Life
NEW CENTURY

- ☑ 想知道你的电脑是怎样崩溃的吗？
- ☑ 怎样让电脑的硬件稳固工作呢？
- ☑ 电脑中的重要信息是怎样泄露出去的呢？
- ☑ 还在为电脑“偷懒”找不到原因而烦恼吗？

# 第 01 章

# 抨击电脑面临的威胁

今天，娜娜照常打开自己的电脑，但是刚进入桌面就不断地弹出对话框，提示“内存不足”，然后就死机。娜娜一下就傻了，不知道该怎么办才好。阿伟看见这种情况，对她说：“可能是电脑中病毒了，需要进入安全模式进行病毒查杀。”阿伟边操作边为娜娜讲解，最后将问题成功解决。娜娜觉得阿伟太厉害了，想让阿伟教她一些电脑安全方面的知识，于是对阿伟说：“阿伟，你得给我充一下电，以后我就能自己处理一些电脑的问题！”

# 1.1 来自外界的威胁

在为娜娜处理电脑问题时，阿伟告诉她：“电脑最常见的问题是来自外界的威胁，包括黑客的攻击、病毒和木马感染，它们无孔不入。因此，要提高电脑的安全性，首先应认识它们。”娜娜听了以后，迫切地要求阿伟逐一为她讲解这些知识。

## 1.1.1 黑客攻击

在计算机领域中，人们对黑客的态度褒贬不一。黑客的破坏性不容忽视，已经成为网络安全的克星，但也正因为黑客的存在，才促进了网络安全技术的不断发展。

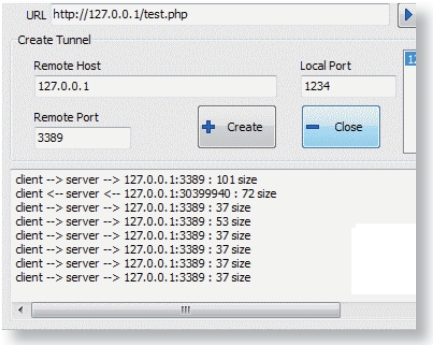
新手解惑

**Q：黑客这个名字的来源是什么？**

A：提起黑客，人们都觉得它很神秘。黑客可以是那些热衷于电脑技术并且水平高超的电脑专家，也可以是那些专门利用电脑网络搞破坏或恶作剧的家伙。黑客攻击电脑的主要目的是通过伪装自身，利用漏洞获取电脑信息或对电脑进行攻击。

知识点拨

黑客攻击的主要内容是什么呢？最常见的就是对网络端口进行监测以及通过漏洞和后门对网站进行攻击，下面将进行简单介绍。



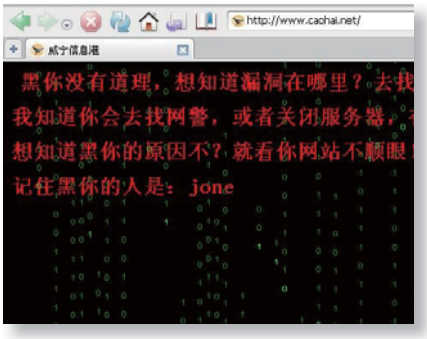

### 1. 监测网络端口

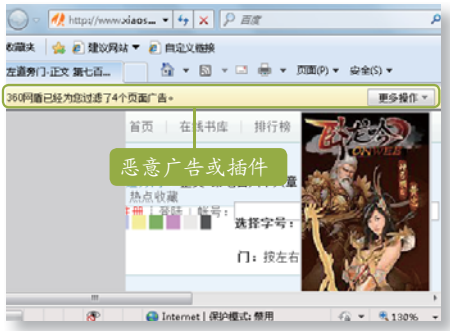
网络端口是黑客主要的监测对象，它是电脑与外界通信交流的出口，因此，黑客可以利用监测所得的端口信息进行分析，确定攻击对象，达到破坏电脑的目的。

### 2. 攻击网站

黑客通过网页的漏洞，很容易得到网络管理员的账号和密码，甚至可得到一些网站权限设置不到位的服务器的最高权限，从而对网站进行入侵修改，以及信息获取。

黑客还可以利用一些人为因素进行攻击，即利用攻击目标的心理弱点来获取目标的信息。




### 3. 植入恶意广告和插件

浏览网页时，经常会有网站附带的插件或广告页面弹出，要求用户安装，甚至有时直接进行安装。这些广告和插件有可能是黑客植入进去的，会给用户带来极大的安全隐患。

## 1.1.2 病毒感染

很多人会感到疑惑，病毒到底是什么呢？一种专业的解释就是通过自身复制传播而产生破坏电脑功能或毁坏电脑数据的程序。其实，病毒就是作用在电脑中的一种病，它具有各种病状，也可通过“治病的良药”进行调理。


### 1. 病毒有哪些

电脑病毒的种类很多，主要分为引导型病毒、文件型病毒、蠕虫病毒、宏病毒和混合型病毒等。它们都具有各自的特征和感染对象。如近几年出现的一种著名病毒——熊猫烧香病毒，被感染的操作系统中所有.exe可执行文件全部被改成熊猫举着三根香的模样。

教你一招

**防止电脑被黑客攻击和感染病毒的方法**

在电脑中安装杀毒软件或安装防火墙能有效降低电脑被黑客攻击以及被病毒感染的频率，但因技术的发展和病毒的变异并不能完全阻止其威胁。

### 2. 判断电脑是否感染病毒

首先可以打开“任务管理器”，查看电脑中运行的进程，根据CPU和内存的占用率初步判断是否感染了病毒，其次可以查看CPU和内存的使用情况，确定电脑中是否存在病毒。

通常情况下，病毒会使CPU和内存的占用率提高，使其处于一个不正常的工作状态。


新手解惑

**Q：病毒具有哪些特点？**

A：病毒是通过自身复制传播而产生破坏电脑功能或毁坏数据作用的程序，一般寄生在系统引导扇区、设备驱动程序或者可执行文件内，并能够利用系统资源进行自我繁殖，从而破坏电脑系统。

### 3. 病毒导致系统文件丢失

系统文件丢失可能是由于病毒感染并破坏系统程序而导致的结果；卸载程序也可能导致系统文件丢失的现象，有的软件可能会共用一个系统文件，但被卸载后文件不见了，从而引起电脑频繁异常重启或者关机，当操作系统异常结束后，会对系统造成严重损伤。

教你一招

**怎样判断系统文件是否丢失**

大多数情况下，系统文件丢失都会弹出提示对话框，在其中将显示系统丢失的文件，通常表现为系统中相关功能或程序软件不可用。另外，系统文件丢失，也会造成系统无法启动等现象，具体应查看其错误提示。

## 1.1.3 木马威胁

木马程序是一种掩藏在美丽外表下打入电脑内部的东西。确切地说，它是一种经过伪装的欺骗性程序，即通过将自身伪装吸引用户下载执行，从而破坏或窃取使用者的重要文件和资料。

知识点拨

下面介绍木马的一些主要特征。

| 排名 | 中文名 | 病毒名 |
|---|---|---|
| 1 | 网游盗号木马 | Win32.Troj.OnlineGamesT |
| 2 | AUTO病毒 | Win32.Troj.AutoRun |
| 3 | 灰鸽子 | Win32.Hack.Huigezi |
| 4 | 熊猫烧香 | Worm.WhBoy |
| 5 | AV终结者 | Win32.Troj.AVKiller |
| 6 | 艾妮 | Win32.MyInfect |
| 7 | MSN机器人 | Worm.MSNBot |
| 8 | 维金变种 | Worm.Viking.gm |

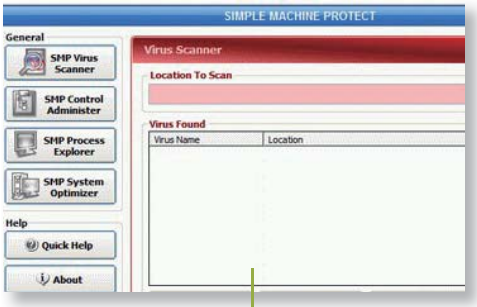
常见木马的排名

### 1. 木马的特点

木马程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开目标电脑的门户，使施种者可以任意毁坏、窃取目标电脑中的文件，甚至远程操控目标电脑。

### 2. 木马的启动方式

木马最常用的启动方式是通过注册表、win.ini、system.ini、某些特定程序或文件以及文件关联5种方式进行启动运行以控制并破坏电脑。




木马控制端

提示：通过注册表启动是最常用的木马启动方式，通过win.ini启动方式只被一些初级的木马设计者使用，木马程序在system.ini文件中加上其路径，也就可以保证永远随Windows启动，通过特定程序和文件启动方式又包括寄生于特定程序中与将特定的程序改名，文件关联启动方式是指木马程序会将自己与TXT文件或EXE文件关联。

新手解惑

**Q：按木马的发展过程，可将其分为哪几个种类？**

A：第一代木马：这一代木马功能简单，主要针对UNIX操作系统进行攻击，而针对Windows操作系统的木马则不多。该时期具有代表性的木马为BO、Netspy等。

第二代木马：这一代木马功能在大大加强，几乎能够进行所有的操作，且随着Internet的普及，开始通过网络进行大范围的传播。该时期具有代表性的木马主要有冰河与广外女生等。

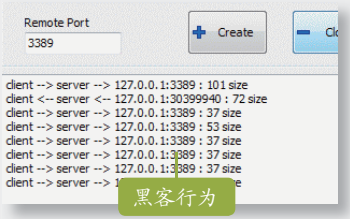
第三代木马：这一代木马继续完善连接与文件传输技术，除此之外，还增加了可以穿越防火墙的功能，并出现“反弹端口”技术，如灰鸽子等。

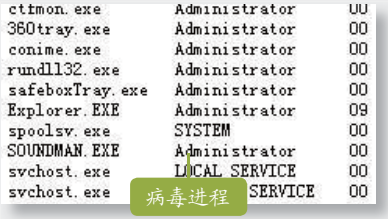
第四代木马：这一代木马除完善之前的所有技术外，还增加了进程隐藏技术，使被控端更难发现木马的存在，如广外幽灵与广外男生等。

跟我练习

**认识并区别黑客、病毒和木马的特点**

黑客利用监测所得的端口信息进行分析，确定攻击对象，达到破坏电脑的目的，并且黑客能利用病毒和木马来攻击电脑。病毒则是一种通过自身复制传播而产生破坏电脑功能或毁坏数据作用的程序。木马是一种经过伪装的欺骗性程序，通过将自身伪装吸引用户下载执行，以破坏或窃取对方的重要文件和资料。



# 1.2 电脑自身安全隐患

娜娜了解到黑客、病毒和木马对电脑的危害后又产生疑惑了，因为她以前遇到过很多造成电脑瘫痪的情况都与阿伟讲的不符，于是又问阿伟：“除了这些以外还有其他的原因会对电脑造成破坏吗？”阿伟告诉她：“当然还有，其实电脑自身的很多因素都会使其产生重大灾难，下面就给你详细讲解！”

## 1.2.1 电脑硬件的安全隐患

电脑硬件是影响电脑正常工作的主要因素，只有硬件稳固工作才能保证电脑的正常运行。

知识点拨

电脑硬件经常会因灰尘过多导致无法散热而产生电脑故障，或因天气的原因使其受潮等，因此灰尘和受潮等是影响电脑硬件安全的因素。但这些都能通过对其维护而得以解决。

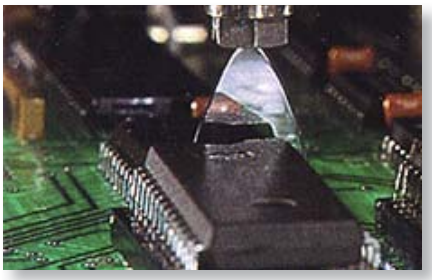
将电脑放置于整洁的房间，并可套上防尘罩，避免灰尘太多对各电脑配件造成不良影响。

### 1. 灰尘

定期为电脑的重要硬件或易被灰尘侵袭的硬件进行除尘也非常必要，可以延长其使用寿命。

### 2. 受潮

电脑如果长期不使用，应该切断电源，但要定期开机运行一下，驱除其内的潮气，或将其重要部件喷上保护层以防止受潮 。



### 3. 电磁

电脑应该远离电场和磁场，通常电磁干扰来源于音响设备和大功率电器。较强的磁场不仅影响电脑的正常运行，甚至会使显示器出现抖动或花斑等现象，或使硬盘中的数据丢失或损坏。

### 4. 错误的使用

电脑各硬件组成电脑的硬件系统，电脑的运行是通过硬件的相互协作所支持的，如果电脑中的任意硬件设备使用不当，将会造成电脑的运行不正常，甚至会给电脑的其他硬件造成损坏。

### 5. 硬件自身质量问题

用户在选择电脑硬件时，通常会被市场上杂乱的品牌所迷惑，如不能很好地辨认其硬件好坏，很可能会购买到劣质的硬件设备，这些硬件本身存在着质量问题，因此，在使用过程中将存在较大的安全隐患。

教你一招

**电脑硬件不兼容带来的安全隐患**

电脑的各种硬件都是由不同厂家生产和研发的，如主板的生产厂家有华硕、技嘉、微星以及精英等，即使各厂家之间尽量相互支持，但由于产品众多，且良莠不齐，因此，产品之间的兼容性问题在所难免。如用户电脑中的硬件兼容性存在问题，将会导致电脑使用不正常。

新手解惑

**Q：影响电脑硬件正常工作的因素有哪些？**

A：电脑硬件由众多元件组成，它是一个物理整体。影响电脑各硬件正常工作的因素主要有环境、电压与静电等，其具体内容介绍如下。

电脑的硬件系统

**环境**　温度范围：10~45℃，湿度范围：30%~80%

**影响原因：**电脑的元件都非常精密，对所处的环境有一定的要求，其室内温度应保持在10～45℃之间，湿度范围最好在30%～80%之间，周围环境应洁净等。只有满足这些条件，才能使其正常工作，否则易引起元器件损坏，从而影响电脑的正常运行。

**电压**　电压范围：220V±10%，频率范围：50Hz±5%

**影响原因：**电脑正常工作的电压范围为220V±10%，频率范围为50Hz±5%。日常所使用的电压经常发生波动，这种情况容易对电脑的电路与部件造成损害。

**静电**　防止静电

**影响原因：**在安装或拆卸电脑时会产生静电，其对电脑硬件的危害最大，不仅会影响电脑部件的正常工作，严重时可能会击穿CPU、主板及内存等。

## 1.2.2 操作系统的安全隐患

操作系统是电脑运行的基本平台，也是文件操作和各种应用软件运行的场所，由于其结构相当复杂，其文件如果稍有差错将出现问题。


操作系统出现问题的主要原因包括其自身问题、进程管理、网络文件系统服务等，下面将分别进行讲解。

| | |
|---|---|
| KB978632 | Windows 7安全更新程序 |
| KB981715 | 2007 Microsoft Office system 更新 |
| KB980368 | Windows系统安全更新程序 |
| KB983484 | Windows 7 更新程序 |
| KB982300 | Windows 7更新程序 |
| KB2202188 | Microsoft Office 2010 修补程序 |
| KB2259539 | Windows 7任务栏缩略图控制更新 |
| KB2028560 | Windows 7更新程序 |
| KB2289116 | Outlook Social Connector更新(32位) |

### 1. 操作系统自身的问题

操作系统是一个庞大的软件系统，负责支撑应用程序的运行环境以及提供用户操作环境，同时也是电脑系统的核心与基石。它涉及了很多方面的应用，因此不可避免地存在一些缺陷（Bug）。黑客就是利用这些Bug作为攻击用户电脑系统的通道。


：操作系统的一些Bug可利用相关的软件进行修复，确保这些缺陷不被黑客等利用以危害系统安全。

### 2. 操作系统的进程管理

当创建的远程进程通过各种途径安装到电脑中时，用户将可以通过网络远程启动它们，从而使操作系统处于一个危险的环境中。


：在操作系统中，用户可以创建进程，甚至可以在网络上的其他电脑中创建并激活远程进程，而且所创建的远程进程将继承创建进程的某些权限。

### 3. 网络文件系统服务

用户在网络中的共享数据是通过操作系统中的文件系统服务得以实现的，操作系统为其提供的安全验证功能是有限的，因此，网络文件系统服务也是操作系统的一个重要的安全隐患。

### 4. 操作系统后门

操作系统后门是在操作系统的开发阶段，程序员常会在其中创建一些方便的后门，以便修改程序中的缺陷。如果后门被黑客探测到，或在操作系统发布之前未删除，那么它就成了安全隐患。

### 5. 操作系统自身的应用程序

操作系统具有自身的应用程序，通常这些应用程序也会存在威胁，如Adobe Flash以及IE浏览器，它们是操作系统中存在的最大威胁，很容易被黑客等利用，威胁电脑的安全。

## 1.2.3 个人信息的安全隐患

电脑中的个人信息除了各种应用程序、图形、文档、视频与音频等信息外，还包括账号和密码等信息，它们主要存储在电脑的硬盘、光盘、U盘或移动硬盘中，因此，当这些存储介质受到破坏时，其信息的安全将无法保证。

**知识点拨**

电脑的相关存储设备存在着许多与信息安全密切相关的特性，主要包括如下几方面。

问题1：存储过程中的损坏

损坏原因：当使用移动存储介质存储数据信息时，如果在存储的过程中意外中断或不正确退出，将有可能对资料造成破坏。

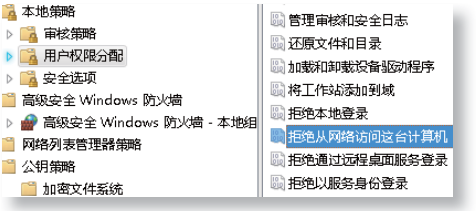
保证正确使用设备进行存储信息将有利于信息的安全存储。

提示：在电脑中，使用自身硬盘可以存储大量的信息，使用移动硬盘与U盘可以随身携带，在其存储或使用过程中很容易受到意外损坏，从而导致信息的损坏。

问题2：网络中用户对数据的访问

损坏原因：如果无任何权限设置，数据在网络中将被其他用户访问、更改，甚至破坏。

可在“本地安全策略”中设置拒绝从网络访问这台计算机，这样将有效保证数据的安全性。




提示：电脑中的数据可以很容易地被其他用户浏览或复制而不留痕迹，并且当网络中的用户获得访问个人数据的权限后，可以连接到存储信息的电脑中，并按其需要对信息进行复制或修改，甚至破坏。


问题3：黑客破坏数据的安全性

损坏原因：用户电脑中的信息可通过设置安全屏障以减少网络中各种不安全的访问，如开启系统的防火墙。

这种设置只对一般的使用者有效，对拥有高超的电脑技术的人或黑客则用处不大。

提示：用户在电脑中可以采用某些方法增加信息的安全性，但对于一些专业人员或黑客来说，将可能会越过这些屏障，破坏信息的安全，并且由于网络的发展，降低了信息的安全性。


问题4：个人用户密码的安全

损坏原因：用户在使用重要通信软件或网上银行时，对密码的设置应该谨慎，需要使用相对复杂的密码。

如用户使用的QQ软件，若账号密码丢失将使个人的聊天记录泄露，用户应通过对其设置密码保护等方式保护密码的安全。

教你一招

**如何保护个人信息的安全**

除将重要数据备份外，用户还可以将其加密并设置访问权限，防止他人对其进行破坏。

## 1.2.4 网络信息安全问题

随着Internet技术的发展，电脑中的信息都可在网络中共享。电脑网络信息的共享虽然给人们带来了极大的便利，但也将受到某些不安全因素的影响，从而出现安全问题，下面将分别对其进行讲解。

知识点拨

网络信息的安全问题包括网络管理员安全配置不当、用户安全意识不强等用户自身疏忽而造成的安全漏洞；或利用网络中信息的共享性而在用户电脑中种植木马；某些不法人员利用软件对电脑网络进行攻击，或传播非法信息等。


### 1. 管理员安全配置不当

用户在为电脑进行管理员安全配置时，如果对其安全属性配置过低，则很容易被网络中的木马程序盗取账户和密码。

获得管理员的账户和密码即可登录系统进行数据或信息的获取和修改，使网络信息的安全受到威胁。

### 2. 信息共享性的利用

一些不法分子在网络中种植木马程序，如果木马程序感染了用户电脑，木马施种者就可以通过木马修改并获取用户的数据信息。

网络信息的安全将因此而没有保证，可通过在电脑中安装木马防御工具来预防木马的活动。



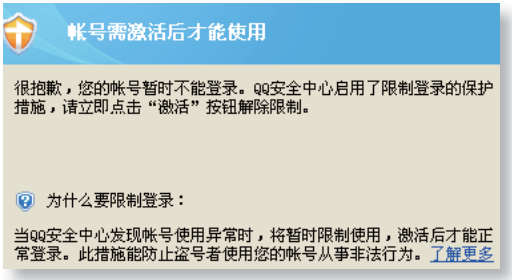
### 3. 利用软件攻击网络

在电脑中可利用软件收集网络中的信息，并且捕捉网络中电脑的物理地址或IP地址，然后通过所收集的信息攻击电脑，从而使网络信息的安全遭遇破坏。

教你一招

**网络信息安全防御**

要使网络信息更安全，用户在使用电脑上网时应小心谨慎，不浏览一些存在安全隐患的信息，同时在电脑中应安装相关的病毒木马防护软件。




### 4. 网络口令的泄露

泄漏网络信息操作的口令将可能使网络中的重要信息以及电脑中的机密文件被他人利用。口令的泄露主要是由于用户安全意识不强，设置的口令过于简单或者与他人共享一个ID，或者将自己的账户和口令告诉了他人。

### 5. 利用网络传播非法信息

一些不法分子在利用软件或其他的黑客手段获取用户的论坛或其他的聊天软件账号后，将使用其传播非法信息，这不仅给用户带来了诸多烦恼，还形成了网络信息安全的重大安全隐患，使用户对网络信息产生了极大的不安全感。对于该情况，用户需正确地判断，理智地对待。


跟我练习

**认识电脑自身的安全因素**

电脑自身的安全隐患同样很多，前面讲解的只是一部分典型的安全隐患，下面通过所学知识，总结电脑自身的安全因素。

任务1：收集电脑硬件的安全隐患，并了解其维护方法及标准。

任务2：总结并查询操作系统的安全隐患，针对相应的安全隐患总结出其防范措施。

任务3：结合个人信息和网络信息的安全隐患，区别其相同点和不同点，并通过上网查询了解一些防范措施。

# 1.3 更进一步——电脑安全技术

通过阿伟前面的讲解，娜娜已经懂得了电脑所面临的一些来自外界或自身的安全隐患。她没想到尽管电脑不大，但它所存在的威胁却这么多。阿伟感觉到娜娜好像对电脑的这些问题很在意，于是想给她讲几个电脑安全中常用的技术和方法，娜娜欣然接受了。

## 第1招 病毒防范技术


病毒在网络中传播扩散得很快。要杜绝网络病毒，除了要用单机防病毒产品外，还必须有适合于局域网的全方位防病毒产品。

360杀毒软件是目前应用最广的免费杀毒软件之一，用户可使用其进行病毒查杀，其操作方法如下。

①安装360杀毒软件。

②启动其进入主界面，单击按钮快速扫描磁盘。

③完成扫描后，单击按钮关闭窗口即可。

## 第2招 修复系统漏洞


提示：可选择目前使用最广泛的360安全卫士进行漏洞的修复，它可以智能地选择要修复的高危漏洞进行修复，同时过滤不必修复的漏洞。

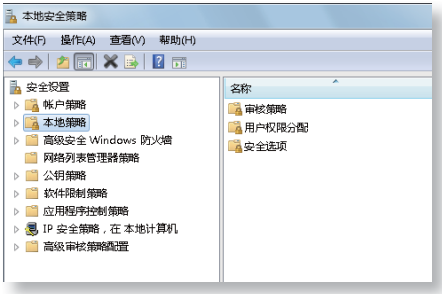
## 第3招 充分利用防火墙

利用防火墙对网络进行访问控制设置之后，系统在运行新程序时会通知用户，从而最大限度地阻止网络中的黑客访问电脑，防止其随意更改、移动甚至删除网络上的重要信息。


**提示**：开启系统防火墙后，当黑客进行攻击操作时会进行拦截，并弹出通知窗口，提示用户做出相应的操作。

## 第4招 访问控制技术

访问控制的主要任务是保证网络资源不被非法使用和访问，是对信息系统资源进行保护的重要措施，同时也是电脑系统重要的安全机制。其主要通过设置用户的安全策略得以实现。

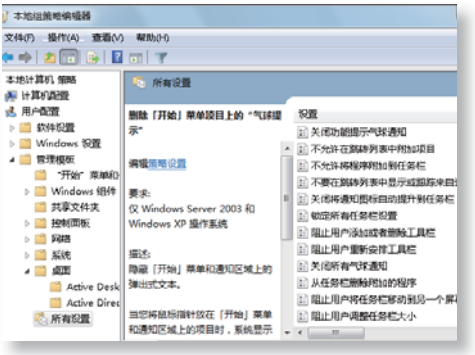



**提示**：设置访问控制决定了能够访问系统的用户，并且将设定访问和控制系统资源的权限。设置系统的访问控制也能阻止未经允许的用户获取数据并控制电脑的资源权限。访问控制的方法可以通过用户识别代码、口令、登录控制、资源授权、授权核查、日志和审计等来实现。

## 第5招 为电脑设置权限

为电脑设置权限，可以保证合法用户按照权限使用电脑系统。

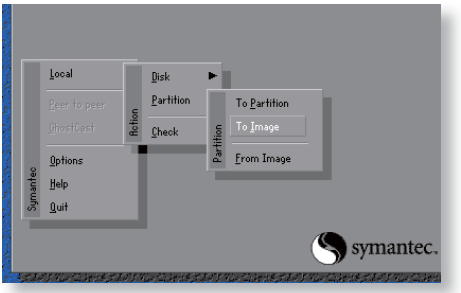
在本地组策略编辑器中可对电脑的使用权限进行设置。



## 第6招 备份与恢复数据

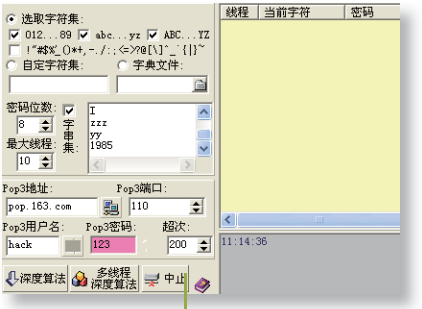
并不是所有的数据都需要备份，通常备份的是重要数据，如硬盘分区表与引导记录、操作系统等。当电脑系统被破坏时，使用备份文件即可进行恢复，从而有效保证信息的完整性。

使用Ghost软件可方便地对电脑中的重要数据进行备份。

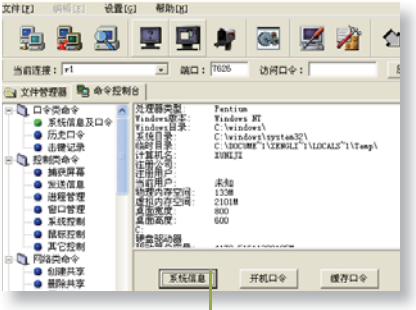



# 1.5 活 学 活 用

（1）收集相关黑客软件（黑雨邮箱密码探测器）和木马病毒（冰河木马）进行使用，体验使用软件或程序对电脑进行控制和检测。




黑雨邮箱密码探测器

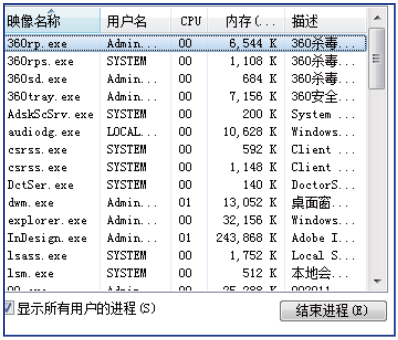


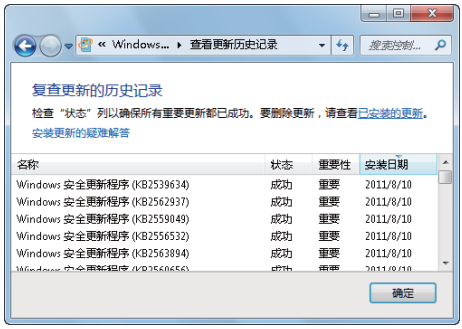

冰河木马

（2）使用专用工具（吹吸风机）为长期使用的电脑进行清尘，保证电脑的正常运行。在清理过程中注意不能损坏电脑的硬件。

提示：在吹风过程中，注意将其方向对准机箱后挡板有孔的地方，以确保灰尘顺利被除尽。

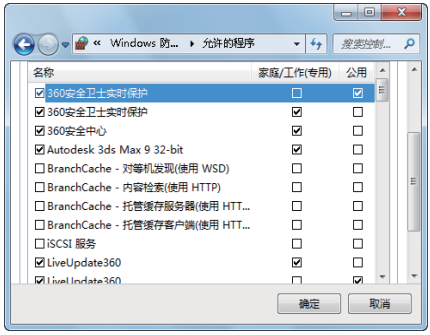
（3）通过所学知识，查看自己的电脑中是否存在高危漏洞，并在任务管理器中查看是否存在恶意进程。



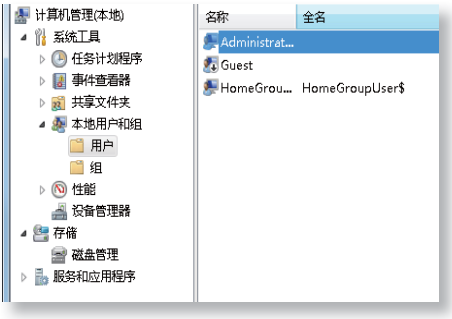



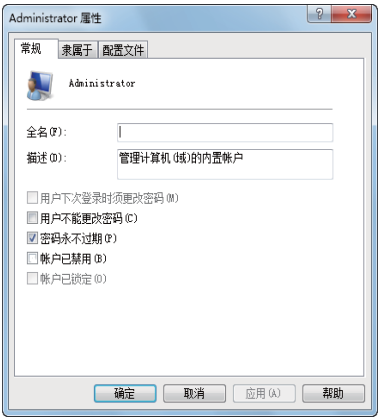

提示：除了可在操作系统中查看漏洞更新情况外，使用360安全卫士也可以查看。

（4）在使用电脑过程中，经常会遇到安装某个应用程序时系统弹出拦截对话框。利用所学知识查看系统防火墙的防护状况。

（5）在电脑中查看管理员的安全配置是否正确，以保障网络信息的安全性。




（6）结合本章所学知识，总结黑客、病毒和木马等外界因素影响电脑安全的方式，并列举电脑自身的安全隐患。