电脑报 总策划

新手入门

黑客

鹰派联盟权威推荐
中国第一黑客团队

攻防36计

上兵伐谋 不战而屈人之兵

【谋略·技巧篇】

仲治国 编著

挑战黑客

远程控制运筹帷幄
木马病毒秘密潜入
扫描嗅探守株待兔
黑客追踪雁过留声
日志擦除踏雪无痕
密码破译穷追不舍
跳板攻击隔山打牛
网络炸弹赶尽杀绝

超值光盘

价值98元正版软件大礼包
华夏黑客同盟视频教程
Windows优化工具
系统升级补丁
漏洞扫描工具
数据加密工具

山东电子音像出版社出版

攻防36计

【谋略·技巧篇】

仲治国 编著

山东电子音像出版社出版

内容提要

《黑客攻防36计》是“黑客道”系列图书中的“谋略技巧篇”，全书以我国古代卓越的兵书《三十六计》的谋略精髓为指引，以初、中级电脑安全人员的角度，从36个方面详细剖析了网络安全与黑客攻防的实战技巧，为读者揭开黑客世界的神秘面纱。

全书内容涵盖聊天工具攻防、系统账号密码保护、系统漏洞攻防、黑客扫描与嗅探、IP地址追踪、病毒木马攻防、文件加密与破解、远程控制等。为了方便读者更好地理解这三十六条计谋，在图书的编排中，每一计都引入了一个相关的历史故事，让你在掌握兵法奇谋的同时，轻松应对黑客来袭。

本书既可以作为初、中级读者的安全类入门读物，也可以作为资深网管和黑客的案头必备参考手册。

多媒体教学光盘运行说明

运行环境：Windows 98/Me/2000/XP/2003；

操作说明：光盘放入光驱后会自动运行，也可以打开光盘目录，运行hacker.exe文件即可；

光盘内容：图书配套软件以及精彩黑客攻防视频教学（参见“多媒体光盘内容简介”页）。

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！

书　　名：黑客攻防36计
编　　著：仲治国
执行编辑：李　勇　何　磊
封面设计：程　佳
责任编辑：李　萍
监　　制：吕美亮
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)82098390
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：重庆现代彩色书报印务有限公司
开本规格：787mm × 1092mm　1/16　17印张　250千字
版 本 号：ISBN 978-7-89481-003-8
版　　次：2007年7月第1版　2007年7月第1次印刷
定　　价：28.00元(1CD+配套书)

序 Preface

计谋迭出，胸藏攻防先见之明
谈笑之间，指点网络诡诈真伪

网络就是战场，安全就是用兵。

战场上硝烟弥漫，鲜血迸溅；网络中黑客针锋相对，明争暗斗！

黑客世界的刀光剑影总让人感到神秘莫测。

正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

“黑客道”丛书自2005年推出以来，得到了很多读者的喜爱和好评，多次荣登全国图书畅销排行榜，图书历经多次加印，累计销售达20万册，创下黑客类图书的多个NO.1：

第一套兵法战术与电脑安全相结合的黑客类图书

第一套讲故事与授谋略相结合的黑客图书

第一套将古代兵法完美演绎的黑客实战宝典

……

应读者的要求，再版的“黑客道”丛书进行了全新修订：增加了最新出现的各种黑客技术和黑客工具的应用内容，新版“黑客道”将带给大家更加实用的黑客技巧与安全方案，让你完全了解网络安全之道，有效防范黑客攻击。

一名技艺高超的黑客无非体现在以下两方面：其一是娴熟的黑客工具应用，其二是独到的谋略技巧施展。**“黑客道”**丛书正是从以上两个方面的黑客攻防必备技能展开。丛书内容设置为：

《黑客攻防36计》（谋略●技巧篇）：以我国最负盛名的神奇兵书**《三十六计》**为蓝本，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，将古代兵法韬略在黑客攻击防范中体现得淋漓尽致！

《黑客7种武器攻防108招》（工具●实战篇）：源自武侠巨匠古龙大师的扛鼎之作**《七种武器》**，并结合当前黑客最流行的一百零八种工具进行了详细的讲解。

黑客其实就这么几招，有效防范黑客入侵也并非只是专家的绝活，是要你有兴趣和决心，你一样能行！

最后，衷心地祝愿广大读者通过本书的阅读快速了解黑客知识：掌握黑客绝技高招，轻松捍卫网络安全！

编者

2007年7月

多媒体光盘内容简介

● 黑客攻防视频教程

（华夏黑客同盟网站授权）

※Windows 下 apache 服务器的搭建
※Autoruns 的使用
※批处理保护你的 CMD
※认识病毒
※病毒防范技巧
※用 Ipsec 防 DDos
※Windows 下 Guest 帐户的删除
※妙招下载在线娱乐类资源
※FinalData 的使用方法
※Regsnap 的使用技巧

● 电脑报专用版软件

本栏目赠送的是电脑报专用版软件：《FileGee 个人同步备份系统》、《蓝郁系统保护专家》，两款系统安全工具可以让用户有效地保护系统和文件的安全。

● Windows 优化工具

本栏目收录了 Windows 系统优化工具，根据软件灵活的设置，自定义个性化系统。

● 系统升级补丁

本栏目中的系统升级补丁让你尽快修补漏洞，保障系统安全。

● 漏洞扫描工具

本栏目中收录的扫描工具可以高效可靠地扫描出系统潜在漏洞，让用户提早做好安全防范。

● 数据加密工具

本栏目收录的软件让你轻松加密数据，更好地保护隐私。

目录

【胜战计】篇

目录

【敌战计】篇

目录

攻战计篇

目录

混战计篇

目录

【并战计】篇

目录

败战计篇

附录

附录　黑客快速入门的36条锦囊

目录

附录

谋

〈胜战计〉篇

胜战计篇讲述的是处于优势下的作战谋略，作为三十六计的第一部分，胜战计篇倍受世人所推崇。

瞒天过海——反钓鱼网站实战

围魏救赵——数据加密传输保安全

借刀杀人——网页恶意代码防范

以逸待劳——透过服务器破解网站

趁火打劫——远程控制实例演练

声东击西——利用第三方漏洞入侵服务器

第一计 瞒天过海——反钓鱼网站实战

“瞒天过海”被列为三十六计之首，实有其当仁不让之处！试想，单是“过海”已属不易，况且还要“瞒天”？可知，这里包含了多少古人们对天机人事的犀利认识！作为一种示假隐真的疑兵之法，该计利用了人们熟视无睹、常见不疑的心理错觉，以假象迷惑对方，掩饰自己的真正意图，并藉此达到最终目的。“瞒”是计谋的手段，“过”是计谋的目的，就是战胜对手。

在本计网络安全应用中，“瞒天过海”的“瞒”可以理解为恶意网站利用各种方法修改用户的网站访问途径，“过”可以理解为用户被“钓鱼”网站欺骗，进而导致银行帐号与密码被盗的过程。

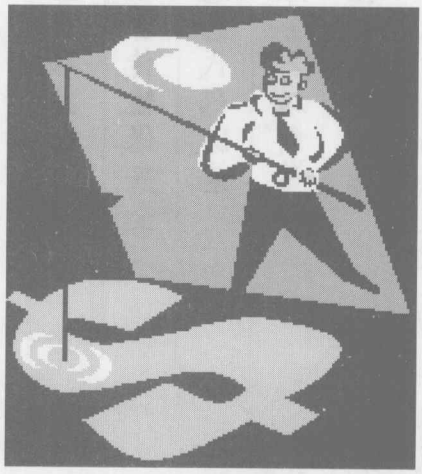
一、当心假冒的在线支付网站

近来，通过网络在线支付款项引发的安全问题屡屡见诸报端：

某网络银行用户甲，在IE浏览器窗口中输入某银行网站网址后，在登录到的网站中输入了帐户名与密码后，却发现无论如何也登录不到银行的帐户中心。用户甲以为是银行的网站系统出现的问题，所以只好通过银行柜台来完成相关的业务。在持续的几天内，用户甲再次登录网上银行时，始终发现问题依旧。

由于一直无法登录到网上银行账户中心，所以用户甲也无法管理自己的账户。如此半月有余，当用户甲再次通过银行柜台办理业务时，突然发现自己的账户中已经只剩下区区几元了，其余的大笔款项已经不翼而飞。在通过银行提供的上网登录银行网站后，他惊讶地发现自己的款竟然是在家里无法登录到网上银行账户中心的那段时间里被提取的。

“为什么我不能登录网上银行的账户中心，别人却可以划走其中的款？”在用户甲百思不得其解的时候，银行的客服人员告诉他可能是被“钓鱼”网站欺骗了！



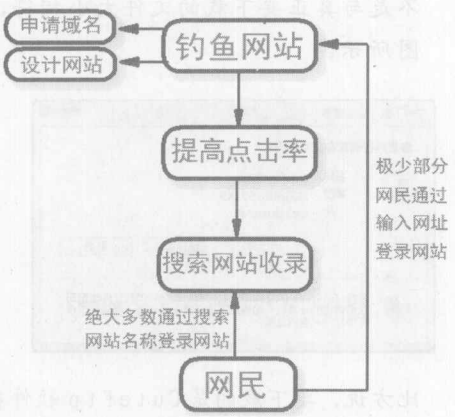
提示

什么是“钓鱼”网站？“钓鱼”网站指的是一些欺诈性的网站，浏览这些网站可能会导致计算机用户泄露个人信息或财务信息。通常，“钓鱼”网站不会去强迫网民访问——它使用了类似于“钓鱼者稳坐台上，静候鱼儿上钩”的方法。故而，我们称这类网站为“钓鱼网站”。

二、揭秘“钓鱼”网站的骗局

常见的仿冒骗局，常常是一个可以提供用户输入个人信息的网站，进而实现用户信息的窃取。这样的骗局在2007年已经被各大媒体曝光多次，如假冒的中国工商银行网站使用的域名为“www.1cbc.com.cn”，它与真正的中国工商银行网站域名“www.icbc.com.cn”只有很小的不同，普通网民很多不会对这点不同而产生怀疑，进而导致了自己的账户信息被窃。

下图给出一个钓鱼网站常用的设局过程：



现在，让我们来解释一下这个过程：

第1步：首先，恶意用户会分析要假冒的网站域名组成部分，并会对域名中最容易让网站产生迷惑的地方下手。比方说，真正的中国工商银行网站域名“www.icbc.com.cn”，那么假冒的中国工商银行网站就可以使用“www.1cbc.com.cn”这个域名。

第2步：在完成域名的申请后，恶意用户会设计一个与要假冒的网站界面完全相同的网站。这样的设计对于稍微熟悉网站美工、制作的人来说，不会存在任何的障碍。

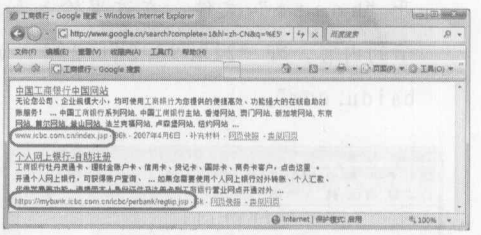
第3步：在完成了网站与域名的设计后，如何才能让网民来访问？通常，恶意用户会通过如下方法来骗取网民来访：

（1）静候网民通过输入网址来访。这种来访的可能性在域名只有微弱差别时，有万分之几的可能性。如果域名相差较大，则可能几乎是等于零。

（2）发送仿冒电子邮件。通过大量发送垃圾邮件，以种种优惠、活动的内容来吸引网民来访，这种方法的成功率为20%甚至更高。

（3）通过病毒的方法。通过在下载量较大的网站、论坛中提供带有病毒的程序，使得网民的IE浏览器自动访问或是修改真实网民的访问途径，来强迫或欺骗网民来访并上当。

（4）通过搜索引擎。这是所有诱骗网民来访方法中的上策，恶意用户要做的事情就是拼命的提高网站的点击率，这样可以让各大搜索引擎自动收录仿冒网站。由于仿冒网站的网站名称与被假冒的网站名称完全一致，所以很容易就会让用户产生有多个服务网站的错觉。在下图中可以看到有些银行自身也会提供多个网站来提供不同的服务。



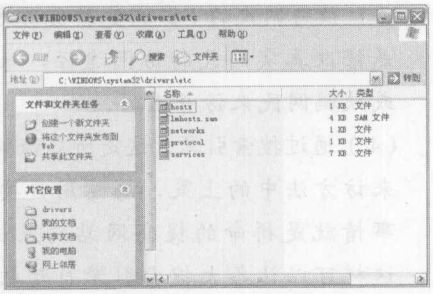
第4步：在网民一不小心被上述的几种方法之一欺骗，并登录到虚假的网站后。很多人都会产生“既然已经到网站，那就输入账户看看还有多少余额”等心理，这样一来就会给仿冒网站有可乘之机了！

三、钓鱼网站制作过程分析

1．钓鱼网站制作过程

现在，让我们来通过一个非常简单的实例看看仿冒网站是如何设计出来的。通过如下方法，可以将网民们输入“http://www.baidu.com”这个网址后访问的网站，自动转向到架设的仿冒网站中。简要的实现过程是：

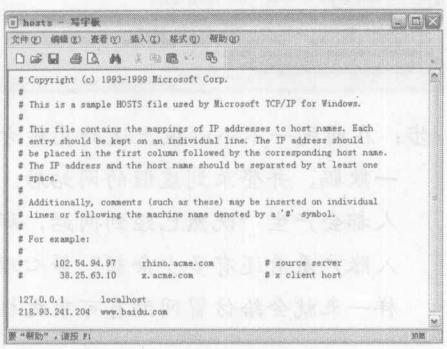
第1步：首先，在“我的电脑”窗中打开“C:\WINDOWS\system32\drivers\etc”文件夹，在这里可以看到有一个“hosts”文件，如图所示。



注意

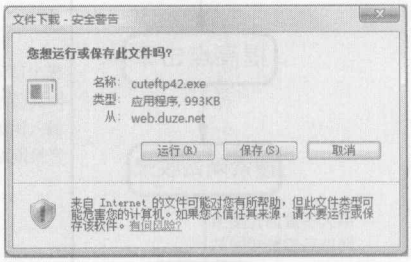
“hosts”文件不具有扩展名，它的内容以明文的方式进行存储。

第2步：接着，运行记事本或写字板程序并打开“hosts”文件，在这里输入如图所示的内容，即“218.93.241.204　www.baidu.com”。



第3步：在完成这个内容的编辑后，编写一个可以将“hosts”文件覆盖用户源文件的exe。在通过邮件附件、网站提供冒名（即提供其他软件的名称，实际上是下载这个exe文件）下载等方法诱骗点击此exe文件，进而实现用户计算机中“C:\WINDOWS\system32\drivers\etc”文件夹下的“hosts”文件的修改。

说到这儿，要提醒读者们注意了。在下载文件时，最好是先使用IE的内置下载功能，先检查一下要下载的文件大小是不是与真正要下载的文件大小相符，如图所示。



比方说，要下载的是Cuteftp软件在网站标出应该有900KB左右，可是弹出的对话框中显示文件只有几KB。那么，这个下载的文件就可能有问题，此时最好的方法就是换个网站下载。

第4步：在网民计算机中的“hosts”文件被覆盖后，当用户在IE浏览器的地址栏输入“http://www.baidu.com”这个网址后，将会自动访问“218.93.241.204”这个IP地址中对应的网站。

看，明明IE浏览器中地址栏里输入的网址是百度搜索引擎网站的网站，可访问的却是别的网站内容。甚至在“命令提示符”窗口中使用Ping命令时，也会因仿冒网站确实存在而使得Ping的结果正常，如图所示。