###### **Linux操作系统基线配置检查**

Linux操作系统基线配置存在的问题有：

|  |  |  |  |
| --- | --- | --- | --- |
| **项目**  **编号** | **安全基线检查项目** | **安全基线检查标准** | **安全基线检查符合性判定依据** |
| L-JX-01 | 用户口令设置 | 帐号与口令-用户口令设置，配置用户口令强度检查达到12 位，要求用户口令包括数字、小写字母、大写字母和特殊符号4 类中至少2 类，密码有效期为90天； | 1、不允许存在简单密码，密码设置至少包括一个数字和一个特殊字符，长度至少 为 12 位  2、修改已有用户的口令生存期和过期告警天数  3、密码有效天数设置为90天  **操作建议：**  1、口令周期  修改/etc/login.defs文件值如下：  PASS\_MAX\_DAYS 90  PASS\_MIN\_DAYS 0  PASS\_MIN\_LEN 8  PASS\_WARN\_AGE 7  2、密码复杂度策略  在/etc/pam.d/system-auth中新增一行：  password requisite pam\_cracklib.so try\_first\_pass retry=5 dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1 minlen=8 remember=5 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-02 | UID为0的用户 | 帐号与口令检查是否存在除root之外UID为0的用户 | 除root外不允许存在其他UID为0的用户 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-03 | 无用帐号 | 帐号与口令 -检查是否存在如下不必要账户：lp, sync, shutdown, halt, news, uucp, operator, games, gopher等； | 无特殊情况发现lp, sync, shutdown, halt, news, uucp, operator, games, gopher账户，则低于安全要求；  **操作建议：**  #userdel -r user删除user用户，并将/home目录下的user目录一并删除 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-04 | 帐号锁定 | 设置帐号在3次连续尝试认证失败后锁定，锁定时间为5分钟，避免用户口令被暴力破解。 | **操作建议：**  在文件/etc/pam.d/sshd中配置auth required pam\_tally2.so deny=3 unlock\_time=300 even\_deny\_root root\_unlock\_time=300 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-05 | 帐号权限 | 帐号与口令检查除ROOT外是否有其他账户拥有shell 权限 | 无非root账户设置/bin/bash或/bin/sh权限 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-06 | 远程连接限制 | 配置tcp\_wrappers，限制允许远程登陆系统的IP范围。 | 在文件/etc/hosts.allow或/etc/hosts.deny中添加特定IP地址为登录许可地址 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-07 | umask安全 | 帐号与口令用户的umask 安全配置 | **操作建议：**  (1) 设置用户目录默认权限，执行命令vi /etc/profile，编辑文件；  (2) 在文件中设置umask 027或UMASK 027，将缺省访问权限设置为750。如果文件中含有umask参数，则需要在最后面设置该参数 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-08 | 登录事件记录 | 日志审计 -syslog 登录事件记录 | 执行命令： more/etc/rsyslog.conf  查看参数 authpriv 值authpriv.\* /var/log/secure  若未对所有登录事件都记录，则低于安全要求。 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-09 | 日志配置审核 | 开启系统的审计功能，记录用户对系统的操作，包括但不限于帐号创建、删除，权限修改和口令修改。 | 1、判定条件  系统能够审计用户操作。   1. 查看审计服务是否开启   service auditd status   1. 查看日志服务是否开启   service rsyslog status  2、可通过 aureport 、 ausearch 命令查看审计日志。 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-10 | 系统查实注销 | 设置帐号超时自动注销。 | **操作建议：**  在文件/etc/profile中设置TMOUT=600，十分钟无操作情况下，超出TMOUT时间，系统自动注销。 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-11 | 禁用非必要服务 | 据实际情况，关闭不必要的系统服务，如：telnet,RPC,imap、nfs等 | 在无特殊应用情况下，若有非必要的服务开启，则不符合要求。 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| L-JX-12 | 防病毒 | 对服务器主机应当安装部署服务器专版杀毒软件，并打开自动升级病毒库选项。 | 如不存在杀毒软件或者没打开自动更新即为不合规。 |
| **（IP1）安全基线检查结果及配置现状截图：** | | | |
| **配置影响地址** | | | |
|  | | | |