Linux系统安全设置全面坚固你的系统 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/244/2021_2022_Linux_E7_B3_BB_E7_BB_c103_244549.htm 不久前，我以极大的耐心下载了最新的内核版本，那可是通过拨入连接完成的。在整个下载的过程中，我渴望有一天在家里就能使用高速的Internet连接。xDSL和线缆猫的到来使其成为可能，但这并不包括价格因素。 在我写此文章的同时，在世界的某个地方，也许正有一个人在他家里的计算机上第一次安装发布的Linux。一个新的Linux的管理员通过为其家人和朋友设置帐户来使系统运转起来。也许在初次安装完成后的不长时间里，这个Linux系统就会以令人感激涕零的高速DSL接入Internet。 还是容易被攻击 今天几近所有可用的linux发布在安全方面存在漏洞，其中的多数漏洞是很容易被攻入的，但不幸的是依惯例和习惯做法，他们是开放的。典型安装的Linux首次启动时就提供了多种多样的可被攻击的服务，譬如SHELL,IMAP和POP3。这些服务经常会被游手好闲的网民按其需要用来作为系统突破的切入点，这不仅是Linux的局限 -- 久经风霜的商业UNIX也提供此类服务，而且也会被突破。 不用抱怨和指责，新系统的锁定(坚固系统的专业说法)是非常重要的。信不信由你，一个Linux系统的坚固过程是不需要过多的系统安全专门知识。实际上，你可以在5分钟之内就可以将百分之九十的不可靠因素屏蔽掉。 开始吧 在开始坚固系统前，要问清自己你的机器担当的角色和用来接入Internet的舒适度。要仔细确定你要对整个世界范围提供的服务，如果你还不能确定，最好什么也不要做。明确自己的安全策略是非常重要的。要决定你自己

的系统上哪些使用是可接受的而哪些是不可接受的。 本文中范例机器的目标是作为工作站用来收发mail，阅读新闻，浏览网页等等。 确立网络服务安全 首先，以超级用户(root)登入系统，用netstat命令(这是多数Linux系统标配的网络工具)查看一下当前的网络状态，输出的结果譬如是： root@percy / ]# netstat -a Active Internet connections (servers and established) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 *:imap2 *:* LISTEN tcp 0 0 *:pop-3 *:* LISTEN tcp 0 0 *:linuxconf *:* LISTEN tcp 0 0 *:auth *:* LISTEN tcp 0 0 *:finger *:* LISTEN tcp 0 0 *:login *:* LISTEN tcp 0 0 *:shell *:* LISTEN tcp 0 0 *:telnet *:* LISTEN tcp 0 0 *:ftp *:* LISTEN tcp 0 0 *:6000 *:* LISTEN udp 0 0 *:ntalk *:* udp 0 0 *:talk *:* udp 0 0 *:xdmcp *:* raw 0 0 *:icmp *:* 7 raw 0 0 *:tcp *:* 7 如你所见到的输出结果，最初的安装对一定数量的服务并未侦听，而这些服务的大多数就是麻烦的制造者，在配置文件/etc/inetd.conf中就可以行使禁止。 用你喜欢的文本编辑器打开这个文件，注销你不想提供的服务，这只需在包含服务内容的行前面添加一个`#，在本例中所有的服务都被注销了，当然，如果你决定要提供这些服务中的某几个，那由你自己来决定。 现在，重新启动 inetd 来使这些改变的内容起作用，这根据系统的不同会有多种方法，一个例子是： killall -HUP inetd,依诀窍，重新用netstat检查开放的socket并注意发生的变化。接下来，查看还有哪些进程在运行。通常会看到sendmail、lpd和snmd 在等待接入的请求。因此机器不对此类的任何请求提供服务，所以他们应当终止运行。 通常，这些服务是由系统初始化脚本启动，脚本会因发布的不同而异，一般可以在/etc/init.d 或 /etc/rc.d中找到。如果

你还不能确定，请参照你所用发布的文档。目标是在系统启动时禁止脚本启动这些服务。 如果你的Linux发布使用的是打包的系统，花点时间移掉你不需的服务。在此范例机器中，包括了sendmail和r字头的服务进程(rwho、rwall等)，lpd、ucd-snmp和apache。这是确保此类服务不会因意外而激活的最简捷的途径。 X坚固手段 近来多数的发布都支持机器首次启动时就登陆进入X窗口例如xdm进行管理，不幸的是，这也是主要的攻击点。默认方式下，机器允许任何主机请求登陆窗口，即使此机器仅仅只有一个用户直接从控制台登陆，这种特性亦需屏蔽。 配置文件会赖于你所使用的登陆管理器而变化。本机选用xdm,故而/usr/X11R6/lib/X11/Xaccess文件需进行修改，添加一个`#符号来阻止启动此服务。我的Xaccess如下设置： #* #any host can get a login window #* #any indirect host can get a chooser再次启动xdm时此设置有效。 软件升级 现在一些基本的坚固措施已完成，需要时时注意发行商对发布的升级和增强。缺乏甚至没有维护会是危及系统安全的一大因素。 对开放源代码软件的保障之一是其在不断的发展中，有许多人花费大量的时间在不停地寻找安全方面存在的缺陷。这直接导致了Linux发布不断的维护过程，经常会有升级程序、臭虫补丁程序和安全方面的指导出现在网页中。隔几天或几周就浏览一下发布商的网页看是否有补丁或升级程序贴出来。 后续工作 现在，经处理过的机器比其初次安装后的安全性已提高了，但决不是对任何攻击就牢不可破了，但已不存在明显的可攻击之处了。在此列出的方法就象给你的车子或房子加了锁，一般水平的小偷就会被这类措施所动摇，意识到这是落锁的转而寻找其他没有加以保护的系统。 如果

你认定这些措施没有提供足够的安全性能，也许你还想通过Internet提供一些网络服务，在进行之前需要花费一些时间寻找更高级的安全技术。 但不幸的是，许多Linux的发布商假定他们的客户已经熟知这些服务而且也想使用他们。但对初始用户通常这不是事实，当然，在Linux系统的安全性完全保障之前还有大量的未开发领域。而这些步骤就是对已知晓的系统漏洞加以最基本的安全保障。 时至今日，对于危及系统和网络安全的多数保护手段还相对较弱，而随着Linux的流行且高速Internet存取逐渐实现的时刻，涌向未经预防的Linux 系统的攻击会越来越多 