Linux与Windows的安全性比较 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022_Linux_E4_B8_8EWi_c103_143960.htm 安全问题对于IT管理员来说是需要长期关注的。主管们需要一套框架来对操作系统的安全性进行合理的评估，包括：基本安全、网络安全和协议，应用协议、发布与操作、确信度、可信计算、开放标准。在本文中，我们将按照这七个类别比较微软Windows和Linux的安全性。最终的定性结论是：目前为止，Linux提供了相对于Windows更好的安全性能，只有一个方面例外（确信度）。 无论按照什么标准对Windows和Linux进行评估，都存在一定的问题：每个操作系统都不止一个版本。微软的操作系统有Windows98、Windows NT、 Windows 2000、 Windows 2003 Server和Windows CE，而Linux的发行版由于内核（基于2.2、2.4、2.6）的不同和软件包的不同也有较大的差异。我们本文所使用的操作系统，都是目前的技术而不是那些"古老"的解决方案。 用户需要记住：Linux和Windows在设计上就存在哲学性的区别。Windows操作系统倾向于将更多的功能集成到操作系统内部，并将程序与内核相结合；而Linux不同于Windows，它的内核空间与用户空间有明显的界限。根据设计架构的不同，两者都可以使操作系统更加安全。 Linux和Windows安全性的基本改变 对于用户来说，Linux和Windows的不断更新引发了两者之间的竞争。用户可以有自己喜欢的系统，同时也在关注竞争的发展。微软的主动性似乎更高一些——这是由于业界"冷嘲热讽"的"激励"与Linux的不断发展。微软将在下几个月对Windows安全进行改观，届

时微软会发布Windows XP的Service Pack2。这一服务包增强了Windows的安全性，关闭了原先默认开放的许多服务，也提供了新的补丁管理工具，例如：为了避免受到过多无用的信息，警告服务和信使服务都被关闭。大多数情况下，关闭这些特性对于增强系统安全性是有好处的，不过很难在安全性与软件的功能性、灵活性之间作出折衷。 最显著的表现是：微软更加关注改进可用性的同时增强系统的安全性。比如：2003年许多针对微软的漏洞攻击程序都使用可执行文件作为电子邮件的附件（例如MyDoom）。Service Pack2包括一个附件执行服务，为Outlook/Exchange、 Windows Messenger和Internet Explorer提供了统一的环境。这样就能降低用户运行可执行文件时感染病毒或者蠕虫的威胁性。另外，禁止数据页的可执行性也会限制潜在的缓冲区溢出的威胁。不过，微软在Service Pack2中并没有修改Windows有问题的架构以及安全传输的部分，而是将这部分重担交给了用户。 微软的重点显然是支持应用程序的安全性。Service Pack2中增强的许多方面都是以Outlook/Exchange和Internet Explorer作为对象的。例如：Internet Explorer中有一个智能的MIME类型检查，会对目标的内容类型进行检查，用户可以获悉该内容中是否存在潜在的有害程序。不过这一软件是不是能将病毒与同事的电子数据表区分开来呢？ Service Pack2的另一个新特性是能够卸载浏览器的多余插件，这需要终端用户检查并判断需要卸载哪些插件。Outlook/Exchange可以预览电子邮件消息，因此用户可以在打开之前就将电子邮件删除。另一个应用安全的增强，防火墙在网络协议栈之前启动。对于软件开发者来说，远方过程调用中权限的改变，使得安全性差的代码难以工作

正常。 Service Pack2也为Windows用户提供了许多华丽的新特性，但是问题仍然存在：这些特性会不会对管理员甚至是终端用户造成负担？是不是在增加了Windows操作系统代码安全性的同时让系统变得更加复杂？ 开放源代码、共享源代码Linux和Windows对于代码透明度这一哲学问题上是完全不同的。Linux符合GNU通用公用许可证，用户可以拷贝、复制并分发源代码。Windows使用的是封闭源代码，因此微软的安全方法被称为"通过隐藏来保证安全"。2001年，微软为了响应客户与共享源代码计划的要求，提供了对Windows源代码的访问权。现在，共享源代码计划有一百万的参与者，可以访问的源代码包括Windows2000、WindowsXP、Windows Server2003、Windows CE 3.0、Windows CE 、C#/CLI实现和ASP.NET与Visual Studio.NET。共享源代码计划许可证的对象包括公司用户、政府、合作者、学术机构与个人。 微软的共享源代码计划政策属于"可看但不可修改"，例外的情况是Windows CE共享源代码许可证计划。对于公司来说，可以将基于Windows CE的设备和解决方案推向市场。这是微软共享源代码计划下，源设备制造商（OEM）、半导体提供商、系统集成商可以完全访问Windows CE源代码的唯一项目。所有许可证持有者都有对源代码的完全访问权，当然可以修改代码，但只有OEM才能发布对基于WinCE设备的修改。所有其他的共享源代码许可证持有者，如果要访问该项目不允许的源代码，需要向Redmond.Wash的微软总部请示。 某些用户认为共享源代码计划对于调试程序会有帮助，微软要求编译的时候必须在微软总部，这不得不说是一个很大的限制。尽管微软想尽力增加透明，如果无法编译，就很难确定源代码

在真实的IT环境中是否能正常工作。限制用户修改并编译Windows的源代码，降低了人们访问Windows共享源代码并寻找安全漏洞的热情。 数据中心和桌面下Linux的安全收益 在未来的12个月里，Linux将加强在数据中心的份额，并试图冲击微软在桌面上的垄断。这很大程度上是受益于Linux2.6版内核的新特性与新功能。有了Linux v2.6，安全框架现在已经模块化了。在这种模型下，Linux内核的所有方面都提供了细粒度的用户访问控制，而以前的版本的内核允许超级用户完全控制。现在的实现仍然支持root完全访问系统，但完全可以创建一个不遵循该模型的Liinux系统。 Linux v2.6内核的一个主要变化，就是新增的Linux安全模块（LSM），用户不需要打内核补丁就能为Linux增加更多的安全机制。新版内核，在LSM上建立了多个访问控制机制，其中包括美国国安局（NSA）的Securiy Enhanced Linux（SELinux）。由于国安局对操作系统安全与强制访问控制的兴趣，产生了SELinux。国安局的研究人员正在开发Linux的安全模块，可以支持2.6内核的类型加强、基于脚色的访问控制、多层次安全。SELinux使用了命为"域类型强制"的安全模型，可以将应用程序互相隔离，同时也与基本的操作系统隔离，从而限制入侵后程序或者网络服务造成的影响。 Linux的2.6内核中已经加入了对SELinux的细粒度布尔值标签的支持，其他的厂商也开始利用国安局的SELinux。例如，Immunix提供了一些列产品，包括StackGuard和子域StackGuard模块，可以配置进程只使用某些系统调用。RedHat声称SELinux将在RedHat企业服务器4.0的安全架构上起重要的作用。 今天，Linux的内核中已经有一个功能强大、灵活的强制访问控制子系统。这个系统强制隔离

有机密和完整性要求的数据，因此任何潜在的破坏，即时是由超级用户进程所造成的，都被Linux系统限制起来了。Linux v2.6还提供了对加密安全的支持，包括了IPSec使用的加密API。这样，在网络和存储加密时就可以使用多种算法（例如：SHA-1、DES、三重DES、MD4、HMAC、EDE、和Blowfish）。Linux对IPSec IPv4和IPv6协议的支持是一个很大的进步。由于安全抽象到了协议层，用户程序对潜在攻击程序的脆弱性有所降低。密码加密模块目前还不是Linux内核的一部分，如果Linux真的实现了这样的特性，就可以阻止未签名的模块被内核访问。 现在仍然困扰Windows用户的一个问题就是缓冲区溢出。Linux用户从2.6内核开始就会收益于exec-shield补丁。exec-shield可以阻止许多漏洞攻击程序覆盖数据结构并向这些结构中插入代码的企图。由于不需要重新编译应用程序就能使exec-shield补丁奏效，实现起来很方便。 另外，2.6内核中的抢占式内核，也减少了延迟，使得Linux不但可以应用到数据中心，甚至可以在有软实时要求的应用程序使用。许多Linux用户使用的是硬件厂商和系统提供商的不开源的驱动程序（二进制模块）。问题在于：虽然添加这些驱动和模块有用，对于Linux系统并不一定有益。例如，一个未开源的驱动模块有可能控制系统调用并修改系统调用表。2.6的内核提供了特殊的保护措施，可以对限制未开源驱动或者模块对内核的访问。这一特性增加了稳定性，但从安全角度并没有增加新的限制，也不能阻止黑客编写恶意模块。 许多Linux用户来说，最有创造性的特性就是用户模式Linux了（UML），UML是Linux内核的一个补丁，可以允许可执行二进制文件在Linux宿主主机上编译并运行。使

用UML有很多好处，最有用的特性就是虚拟机。由于对UML的操作不会影响宿主主机，可以把它作为测试软件、运行不稳定发行版、检查有威胁活动的平台。UML最终会创建一个安全架构上完全虚拟的环境。Linux与Windows安全性能的重要结论 对操作系统的安全性进行定性分析，很容易包含主观意见，得到的结论会由于过去和现在的经验而有很大的不同。本文的目标是给用户提供一个框架，让他们更多的理解Windows和Linux的安全性能。下面的分析并不全面，只是终端用户进行评估的起点。Linux和Windows在技术上不断进步，究竟哪个系统更安全的结论也会不断变化。本文分析的结果：Linux提供了比Windows更好的安全特性。 