电脑报 总策划

黑客之道

黑客对抗七十二变

事急用奇 兵危使诈

【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 编著

山东电子音像出版社出版

黑客之道

黑客对抗七十二变

仲治国
张熙 编著

山东电子音像出版社出版

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 万清

《黑客对抗七十二变》

网络欺骗是黑客惯用的伎俩，同时也是安全人士应对黑客的有效对策之一，黑客和安全人士在相互欺“诈”中不断较量，演绎着一段又一段的网络“无间道”！

网络欺骗是对网络安全领域的一个重大挑战，它让大家看到了信息系统存在有价值的、可利用的安全弱点：黑客利用这些安全弱点使出胜似齐天大圣“七十二变”的手段来获取利益；安全人士则故布悬疑、设置陷阱，等着黑客往“圈”里钻……黑客是如何利用各种手段进行欺骗的，安全人士又该如何进行有效的防范，这就是本书要解决的问题。

对于普通网民来说，“网络欺骗”这个词似乎有些陌生，但它确确实实就发生在大家的身边：

你正在访问的网页被黑客篡改了，网页上的信息都是虚假的！黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。正在输入的邮箱用户名和密码的登录对话框是伪造的，当用户名和密码输入完毕后，你的邮箱也就“拱手送人”了！

网络欺骗是一把双刃剑，对于黑客来说，网络欺骗是“攻网略机”的绝佳工具；而对于安全人士来说，网络欺骗可成为追捕黑客的利器——安全人士使用欺骗术可以增加入侵者的工作量和入侵难度，甚至可以用来将黑客锁定并捉拿归案！

网络欺骗是一种入侵技术，也是一种实用且强大的安全防范技术，非常值得深入研究和学习。这项技术中较复杂的有：Web欺骗、DNS欺骗、Cookies欺骗等；简单一些的则包括木马的伪装、IP代理等。黑客可以利用欺骗技术从种种意想不到的角度来完成入侵，而普通用户则可以利用欺骗技术很好地起到保护自身的作用。在《黑客对抗七十二变》中，你将了解到种种匪夷所思的网络欺骗手段和相应切实有效的安全防范措施，让你的网络安全知识得到飞速提升。

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

CONTENTS

目录

黑客 HACKER 对抗七十二变

第一篇 实战账户欺骗

第1变 Administrator 账户的安全管理 2
一、防范更改账户名 3
二、防范伪造陷阱账户 5

第2变 改头换面的 Guest 账户 9
一、虚假的管理员账户 9
二、识破混迹管理员组的 Guest 账户 11
三、Guest 账户的安全管理 11

第3变 识别非法终端管理员 14
一、什么是终端服务 14
二、终端服务器的连接 14
三、非法终端管理员的识别 16

第4变 揪出密码大盗的伪装账户 21
一、本地植入密码大盗 21
二、远程植入密码大盗 23
三、密码大盗防范对策 24

第5变 账户克隆探秘 27
一、Regedit 与 Regedit32 注册表编辑器的区别 27
二、在图形界面建立隐藏的超级用户 29

第6变 邮箱账户欺骗的防范 33
一、邮箱账户的伪造 33
二、巧妙隐藏邮箱账户 35
三、垃圾邮件的防范 35
四、重要邮箱的使用原则 39
五、追踪伪造邮箱账户的发件人 40

第7变 Foxmail 账户解除与防范 40
一、邮箱使用口令的安全防范 41
二、邮箱账户密码的防范 42

第8变 管理员账户解除方法剖析 43
一、利用默认的 Administrator 账户登录系统 43
二、创建密码恢复盘 43
三、通过双系统删除 SAM 文件 47
四、借助第三方密码恢复软件 47

第二篇　病毒与木马欺骗术

第 9 变　变型病毒原理分析与识别 53
一、什么是变型病毒 53
二、变型病毒的特征及分类 53
三、变型引擎的工作原理 54
四、查杀病毒的技巧 56

第 10 变　宏病毒及其防治方法 58
一、宏病毒的基础知识 58
二、什么是宏病毒 59
三、宏病毒的判断方法 59
四、宏病毒的防范和清除 61

第 11 变　网游外挂完全解密 62
一、木马式外挂解除 62
二、加速式外挂解除 64
三、封包式外挂解除 68

第 12 变　冰河陷阱欺骗术 70
一、清除 TXTFile 型关联冰河 70
二、卸载 EXEFile 型关联冰河 72
三、用“冰河陷阱”反攻冰河 73

第 13 变　揭露文本欺骗术 75
一、文本炸弹破坏机理 75
二、文本炸弹的安全防范 78

第 14 变　剖析广外幽灵的隐身 79
一、什么是广外幽灵 80
二、广外幽灵的工作原理 80
三、广外幽灵的清除方法 81

第 15 变　C. I. A 远程控制的深度应用 82
一、初识 C. I. A 82
二、C. I. A 的服务端定制 82
三、如何用 C. I. A 来远程控制 85

第 16 变　真假 Desktop. ini 和 *. htt 文件 87
一、“新欢乐时光”病毒的特征 87
二、清除“新欢乐时光”病毒 88
三、利用 Folder. htt 文件加密文件夹 89
四、用 Desktop. ini 和 Folder. htt 个性化文件夹 90

第三篇　网络代理与黑客追踪

第 17 变　利用代理服务器下载资源 94

一、什么是代理服务器 94
二、代理服务器的几种类型 94
三、如何使用代理服务器 94

第 18 变 利用代理猎手大变脸 98

一、“代理猎手”的安装 98
二、“代理猎手”的基本设置 98
三、“代理猎手”的使用方法 100

第 19 变 用 SocksOnline 变身上网 101

一、SocksOnline 简介 101
二、SocksOnline 操作指南 101

第 20 变 利用代理服务器变幻上网 103

一、代理工具选择 103
二、代理工具安装与设置 103
三、代理工具连通性测试 106

第 21 变 IP 动态自由切换 107

一、代理应用工具选择 108
二、代理应用工具实际操作过程 108

第 22 变 架设 Sock5 代理隐藏 IP 110

一、IP 隐藏原理 110
二、Sock5 代理实际操作过程 111

第 23 变 防范远程跳板式攻击 113

一、扫描选择目标 113
二、代理的架设 114

第 24 变 实战 IP 追踪术 115

一、网络定位 115
二、如何查知他人 IP 地址 116

第四篇 网络欺诈与恶意代码

第 25 变 浏览器执行 exe 文件应变实战 118

一、动鲨网页木马生成器简介 118
二、动鲨网页木马实战 118
三、SEASKY7 网页木马实战 120
四、如何隐藏网页木马 121

第 26 变 防范变幻网页木马 121

一、观察进程寻找木马 122
二、如何用杀毒软件进行快速诊断 122
三、木马的下载与运行 123
四、MIME 简介 124
五、如何清除木马 126
六、网页木马防范方法 126

第 27 变 妙用防问权限保卫 FSO 组件 129
一、神秘的 ASP 文件 129
二、最大危害调查报告 130
三、FSO 组件的保卫奇招 131
第 28 变 剖析执行本地程序的代码 137
一、恶意格式化防范实战 137
二、剖析光驱调用代码 141
第 29 变 解密 Cookies 欺骗 142
一、Cookies 的建立 142
二、Cookies 的读取 144
三、Cookies 欺骗的实现 145
第 30 变 防范恶意代码篡改注册表 147
一、修改 IE 的标题栏 147
二、控制 IE 右键菜单 148
三、搜索引擎的变换 149
四、解除注册表锁定 151
五、防范注册表被修改 152
第 31 变 设置 IE 防范恶意代码 153
一、禁用 IE 的自动登录 153
二、关闭 IE 的颜色足迹 154
三、删除 IE 的 Cookies 155
四、关闭 IE 的自动完成功能 155
五、IE 的安全区域设置 156
第 32 变 QQ 恶意代码防范 156
一、让 QQ 崩溃的代码 156
二、QQ 恶意代码剖析 157
三、QQ 恶意代码防范方法 159

第五篇 网络游戏欺骗术

第 33 变 网络游戏“盗号”骗术防范 162
一、防范木马盗取账号 162
二、防范远程控制方式盗号 163
三、当心利用系统漏洞盗号 164
第 34 变 网站充值欺骗术防范 164
一、欺骗原理 164
二、防范方法 164
三、提高防范意识 165
第 35 变 用内存补丁进行传奇极差外挂验证 166
一、传奇极差外挂介绍 166

二、传奇极差外挂验证 166

第 36 变 防范本地账户解除 169

一、勿用“自动记住密码” 169
二、本地账户破解防范方法 170

第 37 变 CS 的作弊与反作弊 170

一、典型作弊程序介绍 170
二、常见反作弊程序介绍 176

第 38 变 警惕局域网监听 176

一、局域网监听原理 176
二、防范局域网监听 177

第 39 变 透视免费外挂 178

一、免费外挂的剖析 178
二、SQL 指令植入式攻击防范方法 181

第 40 变 DoS 攻击 CS 服务器及防范 183

一、DoS 攻击及其局限性 183
二、DoS 攻击 CS 服务器的实现 183
三、DoS 攻击的防范方法 184

第六篇 网络资源欺骗

第 41 变 加密网页下载实战 186

一、网页加密实战 186
二、下载加密网页实战 189

第 42 变 加密式 Flash 动画下载实战 195

一、查看 Flash 网页源文件 196
二、用 MyIE 查看页面链接 196
三、用 FlashGet 的“站点资源探测器”下载 Flash 动画 198
四、查看 IE 临时文件夹定位 Flash 动画地址 198

第 43 变 特定区域资源下载实战 200

一、什么是特定区域 200
二、防范 IP“欺骗” 200

第 44 变 妙用代理软件共享 IP 204

一、代理软件简介 205
二、代理服务器的设置 205
三、共享实战 205

第 45 变 用肉鸡打造免费网站空间 210

一、什么是肉鸡 210
二、肉鸡的查找 210

三、如何登录肉鸡 211
四、域名申请与设置 212
五、设置服务器 213

第 46 变 突破“封锁”下影片 216

一、搜索下载法 216
二、断线法下载 217
三、巧妙从 ASX 文件中找到下载网址 218
四、下载受保护的流媒体文件 220

第 47 变 FTP 资源搜索与利用 221

一、什么是 FTP 222
二、FTP 资源大搜捕 223

第 48 变 私有化网络“肉鸡”揭秘 228

一、私有型“肉鸡”的重要性 228
二、如何选择“肉鸡” 228
三、“私有化”进程 228

第七篇 加密与解密

第 49 变 解析注册表中的密码 233

一、限制密码最小长度 233
二、限制密码类型 234
三、禁止更改密码 235
四、删除屏幕保护密码 236

第 50 变 制作加密光盘 236

一、加密原理 237
二、加密实战 237
三、刻录进程 239
四、CryptCD 高级应用 240

第 51 变 图片摇身一变成木马 241

一、图片与程序的“捆绑” 241
二、COPY 命令也玩捆绑 242

第 52 变 Windows XP 内置加密工具大揭秘 243

一、加密文件系统 EFS 的应用 243
二、程序访问权限加密及管理 246
三、二级加密 Syskey 249

第 53 变 IP 隐藏保护组合拳 251

一、什么是隐藏 IP 251
二、以假乱真藏 IP 253
三、修改注册表藏 IP 254
四、使用代理藏 IP 255
五、使用提供匿名冲浪服务的网站 255

第 54 变 隐私保护全攻略 256
一、清除操作“痕迹”基本功 256
二、让网站无从窃密——Cookies 的管理 257
三、让隐私数据无法恢复 257
第 55 变 开机加密软盘自己做 259
一、在 Windows 98 中创建加密软盘 259
二、在 Windows XP 中创建开机软盘 261
第 56 变 FTP“秘密通道”完全解析 263
一、必备条件 264
二、制作实战 264
三、加密 FTP 的使用 265
四、隐藏措施 265

第八篇 网络“间谍”实战

第 57 变 SpyBot Search & Destroy 实战间谍软件 267
一、SpyBot Search & Destroy 简介 267
二、使用实战 267
三、对下载软件的监控 268
四、粉碎间谍程序 269
五、查找启动项中的间谍 269
第 58 变 AD-Aware 让间谍程序消失无踪 270
一、间谍软件的危害 270
二、Ad-Aware 应用实战 270
第 59 变 清除服务器中的间谍 272
一、什么是 ASP 木马 272
二、ASP 木马运行条件 272
三、ASP 木马防范实战 272
第 60 变 全面解析隐藏虚拟主页 276
一、隐藏虚拟主页的建立 276
二、保护虚拟目录中的文件 278
第 61 变 DcomRpc 漏洞溢出入侵与防范 280
一、什么是 Dcom 和 Rpc 280
二、什么是溢出入侵 281
三、DcomRpc 漏洞入侵解析 282
四、DcomRpc 漏洞安全防范 283
第 62 变 局域网的间谍——嗅探 286
一、嗅探之 FTP 口令获取 286
二、嗅探的防范 287
第 63 变 通过事件查看器捉“贼” 288

一、事件查看器的基本使用 289
二、事件查看器查获“间谍”实例剖析 289

第 64 变 密罐——安能辨我是雌雄 290

一、什么是蜜罐 290
二、蜜罐陷阱的典型例子 291
三、个人用户密罐系统的实现 292
四、监视的实现 293

第九篇 系统安全设置

第 65 变 组策略安全设置 295

一、组策略概述 295
二、组策略安全实战 295

第 66 变 Windows 2000 系统加固指南 299

一、基本安全加固原则 299
二、“制订”系统安全措施技巧 299
三、使用不同厂商产品加固系统安全 299

第 67 变 Windows XP 加固秘笈 301

一、消灭安装时的危险因素 301
二、Windows 基本安全设置 302
三、Windows 的非常规防范措施 304

第 68 变 Windows Server 2003 安全策略 310

一、安全配置与分析组件 311
二、激活“系统还原”功能 313

第 69 变 数据的备份与还原 314

一、数据的备份 314
二、数据的还原 315
三、恢复软盘的使用 316

第 70 变 服务器数据库的备份与还原 316

一、备份的意义 316
二、AD 数据库备份 316
三、AD 数据库还原 317

第 71 变 加强 IIS 安全机制的策略 318

一、基本安全策略 318
二、高级防护策略 321

第 72 变 用诺顿网络安全特警保卫系统 323

一、诺顿网络安全特警的安装 323
二、诺顿网络安全特警的使用 323
三、程序扫描 324
四、隐私保护 324

第一篇

实战账户欺骗

用户账户在网络安全中的位置无与伦比，想进行任何操作，只要有相应权限的用户账户，都可以轻而易举地实现！

黑客盗取账户的主要手段归纳为以下几种：伪造Administrator账户、利用Guest账户混入管理员组、假冒终端管理员、植入密码大盗、账户克隆、盗取邮箱账户、破解Foxmail账户、破解系统管理员口令。本篇将一一详解它们的来龙去脉，让你能将账户这个开启系统之门的金钥匙紧握在手！

第1变 Administrator账户的安全管理

Administrator是系统安装后默认的系统管理员账户，而系统管理员则具有对系统进行一切管理的权限。

以Windows XP为例，系统管理员可以管理Windows XP中所有的用户；可以安装和卸载系统内核级的程序，包括内置或第三方程序、网络设置、硬件驱动等；可以使用系统中所有的功能。系统管理员与普通受限用户的权限区别如图1-1所示：

	计算机管理员	受限用户
安装程序和硬件	√	
进行系统范围的更改	√	
访问和读取所有非私人文件	√	
创建与删除用户帐户。	√	
更改其他人的帐户	√	
更改自己的帐户名或类型	√	
更改自己的图片	√	√
创建、更改或删除自己的密码	√	√

图 1-1

由此可知，系统管理员的权限也就是系统中最高的权限，所以Administrator账户的重要性可想而知。由于Administrator账户处于一个比较特殊的地位——系统默认管理员账户，轻易无法删除，所以绝大多数的系统管理员都使用了这个默认的管理员账户，至少是未对该账户进行较深一级的保护措施。

通常，扫描软件都是先针对Administrator账户进行密码猜解，如果不对Administrator账户进行适当保护将有多么危险！如图1-2所示：

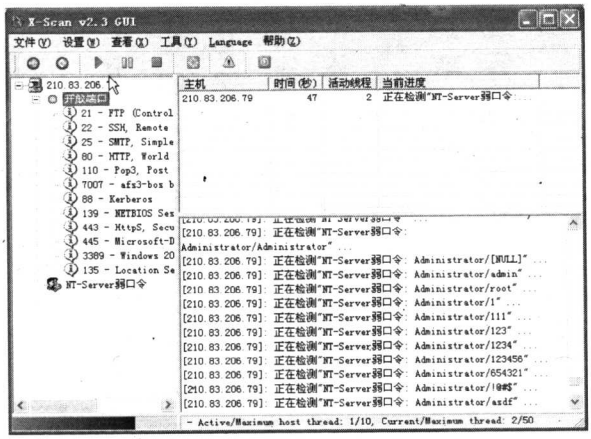


图 1-2

一、防范更改账户名

针对Administrator账户潜在的危险，可以采取一些操作简单也很实用的方法来解决这个问题，如将该账户更名，以降低遭受攻击的可能性。

依次单击“开始→控制面板→管理工具”，打开“计算机管理”窗口。如图1-3所示：

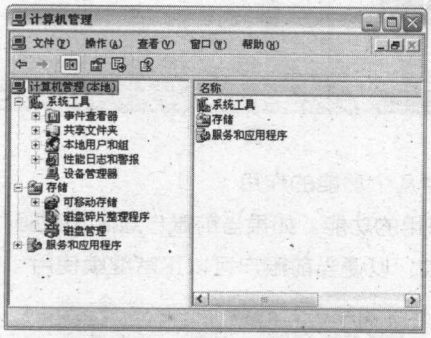


图 1-3

逐层单击依次展开“计算机管理（本地）→系统工具→本地用户和组→用户”，在右侧的用户列表中可以看到Administrator账户名的存在。如图1-4所示：

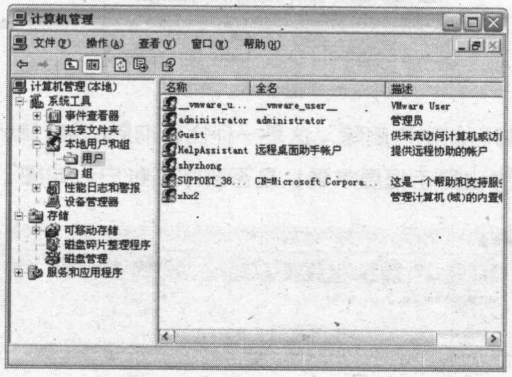


图 1-4

从图中可以看出Administrator账户的描述是“管理员”。现在来删除它，使用鼠标右键选中单击Administrator账户，将会弹出右键菜单。如图1-5所示：

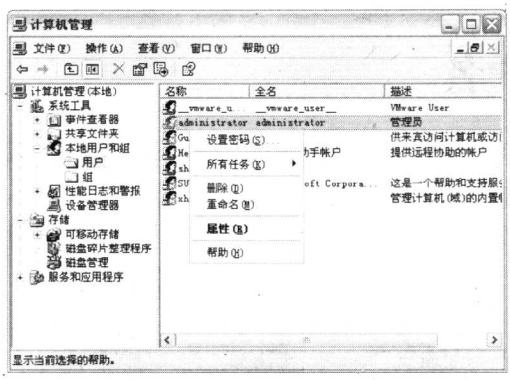


图 1-5

现在来熟悉一下这个菜单中几个功能的作用：

设置密码：这是一个非常有用的功能。如果当前账户遗忘了密码，可以使用其他账户登录，使用这项功能将当前账户密码更改，以便当前账户可以正常继续使用。如图 1-6 所示：

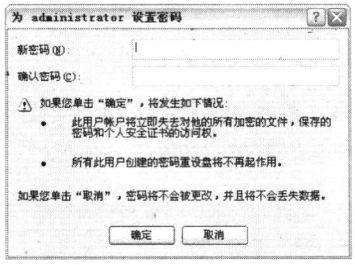


图 1-6

删除：显然它的作用是将当前账户删除，这是一种比较彻底的针对默认管理员账户进行安全管理的措施。单击“删除”将弹出提示框要求确认是否删除该账户。如图 1-7 所示：

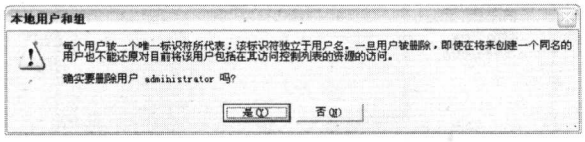


图 1-7

单击“是”按钮，Administrator 账户将会被自动删除，这一点立即就可以从“计算机管理”窗口中的用户列表中看出。如图 1-8 所示：

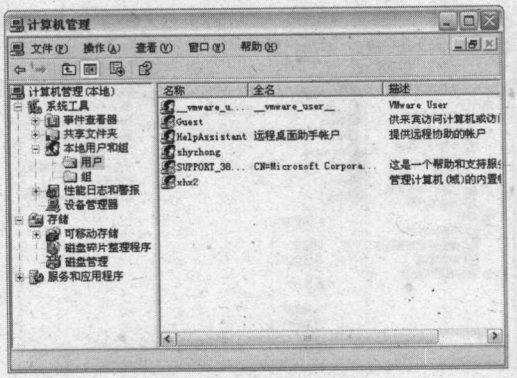


图 1-8

重命名：此功能可以被用作对 Administrator 账户进行伪装，比如将 Administrator 账户名更改为从账户名上无法辨识出属于管理员组的“xhx”等，这样一来就会在一定程度上迷惑入侵者。如图 1-9 所示：

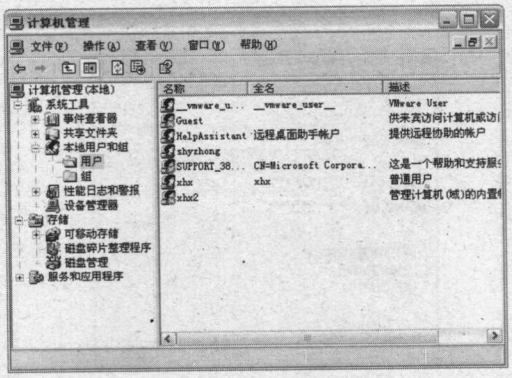
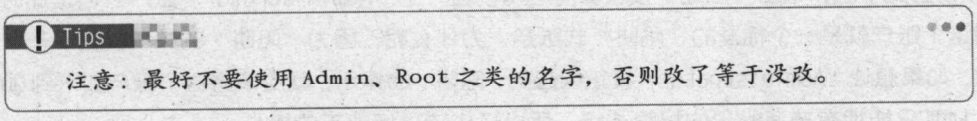


图 1-9



二、防范伪造陷阱账户

比“重命名”伪装更胜一筹的方法就是另建一个“Administrator”的陷阱账号，不赋予任何权限，加上一个超过 10 位的超级复杂密码，并对该账户启用审核。这就能使一些水平不是较高的黑客徒劳。方法是：

(1) 在用户列表的空白处单击鼠标右键，在弹出的菜单中选择“新用户”。如图 1-10 所示：