系统安全之保护Linux系统安全十招搞定 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/268/2021_2022__E7_B3_BB_E7_BB_9F_E5_AE_89_E5_c67_268221.htm 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Runlevelеditor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。 第2招：限制系统的出入 在进入Linux系统之前，所有用户都需要登录，也就是说，用户需要输入用户账号和密码，只有它们通过系统验证之后，用户才能进入系统。 与其他Unix操作系统一样，Linux

一般将密码加密之后，存放在/etc/passwd文件中。Linux系统上的所有用户都可以读到/etc/passwd文件，虽然文件中保存的密码已经经过加密，但仍然不太安全。因为一般的用户可以利用现成的密码破译工具，以穷举法猜测出密码。比较安全的方法是设定影子文件/etc/shadow，只允许有特殊权限的用户阅读该文件。 在Linux系统中，如果要采用影子文件，必须将所有的公用程序重新编译，才能支持影子文件。这种方法比较麻烦，比较简便的方法是采用插入式验证模块（PAM）。很多Linux系统都带有Linux的工具程序PAM，它是一种身份验证机制，可以用来动态地改变身份验证的方法和要求，而不要求重新编译其他公用程序。这是因为PAM采用封闭包的方式，将所有与身份验证有关的逻辑全部隐藏在模块内，因此它是采用影子档案的最佳帮手。 此外，PAM还有很多安全功能：它可以将传统的DES加密方法改写为其他功能更强的加密方法，以确保用户密码不会轻易地遭人破译；它可以设定每个用户使用电脑资源的上限；它甚至可以设定用户的上机时间和地点。 Linux系统管理人员只需花费几小时去安装和设定PAM，就能大大提高Linux系统的安全性，把很多攻击阻挡在系统之外。 第3招：保持最新的系统核心 由于Linux流通渠道很多，而且经常有更新的程序和系统补丁出现，因此，为了加强系统安全，一定要经常更新系统内核。 Kernel是Linux操作系统的核心，它常驻内存，用于加载操作系统的其他部分，并实现操作系统的基本功能。由于Kernel控制计算机和网络的各种功能，因此，它的安全性对整个系统安全至关重要。 早期的Kernel版本存在许多众所周知的安全漏洞，而且也不太稳定，只有2.0.x以上的版本才比较稳定和安全，

新版本的运行效率也有很大改观。在设定Kernel的功能时，只选择必要的功能，千万不要所有功能照单全收，否则会使Kernel变得很大，既占用系统资源，也给黑客留下可乘之机。 在Internet上常常有最新的安全修补程序，Linux系统管理员应该消息灵通，经常光顾安全新闻组，查阅新的修补程序。 第4招：检查登录密码 设定登录密码是一项非常重要的安全措施，如果用户的密码设定不合适，就很容易被破译，尤其是拥有超级用户使用权限的用户，如果没有良好的密码，将给系统造成很大的安全漏洞。 在多用户系统中，如果强迫每个用户选择不易猜出的密码，将大大提高系统的安全性。但如果passwd程序无法强迫每个上机用户使用恰当的密码，要确保密码的安全度，就只能依靠密码破解程序了。 实际上，密码破解程序是黑客工具箱中的一种工具，它将常用的密码或者是英文字典中所有可能用来作密码的字都用程序加密成密码字，然后将其与Linux系统的/etc/passwd密码文件或/etc/shadow影子文件相比较，如果发现有吻合的密码，就可以求得明码了。 在网络上可以找到很多密码破解程序，比较有名的程序是crack。用户可以自己先执行密码破解程序，找出容易被黑客破解的密码，先行改正总比被黑客破解要有利。 