深入分析Linux操作系统深度安全加固（2） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E5_88_86_E6_c103_144455.htm 3. 服务 最少服务原则，凡是不需要的服务一律注释掉在 /etc/inetd.conf 中不需要的服务前加 "#"，较高版本中已经没有 inetd 而换成了 Xinetd. 取消开机自动运行服务，把 /etc/rc.d/rc3.d 下不需要运行的服务第一个字母大写改称小写，或者由 setup 命令启动的 GUI 界面中的 service 更改。 如果你希望简单一点，可以使用 /etc/host.allow，/etc/host.deny 这两个文件，但是本文计划用 iptables 防火墙，所以不在此详述。 4. 文件系统权限 找出系统中所有含 "s" 位的程序，把不必要得 "s" 位去掉，或者把根本不用的直接删除: [root@ayazero /]# find / -type f (-perm -04000 -o -perm -02000) -exec ls -lg {} [root@ayazero /]# chmod a-s filename防止用户滥用及提升权限的可能性,把重要文件加上不可改变属性: [root@ayazero /]# chattr i /etc/passwd [root@ayazero /]# chattr i /etc/shadow [root@ayazero /]# chattr i /etc/gshadow [root@ayazero /]# chattr i /etc/group [root@ayazero /]# chattr i /etc/inetd.conf [root@ayazero /]# chattr i /etc/httpd.conf .....具体视需要而定，我怀疑现在的入侵者都知道这个命令，有些 exploit 溢出后往 inetd.conf 写一条语句绑定 shell 在一个端口监听，此时这条命令就起了作用，浅薄的入侵者会以为溢出不成功。找出系统中没有属主的文件: [root@ayazero /]# find / -nouser -o -nogroup找出任何人都有写权限的文件和目录: [root@ayazero /]# find / -type f (-perm -2 -o -perm -20) -exec ls -lg {} [root@ayazero /]# find / -type d (-perm

-2 -o -perm -20) -exec ls -ldg {}防止入侵者向其中写入木马语句(诸如一个shell的拷贝)或继承属主权限而非法访问。找出并加固那些历来被入侵者利用的文件，比如 .rhosts。编辑 /etc/security/limits.conf，加入或改变如下行: * hard core 0 * hard rss 5000 * hard nproc 20 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