教你安全用电脑:让操作系统更安全稳定Microsoft认证考试
 电脑和网络给我们的生活带来了很大的方便，但随之而来的安全问题也是层出不穷，各种木马病毒日益猖獗，挂马网站的数量也增长迅速，要是我们的电脑中了招，小则导致一些应用程序无法正常使用，大则会被黑客盗走如银行账号密码、个人隐私信息等重要内容，到那时候再亡羊补牢可就晚了。 Windows是目前使用人数最多的操作系统，但Windows的稳定性和安全性却都是很差的，近段时间经常能够看到Windows曝出漏洞的消息，也正说明了这一点，对于未知漏洞目前还没有一个真正有效的防御措施，但对于Windows的已知漏洞，在装好新系统的第一时间我们就应着手为系统打上补丁。 给系统打补丁也有很多种方法，目前大部分的杀毒软件都带有一些系统维护工具，因此，我们可以直接用杀毒软件提供的维护工具来检查系统漏洞并为其打上补丁。以瑞星杀毒软件的“ 瑞星卡卡安全助手 ”为例，扫描、下载和安装补丁都非常简单，基本已经做到了“ 全自动 ”化。 首先，打开瑞星卡卡安全助手后，在“ 常用 ”菜单下选择“ 漏洞扫描与修复 ”，软件便自动对系统进行扫描。扫描结果会告诉用户当前系统中存在几个漏洞，此时点击“ 详细信息 ”。 漏洞扫描结果 在扫描出的补丁列表中将显示所有未安装补丁的安装要求、下载进度（开始下载后显示进度条）、危险等级、漏洞名称、漏洞简介、描述及下载链接。我们可以点击每个补丁右侧的“ 下载 ”链接单独下载补丁，也可以直接将所有补丁全选，点击“ 修

复漏洞 ”进行修复。 下载及安装补丁文件 这里需要提醒大家，如果补丁的安装要求中显示为 “ 独占 ”，那么该补丁是无法与其它补丁同时安装的，需要我们单独下载安装。 补丁的下载速度根据每台电脑的联网情况会有所不同，所有补丁下载完后，便自动开始安装，整个过程无需人工操作。因此即使你的电脑中需要安装的补丁比较多，也不用一直守在电脑旁边。 当看到 “ 修复漏洞结束 ” 的提示文字时，就表示卡卡安全助手已经完成了漏洞修复工作，此时再对电脑重新扫描一次就能看到已经没有存在漏洞的提示信息了。 不装无用组件 除了系统漏洞，Windows中还存在很多其它安全威胁，同样需要我们的注意。 不安装无用的组件 Windows系统在安装时，会提示我们选择安装的组件。一般来说，那些一时用不到的组件，尽量不要安装。比如对于那些既不打算架设个人站点，又不太可能用本地计算机调试ASP等脚本的普通用户来说，就完全没有必要安装Windows2000/XP的Internet信息服务(IIS)，自然也就可以避免诸如.PRINTER、.IDQ、.IDA、WEBDEV等等通过IIS来进行的外部攻击。 如果电脑中已经安装了IIS，我们也可以将其卸载。 首先打开控制面板，选择 “ 添加或删除程序-添加/删除Windows组件 ”，打开Windows组件向导。 Windows组件向导 将 “ Internet 信息服务（IIS） ” 一项前面的勾去掉，选择下一步。 删除IIS 这样，IIS就被我们移出Windows了。 选择安全的文件格式 对于Windows2000/XP的用户而言，NTFS文件格式是最佳选择。因为无论是从文件检索速度、系统资源权限控制上来看，NTFS都明显要优于FAT系统。 我们可以在采用了NTFS格式的磁盘分区上单击鼠标右键，从弹出的菜单中选择 “ 属性 ”，就会看到NTFS格

式下的磁盘属性中多了“ 配额 ”选项卡，用户通过这个选项卡可以详细地设置系统中每个用户对该逻辑盘的访问权限。NTFS文件格式“ 配额 ”选项 采用FAT32文件格式的磁盘信息则无法设置磁盘配额。 FAT32文件格式 定制系统服务 Windows2000/XP系统正常启动后，会为用户提供很多服务，但绝大多数用户并不需要所有的服务。显然，多余的服务只能增加系统负荷和不稳定性。我们可以在桌面上用鼠标右键单击“ 我的电脑-管理 ”，然后在打开的界面左侧窗口中选择“ 服务和应用程序-服务 ”，我们可以在这里关掉那些不必要的服务，以提高系统稳定性、安全性并加快系统运行速度。关闭不需要的服务 需要特别说明的是，Remote Registry Service、Telnet等几个高风险的服务是一定要停止的。 用鼠标双击相应项目，然后在打开的窗口中将它们设置为“ 手动 ”或“ 禁止 ”即可。 禁用高风险服务 定制默认账号 我们说过，凡是默认的，都是不安全的，至少系统账号是这样的，先不说现在大多数朋友使用的密码都简单得可怜，使用空密码的用户也不在少数。重要的是在已知用户名的情况下，从理论上讲密码很难逃脱被暴力破解的厄运。 在桌面上用鼠标右键单击“ 我的电脑-管理 ”，然后在打开的界面左侧窗口中选择“ 系统工具-本地用户和组 ”。然后为“ 用户 ”或“ 组 ”下面的“ Administrators ”账号更名。 为Administrators账号更名 对于那些系统自带的、我们不使用的用户，最好也设置密码，避免被恶意程序或者攻击者利用。 为Guest设置密码 定制安全日志和审核策略 在一场灾难到来之前，我们可以为避免灾难做大量的准备，但是却绝对不能不去考虑如果灾难真的降临，我们该怎么办？对于系统加固来说，我们同样要做好完全

准备，日志和审核策略就是专门针对这个工作的。注意，操作系统在默认情况下不会打开任何安全审核！单击“开始-运行”，键入“Gpedit.msc”后按下回车键，在打开的组策略窗口中依次展开“计算机配置-Windows设置-安全设置-本地策略-审核策略”。 审核策略 然后双击右侧窗口中的“审核账户管理”，将“成功”、“失败”前的复选框全部选中，再“确定”退出。 审核帐户管理 用同样的方法将“登录事件”、“策略更改”、“系统事件”、“账户登录事件”均设置为“成功”、“失败”，将“对象访问”、“特权使用”、“目录服务访问”设置为“失败”即可。微软认证网，加入收藏 接下来在“账户策略-密码策略”中，将“密码复杂性要求”设置为“启用”.将“密码长度最小值”设置为“6位”.将“强制密码历史”设置为“5次”，将“最长存留期”设置为“30天”。 设置密码策略 在“账户策略-账户锁定策略”中，将“账户锁定”设置为“3次错误登录”.将“锁定时间”设置为“20分钟”.将“复位锁定计数”设置为“20分钟”。 其实整个系统加固过程看起来并不复杂，但不得不提醒大家的是，系统安全或不安全，稳固或不稳固，全在乎操作者的心态，你重视它，时时关注它，对新出现的一些问题及时寻找相应的解决办法，你的系统安全性自然会大大提高。 此外，及时升级杀毒软件，保持杀毒软件病毒库始终是最新的，无疑会对系统安全起到最好的保护。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com