深入分析Linux操作系统深度安全加固 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E6_B7_B1_E5_85_A5_E5_88_86_E6_c103_145243.htm Linux 的系统安全不容忽视.然而系统加固又不是一件很容易的事.本文作者简单介绍了一下Linux 系统深度安全加固。 注：以下内容可能不适用于某些场合，请对号入座 1. 安装和升级 尽量选用最新的 Linux 发行版本，安装前拔掉网线，断开物理连接，安装时建议用 custom 自定义方式安装软件包，数量以少为好，一般来说服务器没有必要安装 X-windows，在 lilo/grub 引导器中加入口令限制，防止能够物理接触的恶意用户因为 Linux 安装光盘的 rescue 模式可以跳过这个限制，所以还要给bios加上密码或服务器机箱上锁 /var， /home， /usr， /root 等目录用独立的物理分区，防止垃圾数据和日志填满硬盘而导致 D.o.S 攻击。 root 账号给予强壮的口令，安装完毕立即用 up2date 或 apt 升级系统软件，有时升级内核也是必要的，因为内核出现问题同样会给攻击者提供机会Apt 是 Debian GNU Linux 下的一个强大的包管理工具，也可用于其他版本的 Linux. 2. 账号 如果系统中的用户比较多，可以编辑 /etc/login.defs，更改密码策略,删除系统中不必要帐户和组: [root@ayazero /]# userdel -r username 如果不开匿名 ftp 则可以把 ftp 账号也删了。最安全的方式是本地维护，可惜不太现实，但还是需要限制 root 的远程访问，管理员可以用普通账户远程登录，然后 su 到 root，我们可以把使用 su 的用户加到 wheel 组来提高安全性在 /etc/pam.d/su 文件的头部加入下面两行： auth sufficient /lib/security/pam_rootok.so debug auth required

/lib/security/pam_wheel.so group=wheel 然后把可以执行 su 的用户放入 wheel 组： [root@ayazero /]# usermod -G10 admin 编辑 /etc/securetty，注释掉所有允许 root 远程登录的控制台，然后禁止使用所有的控制台程序： [root@ayazero /]# rm -f /etc/security/console.apps/servicename 登录采用加密的 ssh，如果管理员只从固定的终端登陆，还应限制合法 ssh 客户端的范围防止嗅探及中间人攻击，将命令历史纪录归为零，尽可能的隐藏你做过的事情： [root@ayazero /]# unset HISTFILESIZE 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 5. Banner 伪装 入侵者通常通过操作系统，服务及应用程序版本来攻击，漏洞列表和攻击程序也是按此来分类，所以我们有必要作点手脚来加大入侵的难度。 更改 /etc/issue，因为 reboot 后重新加载，所以编辑 /ect/rc.d/rc.local： # This will overwrite /etc/issue at every boot. So， make any changes you # want to make to /etc/issue here or you will lose them when you reboot. #echo "" > /etc/issue #echo "$R" >> /etc/issue #echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue # #cp -f /etc/issue /etc/issue.net #echo >> /etc/issue Apache 不回显版本，apache 的配置文件，找到 ServerTokens 和 ServerSignature 两个 directive，修改默认属性： #ServerTokens Full ServerTokens Prod 修改 uname，拿出 uname.c 的源码，找到如下行： print_element (PRINT_SYSNAME， name.sysname).//操作系统名如 linux print_element (PRINT_NODENAME， name.nodename).//主机名 print_element (PRINT_RELEASE， name.release).//发行版本，如：2.4.20-18 print_element (PRINT_VERSION， name.version).// print_element (PRINT_MACHINE，

name.machine).//机器类型，如i686 print_element (PRINT_PROCESSOR， processor).//处理器类型 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