

The Bible of Hacking and AntiHacking

黑客任务 大作战

真枪实弹

纸上谈兵

本书列举**143**个黑客攻防操作与问题，彻底了解黑客手法并进行有效防护与阻挡

全面
攻略

浏览网页就植入木马或打开后门……超级大漏洞

黑客隐藏IP的六大方法·简单、有效的瘫痪攻击

黑网页速成大法·破解网页账户密码五大方法

- 黑客隐藏IP的六大方法与破解
- MSN、Skype、Yahoo Messenger、ICQ、QQ取得**好友IP**
- 黑客利用端口139入侵详细流程与防护之道
- 黑客破解各种**网页账户密码**的五大方法与防护
- MSN、Yahoo Messenger、ICQ、QQ 密码、名单、聊天记录……大作战
- Telnet、FTP、终端机服务……攻防大作战
- 打开**Telnet**、**终端机服务**后门自由进出
- 浏览器与邮件夹带之攻防大观
- **黑网页**速成大法与有效防护
- **一步到位法**……远程溢出漏洞入侵技巧与盲点解说
- 简单、迅速又有效的**瘫痪攻击**与防护
- 网络服务器**入侵流程**大公开

……更多攻防密技之研究与实战



程秉辉 编著

兵器工业出版社



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

The Bible of Hacking and AntiHacking

黑客任务 大作战



本书列举143个黑客攻防操作与问题，彻底了解黑客手法并进行有效防护与阻挡

全面
攻略

浏览网页就植入木马或打开后门……超级大漏洞

黑客隐藏IP的六大方法·简单、有效的瘫痪攻击

黑网页速成大法·破解网页账户密码五大方法

- 黑客隐藏IP的六大方法与破解
- MSN、Skype、Yahoo Messenger、ICQ、QQ取得好友IP
- 黑客利用端口139入侵详细流程与防护之道
- 黑客破解各种网页账户密码的五大方法与防护
- MSN、Yahoo Messenger、ICQ、QQ 密码、名单、聊天记录……大作战
- Telnet、FTP、终端机服务……攻防大作战
- 打开Telnet、终端机服务后门自由进出
- 浏览器与邮件客户端攻防大观
- 黑网页速成大法与有效防护
- 一步到位法……迅速找出漏洞入侵技巧与盲点解
- 简单、迅速又有效的瘫痪攻击与防护
- 网络服务器入侵流程大公开

……更多攻防密技之研究与实战

程秉辉 编著

兵器工业出版社



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是从黑客的内心深处来探讨黑客的行为与做法,详细说明黑客实作的流程与步骤。全书列举 143 个黑客攻防实作与问题,帮您彻底了解黑客操作的各种手法,以进行有效的防护与阻挡。本书是研究黑客技术、思考想法、实际操作、心理与防护等集大成之书籍。

主要内容包括:IE 漏洞入侵法、网络密码暴力破解、Windows 网络入侵术、黑客 IP 隐身术、盗取 MSN、Yahoo 即时通资讯、远程溢出漏洞入侵、打开后门自由进出、简单又有效的瘫痪攻击与防护等。

书附光盘中赠送了多种系统防护、网络通信工具,以及全球各地 IP 地址和端口详细列表。

图书在版编目(CIP)数据

黑客任务大作战 / 程秉辉编著. —北京:兵器工业

出版社;北京希望电子出版社,2006.9

ISBN 7-80172-702-9

I. 黑... II. 程... 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(2006)第 071402 号

出版发行:兵器工业出版社 北京希望电子出版社

邮编社址:100089 北京市海淀区车道沟 10 号

100085 北京市海淀区上地 3 街 9 号

金隅嘉华大厦 C 座 611

电 话:(010) 82702660(发行) (010) 62541992(门市)

经 销:各地新华书店 软件连锁店

印 刷:北京双青印刷厂

版 次:2006 年 9 月第 1 版第 1 次印刷

封面设计:刘孝琼

责任编辑:郭春临 宋丽华 李兴旺

责任校对:但明天

开 本:787×960 1/16

印 张:33.75

印 数:1-5000

字 数:607 千字

定 价:48.00 元(配 1 张光盘)

(版权所有 翻印必究 印装有误 负责调换)

作者感言

经过数个月的艰辛苦战，小弟与 John Hawke 老兄终于将本书完成，这本书应该是我们从事写作以来最难写的书，因为其中涉及到许多技术与漏洞的研究、测试、比较，甚至要设计相关的工具程序，就如同 R&D 工作一样辛苦，最后总算不辱使命地将所有成果放在本书中与大家共享。

本书是从黑客的心底深处来探讨黑客的行为与做法，详细说明黑客实作的流程与步骤，如此才能针对各个环节进行防护与阻挡，彻底保障你上网的安全。特别是在 Windows 漏洞方面的研究，更是大规模测试了国内和中国台湾地区以及美国将近 40~50 万台电脑，发现仍然有许多人并不重视网络安全或只是使用杀毒软件和防火墙等一些基本的防护而已，对于漏洞的修补(特别是最新的漏洞)多半付之如阙或处理迟缓。例如，本书中专案研究的 MS06-001 漏洞，几乎对于目前 99% 的 Windows 电脑入侵如同吃饭一样方便，实在很可怕！

虽然本书内容已经相当丰富与完整，但仍然无法涵盖所有的黑客攻防主题，特别是木马这部分，不过有兴趣的读者还是可以参考小弟的另一本书《黑客防护实战——木马防护全攻略》，与本书合并研读相信就可以打通任督二脉，彻底了解与掌握黑客的各种行为，如此才能让你的电脑远离黑客的各种威胁。

这里，笔者提醒各位：本书内容完全从理论与技术的角度来讨论与研究有关黑客攻略的方法，以达到有效防护与阻挡黑客入侵的目的。如果有将本书内容用于任何违反法律的行为，必须自行承担各种相关的法律责任。



程秉辉

Hawke Cheng

2006.7.27

请将下表数据填妥后 发邮件到 hawkegg@gmail.com ,
我们将会不定期地为您提供有关 Windows、Internet 和多
媒体的各种最新信息和相关软件。您也可以到我们的网
站 <http://www.faqdiy.cn/> 获得相关的更新文件与最新信
息。请多多利用, 谢谢!



若您使用电子邮件则请使用本书光盘中所附
的读者服务卡, 不必使用这个读者服务卡。

读者服务卡 REGISTER CARD				
书名	黑客任务大作战			
姓名		性别	☐ 先生 ☐ 小姐	年龄
学历	☐ 研究生 ☐ 本科 ☐ 大专 ☐ 高中 ☐ 初中 ☐ 小学			
您的电子邮件				
传真号码				
购买地区 (选择最 近城市)	☐ 北京 ☐ 上海 ☐ 南京 ☐ 广州 ☐ 深圳 ☐ 武汉 ☐ 重庆 ☐ 成都 ☐ 福州 ☐ 天津 ☐ 大连 ☐ 南昌 ☐ 苏州 ☐ 杭州 ☐ 青岛 ☐ 长沙 ☐ 开封 ☐ 合肥 ☐ 哈尔滨 其他:			
职业	☐ 学生 ☐ 电脑业或 IT 部门 ☐ 非电脑业 ☐ 其他: _____		您认为 本书	☐ 简单 ☐ 适中 ☐ 很难
您在写程序时 常遇到什么样的 的困扰与麻烦?				
您从何处 知道 本书?	☐ 连锁书店 ☐ 一般书店 ☐ 电脑专卖店 ☐ 同学 ☐ 展览 ☐ 亲友 ☐ 广告函 ☐ 因特网 ☐ 报纸: _____ ☐ 杂志: _____ ☐ 其他: _____			
您还需要哪些 方面的书籍?	☐ 其他 Windows 排困解难 ☐ 黑客攻防研究 ☐ 防黑防毒 ☐ 网页设计排困解难 ☐ Java 语言设计 ☐ Windows 程序设计(MFC, SDK) 其他: _____			
您对本书 有何建议?				

目 录

Part 1 黑客入侵基本原理与观念

(Basic Concept for Hacker Intrusion)

创建正确的观念	2
Internet 世界的基本原理	3
端口的角色与功能	4
黑客入侵的原理与方式	10
黑客入侵实作流程	13

Part 2 IP 隐藏术与破解

(Research for Hide IP Address)

Q1 黑客在进行任务时会采取哪些自我保护措施, 以降低风险避免被抓到?	17
Q2 使用公司或单位网络来上网的黑客如何逃避网络连接设备(如路由器或防火墙)的 日志追查到自己的电脑?	17
Q3 什么情况下黑客必须隐藏自己的上网 IP 地址, 否则就有被抓到的危险?	19
Q4 黑客会使用哪些方法来隐藏上网的 IP 地址, 不让被黑者或网管人员找到?	19
Q5 黑客如何利用无线网络来隐藏 IP 地址? 有何缺点?	24
Q6 黑客如何查找可使用的无线网络来上网? 如何让自己的无线基地台不被找到?	24
Q7 黑客会使用哪些方法来破解加密的无线基地台来上网? 如何进行防护?	24
Q8 黑客如何查找与使用代理服务器(Proxy Server)来隐藏上网 IP 地址?	31
Q9 黑客使用代理服务器来进行黑客任务会注意那些地方? 有何优缺点?	31
Q10 如何在不同的代理服务器之间来回切换使用, 降低黑客被抓到的风险?	45
Q11 对于未支持代理服务器的软件, 黑客如何让它们也可以使用代理服务器 来隐藏 IP 地址?	45
Q12 如何让一般上网软件或黑客工具(如 Telnet、各种 IP 或漏洞扫描器、木马程序等) 也可通过 HTTP 代理服务器来实现隐藏 IP 地址?	45
Q13 有些网络软件或黑客工具只能使用 Socks 代理服务器, 黑客如何让它们可以改用 HTTP 代理服务器?	45
Q14 黑客会使用哪些方式不让寄出的信件中包含 IP 地址?	65
Q15 黑客如何让信件中所包含的 IP 地址是无意义的, 这样就无法被追查到?	65

Part 3 目标查找与锁定之攻防

(Search and Lock Target)

Q16	为何黑客必须找出被黑者 IP 地址才可进行攻击或入侵？	69
Q17	黑客使用哪些方法来找出被黑者 IP 地址？	69
Q18	黑客如何找出使用动态 IP 电脑当前 IP 地址？	69
Q19	动态 IP 上网的电脑真的比较安全吗？	
	黑客如何精确找出使用动态 IP 电脑当前上网地址？	69
Q20	我使用动态 IP 上网，为何还是会经常被同一个黑客找到？如何防护？	69
Q21	黑客如何找出特定下手目标的 IP 地址？	72
Q22	黑客如何由网址 (Address)、FTP 地址、域名称 (Domain Name) 中 找出下手目标的 IP 地址？	72
Q23	黑客如何直接向被黑者询问出当前上网的 IP 地址？如何防护？	77
Q24	黑客如何从电子邮件中找出被黑者上网 IP 地址？如何防护？	77
Q25	黑客如何从网络聊天室中找出某人的 IP 地址？如何防护？	77
Q26	黑客如何由实时通讯软件 (如 MSN、Skype、雅虎通、ICQ、QQ 等) 找出某个好友的 IP 地址？如何防护？	86
Q27	黑客如何随意查找下手目标？	90
Q28	黑客如何从特定族群的 IP 地址来快速查找下手的对象？	90
Q29	通常使用各种 IP 扫描工具都会找许久而没有结果， 黑客会用什么快速有效的查找技巧？	90
Q30	如何有效防止被黑客随机选定为下手的目标？	90
Q31	黑客如何快速找到某个公司、单位或学校中连接到 Internet 的一般电脑， 而且使用 Windows 打开了端口 139？	100
Q32	为什么有些网站或个人机的 IP 地址黑客找不到？	104
Q33	被黑者使用固定 IP 上网，为何黑客就是找不到？	104
Q34	黑客为何找不到网吧中某台电脑的 IP 地址？	104
Q35	某人现在就在网上，为何黑客就是没法找到 IP 地址？	104
Q36	若黑客下手的目标是以仿真 IP 或通过局域网中的其他电脑连接到 Internet， 黑客会如何入侵或攻击？	104
Q37	一般上网电脑有什么方法可以避免被黑客扫描 IP 地址或入侵？	104
Q38	黑客如何知道所要下手的目标位于哪个国家或地区？并找出详细的街道图？	107

Q39	黑客如何查出某个网站、某个服务器、某个 IP 地址……是在哪个国家的哪个地区？	107
Q40	如何找出入侵或扫描我电脑的黑客是在哪个国家或地区（并找出详细街道图）？	113
Q41	如何从黑客寄给我的邮件中找出对方的 IP 地址？ 甚至找出寄件者是位于哪个国家或哪个地区？	113

Part 4 Windows 入侵攻防之无孔不入

(Hacking and Defense for Winodws Port 139)

Q42	哪些目标最适合黑客使用端口 139 入侵？	125
Q43	黑客利用端口 139 入侵的详细流程与步骤为何？会遇到哪些困难与麻烦？ 如何解决？	125
Q44	有些黑客可以找到许多打开端口 139 的电脑，但有些黑客却找不到， 这是什么原因？	125
Q45	若端口 139 入侵不成功，黑客还会使用哪些方法来入侵 Windows 电脑？	125
Q46	黑客有什么方法可以将没有共享的磁盘共享出来？	158
Q47	如何利用设置注册表项值就可以让被黑电脑的磁盘共享出来？	158
Q48	如何将需要输入密码的磁盘改为不必输入密码就可进入？	158
Q49	如何彻底防止黑客利用注册表项值来将电脑的磁盘设置共享？	158
Q50	黑客如何利用默认共享漏洞来入侵 Windows NT/2000 电脑？	167
Q51	每次启动进入 Windows 系统都会自动打开默认共享， 如何始终关闭它来防止黑客入侵？	167
Q52	被黑电脑已将默认共享彻底关闭，黑客会如何打开？	167
Q53	Windows NT/2000/XP 的用户名与密码保存在哪里？ 黑客如何破解它？	176
Q54	黑客有哪些方式或技巧比较快速、容易猜到磁盘共享密码？	176
Q55	黑客如何找出磁盘共享的电脑设置了哪些用户名？	176
Q56	如何有效防止黑客猜中磁盘共享密码？	176
Q57	黑客利用什么方法可有效破解 Windows 9x/ME 电脑的磁盘共享密码？	194
Q58	为何黑客利用共享密码漏洞来破解，成功率将近 100%？	194
Q59	如何修补 Windows 9x/ME 的磁盘共享密码漏洞？	194
Q60	若被黑电脑的磁盘只能只读（Read Only），黑客如何更改成可读写？	202
Q61	黑客如何在被黑的 Windows NT/2000/XP 电脑中创建最高权限账户？	202
Q62	如何防止共享磁盘被黑客更改成可读写？	202
Q63	黑客如何对 Internet 任何一台使用 Windows 的电脑发送信息吓对方？	210

Q64	黑客如何假冒他人名义发送信息给 Internet 上的任意 Windows 电脑?	210
Q65	如何让自己的电脑不再收到 Internet 上任意散发的垃圾信息?	210

Part 5 邮件、浏览器之入侵攻防

(Hacking and Antihacking for Web Browser and E-mail)

Q66	网页或邮件中可以包含或夹带什么东西来帮黑客进行工作?	219
Q67	黑客可以利用哪些方法让网页或邮件中包含或夹带的东西运行,来达到入侵或破坏的目的? 如何防护?	219
Q68	黑客如何利用网页或邮件包含的程序码来修改被黑电脑中的注册表项值 (Registry Value)? 可以实现哪些入侵或破坏的工作?	224
Q69	黑客如何使用网页或邮件来更改 IE 浏览器或 Internet 的各项设置?	224
Q70	黑客如何使用网页或邮件来让被黑电脑无法运行任何程序等破坏行为?	224
Q71	黑客如何诱骗被黑者运行网页或信件中包含的程序码?	224
Q72	有什么方法可以有效阻止黑客利用网页或邮件修改我电脑中的注册表项值?	224
Q73	黑客如何利用信件或网页包含的程序码来运行被黑电脑中的某个程序? 可以实现哪些入侵或破坏工作?	240
Q74	黑客如何利用信件或网页对被黑电脑的磁盘进行格式化 (Format)? 如何设计一个格式化网页?	240
Q75	黑客如何利用信件或网页打开被黑电脑中的各种系统服务 (或后门)?	240
Q76	如何有效阻挡恶意的信件或网页运行我电脑中的任何程序?	240
Q77	黑客如何想尽办法让被黑者浏览网页就可以趁机植入木马、运行被黑电脑中的程序、批处理文件或更改注册表项值?	245
Q78	黑客如何处心积虑地利用邮件或浏览器来进行入侵或破坏工作?	245
Q79	浏览器为何成为网络安全的罪魁祸首? 黑客如何利用它?	245
Q80	黑客如何利用人性的弱点或好奇心来更顺利地利用漏洞入侵被黑电脑?	245
Q81	什么是图片查看器处理漏洞 (MS06-001)? 黑客如何利用它? 如何修补?	245
Q82	如何有效防止打开某个网页就自动运行隐藏在其中的恶意源码 (如: 木马、病毒程序、DOS 命令、更改注册表项值等)?	245
Q83	窗口炸弹会对 Windows 系统有哪些破坏与影响?	257
Q84	黑客为何将窗口炸弹放在附件中,而不直接放在 HTML 信件中? 有何优点?	257
Q85	如何避免受到窗口炸弹的攻击?	257
Q86	我受到窗口炸弹攻击,一打开信件程序就会不断地冒出许多窗口,无法收信与寄信,如何解决?	257

Part 6 各类密码骗取与入侵后之攻防

(Hacking & Antihacking for Accounts, Files and Datas)

Q87	黑客会使用哪些方法骗取各类账户与密码? 如何防护?	265
Q88	黑客会使用哪些方法破解或获取各种电子邮件账户(含 Web-Mail)的用户名与密码?	269
Q89	黑客如何随意查找收信服务器, 然后破解出某些被黑者的账户后偷看信件?	269
Q90	如何有效防止电子邮件账户的密码被黑客获取?	269
Q91	黑客如何截取被黑者还未读取的电子邮件而不被发现? 如何防护?	287
Q92	如何防止自己还未读取的信件被黑客偷看?	287
Q93	黑客如何破解从网页登录的电子邮件账户?	295
Q94	黑客如何破解从网页登录的各种用户名与密码 (例如: 情色会员网站、聊天网站、交友网站、购物网站、XX 会员网站等)?	295
Q95	黑客通常将网页密码分为哪几类? 如何决定与分析要下手的网页? 什么样的网页密码黑客会毫不考虑地放弃破解?	295
Q96	如何彻底有效地防止黑客利用暴力破解法来猜出各种用户名与密码?	295
Q97	黑客进入被黑电脑中通常会进行哪些工作?	324
Q98	哪些文件、资料是黑客最可能的下手目标?	324
Q99	若不幸被黑客入侵, 如何有效防止重要文件被黑客偷取, 或让黑客无法打开?	324
Q100	黑客如何获取与查看他人电脑中电子邮件文件中的信件?	334
Q101	如何查看 Outlook Express, Netscape Meeesger, Eudora, FoxMail 等 各种邮件程序(含不同版本)的信件文件?	334
Q102	如何尽可能防止黑客获取你在电脑中保存的电子邮件?	334
Q103	黑客如何查看、修改与删除他人电脑的注册表(Registry)?	341
Q104	系统注册表(Registry)中哪些项值最可能会被黑客更改而要经常查看?	341
Q105	如何防止黑客查看、更改或删除我的注册表(Registry)?	341
Q106	Cookies 文件中可能包含哪些信息?	352
Q107	黑客如何分析获取 Cookies 文件中进入某些网站或 Web-Mail 的用户名与密码?	352
Q108	如何有效防止黑客获取我的 Cookies 文件?	352
Q109	黑客如何破解 ZIP, RAR, ACE, ARJ 等压缩文件的密码? 如何防护?	357
Q110	黑客如何破解各版本 MS-Word, Excel, PowerPoint, Access 等文件的密码? 如何防护?	357

Q111	黑客如何破解 PDF 文件的密码? 如何防护?	357
Q112	黑客如何偷取各类实时信息软件 (IM, 如 MSN、雅虎通、ICQ、QQ) 的 账户、交谈日志、好友名单? 如何防护?	360

Part 7 服务器入侵攻防战

(Hacking & Antihacking for Internet Server)

Q113	黑客为何要入侵或攻击各种网络服务器? 有啥价值?	379
Q114	黑客通常会使用哪些方式入侵服务器? 实作流程为何?	379
Q115	黑客如何在茫茫网海中快速查找提供了 Telnet 服务的电脑?	387
Q116	黑客如何破解 Telnet 登录账户与密码, 然后进行入侵? 如何防护?	387
Q117	黑客如何让一般上网的 Windows 电脑提供 Telnet 服务后进行入侵?	400
Q118	如何查看我的电脑是否提供了 Telnet 服务?	400
Q119	不论是否打开了 Telnet 服务, 如何防止黑客利用 Telnet 服务入侵我的电脑?	400
Q120	黑客为何要入侵提供了 FTP 服务的电脑? 有啥价值?	409
Q121	黑客如何在茫茫网海中快速查找提供了 FTP 服务的电脑来入侵?	409
Q122	黑客如何破解登录 FTP 的账户与密码, 然后进行入侵或更改他人网页? 如何防护?	409
Q123	黑客如何在茫茫网海中快速查找提供了终端机服务的 Windows 电脑?	418
Q124	黑客如何破解登录终端机服务电脑的账户与密码, 然后进行入侵或破坏?	418
Q125	黑客如何打开一般上网电脑的终端机服务后门, 然后进行远程遥控、为所欲为?	418
Q126	如何更改默认的终端机端口 3389 来彻底有效防止黑客入侵?	418
Q127	黑客如何快速查找出目标服务器有哪些漏洞 (包含最新的漏洞), 然后针对这些漏洞来进行入侵或攻击?	427
Q128	服务器漏洞的扫描工具有哪几种? 黑客要如何决定使用哪一种?	427
Q129	黑客如何判断与决定要使用哪个漏洞来进行入侵或攻击?	427
Q130	黑客如何快速查找某个特定漏洞的扫描工具?	427
Q131	若特定漏洞的扫描工具很慢, 黑客会利用什么技巧在茫茫网海中快速地查找到 任意下手的目标?	427
Q132	如何尽快修补 Windows 系统或 Web 系统 (例如: IIS、Apache 等) 的各种漏洞, 让黑客无法利用?	427
Q133	什么是 UPnP 远程溢出入侵漏洞 (MS05-039)? 黑客如何利用它迅速入侵网络服务器或一般电脑而且具有最高权限?	448
Q134	如何修补 UPnP 远程溢出入侵漏洞, 不让黑客利用它来入侵?	448

Q135	一个典型的远程溢出入侵漏洞实作是如何进行的? 有哪些原因造成有漏洞的电脑无法成功入侵?	448
Q136	黑客为何要让某个服务器无法提供网络服务? 有啥价值所在?	456
Q137	什么是拒绝服务攻击 (DoS) 与分布式拒绝服务攻击 (DDoS)? 两者有何不同? 它们的基本原理是什么? 黑客如何实现?	456
Q138	初级黑客如何快速、简单又有效地对目标服务器进行瘫痪攻击?	456
Q139	如何对拒绝服务攻击 (DoS) 与分布式拒绝服务攻击 (DDoS) 进行有效防护?	456
Q140	黑客如何判断与决定是否要清除进行入侵或破坏时留在服务器中的各种日志?	467
Q141	黑客入侵或破坏所可能在服务器中留下的各种日志要如何清理?	467
Q142	如何从各种日志中查看与找出可能的黑客入侵?	467
Q143	有哪些方法可以有效防止各种日志文件被黑客更改或删除?	467

附 录

附录 1	全球各地 IP 地址详细列表	474
附录 2	端口列表	475
附录 3	CurrPorts	476
附录 4	NetStumbler	477
附录 5	ProxyHunter	478
附录 6	MultiProxy	479
附录 7	Socks2HTTP	480
附录 8	SocksCap	481
附录 9	NetInfo	482
附录 10	Angry IP Scanner	483
附录 11	Mail Direct	484
附录 12	NeoTrace Pro	488
附录 13	VisualRoute	489
附录 14	eMailTrackerPro	490
附录 15	Startup	491
附录 16	NetBrute Scanner	492
附录 17	PQwak	493
附录 18	File Encryption Shell Extension	494
附录 19	Brutus-AET2	495
附录 20	Mailbag Assistant	496
附录 21	SuperScan	497

附录 22	X-Scan	498
附录 23	各种软件密码破解工具	499
附录 24	Advanced Instant Messengers Password Recovery	500
附录 25	Magic Mail Monitor	501
附录 26	EmEditor	503
附录 27	wwwhack	505
附录 28	流光 (Fluxay)	506
附录 29	N-Stealth	509
附录 30	Shadow Security Scanner	510
附录 31	SyGate Personal Firewall	511
附录 32	TaskInfo	512
附录 33	Net 命令说明	515
附录 34	at 命令说明	523

PART 1

黑客入侵基本原理与观念

Basic Concept for Hacker Intrusion



黑客任务大作战

黑客任务实战系列是详解黑客攻防的罕见的书籍，因此得到不少读者的支持与鼓励，当然我们也收到许许多多读者反映的各种问题与意见，其中发现仍然有许多读者(特别是初学者)对于黑客入侵的观念相当不正确，甚至完全没有概念，经常提出一些让小弟哭笑不得的问题，所以在本章中将详细地帮你了解正确的黑客入侵观念、Internet 世界的架构与入侵的原理与方式。同样，从防护的角度上讲，也必须彻底了解这些观念与内容，如此才可对症下药，有效阻挡黑客的入侵与攻击。

Tips

本章中所有内容也都适用于其他系统(如：Mac OS、Linux、UNIX等)的黑客入侵与攻击。

Note

如果你对这些内容已经很熟悉，就不需要再看本章的说明与讨论了。

创建正确的观念

某个电脑已打开端口 139，为什么无法进入？

某个服务器已打开端口 80，黑客要如何入侵？

黑客使用什么方法一定可以入侵某台电脑中？

有什么工具或方法一定可以让黑客进入某台电脑或破解某个密码？

为什么无法破解进入某台电脑或网站的密码？

木马已经成功植入被黑电脑中，为何一直连接不到？

...and More

相信只要有些基本网络概念的读者一定都会认为这些问题有些不可思议，如果只是打开某些端口就可轻易进入，那谁还敢上 Internet 啊？相信黑客自己也不敢。怎么可能有一定可以入侵电脑或破解密码的方法呢？如果真能如此，那 Windows 还能用吗？Bill 老大还混得下去吗？

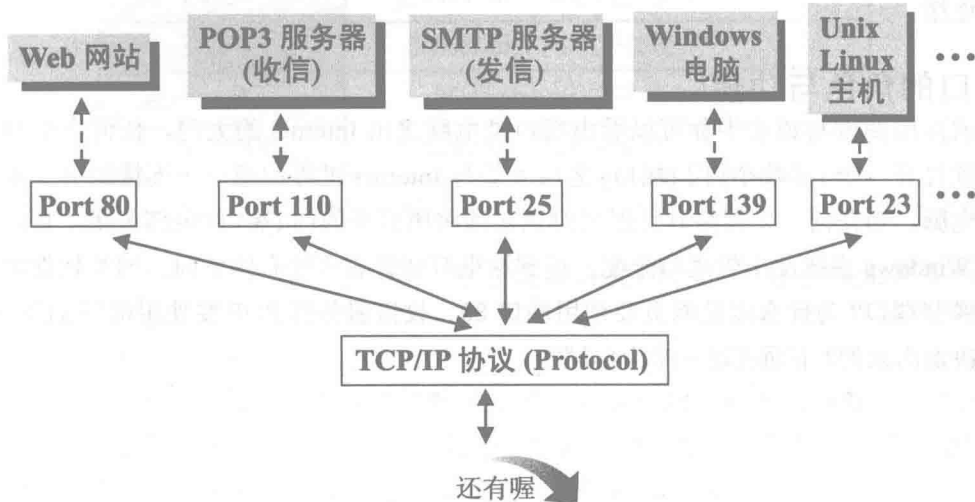


答案当然是否定的，小弟必须强调许多黑客的入侵或攻击虽然没有想象中的困难，但也没有那么容易就可以轻易完成，更没有一定可以入侵某个网站、电脑或破解密码……这种 100% 成功的做法或工具，如果真有的话，那 Internet 世界早就不存在了。这是个非常简单的逻辑，将脑筋转一下就想得出来，所以请各位读者帮帮忙，以后不要再问我们这种逻辑上根本就无法成立的问题了。

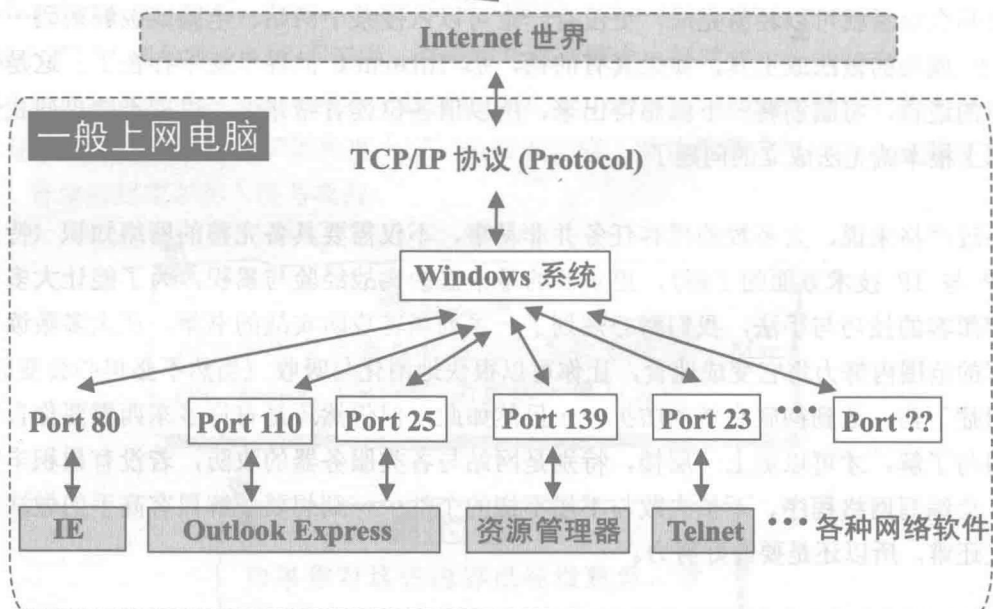
不过严格来说，大多数的黑客任务并非易事，不仅需要具备完整的网络知识（特别是 TCP/IP 与 IP 技术方面的了解），更重要的是丰富的实战经验与累积，为了能让大多数的人了解黑客的技巧与手法，我们精心规划了一系列黑客攻防实战的书籍，在大多数读者可以了解的范围内努力将它变成速食，让你可以很快地消化与吸收（当然不必担心会变胖），然后对症下药，达到彻底有效的防护……虽然如此，但仍然还是有许多东西需要你自己努力学习与了解，才可以更上一层楼，特别是网站与各类服务器的攻防，若没有累积丰富的经验、会编写网络程序、不怕失败与不屈不挠的个性……则想要了解黑客高手的做法肯定比登天还难，所以还是要好好努力。

Internet 世界的基本原理

不论是从黑客或防黑的角度，都必须先了解我们电脑中的程序、Windows 系统如何与 Internet 世界中的各种服务器、网站主机、一般电脑……创建网络连接的关系，也就是 Internet 世界的基本原理架构啦！如下图。



续前页



从上面的图中你可以清楚地看出在你电脑中的各种网络软件都是经由某一个端口再通过 Windows 系统的 TCP/IP 模块连接到 Internet 世界中，而同样的远程的服务器、网站主机或一般电脑也是以相同的方式来接收你电脑的信息 (或发送信息给你的电脑)，以此方式达成网络连接。

端口的角色与功能

由前面的图解与说明中你可以看出端口是电脑进出 Internet 的大门，任何一个网络软件都必须打开一个 (或数个) 门 (端口) 之后才能与 Internet 世界沟通……连接到另一端的服务器或电脑，当任何一个网络软件退出时也必须将所打开的门 (端口) 全部关闭才行，如此才能让 Windows 系统便于管理与分配。说到这里有些读者可能有些疑问：网络软件如何决定打开哪些端口？为什么浏览网页要使用端口 80、收信服务器 POP 要使用端口 110……这是如何决定出来的？下面就逐一为你解答。