目录

目录

1 用户账户

1.1 检查是否存在异常账户

1.1.1 说明

检查当前系统是否存在无用账户、可疑账户，及时对异常账户进行禁用或者删除，可防 止系统被黑客所创建的账户登录或遭到黑客暴力破解。

1.1.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/passwd

2) 根据显示结果检查是否存在异常账户

1.1.3 修改建议

1) 文件的每一行内容含义为：
   用户名：密码保留字段：用户 uid：用户组 gid：个人资料：主目录：登录 Shell
2) 其中主要查看用户 uid 字段，默认系统用户 uid 中，root 为 0；系统用户为 1-999；普通用户为 1000-65535；应保证只有 root 用户的 uid 为 0，并检查有无其他可疑账户，及时进行删除或禁用。
3) 相关命令：
   账户删除命令：
   [root@localhost ~]# userdel -r 用户名
   锁定账户命令：
   [root@localhost ~]# usermod -L 用户名
   解锁账户命令：
   [root@localhost ~]# usermod -U 用户名

1.2 设置账户口令复杂度

1.2.1 说明

为了保证之后所创建的每个账号的口令复杂度均满足实际所需，需更改相应的配置达到 效果。

1.2.2 检查方法

1) 在终端中输入命令：
   [root@localhost ~]# more /etc/security/pwquality.conf

2) 根据显示结果检查相关项是否未被备注或数值不等于 0

3) difok 为不得与上次密码相同的字符个数；

minlen 为密码最小长度；

dcredit 为密码中最少包含数字的个数；

ucredit 为密码中最少包含大写字母的个数；

lcredit 为密码中最少包含小写字母的个数；

ocredit 为密码中最少包含特殊字符的个数；

maxrepeat 为密码中相同字符出现最多的次数；

usercheck 为检测密码是否与用户名相似。

1.2.3 修改建议

1) 使用 vim 编辑器修改口令复杂度文件：

[root@localhost ~]# vim /etc/security/pwquality.conf

2) 修改检查方法中所提的项，数值为-1 时代表至少需要相应字符一位、数值为-2 时代表需要需要相应字符两位，依次类推。

3) 修改例子：（密码最小长度为 8 位，密码需包含大小写字母、数字与特殊字符）

minlen = 8

dcredit = -1

ucredit = -1

lcredit = -1

ocredit = -1

1.3 设置当前已存在账户的密码有效期

1.3.1 说明

定期更改密码有助于提高账户的安全性，设置合理的密码有效期是此项的目的。

1.3.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# chage -l 用户名

2) 根据显示结果检查密码有效期

1.3.3 修改建议

1) 根据需求设置密码有效期

2) 在终端中输入命令：

#设置密码最长有效期为 90 天

[root@localhost ~]# chage -M 90 用户名

#设置密码最短有效期为 1 天

[root@localhost ~]# chage -m 1 用户名#

设置密码过期前 3 天提醒用户

[root@localhost ~]# chage -W 3 用户名

1.4 设置未来新账户的密码有效期

1.4.1 说明

通过之前的命令只可更改当前已存在的账户的密码有效期，为了保障以后新建立的账户 也可遵循相应的密码有效期规则，需要修改相应的配置文件。

1.4.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/login.defs

2) 根据显示结果检查密码有效期

1.4.3 修改建议

1) 使用 vim 编辑器修改密码有效期文件：

[root@localhost ~]# vim /etc/login.defs

2) PASS_MAX_DAYS 后数值为密码最长有效期

PASS_MIN_DAYS 后数值为密码最短有效期

PASS_WARN_AGE 后数值为密码过期前告警天数

3) 修改例子：（设置密码最长有效期为 90 天，最短有效期为 1 天，过期前 3 天提醒）

PASS_MAX_DAYS 90

PASS_MIN_DAYS 1

PASS_WARN_AGE 3

1.5 账户登陆失败锁定

1.5.1 说明

为防止遭受恶意暴力破解，设置账户登录尝试次数并进行锁定，有效保护账户的安全。

1.5.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/pam.d/system-auth

2) 检查是否存在如下内容：

auth required pam_faillock.so preauth audit deny=3 even_deny_root unlock_time=60

auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root unlock_time=60

auth sufficient pam_faillock.so authsucc audit deny=3 even_deny_root unlock_time=60

3) 其中：

deny 为登陆失败尝试次数

even_deny_root 为 root 账户登录达到失败次数也会锁定

unlock_time 为锁定时长，以秒为单位

1.5.3 修改建议

1) 使用 vim 编辑器修改账户策略文件：

[root@localhost ~]# vim /etc/pam.d/system-auth

2) 修改例子：（设置登录失败尝试次数为 5，锁定时长为 5 分钟，包含 root 账户）

auth required pam_faillock.so preauth audit deny=5 even_deny_root unlock_time=300

auth [default=die] pam_faillock.so authfail audit deny=5 even_deny_root unlock_time=300

auth sufficient pam_faillock.so authsucc audit deny=5 even_deny_root unlock_time=300

2 系统服务类

2.1 更改 SSH 端口

2.1.1 说明

更改 SSH 默认端口可在一定程度上防止被黑客使用大批量扫描方式攻击。

2.1.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more +Port /etc/ssh/sshd_config

2) 根据显示结果检查 SSH 服务端口设置

2.1.3 修改建议

1) 使用 vim 编辑器修改 SSH 配置文件：

[root@localhost ~]# vim /etc/ssh/sshd_config

2) 找到或添加以下内容：

Port 端口号

3) 端口号可配置为 1-65535 的任意端口，但应避免端口重复使用。

2.2 限制 SSH 服务可访问源

2.2.1 说明

通过修改 SSH 的配置文件限制可以使用 SSH 服务远程管理的主机。

2.2.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/hosts.deny

[root@localhost ~]# more /etc/hosts.allow

2) 根据显示结果检查 SSH 服务可访问源地址

2.2.3 修改建议

1) 使用 vim 编辑器修改 hosts 限制文件：

[root@localhost ~]# vim /etc/hosts.deny

sshd:ALL

[root@localhost ~]# vim /etc/hosts.allow

sshd:ip 地址或地址段

2.3 限制 SSH 登录用户与登录方式

2.3.1 说明

通过限制使用SSH 直接以root 身份登录，禁用公钥登录的方式加强 SSH 服务的安全性。

2.3.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/ssh/sshd_config

2) PermitRootLogin 为是否允许以 root 用户直接登录

PubkeyAuthentication 为是否允许使用公钥方式登录

PasswordAuthentication 为使用密码方式登录

2.3.3 修改建议

1) vim 编辑器修改 SSH 配置文件：

[root@localhost ~]# vim /etc/ssh/sshd_config

2) 找到或添加以下内容：

PermitRootLogin no

PubkeyAuthentication no

PasswordAuthentication yes

2.4 禁用不必要的服务

2.4.1 说明

关闭当前不需要的服务，以防止黑客通过相关服务的漏洞入侵主机。

2.4.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# systemctl list-unti-files --type=service --state=enabled

2) 根据显示结果检查是否存在多余的服务项

2.4.3 修改建议

1) 正常纯净系统下，以下为默认自启动的服务：

accounts-daemon.service
atd.service
auditd.service
autovt@.service
bluetooth.service
chronyd.service
cron.service
crond.service
dbus-org.bluez.service
dbus-org.fedoraproject.FirewallD1.service
dbus-org.freedesktop.ModemManager1.service
dbus-org.freedesktop.network1.service
dbus-org.freedesktop.nm-dispatcher.service
dbus-org.freedesktop.timesync1.service
display-manager.service
firewalld.service
getty@.service
irqbalance.service
kdump.service

kernel-hash-init.service

kmodprotect-init.service

kylin-activation-check.service

kysec-sync-notify.service

libstoragemgmt.service

lightdm.service

lm_sensors.service

lvm2-monitor.service

mcelog.service

mdmonitor.service

ModemManager.service

netctl-init.service

NetworkManager-dispatcher.service

NetworkManager-wait-online.service

NetworkManager.service

rasdaemon.service

restorecond.service

rngd.service

rpcbind.service

rsyslog.service

rtkit-daemon.service

smartd.service

sshd.service

sssd.service

sysstat.service

systemd-networkd.service

systemd-timesyncd.service

systemtap.service

tuned.service

udisks2.service

2) 如存在其他多余启动项则可使用命令进行关闭：

[root@localhost ~]# systemctl disable --now 服务项

3 安全管控

3.1 开启防火墙

3.1.1 说明

防护墙可以通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部 的信息、结构和运行状况， 以此来实现网络的安全保护。

3.1.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# systemctl status firewalld
   [root@localhost ~]# firewall-cmd --list-all

2) 根据显示结果检查当前防火墙服务是否启用，当前防火墙配置的服务、端口等信息。

3.1.3 修改建议

1) 开启防火墙

   在终端中输入命令：

   [root@localhost ~]# systemctl enable --now firewalld

2) 配置防火墙相应策略

   如开启 Http 服务：

   [root@localhost ~]# firewall-cmd --add-service=http --permanent

   [root@localhost ~]# firewall-cmd --reload

3.2 启用 SELinux

3.2.1 说明

SELinux 是一个内核级别的安全机制，是对于强制访问控制的实现。在这种访问控制体系的限制下，进程只能访问那些在他的任务中所需要文件，提供了强有力的安全保护。

3.2.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# getenforce

2) 根据显示结果检查当前 SELinux 是否开启

3) Disabled：关闭

   Permissive：宽松模式（仅告警）

   Enforcing：强制模式

3.2.3 修改建议

1) 开启 SELinux，在终端中输入命令

[root@localhost ~]# setenforce 1

2) 编辑 SELinux 配置文件，确保重新启动后 SELinux 依旧有效

使用 vim 编辑器编辑 SELinux 配置文件：

[root@localhost ~]# vim /etc/selinux/config

将 SELINUX=一行更改为：

SELINUX=Enforcing

3) 在开启 SELinux 时如遇程序启动失败， 服务访问失败等， 可安装软件包 setroubleshoot 进行排查，具体报错信息可使用命令：

[root@localhost ~]# grep sealert /var/log/message

通过相应的 sealert 的 UUID 查看具体原因并处理。

※注：开启 **Selinux** 可能会出现一定的限制，请自行根据需要进行设置。

3.3 配置 Grub 菜单加密

3.3.1 说明

设置 Grub 菜单密码，防止通过修改 Grub 启动菜单方式来达到破解 root 账户密码等操作，保护系统启动安全性。

3.3.2 检查方法

检查在开机后进入 Grub 引导选择系统界面中，按下“e”键是否要求输入密码。

3.3.3 修改建议

1) 设置 Grub 菜单密码

方式如下：

1.在终端中输入命令：

[root@localhost ~]# grub2-mkpasswd-pbkdf2

2.将生成的散列密码复制

3 使用 vim 编辑器修改 Grub 引导配置：

[root@localhost ~]# vim /boot/grub2/grub.cfg

4.添加如下内容：

set superusers=用户名

password_pbkdf2 用户名 散列密码5.

在终端中输入命令更新 Grub 菜单：

[root@localhost ~]# grub2-mkconfig

3.4 限制计划任务使用

3.4.1 说明

限制指定的管理员账户运行计划任务，防止开机运行不明任务。

3.4.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# more /etc/cron.allow

2) 根据现实结果查看当前允许运行计划任务的用户

3.4.3 修改建议

1) 使用 vim 编辑器编辑计划任务限制文件

   [root@localhost ~]# vim /etc/cron.allow

2) 在文件中添加相应的用户名。

4 权限设置

4.1 管理 sudo 权限

4.1.1 说明

限制用户使用 sudo 权限，防止用户对系统做出破坏性更改或恶意提权操作。

4.1.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# visudo

2) 查找未被“#”注释掉的部分，是否存在类似于：

   root ALL=(ALL) ALL

   字段，有即为定义的 sudo 用户；如存在类似于

   %wheel ALL=(ALL) ALL

   字段，即为定义 wheel 组为 sudo 用户组。

4.1.3 修改建议

1) 使用 visudo 命令检查可执行 sudo 命令的用户、用户组、主机、命令

2) 设置的格式为：

   用户或用户组　主机列表=(提权身份)　[NOPASSWD]:主机列表

3) 举例如：

   test01　ALL=(root)　/usr/bin/systemctl

4.2 启用 sudo 日志

4.2.1 说明

启用 sudo 日志可以审计用户在使用 sudo 时执行了什么命令等相关信息。

4.2.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# visudo
2) 检查是否存在 Defaults logfile 一行

4.2.3 修改建议

开启 sudo 日志需要执行以下操作：

1) 创建 sudo.log 文件

   [root@localhost ~]# touch /var/log/sudo.log
2) 修改文件权限

   [root@localhost ~]# chmod root:root /var/log/sudo.log
3) 修改 rsyslog 配置文件

   [root@localhost ~]# vim /etc/rsyslog.conf

   添加以下内容：

   local2.debug /var/log/sudo.log

   ※空白处用“Tab”键补齐，不可以用空格
4) 重启 rsyslog 服务

   [root@localhost ~]# systemctl restart rsyslog
5) 修改 sudo 配置文件

   [root@localhost ~]# visudo

   添加以下内容：

   Defaults logfile=/var/log/sudo.log

   Defaults loglinelen=0

   Defaults !syslog

4.3 检查权限不当文件

4.3.1 说明

合理设置系统重要目录或文件权限，防止其他用户未授权访问而导致提权等恶意行为。

4.3.2 检查方法

1) 在终端中输入命令：

   [root@localhost ~]# ls -l /etc/ | grep 'shadow\|passwd\|group'

   ※此处可以指定任意文件检查，只要是管理员认为重要的文件。
2) 通过返回结果检查是否设置权限不当

3) 也可通过查找方式查找指定权限文件，在终端中输入命令如：

[root@localhost ~]# find / -perm -g=wx,-o=wx -type f -ls

4.3.3 修改建议

1) 建议对系统关键文件设置为仅 root 用户可访问、执行或写入，即权限为：

u=rwx,g=r,o=r root:root 或更严格 u=rwx,g=---,o=--- root:root

2) 非正常可执行程序或需要的脚本不要给予执行权限，可使用命令：

[root@localhost ~]# chmod -x 文件

消除执行权限。

4.4 限制 **su** 的使用

4.4.1 说明

限制用户使用 su 命令变更为其他用户，防止不当的角色切换。

4.4.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# more /etc/pam.d/su

2) 检查以下行：

auth required pam_wheel.so

是否被注释，是否有添加参数

4.4.3 修改建议

1) 限制可使用 su 命令的用户组，使用 vim 编辑 pam.d 的关于 su 的安全配置文件

[root@localhost ~]# vim /etc/pam.d/su

2) 添加或修改以下内容：

auth required pam_wheel.so group=可使用 su 的组名

3) 赋予用户可使用 su 命令的用户组，在终端中输入命令：

[root@localhost ~]# gpasswd -a 用户名 可使用 su 的组名

4.5 清除没有属组属主的文件或文件夹

4.5.1 说明

查找系统中无用的文件，不再使用的文件可进行删除，以后需要使用的文件表明属主属组。

4.5.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# find / \(-nouser -o -nogroup \) -exec ls -al {} \;

2) 查看执行结果，是否存在可删除的文件

4.5.3 修改建议

使用命令检查出来的文件可能会存在系统需要使用的情况，需要管理员判断相应文件是 否为无用文件再删除。

5 防痕迹清除

5.1 启动 Rsyslog 服务

5.1.1 说明

通过启动日志服务即使记录相关行为的操作用于取证与溯源。

5.1.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# systemctl status rsyslog

2) 根据显示结果检查当前日志服务是否启用。

5.1.3 修改建议

开启日志服务，在终端中输入如下命令：

[root@localhost ~]# systemctl enable --now rsyslog

5.2 设置 NTP 时间同步

5.2.1 说明

设置时间同步保证记录日志的时间的准确性。

5.2.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# chronyc sources -v

2) 观察是否有时间同步服务器信息

5.2.3 修改建议

1) 使用 vim 编辑器编辑 NTP 服务文件

[root@localhost ~]# vim /etc/chrony.conf

2) 添加相应的 NTP 服务器信息，如：

server ntp1.aliyun.com iburst

3) 重新启动 ntp 服务，终端中输入命令：

[root@localhost ~]# systemctl restart chronyd

4) 再次使用检查命令检查是否有时间服务器相关信息

[root@localhost ~]# chronyc sources -v

5.3 加强审计日志文件权限

5.3.1 说明

加强审计日志文件的权限，避免日志信息被恶意操作。

5.3.2 检查方法

1) 在终端中输入命令：

[root@localhost ~]# ls -l /var/log/audit

[root@localhost ~]# ls -ld /var/log/audit

2) 根据回显信息查看权限设置

5.3.3 修改建议

1) 建议将整个 audit 文件夹设置成只允许 root 或审计账户用户操作，文件夹内文件设置具体权限。

2) 修改权限命令如：

[root@localhost ~]# chmod -R 700 /var/log/audit

3) 修改文件所属命令如：

[root@localhost ~]# chown root:root -R /var/log/audit