应用技术:如何给Linux补洞 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/273/2021_2022__E5_BA_94_E7_94_A8_E6_8A_80_E6_c102_273456.htm Linux存在的安全漏洞大部分是可以堵住的，但是传统和习惯的操作方式却使它们完全洞开。其实你可以在5分钟之内完成百分之九十的保护。提高Linux系统的安全性的主要措施有如下几点： 1. 取消不必要的服务 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、用于时间同步的daytime和time等以及报告系统状态的服务，如finger、efinger、systat和netstat等。 2. 加密用户登录密码并设定用户账号安全等级 虽然Linux对用户登录密码加密存放，但仍然不太安全。比较安全的方法是设定影子文件，只允许有特殊权限的用户阅读该文件。很多Linux系统都带有Linux的插入式验证模块工具程序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。
在Linux上每个账号可以被赋予不同的权限，而黑客最喜欢具有root权限的用户账号，这种超级用户有权修改或删除各种系统设置，可以在系统中畅行无阻。因此，在给任何账号赋予root权限之前，都必须仔细考虑。 3. 消除黑客犯罪的温床 在Unix系统中，有一系列r字头的公用程序，它们是黑客用以入侵的武器，非常危险，因此绝对不要将root账号开放给这些公用程序。很多像PAM的安全工具都是针对这一安全漏洞而设计的。 4. 增强安全防护工具 SSL是安全套接层的简称，它是可以安全地用来取代rlogin、rsh和rcp等公用程序的一套

程序组。SSL采用公开密钥技术对网络上两台主机之间的通信信息加密，并且用其密钥充当身份验证的工具。 5. 常抓不懈，共同防御 从计算机安全的角度看，世界上没有绝对密不透风、百分之百安全的计算机系统，Linux系统也不例外。采用以上的安全守则，虽然可以使Linux系统的安全性大大提高，使顺手牵羊型的黑客和电脑玩家不能轻易闯入，但却不一定能阻挡那些身怀绝技的高手，因此Linux系统管理员应该经常光顾在Internet上的安全新闻组，查阅新的修补程序，保持最新的系统核心，同时还要经常提高警惕，随时注意各种可疑状况，并且按时检查各种系统日志文件，包括一般信息日志、网络连接日志、文件传输日志以及用户登录日志等，追踪黑客的踪迹。此外，企业用户还需要借助防火墙等其他安全工具，共同防御黑客入侵，才能确保系统万无一失。 Linux作为开放式操作系统，尽管不可避免地存在缺陷，但这属于前进中的插曲，并不能阻挡Linux强大的发展势头和美好的未来前景，Linux还是值得大力推广的。 