Linux下常用日志分析工具Logcheck简介 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/267/2021_2022_Linux_E4_B8_8B_E5_B8_c103_267179.htm 对于拥有大量账户、系统繁忙的Linux系统而言，其日志文件是极其庞大的，很多没有用的信息会将值得注意的信息淹没，给用户分析日志带来了很大的不便。现在有一些专门用于分析日志的工具，如Logcheck和Friends。 Logcheck用来分析庞大的日志文件，过滤出有潜在安全风险或其他不正常情况的日志项目，然后以电子邮件的形式通知指定的用户。它是由Psionic开发的，可以到http://www.psionic.com/tools/logcheck-1.1.1.tar.gz下载。或者去http://www.psionic.com/abacus /logcheck/看看是否有新的版本。 该程序的安装相当方便。解压后运行make文件，按照它的提示选择操作系统的类型以后就能编译完成了。配置文件和运行脚本默认安装在/usr/local/etc/下。 logcheck.sh 这是Logcheck的shell脚本，用于分析本次的日志文件并汇报结果。 logcheck.hacking 这个文件设置在日志文件中过滤的关键字，该关键字提示了潜在安全风险的信息。用户可以定制自己的日志文件，在logcheck.hacking文件中增加或删除关键字。 logcheck.violations 这个文件设置在日志文件分析过滤系统运行时出现异常情况的关键字。 logcheck.violations.ignore 如果系统出现异常情况，但含有此文件中的关键字，则视为正常，不写入Logcheck的分析报告文件中。 logcheck.ignore 如果系统日志文件记录了可能遭遇攻击的消息，但含有logcheck.ignore文件中的关键字，则Logcheck视为正常，在分析报告文件中不包含这些消息。 安装完Logcheck后，还要修改logcheck.sh文

件中的参数以符合用户的要求。有两点值得注意。下列命令：# Person to send log activity to.SYSADMIN=root Logcheck默认将报告发给root。如果要发给指定的电子邮箱，改动这里就可以了。如果希望将报告发给多个用户，可以定义mail的别名。要检查的日志文件的设置：# Linux$LOGTAIL /var/log/syslog > $TMPDIR/check.$ $LOGTAIL /var/log/messages >> $TMPDIR/check.$用户可以根据需要加上要检查的日志文件例如：$LOGTAIL /var/log/auth.log >> $TMPDIR/check.$$LOGTAIL /var/log/deamon.log >> $TMPDIR/check.$$LOGTAIL /var/log/mail.log >> $TMPDIR/check.$ 最后用cron安排服务器自动定时重复执行logcheck.sh脚本文件。