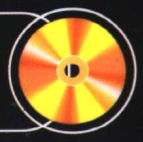
“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

本书提出的 **58** 个问题,完整详实的教授你各式各样的黑客任务秘技
本书CD包含:Port列表,各地IP地址详细列表,ProxyHunter代理杀手,Socks2HTTP,SkSockServer,ASPack,Taskinfo.....等黑客必备软件



北京希望电子出版社 总策划
程秉辉 John Hawke 合 著

黑客任务实战

个人机漏洞篇

- 各种 IP 隐藏法实作大全(快速 Proxy 切换、制作跳板主机)
- 全球最完整、最详尽的 IP 隐藏技术实作
- 如何制作自己的跳板主机?通过多个跳板主机来转向上网
- 如何让各种上网软件通过代理服务器或跳板主机来隐藏 IP
- 黑客远端遥控的最爱..... 远端执行程序大漏洞!如何修补
- 利用流光找出 WinNT 与 Win2K 预设共用漏洞与共享密码破解
- 利用输入法漏洞进行 100% 远端遥控
- IE,OE 的 MIME 自动执行漏洞轻易植入各类程序或取得最高权限,一定要修补
- 关闭 ActiveX 安全警告,利用 VBScript 更改他人电脑密码、执行程序
- 各种漏洞与其他黑客任务的搭配使用、漏洞完全修补
- 附全球 IP 地址详细列表、Port 列表说明、Net 指令完整用法.....

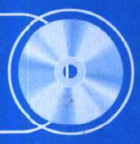
本书中所有内容都经过多次的严格测试,绝不告诉你无法做到的方法

Win9x.WinMe 完全适用 Win2k.WinXP

中国科学出版集团
北京希望电子出版社

“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

本书提出的 **58** 个问题,完整详实的教授你各式各样的黑客任务秘技
本书CD包含:Port列表,各地IP地址详细列表,ProxyHunter代理杀手,Socks2HTTP,SkSockServer,ASPack,Taskinfo.....等黑客必备软件



北京希望电子出版社 总策划
程秉辉 John Hawke 合 著

黑客任务实战

个人机漏洞篇

- 各种 IP 隐藏法实作大全(快速 Proxy 切换、制作跳板主机)
- 全球最完整、最详尽的 IP 隐藏技术实作
- 如何制作自己的跳板主机?通过多个跳板主机来转向上网
- 如何让各种上网软件通过代理服务器或跳板主机来隐藏 IP
- 黑客远端遥控的最爱..... 远端执行程序大漏洞!如何修补
- 利用流光找出 WinNT 与 Win2K 预设共用漏洞与共享密码破解
- 利用输入法漏洞进行 100% 远端遥控
- IE,OE 的 MIME 自动执行漏洞轻易植入各类程序或取得最高权限,一定要修补
- 关闭 ActiveX 安全警告,利用 VBScript 更改他人电脑密码、执行程序
- 各种漏洞与其他黑客任务的搭配使用、漏洞完全修补
- 附全球 IP 地址详细列表、Port 列表说明、Net 指令完整用法.....

本书中所有内容都经过多次的严格测试,绝不告诉你无法做到的方法

中国科学出版集团
北京希望电子出版社

内 容 简 介

本书是继<<黑客任务实战>>(攻略篇) 、<<黑客任务实战>> (防护篇)后的又一部大型力作,重点介绍和分析 PC 机上所使用的 Windows 系统与 IE、Outlook Express 软件漏洞的产生原因、表现形式和修补方法和技巧。

本书的作者以完整的实战经验加上十多年的系统功力，从初级电脑使用者的角度来讲解**黑客入侵的基本原理与观念,IP 的隐藏与研究，一般电脑的漏洞入侵攻击与修补技术**。这使得读者不必要学会写程序、也不需要了解专业的网络知识,即可轻易的按照书中的说明与操作来进行黑客攻击与防护。

本书内容丰富、实用,图文并茂,书中 58 个 PC 机上常见漏洞的来龙去脉用图文并茂的方式作了详尽的描述, 修补方法均进行了严格测试, 内容全方位, 应用白分百。

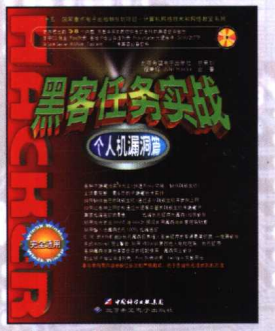
本书面向所有 PC 机用户,对从事计算机安全与防护的开发人员也不失为一本活的指导书。

本书 CD 包含 Port 列表，各地 IP 地址详细列表，ProxyHunter 代理杀手，Socks2HTTP，SkSockServer，ASPack，NetBrute Scanner，Angry IP Scanner，Taskinfo，PQwak，IPHacker，StartupCPL,GetRight 中文版。

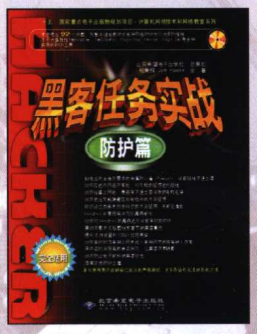
盘书系列名：“十五”国家重点电子出版物规划项目• 计算机网络技术和网络教室系列
盘　书　名：黑客任务实战——个人机漏洞篇
总　策　划：北京希望电子出版社
文本著作者：程秉辉 John Hawke 编写
CD 制作者：程秉辉 John Hawke
CD 测试者：希望多媒体测试部
责任编辑：周艳 杨如林
出版、发行者：北京希望电子出版社
地　　址：北京市海淀区知春路 63 号卫星大厦三层 100080
网址: www.bhp.com.cn E-mail: lwm@hope.com.cn
010-62520290,62521724,62528991,62630301,62524940,62521921,82610344(发行)
010-82675588-202（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 杜海燕
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 28 印张 486 千字
版次 / 印次：2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷
印　　数：0001-5000 册
本　版　号：ISBN 7-900118-51-9
定　　价：45.00 元（本版 CD）

Hotbook好书推荐

你攻我防、道高一尺、魔高一丈、快乐网络人生



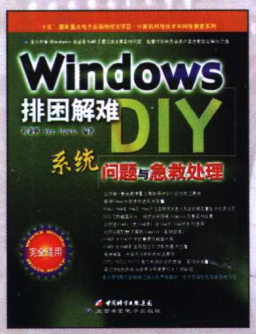
CX-3848
定价：55.00元
ISBN:7900101470



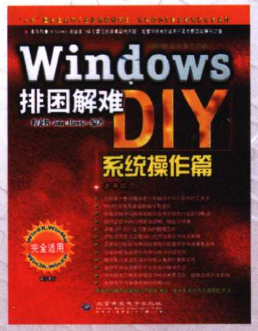
CX-3616
定价：46.00元
ISBN:7900088253

CX-3617
定价：48.00元
ISBN:7900088245

CX-83662
定价:35.00元
ISBN:7900088474



CX-3700
定价:48.00元
ISBN:7900088776



CX-3829
定价：50.00元
ISBN:7900101365

CX-83598
定价：30.00元
ISBN:7900088040

CX-83388
定价:23.00元
ISBN:7900071326

CX-83371
定价：50.00元
ISBN:7900071288

CX-83586
定价:33.00元
ISBN:7900088008

CX-83544
定价:39.00元
ISBN:7980007557

CX-83545
定价:35.00元
ISBN:7980007581

CX-3765
定价：58.00元
ISBN:7900101071

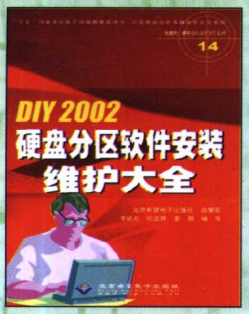
CX-3838
定价：58.00元
ISBN:7900101101

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

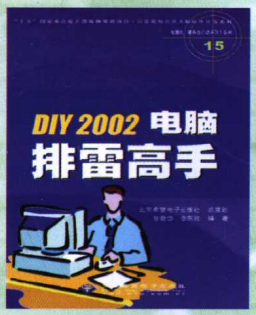
社　　址：北京海淀知春路甲63号卫星大厦三层
通信地址：北京中关村083信箱(100080)
电　　话：(010) 82675588(总机)
传　　真：(010) 62520573

Hotbook好书推荐

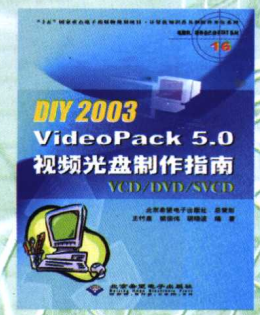
你想自己动手玩转电脑请用热门教程



CX-3849
定价：42.00 元
ISBN:7900101497



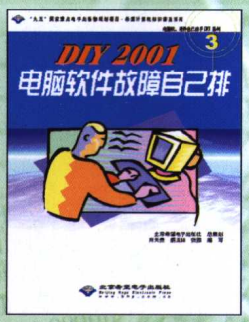
CX-3851
定价：25.00 元
ISBN:7900101829



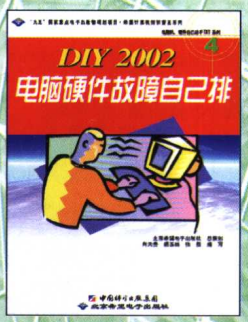
CX-3898
定价：30.00 元
ISBN:7900118314

CX-83328
定价:38.00 元
ISBN:7900056440

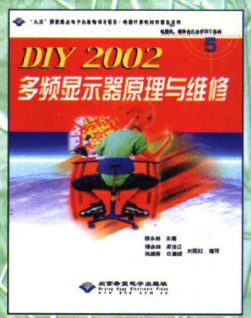
CX-83336
定价:48.00 元
ISBN:7900071105



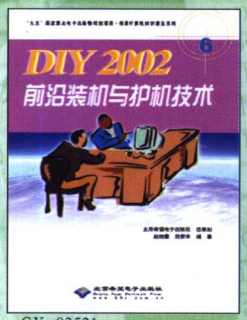
CX-83370
定价:39.00 元
ISBN:790007113X



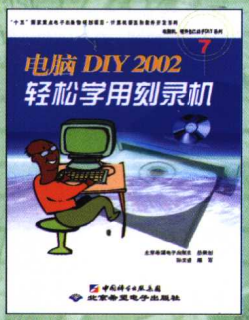
CX-83369
定价:39.00 元
ISBN:7900071237



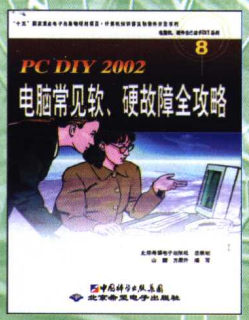
CX-83077
定价:55.00 元
ISBN:7900044841



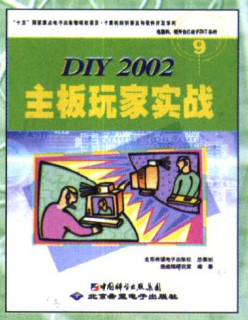
CX-83521
定价:48.00 元
ISBN:7980001664



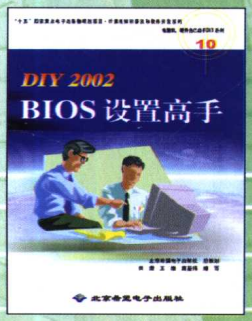
CX-83589
定价:30.00 元
ISBN:7900088121



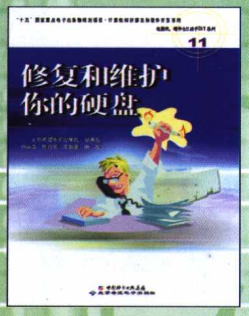
CX-83632
定价:35.00 元
ISBN:790008827X



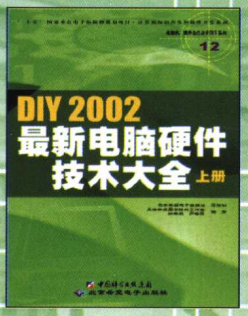
CX-83645
定价:35.00 元
ISBN:7900088334



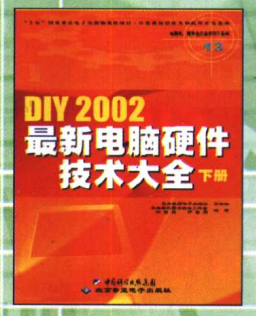
CX-83651
定价:26.00 元
ISBN:7900088377



CX-3685
定价:42.00 元
ISBN:7900088725



CX-3698
定价：50.00 元
ISBN 7900088806



CX-3726
定价：48.00 元
ISBN 7900088989

社址：北京海淀知春路甲63号卫星大厦三层 通信地址：北京中关村083信箱(100080) 电话：(010) 82675588(总机) 传真：(010) 62520573

作者感言

在黑客任务实战系列书籍推出后，受到相当多读者的喜爱、支持、建议与指教，其中大部分的读者都希望能看到续集，这实在让小弟与John Hawke老兄感动的痛哭流涕……怎么大家都不学好，想当黑客！……No，是大家的支持真使我们永生难忘，因此规划了一系列精彩的主题，让你很容易的可以学会各种黑客攻略与防护技巧。

基本上本书是沿续黑客任务实战系列的一贯特色，以讨论个人机上所使用Windows系统与IE、Outlook Express软件漏洞为主，告诉读者如何使用这些漏洞对一般上网的个人机进行各项黑客任务的详细实作，同时也告诉读者如何对这些漏洞进行修补以阻挡黑客的入侵。

之前我们收到的许多信件中发现有些读者有下列两个状况：

- 拿到书中介绍的软件就兴高采烈的去使用，并没有详细阅读书中的操作内容与注意事项，出现问题就写信来询问，其实这些答案在书中都已经有了。

- 依照书中的操作进行到一半有问题，就写信来询问，其实将整个操作完成就会有答案。

所以麻烦请各位进行黑客任务时要有耐心与毅力，多仔细查看书中的内容与说明，从错误与学习中累积经验，这样你才可以真正的学习到东西。

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、某台电脑或各种密码，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，所以请不要写这样的信给我们，谢谢各位读者的合作！

请注意：

- 若你有使用电子邮件则填写本书光盘中的读者服务卡。
- 下一页读者服务卡中的电子邮件地址请写清楚，不要用太草！

EMail　:**hawkes@ms29.hinet.net**
或FAX:00-886-29189919(中国读者)
FAX:001-886-2-29189919(中国 香港读者)

请注意：本书内容完全从理论与技术实务的角度来针对有关黑客攻略进行讨论与研究，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
9.27.2002

请将下表数据填妥后传真至00-886-2-2918-9919
我们将会不定期的提供您有关各种Windows、Internet
与多媒体的最新信息与相关软件，请多多利用，谢谢！
您也可以到我们的网站: **http://faqdiy.go.8866.org**
来获得相关的更新文件与最新信息!!

若您有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。

讀者服務卡 REGISTER CARD

书名	**黑客任务实战-个人机漏洞篇**	本书序列号	**北京希望2K20901**		
姓名		性别	☐先生 ☐小姐	年龄	
学历	☐研究所 ☐大学 ☐专校 ☐高中职 ☐中学☐小学				
您的电邮地址					
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 其它:				
职业	☐学生 ☐电脑业或IT部门 ☐非电脑业 ☐其他:_____	您觉得本书	☐简单 ☐适中 ☐艰深		
在Windows中常遇到什么样的困扰与麻烦?					
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: _____				
您还希望获得那方面解决问题的信息					
您对本书有何建议					

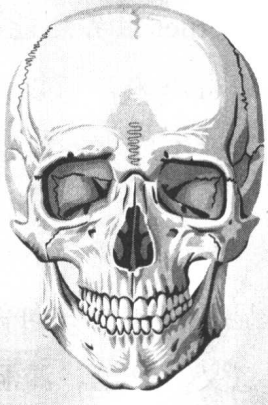
(可填写后复印传真或邮寄或EMail)

目　录

第 1 章

黑客入侵的基本原理与观念

Basic Concept and BaseKnowledge for Hacker Mission



黑客任务实战系列受到许多读者的支持与喜爱，我们也收到许多读者反应的各种问题与意见，其中我们发现仍然有许多读者对黑客入侵的基本原理与观念并不了解，甚至完全不懂，例如：端口所扮演的角色与观念，或是有什么工具或做法一定可以完成某个黑客任务。我们必须说许多黑客任务虽然没有想像中的困难，但也没有那么容易的的轻易完成，更没有一定可以入侵某个网站或电脑……这种 100% 成功的做法或工具。如果真有的话，那 Internet 世界还能存在吗？这是很简单的逻辑，请你脑筋转一下就想得出来，所以请各位读者帮帮忙，不要再问我们这类逻辑上根本就不成立的问题。

由于观念不够的初学者实在很多，所以在本章中我们将以浅显易懂的方式向你说明有关黑客入侵的基本原理与观念、端口的意义与角色、漏洞是什么？如何利用各类系统或软件的漏洞来进行入侵与攻击服务器或一般上网电脑？利用漏洞来进行黑客任务有哪些标准的教战守则……等，由于这些内容都是后面章节进行各项黑客任务的重要基础，所以一定要仔细研读，否则将可能无法顺利的完成各项任务。同样的，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

本章中所说明的各种黑客任务的基本原理与观念也可适用于其他非 Windows 系统中，例如：Linux，UNIX，MacOS，SunOS……。

Q1 入侵或攻击一般上网个人机的原理与观念是什么?

Q2 对一般上网个人机进行黑客任务有哪些方法可使用?各有何优缺点?

相关问题请见 Q3, Q6, Q11

许多黑客任务实战的读者都对黑客入侵与攻击的基本原理与观念都不甚清楚,小弟也经常收到读者如下的问题:

- 我知道某台电脑的 IP 地址,为何无法进入?
- 对方电脑已经打开端口 139,为何我无法进入?
- 有什么方法一定可以入侵某台电脑?
- 请告诉我一定可破解某个密码的方法?

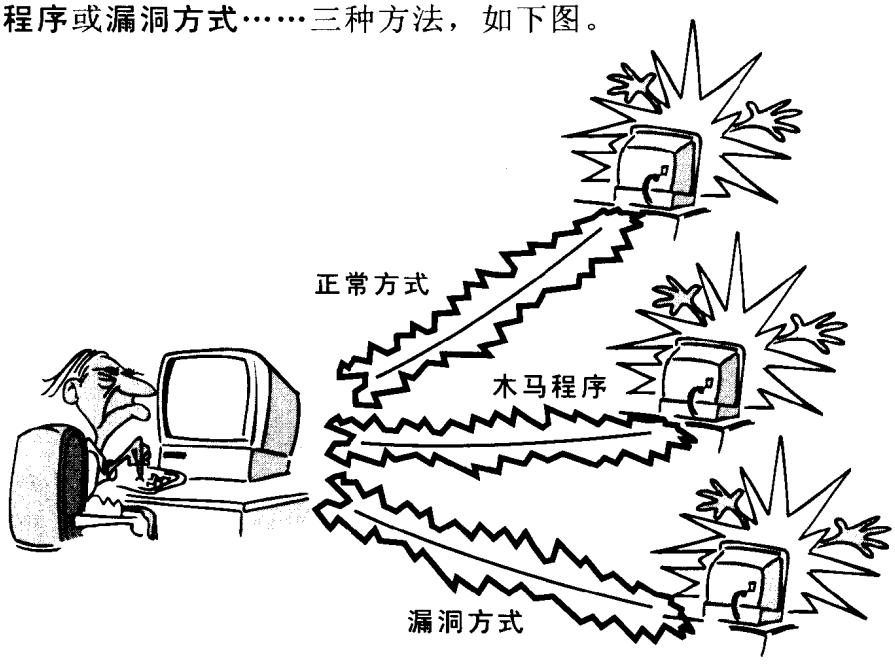
……**and More**

相信只要有些基本概念的读者一定都会觉得这样的问题有些不可思议,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或破解密码的方法?这样 Bill 老大还混的下去吗?黑客任务虽然并不是非常困难,但也没想像中的那么简单,所以在本问题中我们将以 **Top-to-Down** 的方式,详细告诉你要对一般上网的个人机进行黑客任务有哪些方法?它们有那些优缺点?什么情况下适用哪些方法?然后再将各方法分

散到其他问题中个别专论，帮助你更清楚地认识与了解，所以请仔细观看。

❑ 黑客任务的方法

一般通过 Internet 来进行各项黑客任务，不外乎**正常方式**、**木马程序**或**漏洞方式**……三种方法，如下图。



下面我们就对这三种方法来分别讨论与研究。

❑ 方法❶正常方式

所谓的正常方式就是通过 Internet 连接的方式来进入其他上网的计算机中，就像是在局域网 (LAN) 中连接到其他电脑一样，只是 Internet 的世界是广域网络 (WAN) 而不是局域网 (LAN)，而在

Windows 系统中最典型的作法就是通过**端口 139** (也就是**资源共享**) 的方式，使用**资源管理器**或**网上邻居**就可以连接到其他电脑，然后进行各项黑客任务，下面来看看此方法有何优缺点。

优点

这还用说吗? 此方式最大的优点就是进入其他电脑中就像进入你家里一般，想干什么就干什么，算是黑客任务中最简单，也最容易体会黑客快感的方法。

缺点

- 由于此方法是针对许多上网电脑对网络安全的疏忽或不注意而造成黑客容易入侵，因此只要大家都将资源共享的功能关闭，则此方法就没辙了。

- 若遇到要键入密码，则必须要想办法破解之后才能进入，否则此方法一样无效。

- 若是对方电脑中的共享磁盘都设为**只读** (Read Only)，就必须要另想他法来改为可读写，否则黑客任务就受到很大的限制，无法想干什么就干什么。

结论

由上面的几项缺点你可以看出，目前在 Internet 中你可以此方