让Linux更安全的超简配置法Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_AE_A9Linux_E6_9B_c103_644710.htm 一、磁盘分区 1、如果是新安装系统，对磁盘分区应考虑安全性： 1)根目录(/)、用户目录(/home)、临时目录(/tmp)和/var目录应分开到不同的磁盘分区. 2)以上各目录所在分区的磁盘空间大小应充分考虑，避免因某些原因造成分区空间用完而导致系统崩溃. 2、对于/tmp和/var目录所在分区，大多数情况下不需要有suid属性的程序，所以应为这些分区添加nosuid属性. 方法一：修改/etc/fstab文件，添加nosuid属性字。例如： /dev/hda2 /tmp ext2 exec,dev,nosuid,rw 0 0 ^^^^^^ 方法二：如果对/etc/fstab文件操作不熟，建议通过linuxconf程序来修改。 * 运行linuxconf程序. * 选择"File systems"下的"Access local drive". * 选择需要修改属性的磁盘分区. * 选择"No setuid programs allowed"选项. * 根据需要选择其它可选项. * 正常退出。(一般会提示重新mount该分区) 二、安装 1、对于非测试主机，不应安装过多的软件包。这样可以降低因软件包而导致出现安全漏洞的可能性。 2、对于非测试主机，在选择主机启动服务时不应选择非必需的服务。例如routed、ypbind等。 三、安全配置与增强 内核升级。起码要升级至2.2.16以上版本。 GNU libc共享库升级。(警告：如果没有经验，不可轻易尝试。可暂缓。) 关闭危险的网络服务。echo、chargen、shell、login、finger、NFS、RPC等 关闭非必需的网络服务。talk、ntalk、pop-2等 常见网络服务安全配置与升级 确保网络服务所使用版本为当前最新和最安全的版本。 取消匿名FTP访问 去除非必需的suid程序 使

用tcpwrapper 使用ipchains防火墙 日志系统syslogd 一些细节：1.操作系统内部的log file是检测是否有网络入侵的重要线索，当然这个假定你的logfile不被侵入者所破坏，如果你有台服务器用专线直接连到Internet上，这意味着你的IP地址是永久固定牡 刂罚慷岱⑾钟泻芏嗳硕阅愕南低匙elnet/ftp登录尝试，试着运行#more /var/log/secure | grep refused 去检查。 2. 限制具有SUID权限标志的程序数量，具有该权限标志的程序以root身份运行，是一个潜在的安全漏洞，当然，有些程序是必须要具有该标志的，象passwd程序。 3.BIOS安全。设置BIOS密码且修改引导次序禁止从软盘启动系统。 4. 用户口令。用户口令是Linux安全的一个最基本的起点，很多人使用的用户口令就是简单的‘ password，这等于给侵入者敞开了大门，虽然从理论上说没有不能确解的用户口令，只要有足够的时间和资源可以利用。比较好的用户口令是那些只有他自己能够容易记得并理解的一串字符，并且绝对不要在任何地方写出来。 5./etc/exports 文件。如果你使用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。编辑文件/etc/exports并且加：例如： /dir/to/export host1.mydomain.com(ro,root_squash) /dir/to/export host2.mydomain.com(ro,root_squash) /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。 为了让上面的改变生效，运行/usr/sbin/exportfs -a 6.确信/etc/inetd.conf的所有者是root，且文件权限设置为600 。[root@deep]# chmod 600 /etc/inetd.conf ENSURE that the owner is

root. [root@deep]# stat /etc/inetd.conf File: "/etc/inetd.conf" Size: 2869 Filetype: Regular File Mode: (0600/-rw-------) Uid: (0/ root) Gid: (0/ root) Device: 8,6 Inode: 18219 Links: 1 Access: Wed Sep 22 16:24:16 1999(00000.00:10:44) Modify: Mon Sep 20 10:22:44 1999(00002.06:12:16) Change:Mon Sep 20 10:22:44 1999(00002.06:12:16) 编辑/etc/inetd.conf禁止以下服务： ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth, etc. 除非你真的想用它。 特别是禁止那些r命令.如果你用ssh/scp，那么你也可以禁止掉telnet/ftp。 为了使改变生效，运行#killall -HUP inetd 你也可以运行#chattr i /etc/inetd.conf使该文件具有不可更改属性。 只有root才能解开，用命令#chattr -i /etc/inetd.conf 7. TCP_WRAPPERS 默认地，Redhat Linux允许所有的请求,用TCP_WRAPPERS增强你的站点的安全性是举手 之劳，你可以放入“ ALL: ALL ”到/etc/hosts.deny中禁止所有的请求，然后放那些明确允许的请求到/etc/hosts.allow中，如: sshd: 192.168.1.10/255.255.255.0 gate.openarch.com 对IP地址192.168.1.10和主机名gate.openarch.com，允许通过ssh连接。 配置完了之后，用tcpdchk检查 [root@deep]# tcpdchk tcpchk是TCP_Wrapper配置检查工具， 它检查你的tcp wrapper配置并报告所有发现的潜在/存在的问题。 8. 别名文件aliases 编辑别名文件/etc/aliases(也可能是/etc/mail/aliases)，移走/注释掉下面的行。 # Basic system aliases -- these MUST be present. MAILER-DAEMON: postmaster postmaster: root # General redirections for pseudo accounts. bin: root daemon: root #games: root ?remove or comment out. #ingres: root ?remove or comment out. nobody: root 100Test