Linux服务器安全配置Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/642/2021_2022_Linux_E6_9C_8D_E5_8A_c103_642569.htm 众所周知，网络安全是一个非常重要的课题，而服务器是网络安全中最关键的环节。Linux被认为是一个比较安全的Internet服务器，作为一种开放源代码操作系统，一旦Linux系统中发现有安全漏洞，Internet上来自世界各地的志愿者会踊跃修补它。然而，系统管理员往往不能及时地得到信息并进行更正，这就给黑客以可乘之机。相对于这些系统本身的安全漏洞，更多的安全问题是由不当的配置造成的，可以通过适当的配置来防止。服务器上运行的服务越多，不当的配置出现的机会也就越多，出现安全问题的可能性就越大。对此，下面将介绍一些增强Linux/Unix服务器系统安全性的知识。 一、系统安全记录文件 操作系统内部的记录文件是检测是否有网络入侵的重要线索。如果您的系统是直接连到Internet，您发现有很多人对您的系统做Telnet/FTP登录尝试，可以运行\"#more /var/log/secure | grep refused\"来检查系统所受到的攻击，以便采取相应的对策，如使用SSH来替换Telnet/rlogin等。 二、启动和登录安全性 1．BIOS安全 设置BIOS密码且修改引导次序禁止从软盘启动系统。 2．用户口令 用户口令是Linux安全的一个基本起点，很多人使用的用户口令过于简单，这等于给侵入者敞开了大门，虽然从理论上说，只要有足够的时间和资源可以利用，就没有不能破解的用户口令，但选取得当的口令是难于破解的。较好的用户口令是那些只有他自己容易记得并理解的一串字符，并且绝对不要在任何地方写出来。 3．默认账号 应该

禁止所有默认的被操作系统本身启动的并且不必要的账号，当您第一次安装系统时就应该这么做，Linux提供了很多默认账号，而账号越多，系统就越容易受到攻击。 可以用下面的命令删除账号。 # userdel用户名 或者用以下的命令删除组用户账号。 # groupdel username 4．口令文件 chattr命令给下面的文件加上不可更改属性，从而防止非授权用户获得权限。 # chattr i /etc/passwd # chattr i /etc/shadow # chattr i /etc/group # chattr i /etc/gshadow 5．禁止Ctrl Alt Delete重新启动机器命令 修改/etc/inittab文件，将\"ca::ctrlaltdel:/sbin/shutdown -t3 -r now\"一行注释掉。然后重新设置/etc/rc.d/init.d/目录下所有文件的许可权限，运行如下命令： # chmod -R 700 /etc/rc.d/init.d/* 这样便仅有root可以读、写或执行上述所有脚本文件。 6．限制su命令 如果您不想任何人能够su作为root，可以编辑/etc/pam.d/su文件，增加如下两行： auth sufficient /lib/security/pam_rootok.so debug auth required /lib/security/pam_wheel.so group=isd 这时，仅isd组的用户可以su作为root。此后，如果您希望用户admin能够su作为root，可以运行如下命令： # usermod -G10 admin 7．删减登录信息 默认情况下，登录提示信息包括Linux发行版、内核版本名和服务器主机名等。对于一台安全性要求较高的机器来说这样泄漏了过多的信息。可以编辑/etc/rc.d/rc.local将输出系统信息的如下行注释掉。 # This will overwrite /etc/issue at every boot. So， make any changes you # want to make to /etc/issue here or you will lose them when you reboot. # echo \"\" gt.gt.gt.&gt. /etc/issue 然后，进行如下操作： # rm -f /etc/issue # rm -f /etc/issue.net # touch /etc/issue # touch /etc/issue.net 100Test 下载频道开通，各