□□Linux 安全加固

□□注:红色字体暂时没有做操作

□□1.严格按照用户类型分配账号

□□2.系统无效帐户清理

□□检查无用账户More /etc/passwd

□□备份Cp -p /etc/passwd/etc/passwd_bak 锁定Passwd -1 username
检查是否存在空密码的账户 Logins -p 应无回应 备份

□□#cp -p /etc/passwd /etc/passwd_bak cp -p /etc/shadow /etc/shadow_bak

□□锁定 passwd -1 username 或加密 passwd username

□□3.禁止限制超级管理员远程登录

□□4.对系统账号进行登录限制 Vi /etc/passwd 例如修改

□□lynn:x:500:500::/home/lynn:/sbin/bash 更改为:

□□lynn:x:500:500::/home/lynn:/sbin/nologin 该用户就无法登录了。禁止所有用户登录。
touch /etc/nologin

□□除root以外的用户不能登录了。2、补充操作说明

□□禁止交互登录的系统账号,比如daemon,bin,sys、adm、lp、uucp、nuucp、smmsp等等

□□5.为空口令用户设置密码 pwd username

□□6.删除除ROOT以外UID为0的账户 检查方法:

□□#cat /etc/passwd 查看口令文件,口令文件格式如下:

□□login_name:password:user_ID:group_ID:comment:home_dir:command
login_name:用户名

□□password:加密后的用户密码

□□user_ID:用户ID,(1 ~ 6000)
若用户ID=0,则该用户拥有超级用户的权限。查看此处是否有多个ID=0。

□□group_ID:用户组ID

□□comment:用户全名或其它注释信息 home_dir:用户根目录

□□command:用户登录后的执行命令 备份方法:

□□#cp -p /etc/passwd /etc/passwd_bak 加固方法:

□□使用命令passwd -l <用户名>锁定不必要的超级账户。使用命令passwd -u <用户名>解锁需要恢复的超级账户。风险:需要与管理员确认此超级用户的用途。

□□7.设置系统口令策略

□□#vi /etc/login.defs修改配置文件

□□PASS_MAX_DAYS 90 #新建用户的密码最长使用天数 PASS_MIN_DAYS 0 #新建用户的密码最短使用天数

□□PASS_WARN_AGE 7 #新建用户的密码到期提前提醒天数 PASS_MIN_LEN 8 #最小密码长度8

□□8.设置关键目录的权限

□□通过chmod命令对目录的权限进行实际设置。2、补充操作说明

□□etc/passwd 必须所有用户都可读，root用户可写 –rw-r—r— /etc/shadow 只有root可读 –r--------

□□/etc/group 必须所有用户都可读，root用户可写 –rw-r—r— 使用如下命令设置：chmod 644 /etc/passwd

□□chmod 600 /etc/shadow chmod 644 /etc/group

□□如果是有写权限，就需移去组及其它用户对/etc的写权限(特殊情况除外) 执行命令#chmod -R go-w /etc

□□9.设置umask地址 检查方法:

□□#cat /etc/profile 查看umask的值 备份方法:

□□#cp -p /etc/profile /etc/profile_bak 加固方法：#vi /etc/profile

□□默认情况下是022 使用者是002 把022 改成027 umask=027

□□风险:会修改新建文件的默认权限，如果该服务器是WEB应用，则此项谨慎修改。TMOUT=180 export TMOUT

□□10.设置目录权限，防止非法访问目录需要重要目录 1、参考配置操作

□□查看重要文件和目录权限：ls –l 更改权限：

□□对于重要目录，建议执行如下类似操作：# chmod -R 750 /etc/init.d/*
这样只有root可以读、写和执行这个目录下的脚本。

□□11.设置关键文件的属性 # chattr +a /var/log/messages # chattr +i /var/log/messages.* # chattr +i /etc/shadow # chattr +i /etc/passwd # chattr +i /etc/group

□□12.对root为ls、rm设置别名 查看当前shell：

□□# echo $SHELL 如果是csh：# vi ~/.cshrc 如果是bash：

□□# vi ~/.bashrc 加入 alias ls ls -aol alias rm rm -i

□□重新登录之后查看是否生效。回退方案

□□通过chmod命令还原目录权限到加固前状态。

□□13. 限制能够su为root的用户 检查方法：

□□#cat /etc/pam.d/su,查看是否有auth required /lib/security/pam_wheel.so这样的配置条目
备份方法：#cp -p /etc/pam.d /etc/pam.d_bak 加固方法：#vi /etc/pam.d/su 在头部添加：

□□auth required /lib/security/pam_wheel.so group=wheel
这样，只有wheel组的用户可以su到root

□□#usermod -G10 test 将test用户加入到wheel组

□□
当系统验证出现问题时，首先应当检查/var/log/messages或者/var/log/secure中的输出信息，根据这些信息判断用户账号的有效

□□性。如果是因为PAM验证故障，而引起root也无法登录，只能使用single user或者rescue模式进行排错。

□□14.开放tmp目录的权限 chmod +t /tmp

□□15.启用日志记录功能

□□vi /etc/syslog.conf

□□# The authpriv file has restricted access. authpriv.* /var/log/secure

□□* auth, authpriv：主要认证有关机制，例如 telnet, login, ssh 等需要认证的服务都是使用此一机制

□□回退方案 vi /etc/syslog.conf，修改设置到系统加固前状态。

□□16.记录系统安全事件 1、参考配置操作

□□修改配置文件vi /etc/syslog.conf，配置如下类似语句：

□□*.err;kern.debug;daemon.notice; /var/adm/messages 定义为需要保存的设备相关安全事件

□□17.对ssh、su登录日志进行记录

□□1、参考配置操作 # vi /etc/syslog.conf 加入

□□# The authpriv file has restricted access. authpriv.* /var/log/secure 重新启动syslogd：

□□# /etc/rc.d/init.d/syslog restart

□□18.用记录cron行为日志功能 vi /etc/syslog.conf

□□# Log cron stuff cron.* /var/log/cron

□□19.增加ftpd审计功能

□□vi /etc/inetd.conf加入ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l -r -A -S

□□vi /etc/sysylog.conf中加入 ftp.* /var/log/ftpd 重启inetd进程 kill -1 'cat/var/run/inetd.pid'

□□使用ssh加密传输

□□从http://www.openssh.com/下载SSH并安装到系统。

□□20.设置访问控制列表 需要允许访问的主机列表 1、参考配置操作

□□
使用TCP_Wrappers可以使系统安全面对外部入侵。最好的策略就是阻止所有的主机(在“/etc/hosts.deny”文件中加入“ALL:ALL@ALL, PARANOID”)，然后再在“/etc/hosts.allow”文件中加入所有允许访问的主机列表。第一步：编辑hosts.deny文件 (vi /etc/hosts.deny)，加入下面该行：# Deny access to everyone. ALL: ALL@ALL, PARANOID

□□第二步：编辑hosts.allow文件(vi /etc/hosts.allow)，加入允许访问的主机列表，比如：ftp: 202.54.15.99 foo.com

□□202.54.15.99和 foo.com是允许访问ftp服务的IP地址和主机名称。

□□第三步：
tcpdchk程序是TCP_Wrapper设置检查程序。它用来检查你的TCP_Wrapper设置，并报告发现的潜在的和真实的问题。设置完后，运行下面这个命令：# tcpdchk

□□21.更改主机解析地址顺序 vi /etc/host.conf

□□#Lookup names via DNS first then fall back to /etc/hosts.order bind,hosts #We have machines with multiple IP addresses. multi on #Check for IP address spoofing nospoof on

□□22.打开syncookie缓解syn flood攻击 vi /etc/rc.d/rc.local加入

□□#echo 1 > /proc/sys/net/ipv4/tcp_syncookies

□□23.不响应ICMP请求 vi /etc/rc.d/rc.local加入

□□#echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all

□□24.提高未连接队列大小

□□sysctlnet.ipv4.tcp_max_syn_backlog

□□sysctl -w net.ipv4.tcp_max_syn_backlog="2048"直接运行

□□25.关闭无效服务

□□Cat /etc/inetd.conf 查看并记录当前的配置 实施步骤 1、参考配置操作

□□
取消所有不需要的服务，编辑“/etc/inetd.conf”文件，通过注释取消所有你不需要的服务(在该服务项目之前加一个“#”)。

□□第一步：更改“/etc/inetd.conf”权限为600，只允许root来读写该文件。# chmod 600 /etc/inetd.conf

□□第二步：确定“/etc/inetd.conf”文件所有者为root。# chown root /etc/inetd.conf 第三步：编辑 /etc/inetd.conf文件(vi /etc/inetd.conf),

□□取消不需要的服务，如：ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth等等。把不需要的服务关闭可以使系统的危险性降低很多。第四步：
给inetd进程发送一个HUP信号：# killall -HUP inetd 第五步：
用chattr命令把/ec/inetd.conf文件设为不可修改。# chattr +i /etc/inetd.conf

□□/etc/inetd.conf文件中只开放需要的服务。

□□对于启用的网络服务，使用TCP Wrapper增强访问控制和日志审计功能。
建议使用xinetd代替inetd，前者在访问控制和日志审计方面有较大的增强。

□□
这样可以防止对inetd.conf的任何修改(以外或其他原因)。唯一可以取消这个属性的只有root。如果要修改inetd.conf文件，首先要取消不可修改属性：# chattr -i /etc/inetd.conf

□□portmap(如果启动使用nfs等需要rpc的服务，建议关闭portmap服务 cups服务(Common Unix Printing Service，用于打印，建议关闭)

□□named服务(除非主机是dns服务器，否则关闭named服务) apache(http)服务 xfs(X Font Service)服务 vsftpd lpd linuxconf identd smb

□□26.关闭无效服务和进程自动启

□□列举并记录/etc/rc.d/rc[0-9].d脚本目录下的文件 find /etc/rc?.d/ -name "S*"
1、参考配置操作

□□进入相应目录，将脚本开头大写S改为小写s即可。如：

□□# cd /etc/rc.d/rc6.d # mv S45dhcpd s45dhcpd

□□27.禁止/etc/rc.d/init.d下某些脚本 需要具体步骤 # cd /etc/rc.d/init.d

□□在不需要开机自动运行的脚本第一行写入 exit 0。则开机时该脚本exit 0之后的内容不会执行。

□□需要更改的服务包括：identd lpd linuxconf netfs portmap routed rstatd rwalld rwhod sendmail ypbind yppasswdd ypserv

□□具体操作时根据主机的角色请于管理员确认后再实施。

□□28.加固snmp服务 不能执行 chkconfig snmpd off chkconfig snmptrapd off /etc/rc.d/init.d/snmpd stop /etc/rc.d/init.d/snmptrapd stop 如果需要SNMP服务

□□修改vi /etc/snmp/snmpd.conf文件 A、修改默认的community string com2sec notConfigUser default public 将public修改为你才知道的字符串

□□B、把下面的#号去掉

□□#view mib2 included .iso.org.dod.internet.mgmt.mib-2 fc C、把下面的语句

□□access notConfigGroup "" any noauth exact systemview none none 改成：

□□access notConfigGroup "" any noauth exact mib2 none none 3、重启snmpd服务

□□#/etc/rc.d/init.d/snmpd restart

□□29.修改ssh端口 cat /etc/ssh/sshd_config

□□vi /etc/ssh/sshd_config 修改 Port 22 修改成其他端口，迷惑非法试探者

□□Linux下SSH默认的端口是22,为了安全考虑，现修改SSH的端口为1433,修改方法如下：/usr/sbin/sshd -p 1433

□□30.安装系统补丁地址:需下载

□□http://www.redhat.com/corp/support/errata/ RPM包:

□□# rpm -Fvh [文件名]
请慎重对系统打补丁，补丁安装应当先在测试机上完成。补丁安装可能导致系统或某些服务无法工作正常。

□□在下载补丁包时，一定要对签名进行核实，防止执行特洛伊木马。

□□31隐藏系统提示信息

□□编辑"vi /etc/rc.d/rc.local" 全部注释 删除"/etc"目录下的"isue.net"和"issue"文件 rm -f /etc/issue rm -f /etc/issue.net

□□32. 修改帐户TMOUT值，设置自动注销时间 检查方法:

□□#cat /etc/profile 查看有无TMOUT的设置 备份方法:

□□#cp -p /etc/profile /etc/profile_bak 加固方法: #vi /etc/profile 最后一行增加 TMOUT=180 export TMOUT

□□无操作180秒后自动退出 风险:无可见风险

□□33. Grub/Lilo密码 检查方法:

□□#cat /etc/grub.conf|grep password 查看grub是否设置密码 #cat /etc/lilo.conf|grep password 查看lilo是否设置密码 备份方法:

□□#cp -p /etc/grub.conf /etc/grub.conf_bak #cp -p /etc/lilo.conf /etc/lilo.conf_bak
加固方法:为grub或lilo设置密码

□□风险:etc/grub.conf通常会链接到/boot/grub/grub.conf

□□34.去除不必要的SUID/SGID权限 需要具体步骤 给文件加SUID和SUID的命令如下:
chmod u+s filename 设置SUID位 chmod u-s filename 去掉SUID设置 chmod g+s filename 设置SGID位 chmod g-s filename 去掉SGID设置 补充说明

□□suid是4000，sgid是2000，sticky是1000 比如rwsr-xr-x就是4755

□□SUID 是 Set User ID, SGID 是 Set Group ID的意思。
SUID的程序在运行时，将有效用户ID改变为该程序的所有者ID，使得进程在很大程度上拥有了该程序的所有者的特权。如果被设置为SUID

root，那么这个进程将拥有超级用户的特权(当然，一些较新版本的UNIX系统加强了这一方面的安全检测，一定程度上降低了安全隐患)。当进程结束时，又恢复为原来的状态。

□□35.检查/dev下的非设备文件

□□find /dev -type f -exec ls -l {} \; 记录可以文件

□□36.检查非/dev下的设备文件 find / -type b -print | grep -v '^/dev/'

□□37.查找没有属主的文件

□□find / -nouser -o -nogroup -print

□□38.查找所有人可写的文件 find / -perm -2 ! -type l –ls

□□39.查找rhosts文件 find / -name .rhosts -print 补充说明

□□远程登录(rlogin)是一个 UNIX 命令，它允许授权用户进 入网络中的其它 UNIX 机器并且就像用户在现场操作一样。一旦进入主机，用户可以操作主机允许的任何事情，比如：读文件、编辑文件或删除文件等。

□□rlogin设计的初衷是方便同名的用户从一台机器直接登录到另一台机器.

□□比如机器A上有用户test1，机器B上该用户也有一个同名账号test1，
如果机器B上设置好.rhosts的话就test1就可以从机器A上直接登录机器B.

□□
通常在配HA的时候，会将+放进/.rhosts，因为这样做同步的时候就会比较方便，但记得在配置完的时候，把这个+去掉

□□40.文件系统-检查异常隐含文件

□□rm [filename] 补充操作说明
在系统的每个地方都要查看一下有没有异常隐含文件(点号是起始字符的，用“ls”命令看不到的文件)。在UNIX下，一个常用的技术就是用一些特殊的名，如：“„”、“..
”(点点空格)或“..^G”(点点control-G)，来隐含文件或目录。

□□41.查找netrc文件

□□find / -name .netrc -print 4、补充说明

□□有些 命令通过检查 $HOME/.netrc
文件(包含远程主机上使用的用户名和密码)来提供自动登录的功能。

□□如果没有远程主机的 $HOME/.netrc 文件中的有效项，将提示输入登录标识和密码。