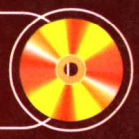
“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

Hacker Mission and Protection for Windows on Internet

本书详细讨论在 Internet 上 Windows 计算机的各种黑客入侵手法与有效防护



北京希望电子出版社 总策划
程秉辉 John Hawke 编 著

黑客任务实战

Windows全攻略

* 最详尽的 Windows 入侵完整流程与攻防操作
* 磁盘共享密码破解全攻略
* 远程查看、编辑他人电脑中的注册表（Registry）
* 如何在他人计算机创建 Telnet 后门
* 电子信箱、Web-Mail、FTP 密码破解全攻略
* 获取与查看他人在各种邮件程序中的信件
* 截取他人一般信箱与 Web-Mail 的信件
* 直接发信到对方信箱，不必使用发信服务器
* MS-Word、Excel、Access…各版本密码破解全攻略
* ZIP、RAR、ACE、ARJ 压缩文件密码破解全攻略
* ICQ 与 OICQ 密码、好友名单、聊天记录…攻防操作
* 邮件、ICQ、OICQ 找出他人 IP 地址详细操作
* 附全球 IP 详细列表、端口列表说明

本书中所有操作都经过多次的严格测试，绝不告诉你无法做到的方法！

电脑——以用为本！
计算机应用文摘

“很强的可操作性，结构上标新立异，相当的人性化。”

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

“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

Hackers Mission and Protection for Windows on Internet

本书详细讨论在 Internet 上 Windows 计算机的各种黑客入侵手

北京希望电子出版社 总策划
程秉辉 John Hawke 编 著

黑客任务实战

Windows全攻略

* 最详尽的 Windows 入侵完整流程与攻略
* 磁盘共享密码破解全攻略
* 远程查看、编辑他人电脑中的注册表
* 如何在他人计算机创建 Telnet 后门
* 电子信箱、Web-Mail、FTP 密码
* 获取与查看他人在各种邮件程序中的
* 截取他人一般信箱与 Web-Mail 的
* 直接发信到对方信箱，不必使用发信
* MS-Word、Excel、Access…各版 密码
* ZIP、RAR、ACE、ARJ 压缩文件密码
* ICQ 与 OICQ 密码、好友名单、聊天
* 邮件、ICQ、OICQ 找出他人 IP 地址
* 附全球 IP 详细列表、端口列表说明

本书中所有操作都经过多次的严格测试，绝不告诉你无法做到的方法！

电脑一以用为本！

计算机应用文摘

“很强的可操作性，结构上标新立异，相当的人性化。”

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

内 容 简 介

黑客任务实战系列推出两年以来广受读者的支持与爱护，由于各种黑客技巧也是随着时间而不断更新，因此本书对 Windows 的入侵攻略与防护进行彻底的整理与翻修，加入了最新、最酷的黑客技巧与攻防，并提供更新、更方便的各种黑客工具，希望能帮助你充分了解黑客的各种手法与行为。同时，针对这些黑客手法也提出有效的防护方式，让你的电脑不再成为黑客下手的目标。

本书中告诉你最完整详尽的 Windows 入侵流程与操作，还包含操作时可能遇到的各种状况与注意事项，让你不必具备丰富的网络知识与经验就可以轻而易举的实现各项黑客任务。黑客入侵他人电脑后会对那些文件或数据有兴趣？如何查看各种邮件程序的信件内容？破解各版本 MS-Office 文件、各种压缩文件（ZIP、RAR、ACE、ARJ）的密码？找出 ICQ、OICQ 密码、好友名单、聊天记录？破解电子信箱、Web-Mail 密码？获取 FTP 帐户与密码后更改他人网页？在他人电脑中打开 Telnet 后门？在本书中都有详细的黑客操作与防护说明。

本书适合于所有上网用户增强网络安全意识，同时对网络管理员和致力于网络安全的开发人员有很大参考价值。

本书 CD 包含全球各地 IP 地址详细列表、端口列表以及 NetInfo、NetScan Pro、NetBrute Scanner 等各种必备网络工具。

盘书系列名：“十五”国家重点电子出版物规划项目　计算机网络技术与网络教室系列
盘　书　名：黑客任务实战——Windows全攻略
总　策　划：北京希望电子出版社
文本著作者：程秉辉 John Hawke
CD 制作者：希望多媒体开发中心
CD 测试者：希望多媒体测试部
责任编辑：大成
出版、发行者：北京希望电子出版社
地　　址：北京市海淀区知春路甲 63 号卫星大厦三层 100080
网　　址　www.bhp.com.cn　E-mail: lwm@bhp.com.cn
电话:010-62520290, 62521724, 62528991, 62630301, 62524940, 62521921,（发行）
82675588-318,62532258,62522329（门市）010-82675588-501,82675588-201
（编辑部）
经　　销：各地新华书店、软件连锁店

排　　版：希望图书输出中心
CD 生产者：北京中新联光盘有限责任公司
文本印刷者：北京双青印刷厂
开本 / 规格：787 毫米×1092 毫米　16 开本　32.125　印张 586 千字
版次 / 印次：2003 年 6 月第 1 版　2003 年 6 月第 1 次印刷
印　　数：0001-5000 册
本 版 号：ISBN 7-900088-03-2
定　　价：45.00 元（本版 CD）

作者感言

黑客任务实战－攻略篇推出近两年以来，受到许多读者的支持与爱护，也给了我们相当多的批评与指教，而各种黑客技巧也是随着时间而不断的日新月异，因此我们就对原来攻略篇中的内容进行彻底的整理与翻修，删除较旧、不合时宜的内容，加入了最新、最酷的黑客技巧与攻防，并提供您更新、更方便的各种黑客工具，希望能帮助您充分了解黑客的各种手法与行为，同样的，我们也针对各种黑客手法提出有效的防护方式，让您的电脑不再成为黑客下手的目标。

本书的内容虽然丰富，但仍然不可能包含许多旁枝末节或其他主题的各种相关黑客技术与技巧，因此如果您已经有**黑客任务实战－个人机漏洞篇**、**服务器攻防篇**、**木马全攻略**(尚未出版)，来交互参考与搭配运用，必定可以让您学习黑客攻防如虎添翼、事半功倍，这是提供您参考并非绝对必要。

由于现在每天要处理的信件很多，所以目前我们只回复与书中内容或所介绍的软件有关的信件，其他不相关的信件将不处理，请您能理解与见谅，毕竟小弟不是 Bill 老大，可以依照不同的问题收取不同的费用来捞钱。另外我们并不会帮任何人或组织去破解或入侵某个网站、某台计算机或各种密码，也无法查看您的文件是否有毒、帮您测试软件、帮您找软件…等，我们很愿意帮各位解决问题，但实在无法处理这些超出范围的要求，非常谢谢您的合作!

请注意：

- 若您使用电子邮件则填写本书光盘中的读者服务卡。
- 下一页读者资料卡中的电子邮件地址请写清楚，不要太草!

请电邮到: **hawkes@ms29.hinet.net**

请注意：本书内容完全以学术与技术操作的角度来针对有关黑客攻略与防护进行讨论与研究，所以若有将本书内容使用于任何违反法律之行为，必须自行承担各种相关的法律责任，请各位读者慎之!慎之!

程秉辉
Hawke Cheng
8.27.2003

目 录

Part 5 电子邮件攻防战（Hacker Mission for E-Mail）

Part 6 ICQ 与 OICQ 攻防战（Hacker Mission for ICQ and OICQ）

PART 1

Windows入侵基本原理与观念

Basic Conecpt for Windows Intrusion

黑客任务实战系列受到许多读者的支持与爱护，我们也收到许许多多读者反应的各种问题与意见，其中发现仍然有许多的读者在对于黑客入侵的观念相当不正确，甚至完全没有概念，甚至提出一些让小弟哭笑不得的问题，所以在本章中将详细的帮你创建正确的黑客观念、Internet 世界的架构与 Windows 入侵的基本原理，而站在防护的角度也必须彻底了解这些观念与内容，如此才可对症下药，阻挡黑客的入侵与攻击。

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。

建立正确的观念

对方电脑有打开端口 139，为什么我无法进入?
对方电脑已打开端口 80，我要如何入侵?
有什么方法一定可以入侵某台电脑?
有什么工具或方法一定可以让我进入某台电脑或破解某个密码?
为什么我无法破解进入某台电脑或网站的密码?

…and More

相信只要有些基础概念的读者一定都会觉得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，那谁还敢上网进入 Internet 中? 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 老大还混的下去吗?

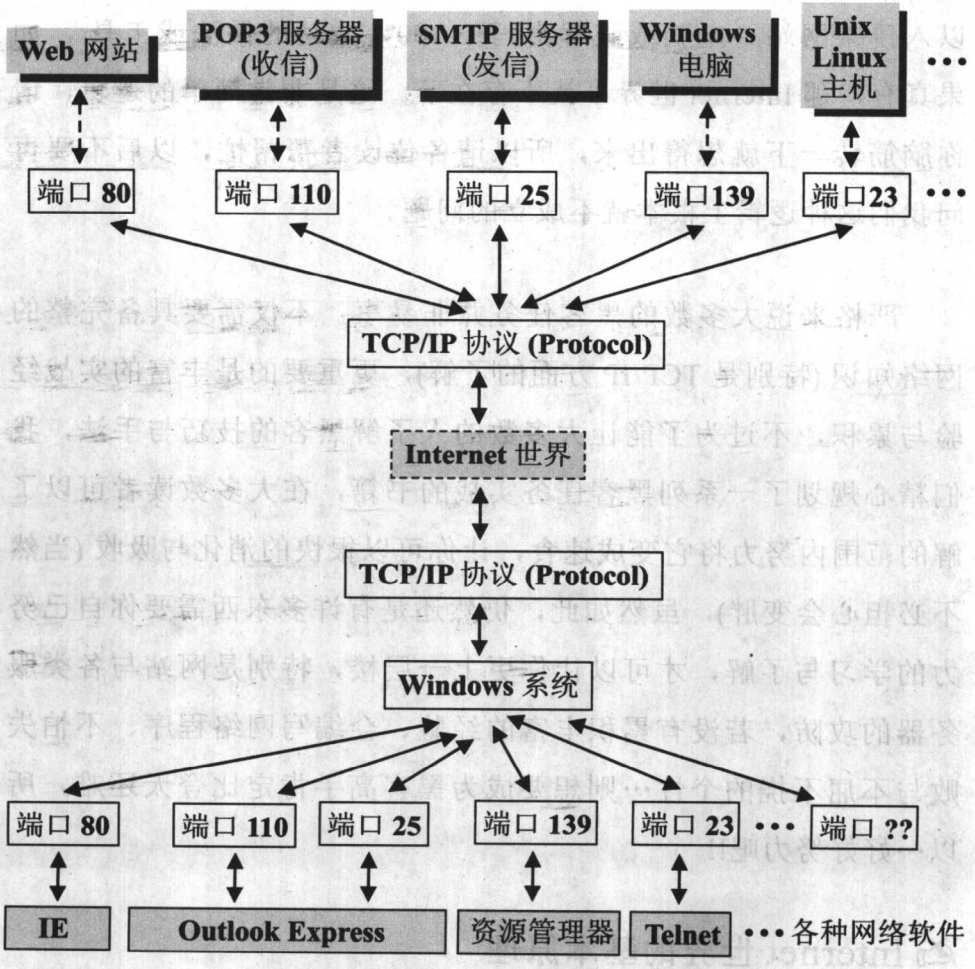
答案当然是**否定**的，小弟必须强调许多黑客任务虽然没有想像中的困难，但也没有那么容易就可以轻易完成，更没有一定可以入侵某网站、电脑或破解密码… 100% 成功的做法或工具，如果真有，那 Internet 世界早就不存在了。这是非常简单的逻辑，请你脑筋转一下就想得出来，所以请各位读者帮帮忙，以后不要再问我们这种逻辑上根本就不成立的问题。

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 方面的了解)，更重要的是丰富的实战经验与累积，不过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任务实战的书籍，在大多数读者可以了解的范围内努力将它变成速食，让你可以很快的消化与吸收 (当然不必担心会变胖)，虽然如此，仍然还是有许多东西需要你自己努力的学习与了解，才可以让你更上一层楼，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…则想要成为黑客高手肯定比登天还难，所以…好好努力吧!!

✍ Internet 世界的基本原理

不论是想做黑客或是防止被黑，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…建立网络连接的关系，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的看出在你电脑中的各种网络软件都是经由某个端口再通过 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你电脑进出 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，当任何一个网络软件退出时也必须将所打开的端口全部关闭才行，说到这里许多读者肯定有些疑问：网络软件如何决定打开那些端口号码呢? 为什么浏览网页要使用端口 80，如何决定出来的? …下面就逐一来为你解答。

如何决定端口号码?

一般来说每个网络软件都可以打开任何一个端口号码来使用 (只要该号码没有其他软件在使用)，不过为了在网络连接时的畅通与避免复杂，有些网络软件 (或硬件) 就会固定使用某一个 (或数个) 端口，而大家也就依循这些不成文的规定来进行，例如：浏览器与远程的网站主机一定是通过端口 80 来进行连接 (一般网页)，但是如果某个网络软件已经先打开端口 80 来使用，此时打开浏览器就无法浏览任何网站 (因为不可用端口 80)，这样懂了吧?!

所以依照目前大多数网络软件所使用的端口号码，下面列出常用的几个端口供你参考。

端口	说　　明
端口 21	FTP 文件下载上传服务
端口 23	Telnet 主机连接服务
端口 25	SMTP 发信服务
端口 80	HTTP 网页服务
端口 110	POP3 收信服务
端口 119	NNTP 新闻讨论服务
端口 139	NetBIOS 网上邻居、资源管理器连接服务
端口 443	HTTPS SSL 加密网页服务
端口 1243, 27374	Subseven 木马程序使用
端口 5631	PCAnywhere 使用
端口 12345	Netbus 木马程序使用

若要查看更多端口已经默认给那些软硬件使用，可查看本书光盘根目录下的 **PortList.txt**，不过请注意下面三点。

- 虽然看来好像大多数的端口号码都已经默认给某个功能使用，但对大多数一般上网的电脑而言其实用到的很少，也就是说除了上表中那些较常使用的网络功能之外 (木马程序不算)，大多数的端口号码根本就没有使用到。

- 有些网络软件会因为某些功能或连接上的需要打开某些端口号码，当你不再使用该功能或不需要时就会自动关闭该端口，例如：IE 浏览器在连接到某些网站时可能会再打开 1~2 个端口，当你不再浏览该网站后就自动关闭。

- 对于黑客而言，若要与植入的木马程序连接，则所使用的端口当然是避开被黑者最常 (或最可能) 使用的端口号码，应该不会笨到使用端口 80 吧?! 只要被黑者无法浏览网站就可能发现有其他程序正在使用端口 80，这不是打草惊蛇吗? 不过在大多数情况下只要不去使用上表中的那些端口号码，则其他号码随便用应该都不会有问题 (当然还是有可能出现意外)。

你的电脑目前打开那些端口?

查看目前是否有黑客入侵你电脑的最好方法就是查看目前你的电脑打开那些端口，而这些端口又与那个网站或电脑连接，这里我们告诉你两种方法来查看。

方法❶ 使用 netstat

这是各版本 Windows 都有提供的基本功能之一，它是显示目前有那些 IP 地址正通过那个端口与你的电脑连接中，以此方式来查看是否有黑客或不明程序正在进行见不得光的勾当，操作方式如下。