

Linux操作系统常用安全检查方法概括介绍 PDF转换可能丢失
图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/251/2021_2022_Linux_E6_93_8D_E4_BD_c103_251754.htm 检查系统密码文件,查看文件修改日期 [root@fedora ~]# ls -l /etc/passwd 查看passwd文件中有哪些特权用户 [root@fedora ~]# awk -F: \$3==0 {print \$1} /etc/passwd 查看系统里有没有空口令帐户 awk -F: length(\$2)==0 {print \$1} /etc/shadow 检查系统守护进程 cat /etc/inetd.conf | grep -v "^#" 检查网络连接和监听端口 netstat an netstat rn ifconfig a 查看正常情况下登录到本机的所有用户的历史记录 last 检查系统中的core文件 find / -name core -exec ls -l {} \. 检查系统文件完整性 rpm -qf /bin/ls rpm -qf /bin/login md5sum b 文件名 md5sum t 文件名 查找是否有后门 cat /etc/crontab ls /var/spool/cron/ cat /etc/rc.d/rc.local ls /etc/rc.d ls /etc/rc3.d find / -type f -perm 4000 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com