Linux网络安全之经验谈(1) PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/143/2021_2022_Linux_E7_BD_91_E7_BB_c103_143824.htm 关于分区 一个潜在的黑客如果要攻击你的Linux服务器，他首先就会尝试缓冲区溢出。在过去的几年中，以缓冲区溢出为类型的安全漏洞是最为常见的一种形式了。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以轻易使得一个匿名的Internet用户有机会获得一台主机的部分或全部的控制权！ 为了防止此类攻击，我们从安装系统时就应该注意。如果用root分区纪录数据，如log文件和email，就可能因为拒绝服务产生大量日志或垃圾邮件，从而导致系统崩溃。所以建议为/var开辟单独的分区，用来存放日志和邮件，以避免root分区被溢出。最好为特殊的应用程序单独开一个分区，特别是可以产生大量日志的程序，还有建议为/home单独分一个区，这样他们就不能填满/分区了，从而就避免了部分针对Linux分区溢出的恶意攻击。 关于BIOS 记着要在BIOS设置中设定一个BIOS密码，不接收软盘启动。这样可以阻止不怀好意的人用专门的启动盘启动你的Linux系统，并避免别人更改BIOS设置，如更改软盘启动设置或不弹出密码框直接启动服务器等等。 关于口令 口令是系统中认证用户的主要手段，系统安装时默认的口令最小长度通常为5，但为保证口令不易被猜测攻击，可增加口令的最小长度，至少等于8。为此，需修改文件/etc/login.defs中参数PASS_MIN_LEN（口令最小长度）。同时应限制口令使用时间，保证定期更换口令，建议修改参数PASS_MIN_DAYS（口令使用时间）。 关于Ping 既然没有

人能ping通你的机器并收到响应，你可以大大增强你的站点的安全性。你可以加下面的一行命令到/etc/rc.d/rc.local，以使每次启动后自动运行，这样就可以阻止你的系统响应任何从外部/内部来的ping请求。 echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all 