪装)的方法进入被入侵主机后,可以悄悄地打开系统的一扇门(端口),这样其客户端就可以立即与其相连接,从而一举攻下系统的完整控制权。



木马示意图

木马一般有两种功能,一种是利用此类程序潜入用户电脑,窃取所需要的数据;二是利用在目标电脑中植入服务器端后,黑客在自己的电脑中通过客户端进行鼠标、文件管理等操作。