七大步骤建立可靠的Linux操作系统 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/294/2021_2022__E4_B8_83_E5_A4_A7_E6_AD_A5_E9_c67_294143.htm 许多刚接触Linux的网络管理员发现，他们很难由指向点击式的安全配置界面转换到另一种基于编辑复杂而难以捉摸的文本文件的界面。本文列出七条管理员能够也应该可以做到的步骤，从而帮助他们建立更加安全的Linux服务器，并显著降低他们所面临的风险。 请任何大型机构的网络管理员对Linux和网络操作系统(如Windows NT或Novell)进行比较，可能他会承认Linux是一个内在更加稳定，扩展性更强的解决方案。可能他还会承认，在保护系统免受外部攻击方面，Linux可能是三者中最难配置的系统。 这种认识相当普遍许多刚接触Linux的网络管理员发现，他们很难由指向点击式的安全配置界面转换到另一种基于编辑复杂而难以捉摸的文本文件的界面。多数管理员充分认识到他们需要手工设置阻碍和障碍，以阻止可能的黑客攻击，从而保护公司数据的安全。只是在他们并不熟悉的Linux领域内，他们不确定自己的方向是否正确，或该从何开始 这就是本文的目的所在。它列出一些简易的步骤，帮助管理员保障Linux的安全，并显著降低他们面临的风险。本教程列出了七个这样的步骤，但您也可以在Linux手册和讨论论坛中发现更多内容。 保护根账户 Linux系统上的根账户(或超级用户账户)就像是滚石演唱会上的后台通行证一样它允许您访问系统中的所有内容。因此，值得采取额外的步骤对它加以保护。首先，用密码命令给这个账户设置一个难以猜测的密码，并定期进行修改，而且这个密码应仅限于公司内的几个主要

人物(理想情况下，只需两个人)知晓。 然后，对/etc/securetty文件进行编辑，限定能够进行根访问的终端。为避免用户让根终端“ 开放 ”，可设置TMOUT当地变量为非活动根登录设置一个使用时间.并将HISTFILESIZE当地变量设为0，保证根命令记录文件(其中可能包含机密信息)处于禁止状态。最后，制订一个强制性政策，即使用这个账户只能执行特殊的管理任务.并阻止用户默认以根用户服务登录。 提示：关闭这些漏洞后，再要求每一个普通用户必须为账户设立一个密码，并保证密码不是容易识别的启示性密码，如生日、用户名或字典上可查到的单词。 安装一个防火墙 防火墙帮助您过滤进出服务器的数据包，并确保只有那些与预定义的规则相匹配的数据包才能访问系统。有许多针对Linux的优秀防火墙，而且防火墙代码甚至可直接编译到系统内核中。首先应用ipchains或iptables命令为进出网络的数据包定义输入、输出和转寄规则。可以根据IP地址、网络界面、端口、协议或这些属性的组合制订规则。这些规则还规定匹配时应采取何种行为(接受、拒绝、转寄)。规则设定完毕后，再对防火墙进行详细检测，保证没有漏洞存在。安全的防火墙是您抵御分布式拒绝服务(DDoS)攻击这类常见攻击的第一道防线。 使用OpenSSH处理网络事务 在网络上传输的数据安全是客户-服务器构架所要处理的一个重要问题。如果网络事务以纯文本的形式进行，黑客就可能“ 嗅出 ”网络上传输的数据，从而获取机密信息。您可以用OpenSSH之类的安全壳应用程序为传输的数据建立一条“ 加密 ”通道，关闭这个漏洞。以这种形式对连接进行加密，未授权用户就很难阅读在网络主机间传输的数据。 100Test 下载频道开通，各类考试题目直接下载

。详细请访问 www.100test.com