WindowsVista遭受的十大安全误解真相 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/283/2021_2022_WindowsVis_c100_283552.htm Windows Vista明显提高了对黑客和恶意入侵者的防范，毫无疑问，它是迄今为止最为安全的微软操作系统。通过诸如用户帐号控制(UAC)、BitLocker驱动器加密、文件/注册表虚拟化、强制完整性控制(MIC)和IE浏览器保护模式等功能，你可以在系统级别或更精细级别来加固Vista的安全性。 然而，由于Vista的安全配置的复杂性，人们对一些Vista安全功能和推荐配置存在很多令人迷惑之处。下面让我们看一下关于Vista安全的十大顶级误解，并给出正确的理解。 1、administrator帐号默认将被禁用? 通常情况下Vista会默认禁用administrator帐号，但是有一个前提：在管理员组里面存在其他活跃的定义好的成员。更准确的说法应该是，如果Vista检测到其他启用的管理员帐号的话，通过禁用真正的administrator帐号，来试图最小化管理员帐号的数量。在新安装Vista的时候，第一个新帐号将被增加到管理员组里，就如同在windows xp和windows 2000中一样，但是后来增加的用户不是。一旦第二个管理员帐号被增加后，Vista将禁用真正的administrator帐号。 需要注意的重要一点是，默认禁用的管理员帐号是没有密码的。你应该对administrator帐号设置一个复杂的密码，即使它是被禁用的。如果你要启用一个被禁用的administrator帐号的话，首先设置密码，然后你就可以启用这个帐号了。 2、Vista只存在四个强制完整性控制级别? 强制完整性控制(MIC)是Vista安全架构中新增加的一种检测机制。Vista中的所有安全性对象和进程都有一个完整性级别，完

整性级别(IL)低的进程不能修改级别高的文件或注册表表项。有四个主要的强制完整性控制(MIC)级别： 低(Low) 中等(Medium) 高(High) 系统(System) 包括管理员组中的非提升权限成员在内的大多数用户，都运行在中等级别。以下是一些其他级别是如何被设定的。 内核级别的Windows文件以系统完整性级别运行 用户级别的代码，例如Windows Explorer和任务管理器，以中等完整级别运行 真正的administrator或系统管理员组中的提升权限的成员以高完整级别运行 保护模式下的IE浏览器以低完整性级别运行 如果一个对象或资源没有明确的设定完整性级别，那么它具有中等完整性级别。 建立强制完整性控制的的主要目的是，使一般用户、程序和在IE保护模式下的下载内容难于修改系统文件。因此，即使一个用户可能是系统管理员组的一个成员，或者甚至即使一个恶意软件设法突破了IE的初级安全防御，它们也难于修改Windows的系统文件。 除了上述四个级别外，至少还有两个人们知道比较少的强制完整性级别：非信任级别和保护进程级别。非信赖完整性可能是级别最低的强制完整性级别，被设置给匿名空连接会话。保护进程可能是级别最高的强制完整性级别，只有在系统需要的时候才会被使用。 或许只有你在进行研究或故障排查的时候才能碰到这些强制完整性级别，你可以认为恶意黑客们将试图获得一个保护进程强制完整性级别的权限，来使Windows更轻松的被攻破。 3、用户帐号控制(UAC)减少管理员被需要的次数? Vista要求用户获得提升的权限和许可来完成系统任务，诸如安装软件、更新内核驱动等等。Vista还有一些新的要求较少管理性帐号的功能，但是用户帐号控制(UAC)不是其中之一。 用户帐号控

制(UAC)明确的要求那些希望完成管理性任务的用户具有提升的本地组中成员资格，例如administrators组或backup operators组。用户帐号控制(UAC)的存在并不会减少对管理性用户的需要，当执行诸如电子邮件或网络浏览等非管理性任务的时候，它提供了针对属于提升权限组的用户的额外的保护。 当一个提升权限的用户(但不是真正的administrator)登录后，用户帐号控制(UAC)设定两个访问安全令牌，也被叫做一个“ 分离令牌split-token ”。直到用户通过用户帐号控制(UAC)提升了访问权限后，标准系统管理员组的成员安全令牌才可用。否则，Vista针对用户的安全令牌采取如下措施 ：Vista移除通常设置给管理员组成员的9个提升的权限 用户的强制完整等级从高等降级为中级 指定禁用安全标示符(deny-only security identifier,deny-only SID) 出现用户帐号控制(UAC)同意提示窗口 应用文件和注册虚拟化 当用户提升它们的session时，那些额外的限制将被移除。但是，Vista要求一个管理员帐号来完成许多普通的系统任务。通过在不明确被需要的时候移除提升的权限和许可，用户帐号控制可以同时保护系统和用户。这样，管理帐号不用在浏览网页或打开恶意电子邮件的时候担心其被提升的安全权限被使用。 在其他方面，Vista的确降低了必需的管理员的数量。首先，Vista已经移除了完成许多普通系统任务对管理员权限的需要，诸如查看或修改时区，配置无线网络，修改电源管理设置，创建和配置一个虚拟专用网络(VPN)连接和安装关键的Windows更新。 其次，Vista让管理员可以定义非管理员帐号可以安装的驱动、设备和ActiveX控制。因此，举个例子来说，你可以让你的用户安装打印机、网卡、USB设备和VPN软件。 第三

，对于基本的网络重新配置任务，你可以增加非管理员用户到网络配置操作组中。在这个组中的用户可以释放IP地址，清空DNS缓存和完成其他普通网络任务。还有很多其他的方式来降低你需要管理员权限的次数。UAC不是其中之一。