口令锁定策略

账号管理

安全基线项名称	口令锁定策略
检查操作步骤	查看配置文件：more /etc/pam.d/password-auth 查看是否存在如下内容：auth required pam_tally2.so deny=5 onerr=fail unlock_time=300 even_deny_root=5 root_unlock_time=600
基线符合性性判定依据	用户连续认证失败次数设置为5即合规，否则不合规。
安全加固方案	参考配置操作 1、执行备份#/etc/pam.d/password-auth_bak 2、修改策略设置，编辑文件vi /etc/pam.d/password-auth 增加如下内容：auth required pam_tally2.so deny=5 onerr=fail unlock_time=300 如果要对root用户生效，请在添加的内容后继续添加 even_deny_root=5 root_unlock_time=600 注：unlock_time和root_unlock_time单位为秒
备注	PAM通过提供一些动态链接库和一套统一的API，将系统提供的服务 和该服务的认证方式分开，使得系统管理员可以灵活地根据需要给不同的服务配置不同的认证方式而无需更改服务程序，同时也便于向系统中添加新的认证手段。 查询被锁定的账号：pam_tally2 -u 手动解锁某个被锁定的账号：pam_tally2 -u 要解锁的用户 -r

口令生存期：

安全基线项名称	口令生存期
检查操作步骤	查看文件：more /etc/login.defs，检查如下参数值是否满足要求： PASS_MAX_DAYS 用户的密码最长使用天数不大于 90PASS_WARN_AGE #用户的密码到期提前提醒天数为7
基线符合性性判定依据	PASS_MAX_DAYS不大于90，PASS_WARN_AGE等于7即合规，否则不合规。
安全加固方案	参考配置操作 1、执行备份：#cp -p /etc/login.defs /etc/login.defs_bak 2、修改策略设置，编辑文件/etc/login.defs(vi /etc/login.defs)，在文件中加入如下内容(如果存在则修改，不存在则添加)： PASS_MAX_DAYS 90 PASS_WARN_AGE 7 执行命令：chage-M 90 -W 7username 修改已有用户的口令生存期和过期告警天数

口令复杂度：

安全基线项名称	口令复杂度
检查操作步骤	执行命令：grep -E "^minlen|^minclass" /etc/security/pwquality.conf 查看是否有返回结果。
基线符合性性判定依据	有返回结果且返回结果等于或者大于minlen = 8，minclass = 3 即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp -p /etc/security/pwquality.conf /etc/security/pwquality.conf_bak 2、执行命令：authconfig --passminlen=8 --passminclass=3 --update #至少包含数字、小写字母、大写字母、特殊字符中的三项，且密码长度>=8 3、执行命令 chage -d 0 username #强制指定的用户下次登录修改密码

检查密码重用是否受限制：

安全基线项名称	检查密码重用是否受限制
检查操作步骤	查看文件：cat /etc/pam.d/system-auth 找到 password sufficient pam_unix.so 这行，检查末尾是否有 remember 参数
基线符合性性判定依据	有remember参数且参数的值大于等于5即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp -p /etc/pam.d/system-auth 2、执行命令：vi /etc/pam.d/system-auth 编辑该文件，找到password sufficient pam_unix.so 这行在末尾添加 remember 参数它的值为5，原来的内容不用更改，只在末尾加 remember=5 即可，它表示禁止使用最近用过的5个密码（已使用过的密码会被保存在 /etc/security/opasswd 下面）。

禁止存在空密码的账户：

安全基线项名称	禁止存在空密码的帐户
检查操作步骤	执行以下命令查看系统中是否存在空口令账号 #awk -F: '($2 == "") { print $1 }' /etc/shadow
基线符合性性判定依据	执行命令后没有返回值即合规，否则不合规。
安全加固方案	参考配置操作 1、为帐户设置满足密码复杂度的密码： #passwd username

检查是否存在除 root 之外 UID 为 0 的用户

安全基线项名称	检查是否存在除root之外UID为0的用户
检查操作步骤	执行命令： awk -F: '($3 == 0) { print $1 }' /etc/passwd 查看返回值。
基线符合性性判定依据	返回值包括“root”以外的条目，则低于安全要求
安全加固方案	参考配置操作 1、执行备份：cp -p /etc/passwd cp -p /etc/shadow 2、执行命令：userdel -r username删除返回值中root除外的其他用户。 或者使用命令：usermod -u uid username 为他们分配新的UID

安全加固，服务管理：

检查是否禁止 SSH 空密码用户登录：

禁止SSH空密码用户登录

安全基线项名称	检查是否禁止SSH空密码用户登录
检查操作步骤	执行命令： more /etc/ssh/sshd_config 查看 PermitEmptyPasswords 配置情况
基线符合性性判定依据	PermitEmptyPasswords 的值设置为no即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak 2、执行命令：vi /etc/ssh/sshd_config 找到 PermitEmptyPasswords 将其设置为no 后保存并退出 3、执行命令：systemctl restrat sshd 重启服务使配置生效

设置 SSH 多次登录失败后锁定用户：

SSH多次登录失败后锁定用户

安全基线项名称	设置ssh多次登录失败后锁定用户
检查操作步骤	执行命令： more /etc/pam.d/sshd 查看是否存在 auth required pam_tally2.so deny=5 unlock_time=300 内容
基线符合性性判定依据	存在该行且 deny小于等于5，unlock_time大于等于300，否则不合规
安全加固方案	参考配置操作 1、执行备份： cp -p /etc/pam.d/sshd /etc/pam.d/sshd_bak 2、执行命令：vi /etc/pam.d/sshd 在文件开头添加一行，内容为 auth required pam_tally2.so deny=5 unlock_time=300，如要对root用户也进行限制，在刚添加的内容后继续添加：even_deny_root=5 root_unlock_time=1200 即可

设置 SSH 多次登录失败后锁定用户：

SSH多次登录失败后锁定用户

安全基线项名称	设置ssh多次登录失败后锁定用户
检查操作步骤	执行命令： more /etc/pam.d/sshd 查看是否存在 auth required pam_tally2.so deny=5 unlock_time=300 内容
基线符合性性判定依据	存在该行且 deny小于等于5，unlock_time大于等于300，否则不合规
安全加固方案	参考配置操作 1、执行备份： cp -p /etc/pam.d/sshd /etc/pam.d/sshd_bak 2、执行命令：vi /etc/pam.d/sshd 在文件开头添加一行，内容为 auth required pam_tally2.so deny=5 unlock_time=300，如要对root用户也进行限制，在刚添加的内容后继续添加：even_deny_root=5 root_unlock_time=1200 即可

限制 root 用户远程登录：

限制root用户远程登录

安全基线项名称	限制root用户远程登录
检查操作步骤	执行命令： more /etc/ssh/sshd_config 查看PermitRootLogin 参数的值
基线符合性性判定依据	PermitRootLogin参数值为no且该行没有被注释即合规，否则不合规
安全加固方案	参考配置操作 1、执行命令：vi /etc/ssh/sshd_config 找到 PermitRootLogin 将其后方的 yes 改为 no 并删除前方的 # 取消该行的注 2、释执行命令：systemctl restart sshd 重启服务使其生效

检查 SSH 使用的端口：

检查SSH使用的端口

安全基线项名称	检查ssh使用的端口
检查操作步骤	执行命令： more /etc/ssh/sshd_config 查看Port 参数的值
基线符合性性判定依据	Port参数值不是默认值（22）且该行没有被注释即合规，否则不合规
安全加固方案	参考配置操作 1、执行命令：vi /etc/ssh/sshd_config 找到 Port 将其后方的 22 改为其他端口号，然后删除前方的 # 取消该行的注释（端口号最好挑10000-65535之间的端口号，10000以下容易被系统或一些特殊软件占用） 2、执行命令：semanage port -a -t ssh_port_t-p tcp 修改后的端口号， 将修改后的端口添加到SELinux开放给ssh使用的端口 3、执行命令：firewall-cmd --zone=public --add-port=ssh端口号/tcp --permanent，防火墙放行刚修改的 ssh 端口号 4、执行命令：systemctl restart sshd ; systemctl restart firewalld 重启ssh和防火墙，使配置生效

设置登录超时自动注销：

设置登录超时自动注销

安全基线项名称	设置登录超时自动注销
检查操作步骤	执行命令： more /etc/profile 查看是否有export TMOUT=180
基线符合性性判定依据	存在export TMOUT且他的值小于等于180即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp - p /etc/profile /etc/profile_bak 2、执行命令：vi /etc/profile 在该文件末尾添加 export TMOUT=180 或者将原来的值修改为180

安全管理-权限管理：

检查默认 umask 值：

检查默认umask值

安全基线项名称	检查用户umask值
检查操作步骤	执行命令：more /etc/profile 查看该文件末尾是否设置umask值
基线符合性性判定依据	/etc/profile文件末尾存在umask 027，则合规，否则为不合规。
安全加固方案	参考配置操作 1、执行备份：cp -p /etc/profile /etc/profile_bak 2、执行命令：vi /etc/profile 编辑文件,在该文件末尾添加umask 027 3、执行以下命令让配置生效：source /etc/profile

检查重要目录和文件的权限设置：

检查重要目录和文件的权限设置

安全基线项名称	检查重要目录和文件的权限设置
检查操作步骤	执行命令：ls -l /etc/passwd /etc/shadow /etc/group /etc/gshadow /etc/hosts.allow /etc/hosts.allow /etc/services /etc/ssh/sshd_config 查看文件权限
基线符合性性判定依据	/etc/passwd文件的权限<=644 /etc/shadow文件的权限<=600 /etc/group文件的权限<=644 /etc/gshadow文件的权限<=600 /etc/hosts.deny文件的权限<=644 /etc/hosts.allow文件的权限<=644 /etc/services文件的权限<=644 /etc/ssh/sshd_config文件的权限<=600 以上条件同时满足则合规，否则不合规。
安全加固方案	参考配置操作 1、执行命令：ls -l /etc/passwd /etc/shadow /etc/group /etc/gshadow /etc/hosts.allow /etc/hosts.allow /etc/services /etc/ssh/sshd_config 查看文件权限 2、对不符合要求的文件使用chmod命令修改权限，如 chmod 644 /etc/passwd

限制可以 root 的用户：

限制可以su为root的用户

安全基线项名称	限制可以su为root的用户
检查操作步骤	执行命令：more /etc/pam.d/su 找到 auth required pam_wheel.so use_uid 查看该行是否存在且是否被注释
基线符合性性判定依据	auth required pam_wheel.so use_uid 存在且未被注释即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp - p /etc/pam.d/su /etc/pam.d/su_bak 2、执行命令：vi /etc/pam.d/su 找到 auth required pam_wheel.so use_uid 删除该行前面的 # 使其生效，如果该行不存在则在文件末尾添加该行。 3、将需要su为root的用户使用命令：usermod -G wheel username 加入 wheel 组，该用户即可su为root用户。如果需要将某个用户移出wheel组，可使用命令：gpasswd -d username wheel

日志管理：

检查rsyslog服务启用状况以及对登录事件的记录

安全基线项名称	检查rsyslog服务是否启用且对所有登录事件都记录
检查操作步骤	执行命令：more /etc/rsyslog.conf 查看authpriv的值
基线符合性性判定依据	authpriv值为authpriv.* /var/log/secure即合规，否则不合规 注：/var/log/secure为可变项
安全加固方案	参考配置操作 1、执行备份：cp - p /etc/rsyslog.conf /etc/rsyslog.conf_bak 2、执行命令：systemctl enable rsyslog 添加开机自启动 3、执行命令：systemctl start rsyslog 启动服务 4、执行命令：vi/etc/rsyslog.conf 查看authpriv值 将其设置为 authpriv.*/var/log/secure # 将 authpirv 的任何级别的信息记录到 /var/log/secure 文件中 5、执行命令：systemctl restart rsyslog
备注	rsyslog文件解析.docx

/etc/rsyslog.conf 文件中的每一行代表一条设置值，每一条设置值的语法为：消息类型 执行动作

"消息类型"指定哪些消息需要记录，"执行动作"则告诉系统日志服务该如何处理这些消息

"消息类型"以 消息来源.优先级 的格式指定消息的种类

"消息来源"表示消息是从哪个子系统传送过来的，来源主要有以下这些：

- authpriv：与用户安全、验证有关的消息；
- cron：与计划任务有关的消息；
- daemon：与一般服务有关的消息；
- kern：来自系统内核的消息；
- mail：来自邮件系统的消息；
- localN：保留

"优先级"则用来指出消息的优先等级，即消息的重要程度。其优先级别如下（数字等级越小，优先级越高，消息越重要但记录的信息越少）：

- 0 EMERG（紧急）：会导致主机系统不可用的情况。
- 1 ALERT（警告）：必须马上采取措施解决的问题。
- 2 CRIT（严重）：比较严重的情况。
- 3 ERR（错误）：运行出现错误。
- 4 WARNING（提醒）：可能影响系统功能，需要提醒用户的重要事件。
- 5 NOTICE（注意）：不会影响正常功能，但是需要注意的事件。
- 6 INFO（信息）：一般信息。
- 7 DEBUG（调试）：程序或系统调试信息等。

除此之外，"消息来源"与"优先级"可以使用星号（*）代表所有，因此*.*就表示来自所有子系统的所有级别的消息。

而"执行动作"字段则用来定义如何处理接收到的消息，可以指定如下几项内容：

/PATH/FILENAME：将消息存储到指定的文件中，文件必须以斜线（/）开头的绝对路径命名；

USERNAME：将消息发送给指定的已经登录的用户；

@HOSTNAME：将消息转发到指定的日志服务器；

*：将消息发送给所有已经登录的用户。

查看SSH LogLevel设置是否为INFO

安全基线项名称	确保SSH LogLevel设置为INFO
检查操作步骤	执行命令：more vi /etc/ssh/sshd_config 找到 LogLevel 查看设置的级别是否为INFO
基线符合性性判定依据	LogLevel 的级别是INFO 且该行未被注释即合规，否则不合规
安全加固方案	参考配置操作 1、执行备份：cp - 2、执行命令：vi /etc/ssh/sshd_config 找到 LogLevel 将其设置为 INFO，如果该行被注释，还应删掉该行前方的 # 3、执行命令：systemctl restart sshd 重启ssh服务使其生效

是否将 /var/log/messages 文件设置为只可追加

安全基线项名称	是否将 /var/log/messages 文件设置为只可追加
检查操作步骤	执行命令：lsattr /var/log/messages 查看该文件属性第六位是否为a
基线符合性性判定依据	为a即合规，否则不合规
安全加固方案	参考配置操作 执行命令：lsattr /var/log/messages 查看该文件属性第六位是否为a 不为a则执行命令：chattr +a /var/log/messages 将该文件的属性修改为只可追加

基线项名称	检查是否存在空密码账户
检查步骤	执行命令：awk -F: '($2 == "") { print $1}' /etc/shadow查看是否有返回信息，没有返回信息说明系统当中没有空密码账户，如果有返回值，参照下方的加固步骤进行操作。
基线合规性判定	没有返回信息即合规，否则不合格
加固步骤	执行命令：cp /etc/shadow /etc/shadow_bak 对文件进行备份 执行命令：passwd username 为用户设置密码或者执行命令：userdel username 删除空密码用户

删除空密码账户：userdel 用户名

基线项名称	检查密码失效时间
检查步骤	执行命令：cat /etc/login.defs 查看 PASS_MAX_DAYS 参数设置是否为60-180 之间
基线合规性判定	PASS_MAX_DAYS 参数设置为 60-180 之间即合规，否则不合规
加固步骤	执行命令：cp /etc/login.defs /etc/login.defs_bak 对文件进行备份 执行命令：vi /etc/login.defs 将PASS_MAX_DAYS 参数设置为60-180之间，如：PASS_MAX_DAYS 90 执行命令：chage -M 90 username 修改之前已存在用户的密码到期时间

基线项名称	确保密码到期警告天数为7或更多
检查步骤	执行命令：cat /etc/login.defs 查看 PASS_WARN_AGE 参数设置是否为 7-14 之间
基线合规性判定	PASS_WARN_AGE 参数设置为 7-14 之间即合规，否则不合规
加固步骤	执行命令：vi /etc/login.defs 将PASS_WARN_AGE 参数设置为7-14之间，建议为7 执行命令：chage -W 7 username 修改之前已存在用户的密码修改最小间隔时间

基线项名称	确保root是唯一的UID为0的帐户
检查步骤	执行命令：awk -F: '($3 == "0") {print $1}' /etc/passwd 查看返回值是否有 root 之外的用户
基线合规性判定	返回值只有 root 即合规，否则不合规
加固步骤	执行命令：userdel -rf username 删除root之外的UID为0的用户

基线项名称	检查密码复杂度要求
检查步骤	执行命令：grep -E '^minlen|^minclass' /etc/security/pwquality.conf 查看返回值当中是否有 minlen 和 minclass，并且minlen设置是否为8-32之间，minclass设置是否为3或4
基线合规性判定	返回值当中存在上述两项且minlen设置为8-32之间，minclass设置为3或4即合规，否则不合规
加固步骤	执行命令：cp /etc/security/pwquality.conf /etc/security/pwquality.conf_bak 对文件进行备份 执行命令：authconfig --passminlen=10 --passminclass=3 --update 设置密码长度最小值与密码所需要的最少字符类型并更新设置

基线项名称	检查密码重用是否受限制
检查步骤	执行命令：cat /etc/pam.d/password-auth 和 cat /etc/pam.d/system-auth 查看上述两文件中 这行末尾是否存在 remember参数
基线合规性判定	上述两文件中的password sufficient pam_unix.so 末尾存在remember参数且值为5-24之间即合规，否则不合规。
加固步骤	执行命令：vi /etc/pam.d/password-auth 和 vi /etc/pam.d/system-auth 分别找到两文件中的 password sufficient pam_unix.so 在该行末尾添加remember=5即可

基线项名称	禁止SSH空密码用户登录
检查步骤	执行命令：cat /etc/ssh/sshd_config 查看文件中 PermitEmptyPasswords 参数是否为 no 且该行是否被注释
基线合规性判定	/etc/ssh/sshd_config 文件中 PermitEmptyPasswords 参数为 no 且该行未被注释即合规，否则不合规。
加固步骤	执行命令：cp /etc/ssh/sshd_config_bak对文件进行备份执行 命令：vi /etc/ssh/sshd_config 将PermitEmptyPasswords配置为no 并删除注释符号 # 执行命令： 重启sshd服务使配置生效

基线项名称	确保SSH MaxAuthTries设置为3到6之间
检查步骤	执行命令：cat /etc/ssh/sshd_config 查看文件中 MaxAuthTries 参数是否为 3-6 之间
基线合规性判定	/etc/ssh/sshd_config 文件中 MaxAuthTries 参数为 3-6 之间且该行未被注释即合规，否则不合规。
加固步骤	执行命令：vi /etc/ssh/sshd_config 将MaxAuthTries配置为3-6之间，建议为 4，并删除注释符号 # 执行命令：systemctl restart sshd 重启sshd服务使配置生效

基线项名称	确保SSH LogLevel设置为INFO
检查步骤	执行命令： cat /etc/ssh/sshd_config 查看文件中 LogLevel 参数
基线合规性判定	LogLevel设置为 INFO且未被注释即合规，否则不合规
加固步骤	执行命令：vi /etc/ssh/sshd_config 将LogLevel INFO，并删除注释符号 # 执行命令：systemctl restart sshd 重启sshd服务使配置生效

基线项名称	访问控制配置文件的权限设置
检查步骤	执行命令： ll 查看文件权限与所有者等信息
基线合规性判定	/etc/hosts.allow 和 /etc/hosts.deny 的所有者与所有组均为root且权限为 644 即合规，否则不合规
加固步骤	执行命令：chown root:root /etc/hosts.allow /etc/hosts.denychmod 644 /etc/hosts.deny /etc/hosts.allow为两文件设置权限及所有者等信息

基线项名称	确保rsyslog服务已启用
检查步骤	执行命令： systemctl status rsyslog 查看 rsyslog 服务是否启动 执行命令：systemctl is-enabled rsyslog查看rsyslog是否设置开机自启
基线合规性判定	已启动rsyslog服务且设置了开机自启动即合规，否则不合规
加固步骤	执行命令：systemctl enable rsyslog 执行命令：systemctl start rsyslog

基线项名称	开启地址空间布局随机化
检查步骤	执行命令： cat /etc/sysctl.conf 查看文件当中是否存在 kernel.randomize_va_space = 2
基线合规性判定	存在即合规，否则不合规
加固步骤	执行命令：vi /etc/sysctl.conf 在文件内添加一行 kernel.randomize_va_space = 2 执行命令：sysctl -w kernel.randomize_va_space=2 注：使用ldd命令就可以观察到程序所依赖动态加载模块的地址空间

基线项名称	确保SSH MaxAuthTries设置为3到6之间
检查步骤	执行命令：cat /etc/ssh/sshd_config 查看文件中 MaxAuthTries 参数是否为 3-6 之间
基线合规性判定	/etc/ssh/sshd_config 文件中 MaxAuthTries 参数为 3-6 之间且该行未被注释即合规，否则不合规。
加固步骤	执行命令：vi /etc/ssh/sshd_config 将MaxAuthTries配置为3-6之间，建议为 4 ，并删除注释符号 # 执行命令：systemctl restart sshd 重启sshd服务使配置生效