如何搭建安全的Linux操作系统平台 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E5_A6_82_E4_BD_95_E6_90_AD_E5_c103_145286.htm 到目前为止，您安装了Linux的计算机如果还没有任何安全措施的话，那我觉得您应该了解一些有关Linux的安全知识了，并且在此基础上运用本文介绍的方法让您的Linux平台更安全。当然，我只是根据自己的需求来让加固Linux平台的，所以不一定能够完全满足您的要求，但是我想也应该会有一些帮助。 安全需求 在家里，我使用的是Red Hat Linux。一般来说，我很少关机，也经常使用这台机器通过宽带连在互联网上。也就是说，我的机器一般情况下都处于在线状态。对于这台计算机的安全性，我有两点考虑： 1. 我要把那些不想让别人看见的数据和文档隐藏起来； 2.不让不速之客用我的计算机资源。 在我的电脑上，有很多重要的数据。我想大部分人电脑上都有自己认为很重要的文档和数据。我不想让除了我之外的任何人读写这些文件。此外，我不想让入侵者使用我的机器来攻击另外一个目标。如果我发现有人使用我的机器来攻击别人，我会感到很气愤。相信大家也会与我有同感。更令人忐忑不安的问题是，有时虽然我们被“ 黑 ”，充当了攻击别人系统的角色，而自己却蒙在鼓里。 做好安全计划 在开始安装Linux系统时，我就要在内核中配置Iptables。Iptabels被认为是Linux中实现包过滤功能的第四代应用程序。第一代是Linux内核1.1版本所使用的，Alan Cox从BSD Unix中移植过来的ipfw。 在Linux 2.0版的内核中，Jos Vos和其它一些程序员对ipfw进行了扩展，并且添加了ipfwadm用户工具。在Linux2.2版内核中

，Russell和Michael Neuling做了一些非常重要的改进。也就是在该内核中，Russell添加了帮助用户控制过滤规则的ipchains工具。现在，Russell又完成了其名为NetFilter的内核框架。NetFilter的目的是为用户提供一个专门用于包过滤的底层结构。并且，用户和开发人员还可以将其内建在Linux内核中。Iptables是一个内建在NetFilter框架中的模块。它可以让用户访问内核过滤规划和命令。如果您了解ipchains，就会发现事实上Iptables和ipchains是非常相似的。 通过对Iptables的配置，我可以阻止任何一个数据包进入或者离开我的机器。这非常重要，因为我的机器24小时在线。有了这个新的保护功能，就使得我的机器时刻都能阻击来自网络上的各种攻击。Iptables的使用和配置并不困难。在此限于篇幅，我就不再讨论(读者可以很容易就在网上找到相关资料)。 接下来要讨论的是LIDS(Linux入侵检测系统)。LIDS以内核补丁的方式存在。LIDS的目的是通过限制对计算机文件和进程的访问，来提高计算机的安全性。在有人试图破坏这些限制时，它就会向你报警。LIDS另外一个优点就是它甚至可以限制root账号的权限。这种限制root账号权限的方法，在入侵者得到root权限时，可以最大限度地降低损失。我使用LIDS来保护二进制系统文件、/var/log目录下的日志文件、/etc目录下的配置文件。我将其标志为Readonly的二进制文件没有任何用户，包括root在内，可以对其进行删改操作。对于日志文件，我将其标识为Append。这样对于该目录里的文件，可以进行写操作，但是不能修改或者删除现存的数据。 下一步我要做的就是要尽量减少在机器上运行的服务。在机器上运行的服务越少，别人入侵我的机器的可能性就越小。在缺省情况下，很

多Linux发行版都会运行很多常驻程序。就我个人看来，这样做并不是十分合理的。所以我关闭了我的Telnet、FTP以及所有以“ R ”字母开头的常驻程序。这样，我就可以避免有时候来不及升级或者安装一些补丁程序而给系统带来威胁。对于那些我一定要使用的服务，我就会尽可能及时地安装安全补丁。并且，如果该服务发现了漏洞，而又没有相关的补丁出现时，我就会暂时关闭该服务，直到有修正补丁出现为止。一旦尽量减少了计算机上运行的服务数量之后，我就使用“ netstat l ”命令来进行监听。这样做的目的是为了确保我没有遗漏任何我不需要的服务。事实上，不做任何监听工作是我们经常容易犯的错误。如果监听到任何我不需要的服务，这时候就可以修正了。