

电脑报 总策划

电脑宝贝 2008

PC Baby

【黑客技巧轻松掌握，实例速查现学现用】

胥阳 熊菲 编著

黑客攻防

实用技巧速查

- ★ 扫描、嗅探、监听练就黑客本领
- ★ 远控、木马、代理尽显黑客真招
- ★ QQ、邮件、密码攻防技巧实例速查

特别采用高质量轻型纸精印

超值光盘提供

- 价值51元【加密特警】
- 黑客扫描利器
- 密码解除工具
- 远程控制工具



电脑报电子音像出版社

特别采用高质量轻型纸精印

TP393.08/239D

2008



黑客攻防 实用技巧速查

胥 阳 熊 菲 编著

电脑报电子音像出版社

内容提要

本手册从应用的角度阐述了黑客常见的攻击手段和步骤，并提出了相应的预防措施和建议，可读性和实践性非常强。主要内容包括扫描与入侵、嗅探与监听、远程控制、木马攻防、突破局域网限制、QQ及电邮攻防、口令破解等实例。

本手册不仅是广大黑客爱好者必备的手册，对网络管理员和系统管理员同样有重要的参考价值。

特别声明：使用网络技术攻击他人电脑的行为属违法行为，读者切勿用本手册中介绍的方法对他人电脑进行恶意攻击，否则后果自负！

光盘内容

光盘里面收录了书中绝大部分涉及的相关软件，由于涉及黑客软件，可能会被杀毒软件查杀，请用户谨慎使用。

- | | |
|----------------|-----------|
| 1. 加密特警(价值51元) | 2. 黑客扫描利器 |
| 3. 密码解除工具 | 4. 远程控制工具 |

书 名：黑客攻防实用技巧速查

编 著：胥 阳 熊 菲

技 术 编 辑：何 磊

封 面 设 计：陈 敏

组 版 编 辑：蒋 洁

出 版 单 位：电脑报电子音像出版社

地 址：重庆市双钢路3号科协大厦

邮 政 编 码：400013

发 行：电脑报电子音像出版社

经 销：各地新华书店、报刊亭

C D 生 产：四川省釜山数码科技有限公司

文 本 印 刷：重庆联谊印务有限公司

开 本 规 格：787mm × 1092mm 1/32 8印张 300千字

版 本 号：ISBN 978-7-900729-12-5

版 次：2008年1月第1版 2008年1月第1次印刷

定 价：15.00元(1CD+配套书)

前言

宝贝在手，应用无忧

PC 宝贝丛书是一系列集实用、便捷、时尚于一身的新型电脑应用手册。自 2002 年初版以来，本系列丛书就以其操作性极强的内容、便携式的开本与迷你光盘，以及超实用的配套软件，迅速赢得了众多“粉丝”。迄今本系列丛书的读者已达百万之众，影响可见一斑。近年来，在部分热心读者的参与下，丛书的编辑团队不断结合电脑应用的最新潮流与趋势，经过逐年与时俱进的修订再版，使得这套丛书无论是在内容抑或形式上都已趋于完美。

内容专注，选题讲究：在选题上，本系列丛书非常讲究贴近实际应用。细心的读者可能注意到，丛书每一分册均选取时下应用最为广泛或关注度较高的某一专题领域进行讲解，这样可以帮助读者在尽可能短的时间内迅速掌握主流的电脑操作与应用。

立体解说，易于上手：在版面编排上，本系列丛书采用把每个学习要点或者操作目标细分步骤，在实际应用或实务操作的基础上进行分解、分析，化难为易，并一律以简明扼要的语言配合直观的图示予以解说，极大限度地提高了学习的效率。

实例丰富，即查即用：本系列丛书大量结合应用

前言

实例进行讲解，内容实用，
条目清晰，非常方便读者学习和
理解。同时由于本系列丛书精致
乖巧、携带方便，用户可以随时
查阅，能真正为用户排忧解难，解决用户的不时之需。

书盘互动，物超所值：随书配套的精美迷你光盘，
包含了与图书内容匹配的大量实用软件。同时每张光
盘都向读者附赠送一个相关的实用正版软件，真正物
超所值，回馈给读者看得见的实惠。

如果你正在为提升自己的电脑操作和应用技巧寻
求帮助，或者你只想花费较短时间就掌握那些最主流
最热门的电脑应用，PC 宝贝丛书应该就是你的首选。
还犹豫什么呢？

编者

2008 年 1 月





第1章 揭秘黑客神秘面纱

【7个典型黑客攻防事例】 1

事例 1

QQ盗号的阴谋与反阴谋 1

1.1.1 知己知彼，盗号技术不再神秘 1

1.1.2 练就慧眼，让木马无处可逃 4

1.1.3 以退为进，给盗号者以致命一击 4

事例 2

劲舞团狂暴升级 7

1.2.1 想怎么“玩”就怎么改 7

1.2.2 劲舞团修改实战 8

1.2.3 巧刷劲舞团韩服 11

事例 3

网银账号泄漏的秘密 12

1.3.1 网银账号是如何泄漏的 12

1.3.2 网络账号保护事项 15

事例 4

ADSL账号被远程盗取 16

1.4.1 密码被盗，ADSL路由拨号惹的祸 17

1.4.2 扫描ADSL在线用户寻找攻击目标 17

1.4.3 单击鼠标轻松破解密码，防范意识需加强 20

事例 5

暗处偷窥的第三只“眼” 23

1.5.1 “黑洞”木马远程开启摄像头 23

1.5.2 揪出隐藏在系统中的“黑洞”木马 26

1.5.3 防范摄像头木马，安全意识很重要 27

事例 6

Windows系统万能登录 29

1.6.1 删除SAM文件 29

1.6.2 利用LC4从SAM文件中找密码 30

1.6.3 巧用屏保破解密码 31

1.6.4 ERD Commander：强大实用的系统拯救工具 32

事例 7

解除ISP限制路由共享上网 35



第2章 是如何锁定“目标”的

【扫描与入侵】 38

2.1 扫描目标主机IP与端口 38

2.1.1 IPScan扫描活动主机 38

2.1.2 使用NetSuper扫描共享资源 39

2.1.3 局域网查看工具LanSee 42

2.1.4 扫描目标主机开启的端口 43

2.1.5 功能丰富的SuperScan端口扫描器 44

2.1.6 综合扫描器X-Scan 51

2.2 一个经典的系统入侵实例 62

2.2.1 扫描远程主机是否存在NT弱口令（获取管理员权限） 62

2.2.2 使用DameWare入侵漏洞主机 64

2.3 如何防范黑客扫描 73

第3章 局域网中的监听者

【嗅探器截取信息】 75

3.1 局域网嗅探与监听 75

3.1.1 谁偷看了我的网络日记 75

3.1.2 活跃在局域网里的“耳朵”们 77

3.2 Sniffer介绍 82

3.3 经典嗅探器Sniffer Portable 84

3.2.1 Sniffer Portable功能简介 85

3.2.2 捕获报文查看 87

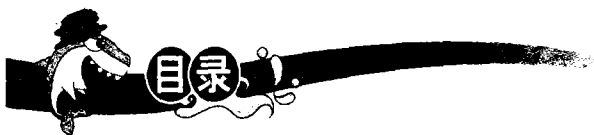
3.2.3 捕获数据包后的分析工作 88

3.2.4 设置捕获条件 90

3.2.5 报文发送 91

3.4 防御Sniffer攻击 92

3.4.1 怎样发现 Sniffer 93



3.4.2 抵御 Sniffer	93
3.4.3 防止Sniffer的工具Antisniff	94
3.5 使用屏幕间谍监视本地计算机	95
3.5.1 软件功能面板	95
3.5.2 记录浏览	98

第4章 千里求助不再难

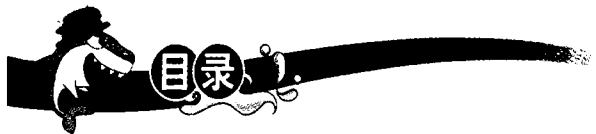
【远程控制应用】	100
----------------	-----

4.1 Windows Vista的远程协助	100
4.1.1 Windows Vista远程协助的改进	101
4.1.2 启动Windows Vista中的远程协助	101
4.1.3 发送远程协助请求	103
4.1.4 接受远程协助请求	106
4.1.5 远程协助其他设置	108
4.2 Windows XP远程协助设置	111
4.2.1 通过XP远程桌面连接	111
4.2.2 家庭版XP的远程协助方案	113
4.2.3 通过软件实现端口映射	114
4.2.4 利用WinVNC的逆向连接	116
4.3 pcAnywhere远程控制计算机	117
4.3.1 pcAnywhere的工作原理	117
4.3.2 被控端的配置	118
4.3.3 主控端的配置	120
4.3.4 网络连接的优化配置	120
4.3.5 远程控制的实现	121

第5章 深入敌后的间谍

【木马植入与防范】	123
-----------------	-----

5.1 什么是木马	123
------------------------	------------

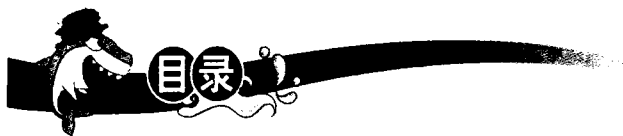


5.1.1 木马的定义	123
5.1.2 木马的特征	124
5.1.3 木马的功能	125
5.1.4 木马的分类	126
5.2 经典木马“冰河”入侵实例	127
5.2.1 配置冰河木马的服务端（被控端）	127
5.2.2 远程控制冰河服务端	129
5.3 冰河木马防范与反攻	131
5.4 新生代“灰鸽子”木马控制实战	132
5.4.1 灰鸽子的特色	133
5.4.2 配置灰鸽子服务端（木马）	134
5.4.3 远程入侵服务端（被控端）	138
5.5 灰鸽子木马常见问题解决方案	142
5.6 清除计算机中的灰鸽子	149
5.7 预防信息泄漏的7种方法	153

第6章 让上网自由自在

【突破网络中的限制】	157
------------------	-----

6.1 使用代理上网突破网络限制	157
6.1.1 突破局域网上网限制	157
6.1.2 用“代理猎手”搜索代理服务器	161
6.1.3 代理猎手使用要点	168
6.2 突破网络下载限制	174
6.2.1 解除禁止右键和网页嵌入播放网页	174
6.2.2 FlashGet添加代理突破下载限制	176
6.2.3 Net Transport突破下载法	178
6.2.4 解除网吧下载限制	179
6.2.5 BT下载穿透防火墙	183
6.2.6 下载swf文件	184



6.2.7 下载在线流媒体	185
6.3 网吧管理限制的漏洞	188

第7章 觊觎QQ、电邮的黑手

【QQ、电邮盗号揭秘】	190
-------------------	-----

7.1 获取QQ密码	190
7.1.1 扫描获取QQ密码	190
7.1.2 揭秘木马如何盗取QQ密码	193
7.2 查看QQ聊天记录	197
7.2.1 利用“QQ聊天记录查看器”查看聊天记录	197
7.2.2 防范聊天记录被偷窥	198
7.3 远程攻击QQ实例	199
7.4 网吧内嗅探出QQ密码的阴谋	201
7.5 QQ避开攻击的七大秘技	203
7.6 电子邮箱入侵实例	204

第8章 管好你的信息安全“钥匙”

【密码入侵与防范】	210
-----------------	-----

8.1 常见系统口令入侵实例	210
8.1.1 解除CMOS口令	210
8.1.2 解除系统密码	212
8.2 巧除Word与Excel文档密码	213
8.2.1 清除Word密码	213
8.2.2 清除Excel密码	214
8.3 清除压缩文件密码	215
8.3.1 密码恢复工具也成黑客帮凶	215



8.3.2 巧妙设置, 让压缩文件无懈可击	218
-----------------------------	-----

8.4 黑客破解密码的心理学	220
----------------------	-----

附录1 黑客必备的网络常识 222

认识IP地址	222
--------------	-----

什么是IP地址	222
---------------	-----

IP的分类	223
-------------	-----

子网掩码	225
------------	-----

IP的种类与获取方式	226
------------------	-----

NAT网络地址转换	228
-----------------	-----

端口——常被黑客利用的通道	229
---------------------	-----

什么是端口	230
-------------	-----

端口是怎样分配的	231
----------------	-----

TCP与UDP端口	232
-----------------	-----

查看端口	234
------------	-----

限制端口	235
------------	-----

附录2 黑客常用命令详解 238

Ping 命令	238
---------------	-----

Netstat 命令	240
------------------	-----

IPConfig 命令	241
-------------------	-----

ARP(地址转换协议)	242
-------------------	-----

Tracert 命令	244
------------------	-----

Route 命令	244
----------------	-----

NBTStat 命令	245
------------------	-----



第1章

揭秘黑客神秘面纱

【7个典型黑客攻防事例】

Internet（因特网）的普及使人们的工作生活发生了翻天覆地的变化，可是在Internet世界中却没有人来管理，如同武侠小说中的“江湖”一样，在这个没有王法的世界中滋生出了许多正派和邪派的力量，他们有秩序的建立者，也有潜在的破坏者，他们被人们统称为——黑客。下面让我们通过7个典型黑客入侵事例，一同揭开黑客神秘的面纱。



QQ盗号的阴谋与反阴谋

很多用户都有过QQ号被盗的经历，即使用“密码保护”功能找回回来后，里面的Q币也已经被盗号者洗劫一空，碰到更恶毒的盗号者，还会将好友统统删除，朋友们将会永远的离去。想过反击吗？什么，反击？别开玩笑，我们只是菜鸟，不是黑客，我们只会看看网页，聊聊天，连QQ号是怎么被盗的都不知道，还能把盗号者怎么样呢？其实喜欢盗号的所谓“黑客”们，也只是利用了一些现成的盗号工具，只要我们了解了QQ号被盗的过程，就能做出相应防范，甚至由守转攻，给盗号者以致命一击。

1.1.1 知己知彼，盗号技术不再神秘

如今，还在持续更新的QQ盗号软件已经所剩无几，其中最为著名，流传最广的则非“啊拉QQ大盗”莫属，目前绝大多数的QQ号被盗事件都是



由这个软件引起的。该软件的使用条件很简单，盗号者只需要有一个支持smtp发信的邮箱或者一个支持asp脚本的网页空间即可。而且该木马可以将盗取的QQ号自动分为靓号和非靓号两种，并将它们分别发送到不同的信箱中，这也是“啊拉QQ大盗”如此流行的原因之一。接下来，便让我们先来了解一下他们是如何盗号的，以便从中找到防范应对措施的良方。

1. 认识“啊拉QQ大盗”

下载“啊拉QQ大盗”解压后有两个文件：“alaqq0210.exe”、“tmdqq.asp”。其中“alaqq0210.exe”是“啊拉QQ大盗”的配置程序，tmdqq.asp 是使用“网站收信”模式时需使用的文件。正式使用前，还需要设置其参数。

盗号者有两种方法接收QQ账号信息——“邮箱收信”及“网站收信”我们主要以“邮箱收信”来进行说明，运行“alaqq0210.exe”，出现如下图所示的配置界面。在“发信模式选择”选项中选中“邮箱收信”；在“邮箱收信”填写电子邮箱地址（默认为163.com网易的邮箱）。

我们以邮箱“system_test_2007@163.com”为例来介绍“邮箱收信”模式中的配置与测试。此外，在“收信箱（靓）”和“收信箱（普）”中可以填入不同的邮箱地址用来接受QQ靓号和普通QQ号。然后在“发信服务器”下拉框中选择邮箱相应的smtp服务器，这里是smtp.163.com。最后填入发信箱的账号、密码、全称即可。

配置“啊拉QQ大盗”参数



设置完毕后，可以来测试一下填写的内容是否正确，单击下方“测试邮箱”按钮，程序将会出现邮箱测试状态。如果测试的项目都显示成功，即可完成邮箱信息配置。



除了选择“邮箱收信”模式之外，盗号者还可以选择“网站收信”模式，让盗取的QQ号码自动上传到指定的网站空间。当然，在使用之前，也需要做一些准备工作。

2. 设置木马附加参数

前面我们了解如何设置“啊拉QQ大盗”向盗号者的信箱发送QQ账号密码的，当“啊拉QQ大盗”生成的木马侦察到使用者的账户名和密码的时候，就会将窃取的信息发送到入侵者设定好的邮箱中。可是，要侦察QQ的账户名和密码，必须要用户输入的时候，才能获得，所以，盗号者还得设置“啊拉QQ大盗”的其他参数。

在“高级设置”栏下如果勾选“运行后关闭QQ”，用户一旦运行“啊拉QQ大盗”生成的木马，QQ将会在60秒后自动关闭，当对方再次登录QQ后，其QQ号码和密码会被木马所截获，并发送到盗号者的邮箱或网站空间中。此外，如果希望该木马被用于网吧环境，那就需要勾选“还原精灵自动转存”，以便系统重启后仍能运行木马。除这两项外，其他保持默认即可。

3. 盗取QQ号码信息

配置完“啊拉QQ大盗”，单击程序界面中的“生成木马”按钮，即可生成一个能盗取QQ号码的木马程序。入侵者通常是将该程序伪装成图片、小游戏，或者和其他软件捆绑后进行传播。当有受害者运行相应的文件后，木马会隐藏到系统中，系统一旦QQ登录时，木马便会开始工作，将相关的号码及

密码截取,并按照此前的设置,将这些信息发送到邮箱或者网站空间。

关于QQ盗号的伎俩,我们将在第7章详细说明,在这里读者可以明白QQ盗号的一般道理,及早做好预防措施。

1.1.2 练就慧眼,让木马无处可逃

我们已经了解了“啊拉QQ大盗”盗号的秘密了,那么如何才能从系统中发现“啊拉QQ大盗”呢?一般来说,如果碰到了以下几种情况,那就应该小心了。

- QQ自动关闭。
- 运行某一程序后其自身消失不见。
- 运行某一程序后杀毒软件自动关闭。
- 访问杀毒软件网站时浏览器被自动关闭。
- 如果杀毒软件有邮件监控功能的,出现程序发送邮件的警告框。

出现上述情况的一种或多种,系统就有可能已经感染了“啊拉QQ大盗”。当然,感染了木马并不可怕,我们同样可以将其从系统中清除出去。

1.手工查杀木马

发现系统感染了“啊拉QQ大盗”后我们可以手工将其清除。“啊拉QQ大盗”运行后会在系统目录中的system32文件夹下生成一个名为NTdhcp.exe的文件,并在注册表的启动项中加入木马的键值,以便每次系统启动都能运行木马。我们首先要做的就是运行“任务管理器”,结束其中的木马进程“NTdhcp.exe”。然后打开资源管理器中的“文件夹选项”,选择其中的“查看”标签,将其中“隐藏受保护的操作系统文件”选项前面的勾去掉。接着进入系统目录中的system32文件夹,删除NTdhcp.exe文件。最后在注册表删除NTdhcp.exe键值,该键值位于HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run。

2.卸载木马

卸载“啊拉QQ大盗”很简单,只要下载“啊拉QQ大盗”的配置程序,运行后单击其中的“卸载程序”按钮即可将木马完全清除出系统。

1.1.3 以退为进,给盗号者以致命一击

忙乎了半天,终于把系统中的“啊拉QQ大盗”彻底清除,那么,面对



可恶的盗号者，我们是不是应该给他一个教训呢？

1. 利用漏洞，由守转攻

这里所谓的“攻”，并不是直接入侵盗号者的电脑只是从盗号软件几乎都存在的漏洞入手，从而给盗号者一个教训。那么这个漏洞是什么呢？从此前对“啊拉QQ大盗”的分析中可以看到，配置部分填写了收取QQ号码信息邮件的邮箱账号和密码，而邮箱的账号和密码都是明文保存在木马程序中的。因此，我们可以从生成的木马程序中找到盗号者的邮箱账号和密码。进而轻松控制盗号者的邮箱，让盗号者偷鸡不成反蚀把米。

提示

以上漏洞仅存在于将QQ号码信息以邮件发送方式的木马，如果在配置“啊拉QQ大盗”的过程中选择使用网站接收的方式则不存在该漏洞。

2. 网络嗅探，反夺盗号者邮箱

当木马截取到QQ号码和密码后，会将这些信息以电子邮件的形式发送到盗号者的邮箱，我们可以从这里入手，在木马发送邮件的过程中将网络数据包截取下来，这个被截获的数据包中就含有盗号者邮箱的账号和密码。截取数据包时我们可以使用一些网络嗅探软件，这些嗅探软件可以很轻松地截取数据包并自动过滤出密码信息。

(1) 命令行下的x-sniff

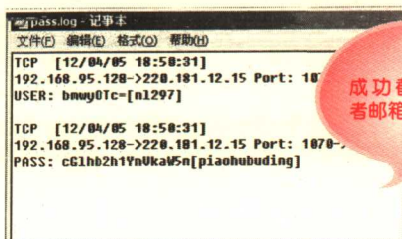
x-sniff是一款命令行下的嗅探工具，嗅探能力十分强大，尤其适合嗅探数据包中的密码信息。

将下载下来的x-sniff解压到某个目录中，例如“c:\”，然后运行“命令提示符”，在“命令提示符”中进入x-sniff所在的目录，然后输入命令“xsiff.exe -pass -hide -log pass.log”即可（命令含义：在后台运行x-sniff，从数据包中过滤出密码信息，并将嗅探到的密码信息保存到同目录下的pass.log文件中）。

嗅探软件设置完毕，我们就可以正常登录QQ。此时，木马也开始运行起来，但由于我们已经运行x-sniff，木马发出的信息都将被截取。稍等片刻后，进入x-sniff所在的文件夹，打开pass.log，便可以发现x-sniff已



经成功嗅探到邮箱的账户和密码。

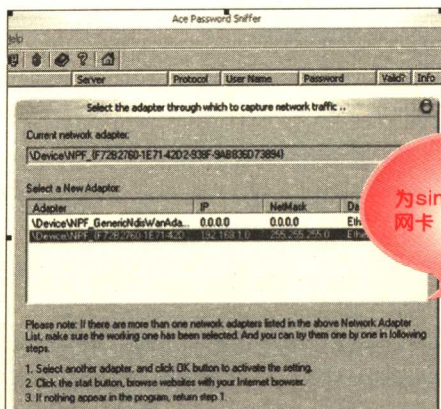


成功截取盗号者邮箱信息

(2) 图形界面的sinffer

可能很多读者对命令行下的东西都有一种恐惧感，所以我们可以使用图形化的嗅探工具来进行嗅探。例如适合新手使用的sinffer。运行sinffer之前，我们需要安装WinPcap驱动，否则sinffer将不能正常运行。到<http://winpcap.polito.it>下载winpcap的安装包，winpcap主要是在驱动层主要作用是获取数据包。执行安装包，这样就能运行winpcap程序了。

运行sinffer。首先我们需要为sinffer.exe指定一块网卡，单击工具栏上的网卡图标，在弹出的窗口中选择自己使用的网卡，点“OK”后即可完成配置。确定以上配置后，单击sinffer工具栏中的“开始”按钮，软件即开始了嗅探工作。



为sinffer绑定网卡