The Bible of Hacking and Anti Hacking

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
- 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）

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 3 目标查找与锁定之攻防
（Search and Lock Target）

Part 6 各类密码骗取与入侵后之攻防

（Hacking & Antihacking for Accounts，Files and Datas）

附 录

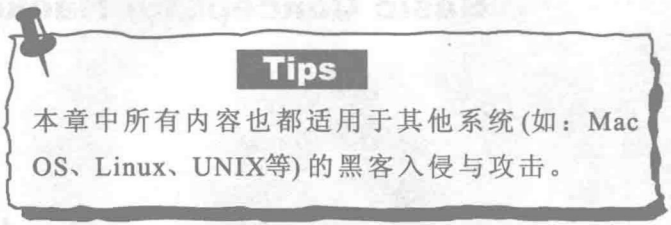
PART 1

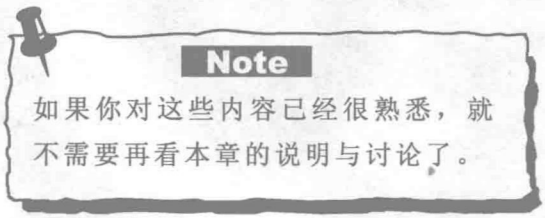
黑客入侵基本原理与观念

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。





✍ 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

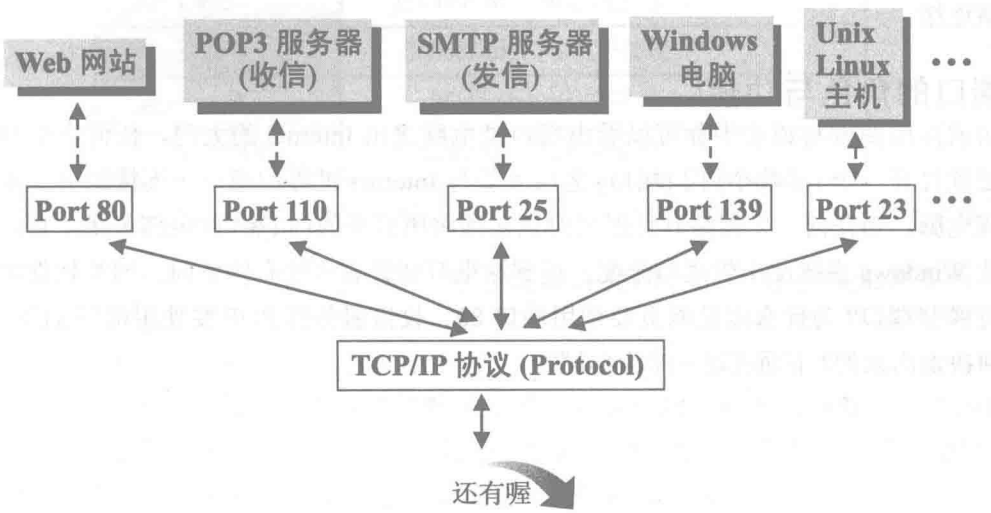
相信只要有些基本网络概念的读者一定都会认为这些问题有些不可思议，如果只是打开某些端口就可轻易进入，那谁还敢上 Internet 啊? 相信黑客自己也不敢。怎么可能有一定可以入侵电脑或破解密码的方法呢? 如果真能如此，那 Windows 还能用吗? Bill 老大还混得下去吗?

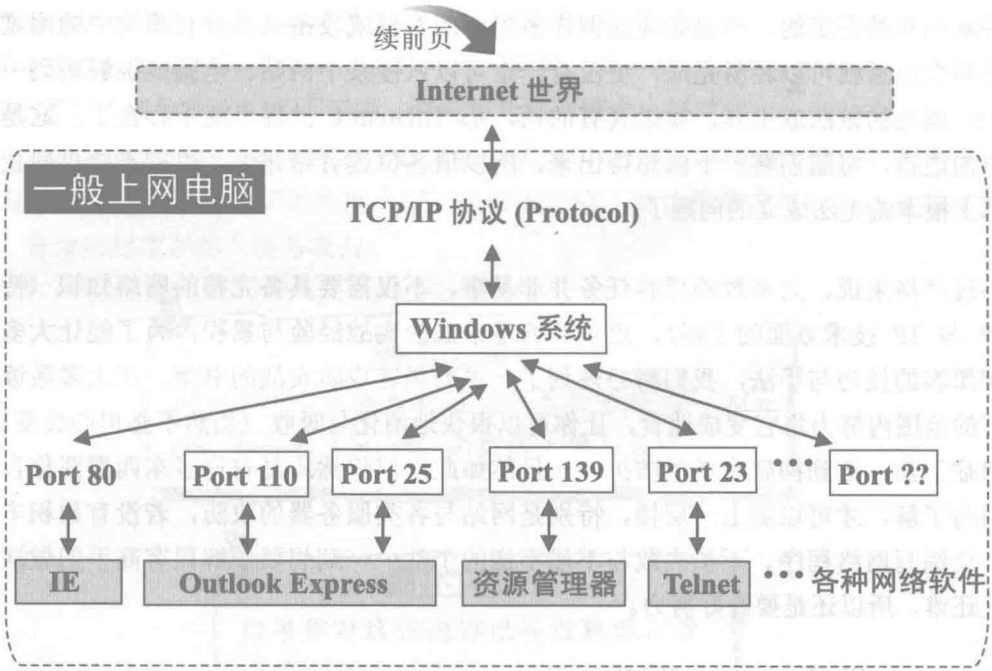
答案当然是**否定的**，小弟必须强调许多黑客的入侵或攻击虽然没有想象中的困难，但也没有那么容易就可以轻易完成，更没有一定可以入侵某个网站、电脑或破解密码……这种 100% 成功的做法或工具，如果真有的话，那 Internet 世界早就不存在了。这是个非常简单的逻辑，将脑筋转一下就想得出来，所以请各位读者帮帮忙，以后不要再问我们这种逻辑上根本就无法成立的问题了。

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。





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? 下面就逐一来为你解答。