提高Linux操作系统安全性的十大招数 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/221/2021_2022__E6_8F_90_E9_AB_98Linu_c103_221638.htm Linux是一种类Unix的操作系统。从理论上讲，Unix本身的设计并没有什么重大的安全缺陷。多年来，绝大多数在Unix操作系统上发现的安全问题主要存在于个别程序中，所以大部分Unix厂商都声称有能力解决这些问题，提供安全的Unix操作系统。但Linux有些不同，因为它不属于某一家厂商，没有厂商宣称对它提供安全保证，因此用户只有自己解决安全问题。Linux不论在功能上、价格上或性能上都有很多优点，然而，作为开放式操作系统，它不可避免地存在一些安全隐患。关于如何解决这些隐患，为应用提供一个安全的操作平台，本文会告诉你一些最基本、最常用，同时也是最有效的招数。Linux是一个开放式系统，可以在网络上找到许多现成的程序和工具，这既方便了用户，也方便了黑客，因为他们也能很容易地找到程序和工具来潜入Linux系统，或者盗取Linux系统上的重要信息。不过，只要我们仔细地设定Linux的各种系统功能，并且加上必要的安全措施，就能让黑客们无机可乘。 一般来说，对Linux系统的安全设定包括取消不必要的服务、限制远程存取、隐藏重要资料、修补安全漏洞、采用安全工具以及经常性的安全检查等。本文教你十种提高Linux系统安全性的招数。虽然招数不大，但招招奏效，你不妨一试。第1招：取消不必要的服务早期的Unix版本中，每一个不同的网络服务都有一个服务程序在后台运行，后来的版本用统一的/etc/inetd服务器程序担此重任。Inetd是Internetdaemon的缩写，它同时监视多个网络端

口，一旦接收到外界传来的连接信息，就执行相应的TCP或UDP网络服务。由于受inetd的统一指挥，因此Linux中的大部分TCP或UDP服务都是在/etc/inetd.conf文件中设定。所以取消不必要服务的第一步就是检查/etc/inetd.conf文件，在不要的服务前加上“#”号。一般来说，除了http、smtp、telnet和ftp之外，其他服务都应该取消，诸如简单文件传输协议tftp、网络邮件存储及接收所用的imap/ipop传输协议、寻找和搜索资料用的gopher以及用于时间同步的daytime和time等。还有一些报告系统状态的服务，如finger、efinger、systat和netstat等，虽然对系统查错和寻找用户非常有用，但也给黑客提供了方便之门。例如，黑客可以利用finger服务查找用户的电话、使用目录以及其他重要信息。因此，很多Linux系统将这些服务全部取消或部分取消，以增强系统的安全性。Inetd除了利用/etc/inetd.conf设置系统服务项之外，还利用/etc/services文件查找各项服务所使用的端口。因此，用户必须仔细检查该文件中各端口的设定，以免有安全上的漏洞。在Linux中有两种不同的服务型态：一种是仅在有需要时才执行的服务，如finger服务.另一种是一直在执行的永不停顿的服务。这类服务在系统启动时就开始执行，因此不能靠修改inetd来停止其服务，而只能从修改/etc/rc.d/rc[n].d/文件或用Run level editor去修改它。提供文件服务的NFS服务器和提供NNTP新闻服务的news都属于这类服务，如果没有必要，最好取消这些服务。