

黑客

入门

云上文化工作室

- 黑客常用哪些工具？
 - 黑客到底怎样入侵、攻击？
 - 黑客如何用不起眼的软件设计出狡诈的木马和病毒？
 - 我们要如何防护才能免除黑客的阴影与威胁？
-

理论 + 实战 图文 + 视频
让你不会也会！



黑客入门

云上文化工作室

名 称：黑客入门

策 划：胡小茜

编 著：云上文化工作室

责任编辑：刁 戈

执行编辑：胡小茜 彭 葵

封面设计：黄 丹

组版编辑：黄 丹 汤 立 邹 萍 丁 洁

出版单位：山东电子音像出版社

地 址：济南市胜利大街39号

邮政编码：250001

电 话：(0531) 2060055-7616

技术支持：(023) 63658888-13102

版权所有 盗版必究

未经许可 不得以任何形式和手段复制或抄袭

发 行：重庆中科普传媒发展股份有限公司发行部

经 销：各地新华书店、报刊亭

光盘生产：四川釜山数码科技文化发展有限公司

文本印刷：重庆华林天美印务有限公司

开本规格：787×1092毫米 1/16 16印张 200千字

版 本 号：ISBN 978-7-89491-967-0

定 价：35元 (1CD+手册)



为什么 购买

特别声明：本书及光盘从技术分析角度出发，对黑客的每个攻击入侵方法和所有实例都进行了测试，全部可以实现和做到，但害人之心不可有，读者诸君切勿将本书及光盘内容用于任何违法行为，否则一切法律责任自负！

本书一改以往黑客类图书文字较多且晦涩等缺点，采用大量的图片，直观地展示了黑客入侵的各式奇技淫巧，让你在一步步跟着学做之后即可熟知那些“神秘”的黑客手法，从而高度重视网络安全，并采取有效手段进行防护，从而免除黑客的阴影和威胁。


适用读者：不需要专业的网络知识，也不需要任何编程基础，光盘中的黑客攻防视频教程，全程语音解说，任何人都没理由看不懂！

特别要指出的是，为了大家携带方便，本书特别采用了轻型纸，在相同页码情况下，采用轻型纸印刷的图书比采用普通胶版纸印刷的图书要轻便很多，拿在手里也不会觉得沉。





CONTENTS

目录

注：本目录中凡标有  的章节均在光盘中有配套教学视频。

第 1 章

入侵，从这里开始 系统入侵与防范

1.1 黑客入侵实作流程	3
 1.1.1 踩点——筛选入侵目标.....	4
1.1.2 扫描——刺探“敌情”.....	5
 1.1.3 入侵——发起攻击.....	6
1.1.4 擦干净脚印——清扫入侵痕迹.....	7
1.2 入侵主机	9
1.2.1 入侵网页服务器.....	9
1.2.2 个人主机如何防范.....	12
1.3 窃取操作系统账号	15
1.3.1 贴身破解密码.....	15
1.3.2 远程登录系统——被忽略的隐藏账号.....	16
1.4 伸向主机的黑手——端口攻防	17
1.4.1 用SuperScan进行端口扫描.....	17
1.4.2 端口监控利器Port Reporter.....	18
1.5 让系统安全运行	20
1.6 安全防范软件	22
1.7 本章习题	22
1.7.1 判断题.....	22
1.7.2 填空题.....	23

第 3 章

形同虚设的密码 密码窃取与防范

2.1 网络访问权限攻防	27
2.1.1 设置IE浏览器访问权限.....	27
2.1.2 破解IE访问的权限密码.....	29
2.1.3 设置网络连接访问权限.....	30
2.1.4 设置账户锁定策略.....	30
2.1.5 解除被锁定的用户账户.....	32
2.2 操作系统密码攻防	32
2.2.1 设置用户账号登录密码.....	33
2.2.2 破解用户账号登录密码.....	33
2.2.3 组策略的密码策略.....	34
2.2.4 破解组策略“自锁”.....	35
2.3 应用软件密码攻防	37
2.3.1 加密Office文档.....	37
2.3.2 破解Office文档.....	37
2.3.3 加密WinZIP文件.....	38
2.3.4 破解WinZIP文件.....	39
2.3.5 加密WinRAR文件.....	40
2.3.6 破解WinRAR文件.....	40
2.4 网管账户攻防	41
2.4.1 使用Administrator账户登录系统.....	41
2.4.2 删除Guest账户.....	42
2.4.3 用AccessDiver破解网管账户.....	44
2.5 网络应用账号攻防	45
2.5.1 提高密码安全性.....	45
2.5.2 用360保险箱保护账号密码.....	45
2.6 本章习题	46

2.6.1 判断题.....	46
2.6.2 填空题.....	46

第三章

常在网上飘，哪有不挨刀 网络攻击与防范

3.1 恶意修改程序.....	49
3.1.1 攻击类别.....	49
3.1.2 有效的安全防范.....	50
3.2 Cookie欺骗.....	52
3.2.1 何为Cookie欺骗.....	52
3.2.2 如何防范.....	53
3.3 Web欺骗.....	54
3.3.1 实施Web欺骗.....	54
3.3.2 防范Web欺骗.....	55
3.4 缓冲区溢出.....	56
3.4.1 何为缓冲区溢出.....	56
3.4.2 缓冲区溢出漏洞攻击.....	57
3.4.3 有效防范.....	57
3.5 IP破解与隐藏.....	58
3.5.1 破解主机IP地址.....	58
3.5.2 隐藏IP地址.....	59
3.6 分布式拒绝服务攻击.....	61
3.6.1 攻击过程.....	61
3.6.2 实施防范.....	62
3.7 Web脚本攻击.....	64
3.7.1 攻击过程.....	64
3.7.2 实施防范.....	64

3.8 本章习题	66
3.8.1 判断题.....	66
3.8.2 填空题.....	67

第四章

网上聊天要小心 聊天软件攻击与防范

4.1 QQ攻击方式	71
4.1.1 用“QQ简单盗”偷密码.....	71
4.1.2 用“QQ临时会话器”强行聊天.....	73
4.1.3 用“飘叶千夫指”进行消息轰炸.....	74
4.2 QQ本地安全防范	75
4.2.1 QQ聊天记录器.....	75
4.2.2 QQ聊天终结者.....	76
4.2.3 保护本地聊天记录.....	77
4.3 防范远程QQ盗号	79
4.3.1 用QQExplorer在线破解QQ.....	80
4.3.2 用X-sniffer简单反击木马盗号者.....	81
4.3.3 清除QQ木马.....	82
4.3.4 通过网络申诉找回QQ密码.....	83
4.4 MSN盗号木马	84
4.4.1 下载MSN Messenger Hacker.....	84
4.4.2 植入木马文件.....	85
4.4.3 盗取MSN账号.....	85
4.5 本章习题	85
4.5.1 判断题.....	85
4.5.2 填空题.....	86

第5章

你的邮箱变他家厨房

邮件攻击与防范

5.1 用WebCracker破解网页邮箱用户和密码	89
5.2 邮件轰炸	91
5.2.1 用随心邮件工具进行邮件轰炸	91
5.2.2 用Foxmail进行邮箱攻击	93
5.3 利用Outlook Express漏洞骗取用户名和邮件内容	96
5.3.1 新建一个邮箱账户	97
5.3.2 改变发送者姓名—给对方来个大忽悠	98
5.4 常用安全防范方法	99
5.4.1 备份Outlook Express	99
5.4.2 为Outlook Express邮件加密	100
5.4.3 Outlook Express防范邮箱炸弹	101
5.4.4 设置Foxmail过滤器	103
5.5 本章习题	104
5.5.1 判断题	104
5.5.2 填空题	104

第6章

狡猾的木马 木马入侵与防范

6.1 漏洞扫描	107
6.1.1 用MBSA发现Windows系统漏洞	107
6.1.2 RPC漏洞扫描	109
6.2 木马植入	110
6.3 常用木马攻防实例	112
6.3.1 经典的反弹性木马—灰鸽子	112

6.3.2 远程控制的利器——网络神偷	113
6.3.3 冰河木马入侵	116
6.4 木马清除	118
6.4.1 用天网防火墙防御木马	118
6.4.2 下载专用的木马清理工具	121
6.4.3 WindowsXP防火墙使用方法	121
6.4.4 用组策略限制系统工具运行	122
6.5 本章习题	123
6.5.1 判断题	123
6.5.2 填空题	123

第 7 章

防杀结合 消除网络威胁

7.1 IP欺骗原理与防范	127
7.1.1 IP欺骗的实施	127
7.1.2 如何防范	128
7.2 网络病毒防范	130
7.2.1 防范网页脚本病毒	130
7.2.2 防范网络蠕虫病毒	131
7.2.3 使用各类病毒专杀工具	132
7.3 网络服务安全防范	132
7.3.1 身份验证的安全隐患和防范	132
7.3.2 关闭不安全的本机网络服务	133
7.4 局域网安全管理工具应用	134
7.4.1 使用局域网安全工具套装	135
7.4.2 局域网安全传输工具	135
7.4.3 使用网络版杀毒软件	137
7.5 无线网络安全	141

7.5.1 网络连接安全控制	141
7.5.2 其他安全设置	142
7.6 本章习题	143
7.6.1 判断题	143
7.6.2 填空题	144

第 4 章

安全压倒一切

网络设备的安全管理

8.1 宽带路由器安全设置	147
8.1.1 从账号方面保护宽带路由器安全	147
8.1.2 从远程控制方面保护宽带路由器	148
8.1.3 防火墙设置	149
8.2 防火墙与入侵检测设备	150
8.2.1 防火墙设备	150
8.2.2 入侵检测设备	153
8.3 网络设备状态检测	156
8.3.1 交换机状态检测	156
8.3.2 网卡状态检测	157
8.3.3 ADSL Modem 状态检测	157
8.4 网络设备访问控制	158
8.4.1 什么是网络设备访问控制	158
8.4.2 访问控制实施方法	159
8.5 本章习题	161
8.5.1 判断题	161
8.5.2 填空题	162

第四章

学会现场自救 抢救系统与数据

9.1 使用数据备份设备	165
9.1.1 磁盘阵列.....	165
9.1.2 磁带库.....	168
9.2 操作系统备份恢复	169
9.2.1 使用“系统还原”功能.....	169
9.2.2 使用Ghost备份软件.....	171
9.3 数据备份修复	172
9.3.1 数据手动备份与恢复.....	172
9.3.2 使用系统自带备份工具.....	175
9.3.3 使用系统自带文件和设置转移向导.....	177
9.3.4 使用专门的数据修复软件.....	178
9.4 操作系统重装升级	182
9.4.1 重新安装操作系统.....	182
9.4.2 用安装脚本实现自动重新安装.....	183
9.4.3 安装一键恢复Ghost工具.....	185
9.4.4 制作自启动U盘.....	186
9.4.5 利用Windows PE 排查修复系统.....	189
9.5 本章习题	191
9.5.1 判断题.....	191
9.5.2 填空题.....	191

附录1：安全防范工具与技巧

附1.1 用奇虎360安全卫士守住系统	193
附1.1.1 清理系统恶评插件.....	193
附1.1.2 自动修补系统漏洞补丁.....	195

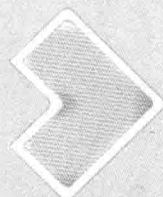
附1.1.3 优化系统性能.....	195
附1.2 用金山毒霸剿灭流行病毒	196
附1.3 非攻善守的“墨者安全专家”	198
附1.3.1 基本设置和检测	198
附1.3.2 特色功能	199
附1.3.3 系统监控和性能优化.....	200
附1.4 通过查看启动项防止木马运行	201
附1.4.1 查看开始菜单启动项	202
附1.4.2 查看注册表中的运行项目.....	202
附1.5 易被攻击的139端口及防范方法.....	203
附1.5.1 139端口如何被攻破	203
附1.5.2 防范139攻击的安全设置.....	205
附1.6 警惕与普通文件捆绑在一起的木马.....	206
附1.7 关闭Telnet服务切断入侵路径.....	209
附1.8 用代理服务器隐藏自己的真实地址.....	210
附1.9 用代理超人查看代理的安全级别	213
附1.10 备份Windows系统的加密证书和密钥	215
附1.11 使用Syskey加密——为系统再上一道安全锁	217
附1.12 卡巴斯基彻底监控本机安全.....	218
附1.12.1 防护设置	218
附1.12.2 杀毒设置	221
附1.12.3 状态查看	222
附1.13 恶意软件清理助手	224
附1.13.1 恶意软件清理.....	224
附1.13.2 修复功能.....	225

附录2：入门必备常识

附2.1 黑客攻击通道-端口大全	227
-------------------------------	------------

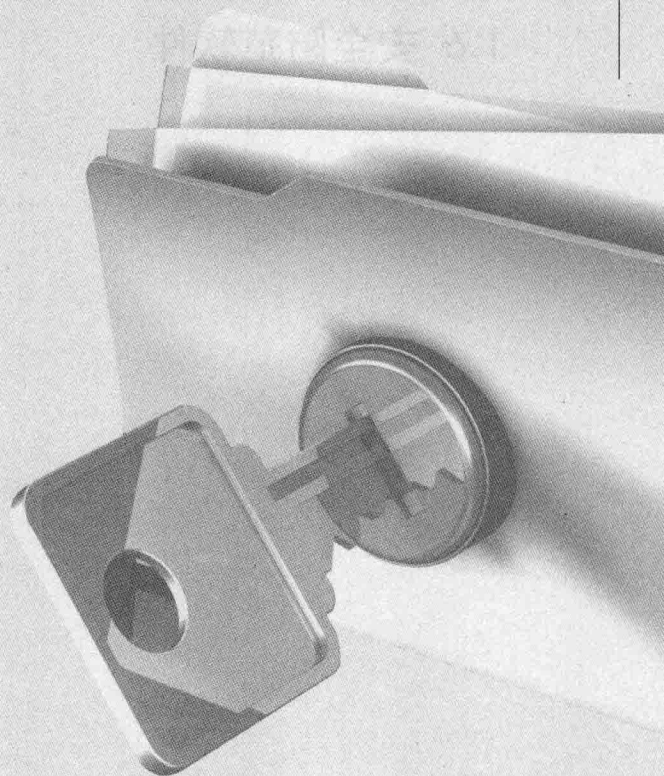
附2.1.1 认识TCP/IP协议端口.....	227
附2.1.2 端口分配.....	227
附2.1.3 端口查看.....	228
附2.1.4 常见端口速查.....	230
附2.2 黑客常用命令——Telnet使用大全.....	230
附2.3 黑客专业术语.....	235

附录3：各章习题答案.....	239
------------------------	------------



第 一 章

入侵，从这里开始 系统入侵与防范

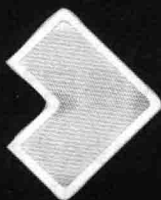
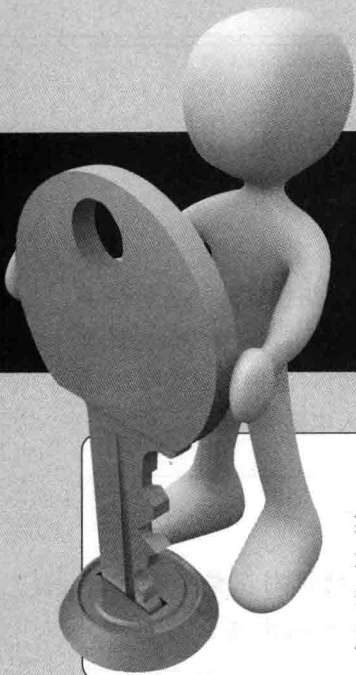




1.1 黑客入侵实作流程	3
1.2 侵入主机	9
1.3 操作系统账号安全	15
1.4 斩断伸向主机的黑手——端口攻防	17
1.5 系统安全运行	20
1.6 安全防范软件	22



第一章



入侵，从这里开始 系统入侵与防范

当黑客打算侵入网络另一端的电脑操作系统时，并非一蹴而就，而是先收集情报，制定攻击方案，一般还要做些试探性的攻击，找出目标电脑的弱点后才真正开始实施入侵，进行植入木马，盗取文件、账号等违法活动。本章中，我们会用一些实例讲解黑客如何攻击，作为普通用户又该如何防范等方面的应用知识。



1.1 黑客入侵实作流程

一般黑客入侵的完整模式分为几个步骤进行，图1-1是一张详细的黑客入侵行为流程图。

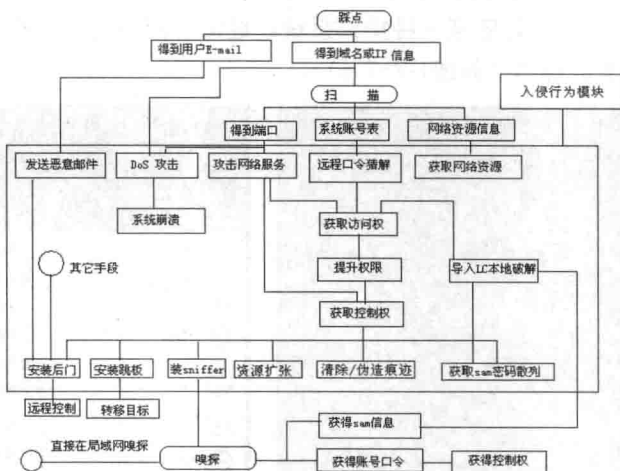


图1-1

我们可以把这个黑客行为的流程概括为以下几方面：

- * 踩点并判断入侵目标的操作系统类型；
- * 扫描端口并判断目标开放了哪些服务；
- * 根据目标的操作系统类型及开放的服务选择入侵方法；
- * 取得系统最高管理权限；