电脑报 总策划

黑客之道

黑客

七种武器一百零八招

工欲善其事 必先利其器

【道可道 非常道 黑客道 非常『道』】

中国第一黑客团队——鹰派联盟权威推荐

仲治国 张熙 滕大鹏 编著

山东电子音像出版社出版

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！

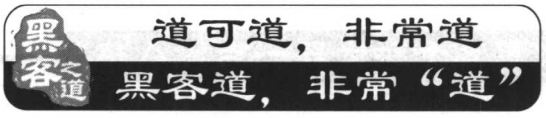
警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

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
CD 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 万清

《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

目录

CONTENTS

黑客七种武器一百零八招 HACKER

第一篇 “孔雀翎”——扫描与反扫描

第二篇 “长生剑”——控制与反控制

第四篇 “碧玉刀”——加密与解密

第六篇 “离别钩”——安全分析与入侵检测

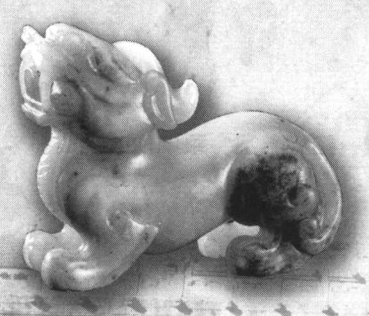
第七篇 “拳头”—— 账号盗取与安全防范

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四个方面，系统地给大家讲解关于「扫描」应用的知识！



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。

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：

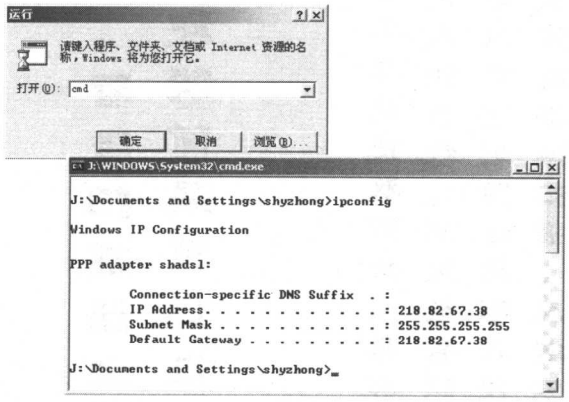


图1-1

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：