马到成功 电脑宝典系列

网络安全 1CD

黑客攻防

黑客攻击秘笈
电脑防黑宝典
黑客攻击原理
黑客入侵手段

相马软件 创作

深圳市相马计算机有限公司
方圆电子音像出版社

网络安全—黑客攻防

相马软件

方圆电子音像出版社

内容简介

长期以来，在我们心中的黑客总是笼罩着一层神秘的面纱，而广为人知的一些黑客行为做法更像传奇故事般。本书将有助于揭开黑客们神奇背面，将其平凡的一面呈现于读者面前，同时也将其“十八般武艺”一一探讨，以求更深入了解。

光盘内容包括：各种有关黑客攻击的工具、系统安全工具、网络工具等等。

郑重声明：为清楚地了解黑客的攻击手法及原理，从而制定相应的对付策略，本书中不可避免地涉及到黑客行为的一些具体实施手法，对此读者如果试图尝试，请一定注意遵守相关的法律法规，若有由此行为而产生的一切后果，本书编者概不负责！

产品名称：网络安全——黑客攻防
开发制作：深圳市相马计算机有限公司
出 版 社：方圆电子音像出版社
出版时间：2001年3月
定　　价：13.80元（1光盘）

光盘的安装与使用方法

把“网络安全—黑客攻防”光盘放入电脑的光驱中，软件自动运行。在“通告说明”窗口里面选择“同意”自动进入主界面(图1)。如果自动运行失效，您也可以打开“我的电脑”，找到您的光驱图标，用鼠标右键单击它，即弹出快捷菜单，然后选择“打开”选项即可打开光盘，找到光盘里的“autorun.exe”文件双击它就可进行手动运行光盘。

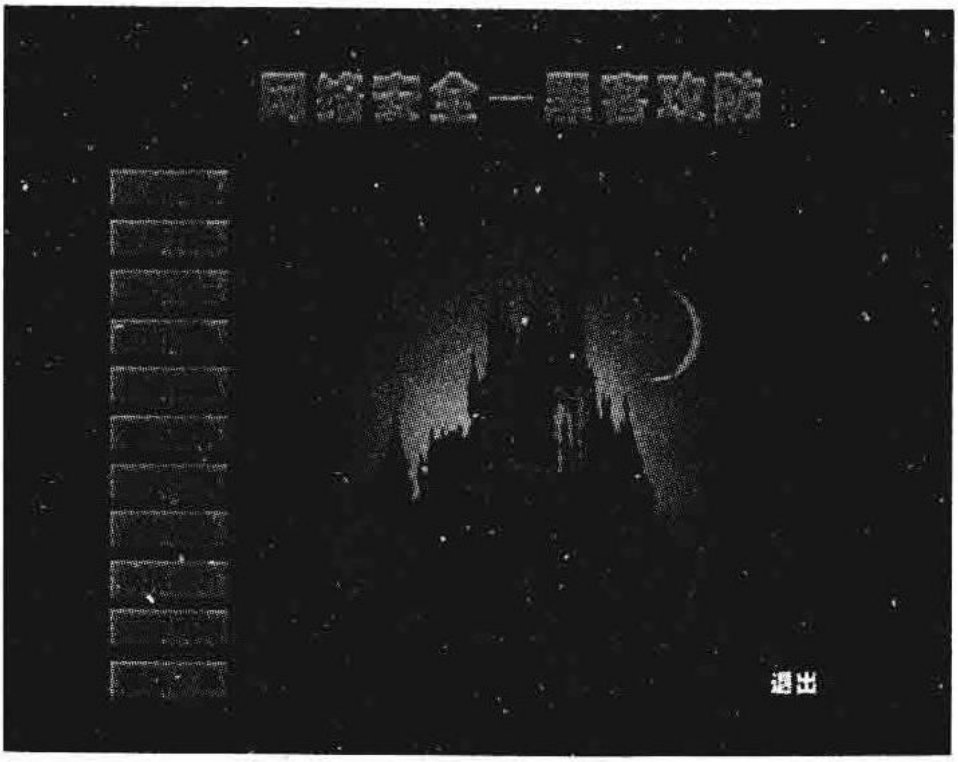

图1

单击“IE浏览器”按钮是进行IE5.0的安装。

单击“相关工具”按钮则打开一对话框，里面

有很多相关工具，如图2所示。

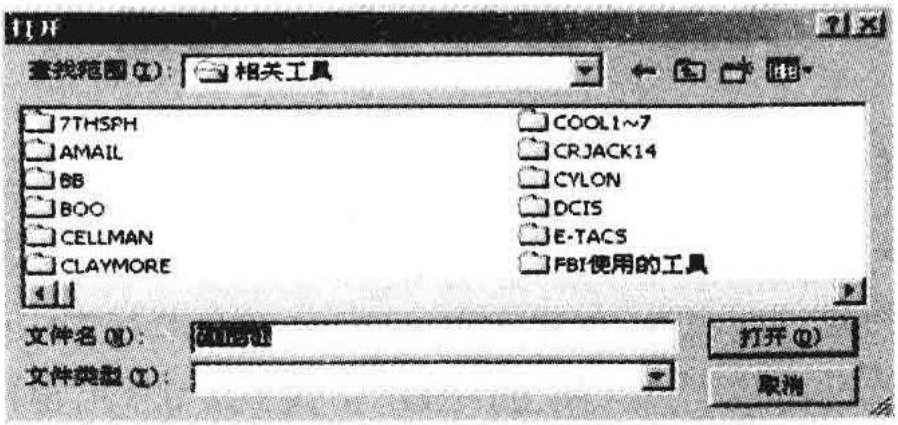

图2

单击其他的按钮则分别进入用IE打开的界面，图3就是单击“最佳工具”后所打开的界面。

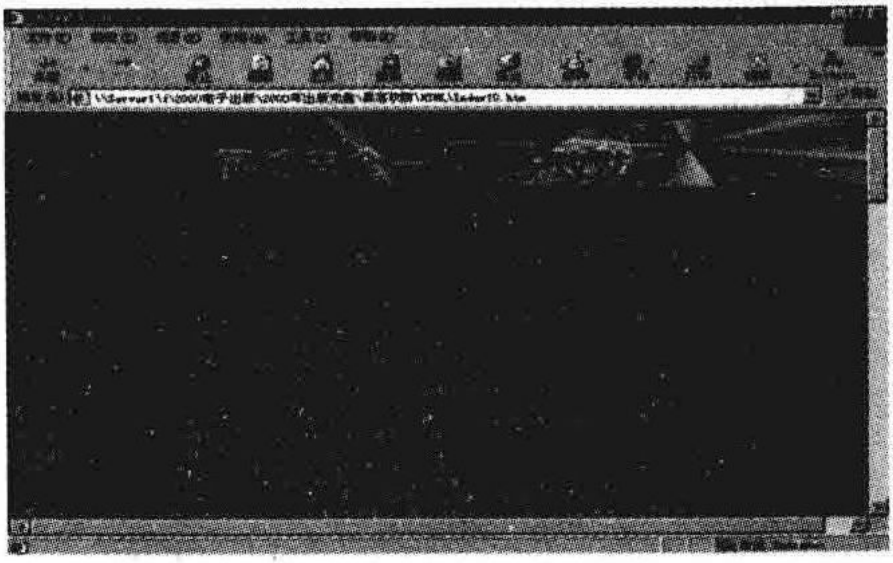

图3

单击“退出”按钮则退出该程序。

注意：在使用软件时请把防毒软件〔防火墙〕关闭，有些黑客程序是防毒软件防范之一，如不关闭会阻碍您的浏览与使用。

目录

第一章 黑客简介.....11
1.1 什么样的人称为“黑客”？.....11
1.2 黑客的行为特征.....13
1.3 Hack 守则.....15
1.4 黑客们要知的秘密.....16

第二章 黑客实战技巧应用.....20
2.1 攻击NT服务器的基本方法.....20
2.2 网络入侵实用战术完全手册 (UNIX)
.....30
2.3 如何入侵Internet上的主机.....70
2.4 FTPBounce跳跃攻击法.....76
2.5 Back Orifice 后门.....86
2.6 “后门”技巧.....88
2.7 扫描到的端口到底有什么用?.....106
2.8 浏览器攻击.....111

2.9 口令攻击术 114
2.10 攻击聊天室 118
2.11 利用 InterNIC 验证缺陷进行域名劫持 122
2.12 了解“偷取别人的oicq密码法” 142
2.13 简单的留言板攻击法的方法 145

第三章 黑客工具软件 148
3.1 攻击软件原理及防范 148
3.2 Bo 2000 使用指南 157
3.3 OICQ黑客软件大曝光 170
3.4 网上十大最佳黑客软件简介 182
3.5 破坏NT安全的工具 189
3.6 扫描器—黑客的基本武器 191
3.7 扫描工具—观 194
3.8 网络监听 200
3.9 常用的监听工具 206
3.10 HAKTEK的用法 213

第四章 黑客攻击手法及防御 216
4.1 服务拒绝攻击 216
4.2 利用型攻击 220

4.3 信息收集型攻击 221
4.4 假消息攻击 224

第五章 安全漏洞 226
5.1 如何发现安全漏洞 226
5.2 安全漏洞概述 238
5.3 TCP/IP服务的脆弱性 246
5.4 留言板漏洞 251
5.5 Microsoft Internet Explorer 5.0 最新安全漏洞 253
5.6 NT与浏览器有关的安全漏洞及防范措施介绍 255
5.7 Microsoft Windows 9x NETBIOS 密码验证漏洞 265
5.8 Windows 2000 安全 (MS,缺陷) 266
5.9 Microsoft NT 4.0 and IIS 4.0 无效 URL 请求导致拒绝服务漏洞 272
5.10 win2000 Statistics Server 远程溢出 274
5.11 Windows NT 4.0 远程注册表拒绝服务攻击漏洞 283
5.12 Microsoft Office 2000 UA Control 安全漏洞 305

5.13 Linux 安全吗？.....306

第六章 安全防范.....312

6.1 冲浪者，小心触礁！（冲浪安全防范种种）.....312

6.2 如何防范D.o.S 攻击.....323

6.3 BO 病毒的主要传播途径以及识别、清除方法.....328

6.4 如何防止自己的 WEB 站点被侵犯.....330

6.5 局域、广域、外部网络安全.....343

6.6 电子邮件安全几招.....350

6.7 互联网十大漏洞与如何补救.....355

6.8 ICQ 的安全问题.....358

6.9 手工清除冰河木马.....360

6.10 如何防范黑客程序—八招.....361

第七章 系统安全.....363

7.1 操作系统安全的脆弱性.....363

7.2 UNIX 安全问题.....366

7.3 Internet 上 WindowsNT 安全措施....377

7.4 WINDOWS NT 如何防范黑客软件 iishack 的攻击.....384

7.5 堵住NT的安全漏洞.....386
7.6 TCP/IP协议安全性能.....388
7.7 NT Administrator权限获得法.....398

第八章 如何发现跟踪黑客.....402
8.1 如何发现黑客.....402
8.2 入侵者的追踪(Intruder Tracing)
.....416

第九章 关于密码与口令.....431
9.1 密码的正确设置.....431
9.2 危险口令排行榜.....432
9.3 Netware超级用户口令遗忘后的对策
.....435

网络安全—黑客攻防

第一章　黑客的简介

第二章　黑客实战技巧应用

第三章　黑客工具软件

第四章　黑客攻击手法及防御

第六章　安全防范

第五章　安全漏洞

第八章　如何发现跟踪黑客

第九章　关于密码与口令

第一章 黑客简介

1.1 什么样的人称为“黑客”？

世界各地对黑客的“定义”都不尽相同。按照东方人的习惯通常对黑客一词还有“侠”的含意。日本1998年新出版的《新黑客字典》把黑客定义为：“喜欢探索软件程序奥秘并从中增长其个人才干的人。他们不象绝大多数电脑使用者，只规规矩矩地了解别人指定了解的狭小部分知识。”1998年夏季，因印尼华人妇女惨遭印尼暴徒有组织的强暴，而激怒了中国黑客奋起袭击并破坏印尼诸网站的事例，则是一种典型的侠客行为。现在“黑客”一词在信息安全范畴内的普遍含义是特指对电脑系统的非法侵入者。多数黑客对电脑非常着迷，认为自己是世界上绝顶聪明的人，能够做其他人所不为。只要他们愿意，就可肆无忌惮非法闯入某些敏感数据的禁区或是内部网络，盗取重要的信息资源，或是与某些政府要员甚至是总统开一个玩笑，或者干脆针对某些人进行人身攻击、诽谤或恶作剧。他们常常以此为乐，做为一种智力的挑战而陶醉。 国际上的著名

黑客大多是15-30岁的年轻人，他们有着共同的伦理观：信息、技术和诀窍都应当被所有用户共享，而不能为个别人或集团所垄断。这些人在计算机方面的天赋，使其常常处于高度兴奋状态，通常彻夜不眠的操纵计算机，攻破网络或信息禁区，偷看敏感数据，篡改网址信息或者删除该网址的全部内容，其行为已经造成恶劣影响。黑客中的很多人具有反社会行为或反传统文化的色彩，与西方社会的“朋客”极其相似，有的还自称为“电脑朋客”(Cyberpunks)。目前黑客已成为一个广泛的社会群体。在欧美等国有完全合法的黑客组织或黑客学会，黑客们经常召开黑客技术交流会，1997年11月在纽约召开了世界黑客大会，参加人数达四五千人。在因特网上，黑客组织有公开网站、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，“2600”是最为著名的一本黑客杂志。由于有黑客组织的技术交流活动的存在，使一般性的“行黑”变得比较容易，普通人也很容易通过互联网轻易学会对网络进攻方法以及下载“后门”程序。黑客们公开Internet网上提出所谓的“黑客宣言”，其主要观点是：

通往电脑的路不止一条

所有信息都应该免费共享

打破电脑集权

在电脑上创造艺术和美

信息无疆界可言，任何人都可以在任何时间地点获取任何他认为有必要了解的任何信息

反对国家和政府部门对信息的垄断和封锁

1.2 黑客的行为特征

根据黑客行为特征可有以下几种表现形式：

1. 恶作剧型

喜欢进入他人网址，以删除某些文字或图像、篡改网址主页信息来显示自己高超的网络侵略技巧。此做法多为增添笑话自娱或娱人，或者进入他人网址内，将其主页内商品资料内容、价格做降价等大幅度修改，使消费者误以为该公司的商品便宜廉价而大量订购，从而产生 Internet 订货纠纷。

2. 隐蔽攻击型

隐蔽在暗处以匿名身份对网络发动攻击性行为，往往不易被人识破，或者干脆冒充网络合法用户，侵入网络“行黑”，该种行为由于是在暗处实施的主动攻击性行为，因此对社会危害极大。

3. 定时炸弹型指的就是网络内部人员的非法行为，他们在实施时故意在网络上布下陷阱或故意在网络维护软件内安插逻辑炸弹或后门程序，在特定

的时间或特定条件下，引发一条列具有连锁反应性质的破坏行动，或干扰网络正常运行或致使网络完全瘫痪。此种黑客在原公司离职后，通过其数据机连线，在得知原公司Internet地址密码的情形下，可从网上再次了解到前公司网络密址及电子邮件中各项文件资料，进而大量截取原公司最新资料，做为不正当竞争之用。这类黑客是企业内部蛀虫，其危害和影响巨大，有时几乎导致企业的破产倒闭。而混在政府内的这类黑客，破坏性更大。

4. 矛盾制造型

非法进入他人网络，修改其电子邮件的内容或厂商签约日期，进而破坏甲乙双方交易，并借此方式了解双方商谈的报价价格，乘机介入其商品竞争。有些黑客还利用政府上网的机会，修改公众信息，造成社会矛盾和动乱，严重者可颠覆国家和军队。

5. 职业杀手型

此种黑客以职业杀手著称，经常以监控方式将他人网址内由国外传来的资料迅速清除，使得原网址使用公司无法得知国外最新资料或订单，亦或者将电脑病毒植入他人网络内，使其网络无法正常运行。更有甚者,进入军事情报机关的内部网络，干扰军事指挥系统的正常工作，任意修改军方首脑的指示和下级通过网络传递到首脑机关的情报,篡改军事战略部署，导致部队调防和军事运输上的障碍，达

到干扰和摧毁国防军事系统的目的。严重者可以导致局部战争的失败。

6. 窃密高手型

出于某些集团利益的需要或者个人的私利,利用高技术手段窃取网络上的加密信息，使高度敏感信息泄密。或者窃取情报用于威胁利诱政府公职人员，导致内外勾结进一步干扰破坏内部网的运行。有关商业秘密的情报，一旦被黑客截获，还可能引发局部地区或全球的经济危机或政治动荡。

7. 业余爱好型

计算机爱好者受到好奇心驱使，往往在技术上追求精益求精，丝毫未感自己的行为对他人造成影响，属于无意性攻击行为。这种人可以帮助某些内部网堵塞漏洞和防止损失扩大。有些爱好者还能够帮助政府部门修正网络错误。因此，这类黑客的出现并非是坏事，至少他们的本意无反社会的色彩，只是受到好奇心驱使而已。

1.3 Hack 守则

1. 不恶意破坏任何系统，这样做只会给你带来麻烦。恶意破坏它人的软体将导致法律刑责，如果你只是使用电脑，那仅为非法使用!! 注意：千万不

要破坏别人的软件或资料 !!

2. 不修改任何的系统档，如果你是为了要进入系统而修改它，请在达到目的后将它改回原状。

3. 不要轻易的将你要 Hack 的网站告诉你不信任的朋友。

4. 不要在 bbs 上谈论你 Hack 的任何事情。

5. 在 Post 文章的时候不要使用真名。

6. 正在入侵的时候，不要随意离开你的电脑。

7. 不要侵入或破坏政府机关的主机。

8. 不在电话中谈论你 Hack 的任何事情。

9. 将你的笔记放在安全的地方。

10. 想要成为 Hacker 就要真正的 Hacking，读遍所有有关系统安全或系统漏洞的文件。

11. 已侵入电脑中的帐号不得清除或修改。

12. 不得修改系统档案，如果为了隐藏自己的侵入而作的修改则不在此限，但仍须维持原来系统的安全性，不得因得到系统的控制权而将门户大开 !!

13. 不将你已破解的帐号分享与你的朋友。

1.4 黑客们要知的秘密

1、能用 Perl(Unix 下的语言，现在已经可以用于 NT 下) 或 C 编程，写一些基本的安全工具，高手们