深入分析Linux操作系统深度安全加固（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E5_88_86_E6_c103_144459.htm Linux 的系统安全不容忽视.然而系统加固又不是一件很容易的事.本文作者简单介绍了一下 Linux 系统深度安全加固。 注：以下内容可能不适用于某些场合，请对号入座 1. 安装和升级 尽量选用最新的 Linux 发行版本，安装前拔掉网线，断开物理连接，安装时建议用 custom 自定义方式安装软件包，数量以少为好，一般来说服务器没有必要安装 X-windows，在 lilo/grub 引导器中加入口令限制，防止能够物理接触的恶意用户因为 Linux 安装光盘的 rescue 模式可以跳过这个限制，所以还要给bios加上密码或服务器机箱上锁 /var， /home， /usr， /root 等目录用独立的物理分区，防止垃圾数据和日志填满硬盘而导致 D.o.S 攻击。 root 账号给予强壮的口令，安装完毕立即用 up2date 或 apt 升级系统软件，有时升级内核也是必要的，因为内核出现问题同样会给攻击者提供机会Apt 是 Debian GNU Linux 下的一个强大的包管理工具，也可用于其他版本的 Linux. 2. 账号 如果系统中的用户比较多，可以编辑 /etc/login.defs，更改密码策略,删除系统中不必要帐户和组: [root@ayazero /]# userdel -r username如果不开匿名 ftp 则可以把 ftp 账号也删了。最安全的方式是本地维护，可惜不太现实，但还是需要限制 root 的远程访问，管理员可以用普通账户远程登录，然后 su 到 root，我们可以把使用 su 的用户加到 wheel 组来提高安全性在 /etc/pam.d/su 文件的头部加入下面两行： auth sufficient /lib/security/pam_rootok.so debug auth required

/lib/security/pam_wheel.so group=wheel然后把可以执行 su 的用户放入 wheel 组：[root@ayazero /]# usermod -G10 admin编辑/etc/securetty，注释掉所有允许 root 远程登录的控制台，然后禁止使用所有的控制台程序：[root@ayazero /]# rm -f /etc/security/console.apps/servicename登录采用加密的 ssh，如果管理员只从固定的终端登陆，还应限制合法 ssh 客户端的范围防止嗅探及中间人攻击，将命令历史纪录归为零，尽可能的隐藏你做过的事情：[root@ayazero /]# unset HISTFILESIZE