 Linux安全检查笔记 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 