Linux网络安全之经验谈(4) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022_Linux_E7_BD_91_E7_BB_c103_645711.htm 关于用户资源 对你的系统上所有的用户设置资源限制可以防止DoS类型攻击，如最大进程数，内存数量等。例如，对所有用户的限制， 编辑/etc/security/limits.con加入以下几行： * hard core 0 * hard rss 5000 * hard nproc 20 你也必须编辑/etc/pam.d/login文件，检查这一行的存在： session required /lib/security/pam_limits.so 上面的命令禁止core files “ core 0 ”，限制进程数为“ nproc 50 “，且限制内存使用为5M “ rss 5000 ”。 关于NFS服务器 由于NFS服务器漏洞比较多，你一定要小心。如果要使用NFS网络文件系统服务，那么确保你的/etc/exports具有最严格的存取权限设置，不意味着不要使用任何通配符，不允许root写权限，mount成只读文件系统。你可以编辑文件/etc/exports并且加： /dir/to/export host1.mydomain.com(ro,root_squash) /dir/to/export host2.mydomain.com(ro,root_squash) 其中/dir/to/export 是你想输出的目录，host.mydomain.com是登录这个目录的机器名，ro意味着mount成只读系统，root_squash禁止root写入该目录。最后为了让上面的改变生效，还要运行/usr/sbin/exportfs -a 关于开启的服务 默认的linux就是一个强大的系统，运行了很多的服务。但有许多服务是不需要的，很容易引起安全风险。这个文件就是/etc/inetd.conf，它制定了/usr/sbin/inetd将要监听的服务，你可能只需要其中的两个：telnet和ftp，其它的类如shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth, etc. 除非你真的

想用它。否则统统关闭之。 你先用下面的命令显示没有被注释掉的服务： grep -v "#" /etc/inetd.conf 这个命令统计面前服务的总数： ps -eaf|wc -l 需要提醒你的是以下三个服务漏洞很多，强烈建议你关闭它们：S34yppasswdd（NIS服务器）、S35ypserv（NIS服务器）和S60nfs（NFS服务器）。 我们可以运行#killall -HUP inetd来关闭不需要的服务。当然，你也可以运行 #chattr i /etc/inetd.conf 如果你想使inetd.conf文件具有不可更改属性，而只有root 才能解开，敲以下命令 #chattr -i /etc/inetd.conf 当你关闭一些服务以后，重新运行以上命令看看少了多少服务。运行的服务越少，系统自然越安全了。我们可以用下面命令察看哪些服务在运行： netstat -na --ip 如果你用的是Redhat那就方便多了。^_^ Redhat提供一个工具来帮助你关闭服务，输入/usr/sbin/setup，然后选择"system services"，就可以定制系统启动时跑哪些服务。另外一个选择是chkconfig命令，很多linux版本的系统都自带这个工具。脚本名字中的数字是启动的顺序，以大写的K开头的是杀死进程用的。 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