电脑报 东方工作室

招招先

曝光黑客

入侵攻防、隐私安全 与 密码保护技巧全接触

金鼎图书工作室 编著

招招先 ②

系统漏洞攻击、安全补遗 绝密技巧

QQ密码破解、文件加密 统统上阵

游戏ID、Password 安全防护 新策略

网络各种 行动痕迹 大扫除

网吧上网彻底 突破 各种限制

木马查杀 一网打尽

内、外网络世界 真正全玩透

电子科技大学出版社

曝光黑客

入侵攻防、隐私安全 与 密码保护技巧全接触

金鼎图书工作室 编著

内容提要

黑客现在已经不再是网络世界中高深的“职业”，开始慢慢走向平民化、大众化，各种黑客工具也如雨后春笋般地涌现出来，越来越多的电脑爱好者把黑客当作崇拜的对象，不断学习各种网络攻击技术，不断发掘各种网络安全漏洞，甚至发起网络攻击。现在黑客工具简单易用，就算是不太懂得电脑的人，也就可以使用黑客工具进行攻击。

本书以典型实例的形式向读者揭露黑客常见的攻击技巧，引导电脑爱好者掌握这些黑客技能，并针对这些攻击技巧进行防范。

本书内容丰富、翔实，并以大量的图片为实例进行讲解，是读者通往电脑高手的最佳指南，也是电脑爱好者预防网络攻击的首选指导教材。

图书在版编目（CIP）数据

曝光黑客——入侵攻防、隐私安全与密码保护技巧全揭秘／金鼎工作室编著. —成都：电子科技大学出版社，2004.7

ISBN 7-900651-98-5

曝光黑客——入侵攻防、隐私安全与密码保护技巧全揭秘

金鼎工作室 编著

出　　版：电子科技大学出版社（成都建设北路二段四号　邮编：610054）
责任编辑：陈建军
发　　行：电子科技大学出版社
印　　刷：重庆升光电力印务有限公司
开　　本：787 × 1092　1/16　印张：17　字数：408
版　　次：2004 年 7 月第 1 版
印　　次：2004 年 7 月第 1 次印刷
书　　号：ISBN 7-900651-98-5/TP · 71
定　　价：22.00 元　（1CD+ 配套手册）

序言 *Preface…*

随着时代的发展，信息科技的不断进步，网络已不再是虚无缥缈的世界，这一切都与“黑客”有关。《黑客帝国》的上演，让大家充满了疑惑：我们到底生活在什么世界？其实，电影是生活的缩影，它起源于现实生活但被艺术化。在真正日常生活中的黑客是怎么生活在网络世界中？在网络世界中避免黑客的侵袭需要掌握哪些技巧？黑客高手是怎么使坏的？本书将为你揭晓答案：曝光黑客！

本书内容丰富，实用性强，是面向电脑爱好者的经典产品。结合大量黑客高手的经验，遵照通俗易懂、循序渐进的原则，全面、系统地讲解各种黑客应用技巧及防御手段。全书共分为 9 章，结构安排如下：

第一章　系统入侵与加密

第二章　网络账号、密码攻防策略

第三章　Web 攻防无限制

第四章　内网安全使用技巧

第五章　不要把秘密留在网络上

第六章　小心你的系统秘密

第七章　木马清除不求人

第八章　密码安全恢复新策略

第九章　确保电脑安全的保护神

本书属于“招招先”系列图书之一，由金鼎图书工作室总策划，夏川编辑完成。它延续了该系列图书“实用+ 技巧”的特点，运用大量的操作实例，使读者能够轻松、快速地解决电脑实际应用中的各类问题。

金鼎工作室

2004 年 7 月

曝光黑客 目录

Contents...

Contents...

第九章 确保电脑安全的保护神

第一章 系统入侵与加密

在大多数的黑客入侵案例中，都是首先对系统进行相关的分析，在确定系统存在相应的缺陷、漏洞后，实施入侵操作，获取相应操作权利的口令或者密码，从而顺利地控制整个电脑系统。以上我们可以看出系统和密码安全是很重要的，针对系统和密码的特殊性必须采取相应的应对策略。

1.1 Windows 系统安全分析

Windows 操作系统是现今使用最为广泛的操作平台，从最早的 3.x 版本发展到现在的 Windows 2003，其系统安全性逐渐提高。但这种系统安全性只具有相对性，并不是如微软所宣传的那样绝对安全，正如 2003 年所爆发的 RPC 漏洞危机所造成的恶劣影响。Windows 系统的安全需要依靠不断更新的系统补丁来支持。同时，系统加密也是提升安全性的一个重要途径。

1.1.1 安全缺陷产生的原因

系统漏洞是威胁安全最根本的原因，而这些漏洞是指某些程序（如操作系统、应用程序等）在开发、设计的时候没有对整体的合理性进行周密的考虑，当在程序运行的过程中遇见一个合法的却无法在实际中处理的问题时会引发不可预见的错误。因此系统漏洞也被称之为“安全缺陷”，如果当系统漏洞被恶意利用，就会造成信息泄露、数据丢失、用户权限被恶意窜改等不可估量的后果。

如果想真正了解“安全漏洞”的意思，列举一个例子大家很快就能明白。如在某些特定的条件下，你的电脑不明不白就出现文件丢失、系统死机等非正常现象（系统硬件存在故障除外），这就是“安全漏洞”造成的。

漏洞产生的原因大致可以分为以下 3 种：

1．程序开发者人为设置

某些程序员为了达到不可告人的目的，有意识地在程序的隐蔽处留下各种各样的后门，

以供自己以后使用。

2．由于硬件设备的原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现。

3．受水平、经验和当时安全加密方法所限制

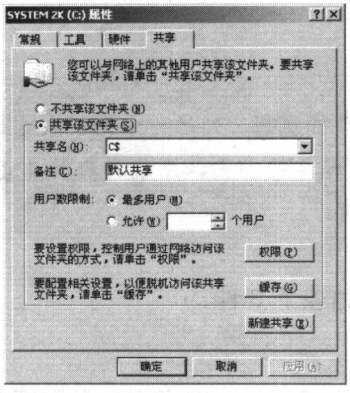
受编程人员的水平、经验和当时安全技术、加密方法所局限，造成程序执行效率降低、非授权用户的权利提升等问题。

1.1.2 系统安全透析

大多数电脑使用者都认为 Windows 系统之所以受到众多黑客的攻击，是因为 Windows 操作系统使用太广泛。除了 Windows 系统外，其他系统好像很少成为黑客攻击的目标。其实，Windows 操作系统本身的设计漏洞才是真正的原因。

微软从一开始就一直提倡“用户所需要的是网络的兼容性和应用程序之间的兼容性”，却从根本上忽略了超强的兼容性会带来不可估量的安全问题，这也就给有恶意企图的黑客提供了方便，造成黑客有机可乘，引发一系列的系统安全危机。

例如，在 Windows 操作系统中的 NetBIOS 就有很鲜明的 Windows 9X 共享密码漏洞，黑客想要进入 Windows 9X 的共享如入无人之境。而号称安全性能极高的 Windows 2000、Windows NT 漏洞更是严重，不仅会泄露当前登录用户的账号和密码，还可以通过 NetBIOS 伪装为当前用户的身份对电脑进行管理。Windows 2000、Windows NT 在默认的情况下，是将系统中所有的硬盘都设置为共享（这种共享是一种隐形共享，没有传统的手形图标，因此一般电脑用户都无法察觉自己的硬盘已经被设置为默认的共享），而几乎所有系统登录用户都是以超级管理员的身份进行操作的，这就更让黑客在伪装身份后变得肆无忌惮。



另外，Windows 服务器的 IIS 服务也被证实是一个超级大漏洞，该漏洞能够让黑客很容易地控制整个电脑，可以随意拒绝服务、泄露信息、泄露源代码、获得更多权限、目录查询、执行任意命令、缓冲溢出执行任意代码等。

在我们使用的电脑中，还存在大量的 IE 浏览器漏洞、Outlook 漏洞、E-mail 服务器漏洞等，这些漏洞一旦被利用就可以让我们的系统瘫痪。

系统漏洞虽然存在，但并不是没有补救措施。只要我们时刻关心操作系统的发展方向，注意更新系统的补丁，谨慎安装和运行一切非正常程序，就可以堵住系统。

1.2 Windows XP 的八大安全操作策略

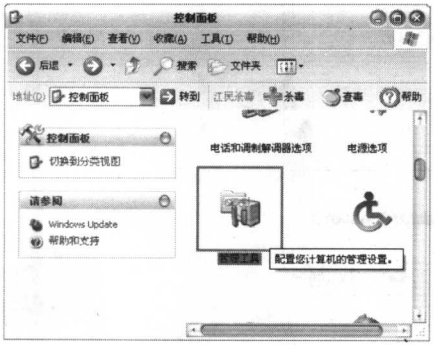
Windows XP 凭借其超强的稳定性和可靠的安全性吸引了众多用户使用它。要想更好地驾御 Windows XP，需要采用以下操作策略。

1. 屏蔽不需要的服务组件

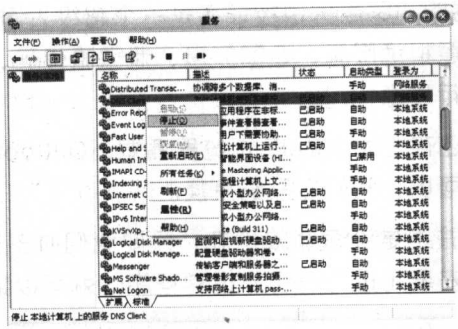
尽管服务组件安装得越多，用户可以享受的服务功能也就越多。但是用户平时使用到的服务组件毕竟还是有限，而那些很少用到的组件不但占用了不少系统资源，会引起系统不稳定外，它还会为黑客的远程入侵提供多种途径，因此我们应该尽量把那些暂不需要的服务组件屏蔽掉。

具体的操作方法为：

（1）在控制面板中找到“管理工具”图标，双击该图标，在打开的窗口中运行“服务”。



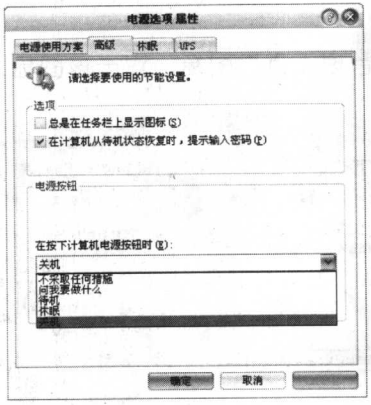
（2）打开“服务”对话框，在该对话框中选中需要屏蔽的程序，并单击鼠标右键，从弹出的快捷菜单中依次选择“属性”和“停止”命令。同时，将“启动类型”设置为“手动”或“已禁用”，这样就可以对指定的服务组件进行屏蔽了。



2. 启用电源保护功能

使用电脑处理文件时，最担心的就是电脑突然掉电，因为这种突然掉电不但会使自己的辛勤劳动成果顷刻间化为乌有，严重的话还能使电脑受到损伤。为了防止各种情况下的意外掉电，保证电脑的安全正常工作，我们应该在电源管理中启用按下电源按钮时询问或直接休眠的功能。

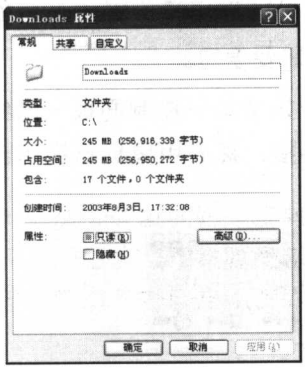
如果要启动电源保护功能，执行“我的电脑→控制面板→电源选项”命令，在弹出的设置框中选择“高级”标签。在对应的标签页面下找到“按下电脑电源按钮时”设置项，然后在设置框中选择“休眠”或者“问我要做什么”选项。如果选择“关机”选项，就相当于没有启用电源保护功能。

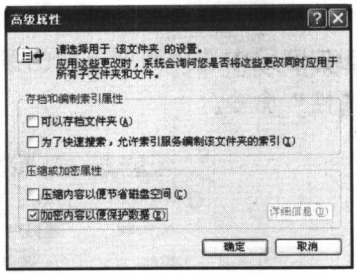


3. 对重要信息进行加密

为防止其他人在使用自己的电脑时，偷看自己存储在电脑中的文件信息，Windows XP 特意为普通用户提供了“文件和文件夹加密”功能，利用该功能我们可以对存储在电脑中的重

要信息进行加密。这样，其他用户在没有密码的情况下将无法访问文件或者文件夹中的内容。在对文件进行加密时，我们首先打开 Windows XP 的资源管理器，然后在资源管理器操作窗口中找到需要进行加密的文件或者文件夹。然后，用鼠标右键单击选中的文件或文件夹，从弹出的快捷菜单中选择“属性”命令，Windows XP 会弹出文件加密对话框。单击对话框中的“常规”标签，然后依次选择“高级→加密内容以便保护数据”就可以了。





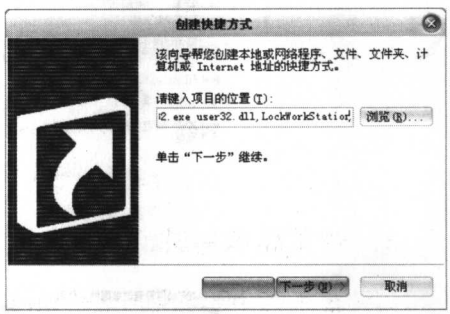
注意：此项策略只能在磁盘格式为 NTFS 的情况下使用。

4. 锁定自己的电脑

如果在使用电脑的过程中因有急事需要短暂离开时，许多人因担心自己的电脑会被别人占用，往往会采取关机的方式。频繁地开关操作对电脑是不利的，有没有办法做到既不关机又能防止其他人使用自己的电脑呢？答案是肯定的。我们可以通过双击桌面快捷方式的办法，迅速锁定键盘和显示器，而无须使用“Ctrl+Alt+Del”组合键或屏幕保护程序。在锁定电脑时，可以参照如下的步骤来执行：

(1) 用鼠标右键单击 Windows XP 的桌面，在右键菜单中执行“新建→快捷方式”。

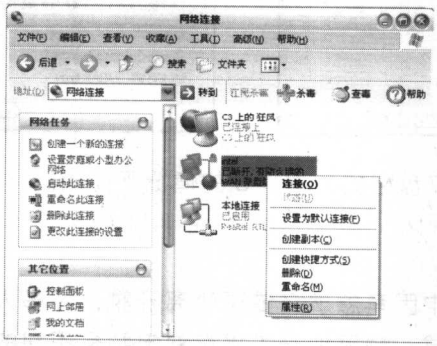
(2) 随后按照屏幕提示，在命令行的文本框中输入“rundll32.exe user32.dll, Lock Work Station”命令字符，再在随后的向导窗口中输入对应该快捷方式的具体名称，在这里为方便以后调用，可以直接为该快捷方式取名为“锁定电脑”。以后只要双击桌面上的“锁定电脑”，就可以达到锁定的目的了。



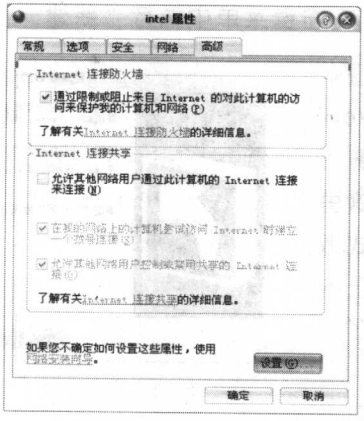
5. 使用“连接防火墙”功能

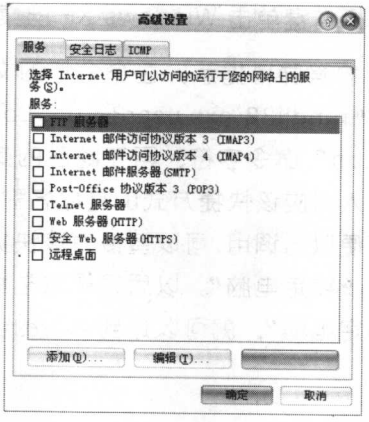
在网络时代中，病毒的传播方式、传播速度和破坏力发生了巨大的变化，而且黑客行为也正在全世界范围内流行。为了防止病毒和黑客的随意入侵，不少用户在电脑中安装了防火墙。而 Windows XP 就加入了免费的“Internet 连接防火墙”功能，利用该功能，Windows XP 能对出入系统的所有信息进行动态数据包筛选，允许系统同意访问的人与数据进入自己的内部网络，同时将不允许的用户与数据拒之门外，最大限度地阻止网络中的黑客来访问自己的网络，防止他们随意更改、移动甚至删除网络上的重要信息。

（1）在使用“连接防火墙”功能时，执行“开始菜单→控制面板→网络连接”命令，然后从弹出的窗口中选择需要上网的拨号连接，然后用鼠标右键单击该连接图标，并选择“属性”命令。



（2）在随后弹出的拨号属性窗口中再单击“高级”标签，在对应标签的页面中选中“Internet 连接防火墙”选项，然后再单击对应防火墙的“设置”按钮，根据自己的要求设置一下防火墙，以便防火墙能更高效地工作。



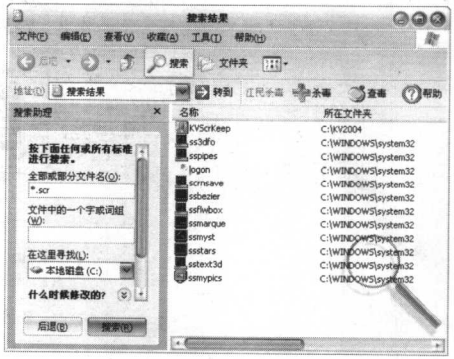


6. 随时启用屏保程序

看到“屏保”二字，大家肯定会很自然地想到电脑中的屏幕保护程序，它主要是通过采用不同方式轮流显示指定图片来达到屏幕保护的目的。但是只有当不操作电脑达到事先设置的时间后，系统才会启动屏幕保护程序，如果我们想在任意指定的时间内启动屏幕保护程序，该怎么办呢？我们可以按照下面的操作方法来实现：

（1）在 Windows XP 的开始菜单中，执行“开始→搜索”命令。

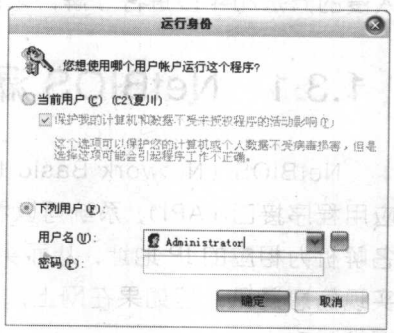
（2）在弹出的搜索对话框中，点击“所有文件和文件夹”类型，并在对应文件名的文本框中输入“*.scr”字符，再在搜索范围下拉列表中，选择“本机磁盘（C:）”或电脑上存储系统文件的驱动器，最后单击“搜索”按钮。



（3）在找到的屏幕保护程序列表中，选择需要的屏保程序，然后给这个屏保程序建立一个存放在桌面上的快捷方式，以后要启动屏保程序时直接用鼠标双击桌面上的屏保快捷方式。

7. 为自己分配管理权限

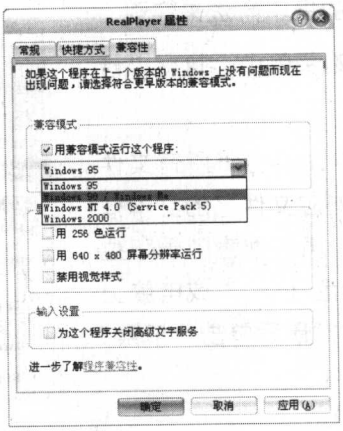
安装在 Windows XP 操作系统中的许多程序，都要求用户具有一定的管理权限才能让用户使用程序，因此为了能够使用好程序，我们有时需要为自己临时分配一个访问程序的管理权限。在分配管理权限时，我们可以先以普通用户身份登录到 Windows XP 的系统中，然后用鼠标右键单击程序安装文件，同时按住键盘上的 Shift 键，从随后出现的快捷菜单中点击“运行方式”，最后在弹出的窗口中输入具有相应管理权限的用户名和密码就可以了。



8. 消除系统假死现象

在操作 Windows XP 中的应用程序时，由于操作不当或者系统本身的问题，导致了操作的程序很长时间没有响应，许多人以为电脑肯定是死机了，于是不少人选择了直接关机或者

使用“Ctrl+Alt+Delete”组合键来重新启动电脑。其实在 Windows XP 中，有些不能正常运行的程序会引起系统任务栏的假死，这种现象主要是由于当前执行的程序与系统无法兼容引起的。遇到这种现象时，我们可以找到该程序的执行文件，然后单击鼠标右键，在弹出的对话框中选择“兼容性”标签，再在“兼容模式”下选择需要的相应运行环境。



1.3 系统漏洞攻防

既然系统存在漏洞，并且某些漏洞是致命性的，那么我们就必须采取一些办法来防御和补救，不让黑客借助这些漏洞来破坏我们的电脑。在进行防御操作前，我们必须对黑客如何入侵的方法和手段进行了解，才能真正达到防御的目的。

1.3.1 NetBIOS 漏洞的入侵和防御

NetBIOS（Network Basic Input Output System）就是网络基本输入输出系统，是一种应用程序接口（API），系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式将 NetBIOS 名解析为相应的 IP 地址，从而实现信息通讯。在局域网内使用 NetBIOS 协议可以非常方便地实现信息通讯，但如果在网上，NetBIOS 就相当于一个后门程序，黑客可以利用 NetBIOS 漏洞发起攻击。

当我们在接入 Internet 时，实际上只需要安装 TCP/IP 协议，但在安装的时候，NetBIOS 被系统作为默认设置已经安装到系统中，因此电脑就具有了 NetBIOS 本身的开放性，139 端口被打开，进一步来说，就是在我们不知不觉中，网络中的电脑已经被默认打开了一个很危险的“后门”，通过这个危险的“后门”，黑客可以利用一些特殊的工具轻松地扫描出我们的