0.0.0.0:

注：标注(x)的项目为不合格项

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **检测项** | **检测结果** | **不合规项目修复建议** |
| 1 | 网卡信息 |  | 略 |
| 2 | 系统类型及内核 |  | 略 |
| 3 | 检查UID为0的账户 |  | 删除UID为0的非root用户。 |
| 4 | 检查可登录账户 |  | 请检查该用户是否为正常账户 |
| 5 | 检查root组账户 |  | 请检查该用户是否为正常账户 |
| 6 | 检查可使用sudo su命令提升权限为root的用户 |  | 请检查该用户是否为正常账户 |
| 7 | 检查口令强制更改周期（PASS\_MAX\_DAYS） |  | 值大于90不符合，修改/etc/login.defs中PASS\_MAX\_DAYS参数 |
| 8 | 检查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 |
| 9 | 检查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 |
| 10 | 检查密码最小长度（PASS\_MIN\_LEN） |  | 值小于8不符合，修改/etc/login.defs中PASS\_MIN\_LEN参数 |
| 11 | 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 |
| 12 | 检查系统当前umask值 |  | 使用umask 0022命令设置为0022 |
| 13 | 检查rsyslog或syslog是否启用 |  | 开启rsyslogd或syslogd服务 |
| 14 | 检查是否开启auditd日志审计服务 |  | 开启auditd服务 |
| 15 | 检查是否有登录错误日志（btmp）、登录日志（wtmp）、安全日志（secure）、最近一次登录信息（lastlog） |  | 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） |
| 16 | 检查是否禁用root用户远程登录 |  | 修改/etc/ssh/sshd\_config文件PermitRootLogin内容 |
| 17 | 检查是否关闭telnet服务 |  | 关闭telnet服务 |
| 18 | 检查是否配置ssh免密登录 |  | 删除用户目录下.ssh/ authorized\_keys文件 |
| 19 | 检查web服务运行权限 |  | 建议使用非root权限运行web服务 |
| 20 | 检查Linux硬盘使用率 |  | 使用率大于80%不合格，建议规划硬盘使用空间 |
| 21 | 重要文件的文件权限异常 |  | 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 |