

Linux操作系统安全性能检查笔记 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_251758.htm Linux安全检查笔记 1

1. Accounts检查 # less /etc/passwd # grep :0: /etc/passwd 注意新的用户，和UID,GID是0的用户。 2. Log检查 注意“entered promiscuous mode” 注意错误信息 注意Remote Procedure Call (rpc) programs with a log entry that includes a large number (> 20) strange

characters(-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM) 最后一条目前还没理解，也没碰到过，请指点。 3. Processes检查 # ps -aux 注意UID是0的 # lsof -p 可疑的进程号 察看该进程所打开端口和文件 4. Files检查 # find / -uid 0 perm -4000 print # find / -size 10000k print # find / -name “...” print # find / -name “..” print # find / -name “.” print # find / -name “ ” print 注意SUID文件，可疑大于10M，...，...，...和空格文件 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