# Linux服务器基线检查结果汇总

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 问题描述 | 影响对象 | 加固建议 |
| 1 | 口令强制更改周期（PASS\_MAX\_DAYS）值大于90不符合。 |  | 修改/etc/login.defs中PASS\_MAX\_DAYS参数 |
| 2 | 口令更改最小时间间隔（PASS\_MIN\_DAYS）值存在或不为0不符合。 |  | 修改/etc/login.defs中PASS\_ MIN \_DAYS参数 |
| 3 | 口令过期警告时间天数（PASS\_WARN\_AGE）  值小于3不符合。 |  | 修改/etc/login.defs中PASS\_WARN\_AGE参数 |
| 4 | 密码最小长度（PASS\_MIN\_LEN）值小于8不符合 |  | 修改/etc/login.defs中PASS\_MIN\_LEN参数 |
| 5 | 检查密码错误次数和锁定时间，未设置或设置次数大于5，时间小于600秒不符合 |  | 修改/etc/pam.d/login和/etc/pam.d/sshd中设置auth required pam\_tally2.so deny=3 unlock\_time=600 even\_deny\_root root\_unlock\_time=600 |
| 6 | 系统当前umask值不为0022不符合 |  | 使用umask 0022命令设置为0022 |
| 7 | rsyslog或syslog服务未开启 |  | 开启rsyslogd或syslogd服务 |
| 8 | auditd日志审计服务未开启 |  | 开启auditd服务 |
| 9 | 缺失登录错误日志（btmp）或登录日志（wtmp）或安全日志（secure）或最近一次登录信息（lastlog） |  | 开启登录错误日志（btmp）、登录日志（wtmp）、安全日志（secure）、最近一次登录信息（lastlog） |
| 10 | 未禁用root用户远程登录 |  | 修改/etc/ssh/sshd\_config文件PermitRootLogin内容 |
| 11 | 未关闭telnet服务 |  | 关闭telnet服务 |
| 12 | 用户配置了ssh免密登录 |  | 删除用户目录下.ssh/ authorized\_keys文件 |
| 13 | 以root权限运行web服务运行权限 |  | 建议使用非root权限运行web服务 |
| 14 | Linux硬盘使用率大于80% |  | 建议规划硬盘使用空间 |
| 15 | 检查重要文件的文件权限 |  | 修改/etc/passwd(-rw-r--r--)、/etc/shadow(----------)、/etc/sudoers(-r--r-----)、/etc/group(-rw-r--r--)、/etc/profile(-rw-r--r--)文件权限 |