

中国第一黑客团队——鹰派联盟权威推荐

# 黑客

仲治国 张熙 滕大鹏 编著

道可道 非常道  
黑客道 非常「道」

## 七种武器 一百零八招

工欲善其事 必先利其器



黑客之道

# 黑客七种武器一百零八招

仲治国

张熙编著

滕大鹏



山东电子音像出版社出版

## 内容提要

“工欲善其事，必先利其器”，对于一个电脑爱好者来说，手中没有几款得心应手的“兵器”怎么能在安全领域这个波谲云诡的江湖放心行走？

《黑客七种武器一百零八招》为广大读者披露了黑客使用的七种武器共108招：孔雀翎——扫描与反扫描、长生剑——控制与反控制、多情环——嗅探与欺骗、碧玉刀——加密与解密、霸王枪——暴力攻击与恶意绑架、离别钩——安全分析与入侵检测、拳头——账号盗取与安全防范。只有深入了解黑客的使用的工具，我们才能针锋相对地进行防范！

本手册采用全程图解、攻防兼备的形式，让即便是菜鸟级的读者也可以随学随用、即查即知，最终成就一名合格的网络安全高手！

**警告：**文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

## 光盘内容

1. 《黑客七种武器一百零八招》电子书
2. 天网防火墙(电脑报专用版)
3. Windows 系统补丁集
4. 电脑报超人气栏目《黑客营》精彩文章荟萃
5. 中国鹰派联盟会歌

书 名：黑客七种武器一百零八招  
编 著：仲治国 张 熙 滕大鹏  
执行编辑：李 勇 曾 茜 朱治军  
封面设计：刘学敏  
责任编辑：李 萍  
监 制：时均建  
出版单位：山东电子音像出版社  
地 址：济南市胜利大街39号  
邮政编码：250001  
电 话：(0531)2060055-7616  
发 行：山东电子音像出版社  
经 销：各地新华书店、报刊亭  
C D 生产：北京中联光碟有限公司  
文本印刷：重庆大学建大印刷厂  
开本规格：787mm × 1092mm 1/16 21印张 250千字  
版 本 号：ISBN 7-89491-173-9  
版 次：2005年4月第1版 2005年4月第1次印刷  
定 价：28.00元(1CD+手册)



# Preface

黑客之道

道可道，非常道  
黑客道，非常“道”

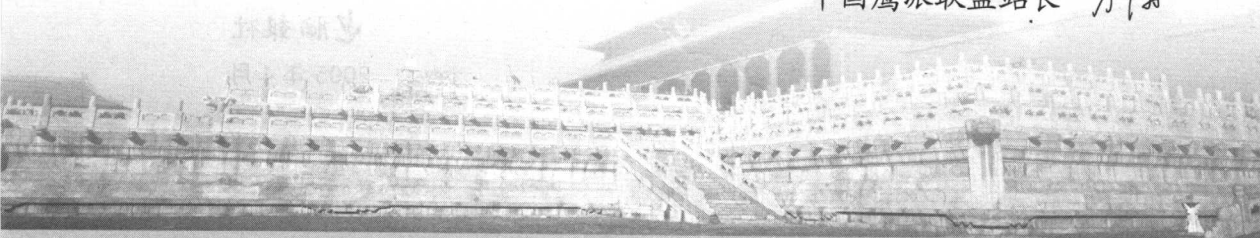
“黑暗给了我黑色的眼睛，我却要用它来寻找光明”——这是已故诗人顾城的名句，现在已成为中国鹰派联盟的会歌。黑客本亦寻常人，网络大势造英雄！是非成败凭人论，彰显正义天地间。黑客者，潇洒自如，原作网络时代侠士讲，受人景仰；现如今却龙蛇混杂，作秩序破坏者讲，遭人唾弃。对黑客的是非善恶，众说纷纭、莫衷一是，但是无庸讳言，黑客已经成为一种不容忽视的网络力量。

那么，究竟神龙见首不见尾的黑客都有哪些神秘之处？他们的“潘多拉魔盒”里面都装着什么宝贝？他们是否真的像电影大片《黑客帝国》中的主人公那样，都拥有一身超凡脱俗的本领？在《黑客之道》系列丛书中，将以三十六计、七十二变和一百零八招的庞大阵容，给读者诸君解读黑客精神！

其中《黑客攻防三十六计》一书是以我国最负盛名的兵学奇书《三十六计》为模式，从三十六个方面详尽地进行了实战式的黑客入侵与防御演练；《黑客对抗七十二变》一书则与当今黑客层出不穷的奇思异谋相符，正所谓“千变万化，不离其宗”，其攻城略地之七十二般变化即使如齐天大圣般神通广大，也飞不出本书的五指山；《黑客七种武器一百零八招》则是源出武侠巨匠古龙大师的扛鼎之作《七种武器》，但本书根据当前黑客最流行的一百零八种工具，做了进一步的细化与讲解。

《黑客之道》系列丛书倾情奉献目前最流行的黑客奇谋与利器大全，数百个攻防实战演习，超强的黑客铁三角组合将使成就网络安全高手变得易如反掌，你还犹豫什么呢？在网络的沙场上金戈铁马驰骋纵横，在安全领域中扬鞭奋蹄大显身手，这些不正是我们梦寐以求的吗？

中国鹰派联盟站长 万涛



## 《黑客七种武器一百零八招》

针对电脑安全，拥有一款得心应手的工具软件非常重要。虽然顶尖级别的黑客是不屑于使用什么工具软件的——他们大概已达到“草木竹石皆为剑，摘叶飞花俱伤人”的境界，但对于更多普通的电脑用户来说，无论是对抗黑客的入侵与攻击，还是做好系统的安全管理，都离不开各种安全工具。

《黑客七种武器一百零八招》从古龙名著《七种武器》演绎而来，在《黑客七种武器一百零八招》中，将为读者诸君展现七大类多达一百零八种的安全攻防武器，它们都是成为安全高手道路上必知、必会、必用的工具。熟悉并掌握了它们，即使是最初对安全领域一无所知的人士，也可以快速成为一名安全高手！

- ◆ 一本108个网络攻防实战演习的精彩瞬间展现！
- ◆ 一本完全摒弃了枯燥理论的实战宝典！
- ◆ 一个让你走近真实的网络安全的机会！
- ◆ 众多资深网络安全高手倾力打造的网络攻防真经！
- ◆ 一本值得收藏的攻防工具使用与技巧速查手册！

本书较好地解决了安全管理人员终日东奔西找去寻求安全工具的尴尬，使之可以省却大量寻找、试用的时间——只需按照本书的工具应用范围提示，即可快速查找到自己所需要的工具。

七种武器在手，任你笑傲网络江湖；一百零八招艺成，问谁是安全领域真英雄！

### 必要建议：

基于部分网络安全工具使用不当会给计算机带来安全隐患这一特殊性考虑，所以请广大读者首先在虚拟机中对一些颇具危险性的网络安全工具使用几遍，当有了可以完全控制的把握后再在本机中使用，否则极有可能会让你的计算机产生一些安全隐患。

在本书编写过程中，中国鹰派联盟在技术上给予了大力支持，在此表示特别感谢！

电脑报社

2005年4月

## 第一篇 “孔雀翎”——扫描与反扫描

<b>第1招</b> X-scan 查本机隐患 .....	2
一、用 X-scan 查看本机 IP 地址 .....	2
二、添加 IP 地址 .....	2
三、开始扫描 .....	3
四、高级设置 .....	4
<b>第2招</b> 妙用流光扫描主机漏洞 .....	8
一、认识流光 .....	8
二、批量主机扫描 .....	8
三、指定漏洞扫描 .....	12
<b>第3招</b> LANSS 扫描局域网安全隐患 .....	15
一、扫描局域网内计算机的安全漏洞 .....	15
二、查看扫描结果 .....	19
<b>第4招</b> Windows 系统安全检测仪 .....	20
一、MBSA 特色功能 .....	20
二、安装设置 MBSA .....	21
三、检测单台计算机 .....	23
四、检测多台计算机 .....	24
<b>第5招</b> 用诺顿网络安全特警在线扫描 .....	25
一、登录网站扫描 .....	25
二、查看检测结果 .....	27
<b>第6招</b> RPC 漏洞扫描器 .....	28
一、RPC 漏洞带来的危险 .....	28
二、深入浅出 RPC .....	28
三、扫描 RPC 漏洞 .....	29
<b>第7招</b> WebDAVScan 漏洞扫描器 .....	30
一、WebDAV 漏洞解析 .....	30
二、扫描 WebDAV 漏洞 .....	31
三、解决方法 .....	32
<b>第8招</b> SQL 安全扫描器 Hscan .....	32
一、危险的由来 .....	32
二、黑客入侵解析 .....	33
<b>第9招</b> 用 ProtectX 防御扫描器追踪 .....	34
一、ProtectX 实用组件解析 .....	35
二、防御扫描器攻击 .....	36

<b>第 10 招</b> 网页安全扫描器 .....	37
一、漏洞扫描 .....	37
二、查看安全漏洞 .....	38
<b>第 11 招</b> 玩转 NC 监控与扫描功能 .....	40
一、监听本地计算机端口数据 .....	40
二、监听远程计算机端口信息 .....	41
三、将 NC 作为扫描器使用 .....	42
<b>第 12 招</b> 用 RegShot 监控注册表修改 .....	42
一、认识 RegShot .....	43
二、注册表的监控 .....	43
<b>第 13 招</b> 文件操作监控大师 .....	46
一、捕获事件 .....	47
二、事件的识别 .....	47
三、存储数据 .....	48
<b>第 14 招</b> 还有什么我不知道——Real Spy Monitor .....	49
一、添加使用密码 .....	49
二、设置弹出热键 .....	50
三、监控浏览过的网站 .....	51
四、键盘输入内容监控 .....	52
五、程序执行情况监控 .....	53
六、即时截图监控 .....	54
<b>第 15 招</b> 局域网监控大师 LanSee .....	55
一、搜索计算机 .....	55
二、搜索共享资源 .....	56
三、检查端口连接状态 .....	56

## 第二篇 “长生剑”——控制与反控制

<b>第 16 招</b> 妙用“冰河陷阱”防冰河 .....	59
一、冰河陷阱简介 .....	59
二、清除冰河木马 .....	60
三、诱骗黑客 .....	61
<b>第 17 招</b> 木马克星 .....	63
一、检测木马 .....	64
二、激活防火墙 .....	65
三、强大的扫描功能 .....	65
<b>第 18 招</b> 使用 SuperScan 监控端口 .....	66
一、认识 SuperScan .....	66
二、监控端口 .....	67
<b>第 19 招</b> 用 WinVNC 体验远程控制 .....	69
一、配置服务器 .....	69
二、客户端连接 .....	70
<b>第 20 招</b> 用 TFTP 实现上传下载 .....	71

一、安装 TFTP 服务 .....	71
二、使用 TFTP 服务 .....	73
三、防范 TFTP 入侵 .....	74
<b>第 21 招 使用 WinShell 实现远程控制 .....</b>	<b>74</b>
一、WinShell 简介 .....	75
二、配置服务器端 .....	75
<b>第 22 招 使用 QuickIP 进行多点控制 .....</b>	<b>78</b>
一、QuickIP 功能介绍 .....	78
二、设置 QuickIP 服务器端 .....	78
三、设置 QuickIP 客户端 .....	80
四、远程控制 .....	81
<b>第 23 招 巧用屏幕间谍定时抓屏 .....</b>	<b>83</b>
一、屏幕截图 .....	83
二、设置抓取时间间隔 .....	84
<b>第 24 招 实战命令行下的远程控制 PsExec .....</b>	<b>86</b>
一、进入 Telnet 操作状态 .....	86
二、执行本地程序 .....	87
三、启动远程服务 .....	87
<b>第 25 招 用灰鸽子透过局域网进行远程管理 .....</b>	<b>87</b>
一、灰鸽子简介 .....	87
二、灰鸽子远程管理 .....	88
三、卸载灰鸽子 .....	90
<b>第 26 招 感受 Serv-U 的远程控制 .....</b>	<b>92</b>
一、服务器配置 .....	93
二、工作站配置 .....	94
<b>第 27 招 用 URLy Warning 监控远程信息 .....</b>	<b>95</b>
一、URLy Warning 简介 .....	95
二、URLy Warning 远程监控 .....	96
<b>第 28 招 用 Simple Bind 自制远程控制程序 .....</b>	<b>97</b>
一、合并 EXE 文件 .....	97
二、修改合并后的 EXE 文件图标 .....	98
<b>第 29 招 远程控制好帮手 PcAnywhere .....</b>	<b>99</b>
一、PcAnywhere 的安装 .....	99
二、PcAnywhere 的基本设置 .....	100
三、使用 PcAnywhere 进行远程控制 .....	101
<b>第 30 招 探密远程开启视频的木马 .....</b>	<b>105</b>
一、远程开启视频的必要性 .....	105
二、如何开启远程视频 .....	105
三、服务器端的清除 .....	108

## 第三篇 “多情环”——嗅探与欺骗

<b>第 31 招 经典嗅探器之 Iris .....</b>	<b>110</b>
---------------------------------	------------



一、Iris 的工作原理 .....	110
二、用 Iris 捕获数据 .....	111
三、怎样防御 Iris 的嗅探 .....	114
<b>第 32 招   经典嗅探器之 NetXray .....</b>	<b>114</b>
一、认识 NetXray .....	114
二、NetXray 捕获数据 .....	115
三、NetXray 其他功能 .....	117
<b>第 33 招   经典嗅探器之 SpyNet Sniffer .....</b>	<b>118</b>
一、用 SpyNet Sniffer 播放音乐或视频 .....	118
二、用 SpyNet Sniffer 捕获下载地址 .....	118
<b>第 34 招   艾菲网页侦探 .....</b>	<b>119</b>
一、艾菲网页侦探的基本设置 .....	119
二、捕获网页内容 .....	120
三、下载软件的监控 .....	121
<b>第 35 招   用 MSN Sniffer 监听聊天内容 .....</b>	<b>122</b>
一、MSN Sniffer 简介 .....	122
二、监控聊天内容 .....	122
<b>第 36 招   影片嗅探也疯狂 .....</b>	<b>123</b>
一、影片嗅探的基本功能 .....	123
二、影片嗅探的配置 .....	123
三、搜索影片下载地址 .....	124
<b>第 37 招   影片嗅探之影音神探 .....</b>	<b>124</b>
一、初识“神探” .....	124
二、“神探”的基本设置 .....	125
三、影片下载实战 .....	125
<b>第 38 招   命令行下的嗅探器 WinDump .....</b>	<b>126</b>
一、WinDump 简介 .....	126
二、WinDump 监听网卡 .....	126
<b>第 39 招   看不见的网管专家 Sniffer Portable .....</b>	<b>129</b>
一、Sniffer Portable 基本功能 .....	129
二、安装要点与基本设置 .....	130
三、数据捕获 .....	132
<b>第 40 招   无线嗅探器之 NetStumbler .....</b>	<b>133</b>
一、无线安全的重要性 .....	133
二、Netstumbler 嗅探无线网络 .....	133
三、拒绝笔记本 ad-hoc 方式接入 .....	135
<b>第 41 招   用网络执法官拒绝恶意接入 .....</b>	<b>136</b>
一、网络执法官安装 .....	136
二、查看目标计算机属性 .....	137
三、批量保存目标主机信息 .....	137
四、设置关键主机 .....	138
五、设置默认权限 .....	139
六、禁止目标计算机访问网络 .....	140

<b>第 42 招</b>	傻瓜化的蜜罐 KFSensor .....	140
	一、蜜罐设置 .....	140
	二、蜜罐诱捕 .....	141
<b>第 43 招</b>	用 SyGate 突破封锁上网 .....	141
	一、实现的基础 .....	142
	二、设置 SyGate 服务器 .....	142
	三、SyGate 客户端设定 .....	143
<b>第 44 招</b>	E 时代隐私卫士—— Surfsecret .....	144
	一、安装 Surfsecret .....	145
	二、常规选项的设置 .....	145
	三、浏览器清理 .....	146
<b>第 45 招</b>	用 Privacy Defender 实现安全的网际畅游 .....	147
	一、Privacy Defender 的安全演示 .....	147
	二、Privacy Defender 清除上网痕迹 .....	147

## 第四篇 “碧玉刀”——加密与解密

<b>第 46 招</b>	Foxmail 邮件查看器 .....	150
	一、Foxmail 邮件查看器简介 .....	150
	二、查看 Foxmail 加密账户邮件 .....	150
<b>第 47 招</b>	ACCESS 密码查看器 .....	151
	一、ACCESS 文件加密 .....	152
	二、ACCESS 文件解密 .....	152
<b>第 48 招</b>	密码时代终结者 Cain .....	153
	一、解除 PWL 密码 .....	153
	二、解除拨号连接密码 .....	155
<b>第 49 招</b>	MD5 密码转换器 .....	155
	一、什么是 MD5 密码 .....	156
	二、MD5 密码转换器应用实战 .....	156
<b>第 50 招</b>	“WordKey” 恢复 Word 密码 .....	157
	一、创建加密文件 .....	157
	二、使用 WordKey 解密 .....	158
<b>第 51 招</b>	Batch HTML Encryptor 加密网页 .....	159
	一、认识 Batch HTML Encryptor .....	159
	二、Batch HTML Encryptor 加密网页 .....	159
<b>第 52 招</b>	ERD Commander 2003 恢复 XP 密码 .....	161
	一、创建并使用 ERD 启动系统 .....	161
	二、使用 LockSmith “开锁” .....	163
<b>第 53 招</b>	应用程序加密专家 PrivateEXE .....	164
	一、认识 PrivateEXE .....	164

二、PrivateEXE 加密应用程序 .....	165
<b>第 54 招</b> 超级密码卫士保存密码 .....	166
一、超级密码卫士简介 .....	166
二、建立密码库保存密码 .....	166
<b>第 55 招</b> “私人磁盘”隐藏大文件 .....	168
一、认识“私人磁盘” .....	168
二、大文件的隐藏 .....	168
<b>第 56 招</b> 黑雨密码探测器恢复邮箱密码 .....	170
一、邮箱密码恢复的原理 .....	170
二、黑雨密码探测器的功能 .....	170
三、邮箱密码的恢复 .....	171
<b>第 57 招</b> RAR Password Cracker 恢复 RAR 密码 .....	172
一、创建加密文件 .....	172
二、恢复 RAR 文件密码 .....	173
<b>第 58 招</b> 巧用“渗透”将秘密藏在图片中 .....	176
一、渗透原理 .....	176
二、文件加密 .....	176
三、文件解密 .....	178
<b>第 59 招</b> 系统全面加密大师 PC Security .....	179
一、锁定驱动器 .....	179
二、锁定系统 .....	180
三、验证加密效果 .....	183
<b>第 60 招</b> 超级桌面锁 .....	183
一、生成后门口令 .....	184
二、设置登录口令 .....	184

## 第五篇 “霸王枪”——暴力攻击与恶意绑架

<b>第 61 招</b> IP 炸弹工具 IP Hacker .....	186
一、防范攻击 Windows 98 .....	187
二、防范攻击 Windows NT .....	187
<b>第 62 招</b> 邮箱炸弹亿虎 Email 群发大师 .....	188
一、亿虎 Email 群发大师基本应用 .....	188
二、亿虎 Email 群发大师高级应用 .....	189
三、邮件炸弹的防范 .....	190
<b>第 63 招</b> OICQ 炸弹——QQ 砸门机 .....	190
一、QQ 砸门机的使用 .....	191
二、防范 QQ 砸门机 .....	192
<b>第 64 招</b> MSN 消息攻击机 .....	192

一、MSN 消息攻击原理 .....	192
二、防范攻击 .....	193
<b>第 65 招</b> Ping 攻击的安全防范 .....	194
一、Ping 命令详解 .....	194
二、防范被人 Ping .....	196
<b>第 66 招</b> Printer 溢出工具 IIS5Exploit .....	197
一、什么是溢出 .....	198
二、微软的公告 .....	198
三、Printer 溢出实例 .....	198
<b>第 67 招</b> IDQ 攻击溢出工具 .....	200
一、漏洞描述 .....	200
二、入侵 IDQ 漏洞 .....	200
三、防范 IDQ 攻击 .....	201
<b>第 68 招</b> RPC 溢出工具 .....	201
一、漏洞描述 .....	202
二、入侵实战 .....	202
三、防范方法 .....	205
<b>第 69 招</b> Messenger 溢出工具 .....	205
一、漏洞简介 .....	205
二、漏洞扫描 .....	206
三、溢出方法 .....	207
四、漏洞修补方法 .....	209
<b>第 70 招</b> Windows logon 溢出工具体验 .....	210
一、漏洞初识 .....	210
二、远程溢出 .....	210
三、漏洞防范 .....	212
<b>第 71 招</b> Google Toolbar 解除恶意绑架 .....	212
一、Google Toolbar 简介 .....	212
二、解除恶意绑架 .....	213
<b>第 72 招</b> SpyBot Search & Destroy 实战间谍软件 .....	215
一、SpyBot Search & Destroy 简介 .....	215
二、揪出隐藏的间谍 .....	215
三、让系统具有“免疫”功能 .....	217
<b>第 73 招</b> 防暴专家 AtGuard .....	218
一、AtGuard 简介 .....	218
二、AtGuard 的个性化设置 .....	219
<b>第 74 招</b> 浏览器绑架克星 HijackThis .....	223
一、系统检测 .....	223
二、编号识别 .....	224
<b>第 75 招</b> IE 防火墙 .....	225
一、窗口管理全攻略 .....	225
二、修复 IE .....	226

# 第六篇 “离别钩”——安全分析与入侵检测

<b>第 76 招</b>   天网防火墙 .....	228
一、天网防火墙初步应用 .....	228
二、天网安全设置 .....	228
三、检查并修复系统漏洞 .....	231
<b>第 77 招</b>   上传文件检测之思易 ASP 木马追捕 .....	232
一、思易 ASP 木马追捕简介 .....	232
二、检测网页木马 .....	232
<b>第 78 招</b>   单机版入侵检测系统 NID .....	234
一、NID 简介 .....	234
二、NID 基本设置 .....	234
三、NID 规则设置与使用 .....	235
<b>第 79 招</b>   日志分析利器 WebTrends .....	237
一、创建日志站点 .....	238
二、日志报表的生成 .....	239
三、查看日志 .....	240
<b>第 80 招</b>   远程日志清除工具之 elsave .....	240
一、用小榕的 elsave 远程清除日志 .....	241
二、手工清除日志法 .....	241
<b>第 81 招</b>   远程维护日志之“计算机管理”功能 .....	243
一、启动远程连接 .....	243
二、常见日志解释 .....	244
<b>第 82 招</b>   用 IIS Lock Tool 检测网站安全 .....	246
一、IIS Lock Tool 简介 .....	247
二、IIS Lock Tool 的基本应用 .....	247
三、IIS Lock Tool 的高级设置 .....	248
<b>第 83 招</b>   诺顿网络安全特警 .....	251
一、配置安全特警 .....	251
二、启用诺顿网络安全特警 .....	252
三、程序扫描 .....	254
四、隐私控制 .....	255
五、在线安全检测 .....	256
六、封锁恶意 IP .....	257
七、端口防范 .....	258
<b>第 84 招</b>   路由安全检测 SolarWinds .....	259
一、基本常识 .....	259
二、检查路由器的安全隐患 .....	259
<b>第 85 招</b>   单机版极品安全卫士 CATHER .....	262
一、安装要点 .....	262
二、用 CATHER 进行安全分析 .....	262
<b>第 86 招</b>   大家闺秀 ISA Server .....	266

一、ISA Server 简介	266
二、ISA Server 安装要点	266
三、阻断病毒通信	267

## 第 87 招 利用 WAS 检测网站承受压力 271

一、什么是 DDoS 攻击	272
二、Web Application Stress Tool (WAS) 简介	273
三、检测网站的承受压力	273
四、数据分析	277

## 第 88 招 用无处藏身检测恶意 IP 280

一、发现恶意 IP	280
二、追踪恶意 IP	280

## 第 89 招 免费的专业防火墙 Kerio 281

一、Kerio 基本应用	281
二、调整 Kerio 过滤机制	282

## 第 90 招 专业入侵检测系统 BlackICE 284

一、初识 BlackICE	284
二、BlackICE 的安装必知	284
三、BlackICE 的应用实战	285

## 第 91 招 用 VisualRoute 检测通信故障 286

一、VisualRoute 简介	287
二、分析与跟踪	287

# 第七篇 “拳头”——账号盗取与安全防范

## 第 92 招 当心“QQ 掠夺者”盗取 QQ 290

一、认识 QQ 掠夺者	290
二、QQ 盗取曝光	290
三、防范 QQ 掠夺者	291

## 第 93 招 防范“QQ 破密使者”盗取 QQ 291

一、本地破解 QQ 破密使者	292
二、防范 QQ 破密使者	293

## 第 94 招 在线破解 QQ 揭秘 294

一、在线破解	294
二、QQExplorer 在线破解及其防范	294

## 第 95 招 解读“密码使者”截获 QQ 295

一、初识“密码使者”	295
二、“密码使者”作案剖析	295
三、应对措施	297

## 第 96 招 来自“QQ 枪手”的攻击 297

一、QQ 枪手简介	297
二、QQ 枪手盗号探密	297

## 第 97 招 “QQ 机器人”盗号也疯狂 298

一、安装运行 QQ 机器人	298
---------------	-----

二、配置QQ机器人 .....	299
<b>第98招</b> 防范“OICQ密码轻松盗”监听 .....	300
一、曝光盗号方法 .....	300
二、防范OICQ密码轻松盗的监听 .....	301
<b>第99招</b> 提防“好友号好好盗”攻击 .....	301
一、认识远程盗号工具 .....	301
二、黑客盗号步骤剖析 .....	301
<b>第100招</b> “QQ远控精灵”远程控制计算机 .....	303
一、QQ远控精灵介绍 .....	303
二、远程控制实例 .....	303
三、防范QQ远控精灵 .....	305
<b>第101招</b> 识破“QQ密码保护”的骗局 .....	305
一、认识“QQ密码反保精灵” .....	306
二、“QQ密码反保精灵”骗术曝光 .....	306
三、防范QQ密码保护的骗术 .....	306
<b>第102招</b> 用“防盗专家”为QQ保驾护航 .....	307
一、认识防盗专家 .....	307
二、自动关闭QQ广告 .....	307
三、取回密码 .....	307
四、内核修改 .....	308
五、病毒查杀 .....	309
六、无敌外挂 .....	309
七、其他功能 .....	310
<b>第103招</b> 伸向MSN的黑手——Msn Messenger Hack .....	310
一、认识Msn Messenger Hack .....	310
二、MSN盗取揭秘 .....	311
三、防范Msn Messenger Hack .....	312
<b>第104招</b> MSN密码查看帮凶——MessenPass .....	313
一、MessenPass简介 .....	313
二、查看MSN密码解析 .....	313
三、防范MessenPass .....	313
<b>第105招</b> 防范E话通靓号被盗 .....	314
一、解读E话通号码被盗 .....	314
二、防范E话通靓号被盗 .....	316
<b>第106招</b> 联众密码也受伤 .....	316
一、当心“联众密码监听器”的监听 .....	316
二、找回丢失的联众密码 .....	317
<b>第107招</b> 防范“传奇密码邮差” .....	317
一、传奇密码盗取方式揭秘 .....	317
二、警惕“传奇密码邮差” .....	318
三、拒绝传奇盗号 .....	318
<b>第108招</b> 揪出内鬼——密码监听器 .....	319
一、“密码监听器”盗号披露 .....	320
二、找出“卧底”拒绝监听 .....	322

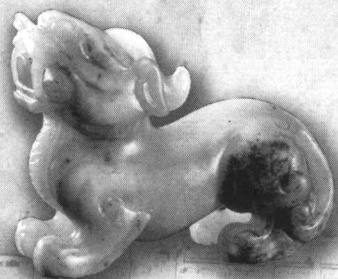
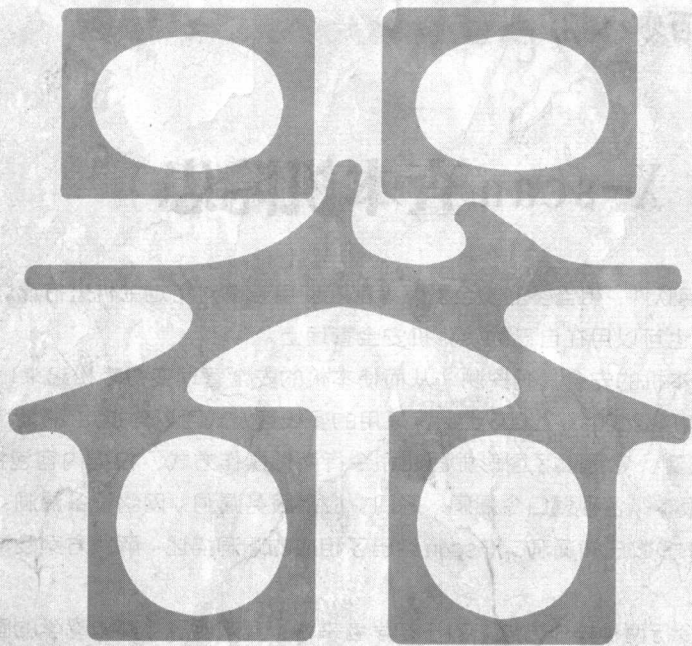
# 第一篇

## 孔雀翎——扫描与反扫描

信心，看看扫描器上无数的漏洞，即使你是菜鸟也会信心十足。

安全扫描工具是把双刃剑，黑客利用它可以扫描别人的系统，而系统管理员掌握它以后又可以有效地防范黑客入侵。在本篇中，将从系统漏洞扫描、局域网安全扫描、文件动态扫描、注册表变动扫描、恶意扫描的安全防范等多个方面，系统地给大家讲解关于「扫描」应用的知识！

HACKER





# 第 1 招 X-scan 查本机隐患

X-scan 作为国内最著名的扫描软件，相当多的安全爱好者都在使用它来对特定主机进行漏洞扫描与探测。但你知道吗，X-scan 也可以用在自己的计算机安全管理上。

利用 X-scan，可以高效实现本机的安全漏洞探测，从而使本机的安全管理变得轻松起来！

X-scan 可以安装在 Windows NT4/2000/XP/2003 上，其采用的多线程方式可以对指定 IP 地址段（或单机）进行高速的安全漏洞检测，它提供了图形界面和命令行两种操作方式，扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，X-scan 给出了相应的漏洞描述、解决方案及详细描述链接。

X-scan 提供了图形界面和命令行两种操作方式。对于初学者来说，直观明了、简单易学的图形界面操作显然是最适合不过的了，所以下面将着重讲解图形界面下的使用方法。

黑客之道

## 一、用 X-scan 查看本机 IP 地址

首先需要指定扫描的 IP 范围。由于是探测本机，所以应首先在“运行栏”中输入“cmd”命令打开“命令提示符窗口”，在命令行中输入“IPconfig”命令，来查知本机的当前 IP 地址。如图 1-1 所示：

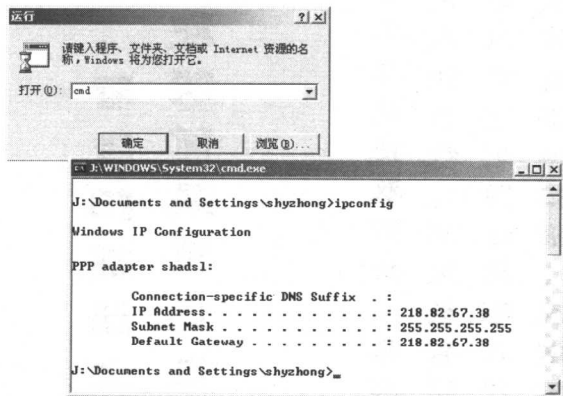


图 1-1

从返回的信息可以看出，当前本机的 IP 地址为“218.82.67.38”。

## 二、添加 IP 地址

在得到了本机的 IP 地址后，就可以在 X-scan 主窗口点击“设置→扫描参数”菜单项，准备将 IP 地址添加到 X-scan 中。如图 1-2 所示：