

章节检查项级别调整要求检查项说明标准值检查情况符合性调整情况原因

- 2.1检查是否以设置口令生存周期重要建议调整长期不修改密码会增加密码暴露风险，除入
- 2.2检查是否设置口令最小长度重要建议调整密码长度过短会增加密码被爆破风险，按照企
- 2.3检查是否设置口令过期警告天数重要建议调整除入域服务器超管账号分段管理无需配置外
- 2.4检查设备密码复杂度策略重要建议调整密码复杂度过低会增加密码被爆破风险，按照企
- 2.5检查是否存在空口令账户重要建议调整由于空口令会让攻击者不需要口令进入系统，存
- 2.6检查是否设置除root之外UID为0的用户一般建议调整不可设置除root之外，第二个具有r
- 3.1检查用户umask设置一般建议调整umask配置后，创建系统用户时所赋予的权限为最高权限
- 3.1.1检查/etc/csh.cshrc中umask设置一般建议调整详情参考父项3.1077/027 002FAIL
- 3.1.2检查/etc/bashrc文件中umask设置一般建议调整详情参考父项3.1077/027 002FAIL
- 3.1.3检查/etc/profile文件中umask设置一般建议调整详情参考父项3.1077/027 002FAIL
- 3.2检查重要目录或文件权限设置一般自行判断需检查重要目录或文件权限设置是否合规，在
- 3.2.1检查/etc/xinetd.conf文件权限一般自行判断参考父项3.2>=600文件不存在TRUE
- 3.2.2检查/etc/group文件权限一般自行判断参考父项3.2>=644644TRUE
- 3.2.3检查/etc/shadow文件权限一般自行判断参考父项3.2>=4000FAIL
- 3.2.4检查/etc/services文件权限一般自行判断参考父项3.2>=644644TRUE
- 3.2.5检查/etc/security目录权限一般自行判断参考父项3.2>=600755TRUE
- 3.2.6检查/etc/passwd文件权限一般自行判断参考父项3.2>=644644TRUE
- 3.2.7检查/etc/rc6.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.8检查/etc/rc0.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.9检查/etc/rc1.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.10检查/etc/rc2.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.11检查/etc目录权限一般自行判断参考父项3.2>=750755TRUE
- 3.2.12检查/etc/rc4.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.13检查/etc/rc5.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.14检查/etc/rc3.d目录权限一般自行判断参考父项3.2>=750777TRUE
- 3.2.15检查/etc/rc.d/init.d目录权限一般自行判断参考父项3.2>=750755TRUE
- 3.2.16检查/tmp目录权限一般自行判断参考父项3.2>=7501777TRUE
- 3.2.17检查/etc/grub.conf文件权限一般自行判断参考父项3.2>=600目录不存在TRUE
- 3.2.18检查/etc/grub/grub.conf文件权限一般自行判断参考父项3.2>=600文件不存在TRUE
- 3.2.19检查/etc/lilo.conf文件权限一般自行判断参考父项3.2>=600文件不存在TRUE
- 3.3检查重要文件属性设置一般建议调整需检查重要目录或文件属性设置是否合规，保障系
- 3.3.1检查/etc/passwd的文件属性一般建议调整参考父项3.3iFAIL
- 3.3.2检查/etc/shadow的文件属性一般建议调整参考父项3.3iFAIL
- 3.3.3检查/etc/group的文件属性一般建议调整参考父项3.3iFAIL
- 3.3.4检查/etc/gshadow的文件属性一般建议调整参考父项3.3iFAIL
- 3.4检查用户目录缺省访问权限设置重要建议调整控制用户缺省访问权限，当在创建新文件时
- 3.5检查是否设置SSH登录前警告Banner可选建议调整检查是否设置ssh登陆前的警告Banner并
- 4.1检查是否配置远程日志功能可选建议调整应对远程日志至进行筛选与审核。此检查项建议调
- 4.2检查安全事件日志配置可选建议调整应对安全时间日志文件进行配置。此检查项建议调
- 4.3检查日志文件是否全局可写可选建议调整应配置日志文件非全局可写，保证日志不可篡
- 4.3.1检查/var/log/cron可选建议调整参考父项4.4>=755600FAIL
- 4.3.2检查/var/log/secure可选建议调整参考父项4.4>=755600FAIL
- 4.3.3检查/var/log/messages可选建议调整参考父项4.4>=755600FAIL
- 4.3.4检查/var/log/boot.log可选建议调整参考父项4.4>=755600FAIL
- 4.3.5检查/var/log/mail可选建议调整参考父项4.4>=755文件不存在TRUE
- 4.3.6检查/var/log/localmessages可选建议调整参考父项4.4>=755文件不存在TRUE
- 4.3.7检查/var/log/spooler可选建议调整参考父项4.4>=755600FAIL
- 4.3.8检查/var/log/maillog可选建议调整参考父项4.4>=755600FAIL
- 4.4检查是否对登录进行日志记录重要建议调整应对登录时间日志文件进行配置，保证日志自
- 4.5检查是否配置su命令使用情况记录可选建议调整应配置su命令使用情况记录，保证高权限

- 5.1检查系统openssh安全配置一般建议调整openssh是使用加密的远程登录实现，可以有效防止被窃听
- 5.2检查是否修改SNMP默认团体字一般建议调整snmp的默认团体字存在安全漏洞，容易导致信息泄露
- 5.3检查使用ip协议远程维护的设备是否配置ssh协议，禁用telnet协议重要建议调整Telnet默认配置为明文传输
- 5.4检查是否禁止root用户登录FTP一般建议调整由于root用户权限过大，容易导致系统文件被篡改
- 5.5检查是否禁止匿名用户登录FTP重要建议调整由于匿名用户对被黑客用来进入ftp，导致系统文件被篡改
- 6.1检查是否设置命令行界面超时退出重要自行判断根据等保要求，建议设置超时时间不大于一小时
- 6.3检查系统coredump设置一般建议调整需要检查系统core dump设置，防止内存状态信息暴露
- 6.4检查历史命令设置可选建议调整根据等保要求，需保证历史命令文件HISTSIZE的值修改为1024
- 6.5检查是否使用PAM认证模块禁止wheel组之外的用户su为root重要建议调整禁止wheel组外用户通过su命令切换为root
- 6.6检查是否对系统账户进行登录限制可选建议调整对系统账户登录进行限制，禁止账户交互登录
- 6.7检查密码重复使用次数限制一般建议调整检测密码重复使用次数，预防密码重复使用被攻击
- 6.8检查账户认证失败次数限制可选建议调整应配置密码失败次数限制，预防密码被爆破的风险
- 6.9检查是否关闭ip伪装和绑定多ip功能可选建议调整应关闭此条检查项配置内容，使系统保持默认配置
- 6.9.1检查是否关闭多ip绑定可选建议调整参考父项6.9参考《Linux系统安全配置基线》对IP伪装和绑定多IP功能进行配置
- 6.10检查是否限制远程登录IP范围可选自行判断应配置相关设置防止未知ip远程登录，此检查项建议配置为只允许本地登录
- 6.11检查别名文件/etc/aliases可选自行判断/etc/aliases是linux系统下的一种配置文件，建议配置为只读
- 6.12检查拥有suid和sgid权限的文件可选建议调整suid的管理上有漏洞，易被黑客利用suid权限执行任意命令
- 6.13检查是否配置定时自动屏幕锁定(适用于图形化界面)可选建议调整对具有图形化界面的系统配置定时自动屏幕锁定
- 6.14检查系统内核参数配置一般建议调整该项配置主要为了缓解拒绝服务攻击。此检查项建议配置为默认值
- 6.15检查是否按组进行账号管理可选自行判断该项配置主要偏向于对系统用户的管理，如账号与组名不一致
- 6.16检查是否按用户分配账号可选自行判断该项配置主要偏向于对系统用户的管理，如有未分配账号的用户
- 6.17检查root用户的path环境变量一般建议调整如果将（.和..）这两者写入root的环境变量中，可能导致root用户执行任意命令
- 6.18检查系统是否禁用Ctrl+Alt+Delete组合键一般建议调整linux操作系统只要按下Ctrl+Alt+Delete组合键就会重启系统
- 6.19检查系统是否关闭系统信任机制重要建议调整如不关闭系统信任机制，在信任地址列表中可添加任意地址
- 6.19.1检查是否存在equiv文件重要建议调整参考父项6.19参考《Linux系统安全配置基线》对equiv文件进行配置
- 6.19.2检查是否存在rhosts文件重要建议调整参考父项6.19参考《Linux系统安全配置基线》对rhosts文件进行配置
- 6.20检查磁盘空间占用率可选自行判断磁盘动态分区空间不足，可能会导致系统卡慢与崩溃
- 6.21检查是否删除了潜在危险文件重要建议调整危险文件为删除可能导致用户无口令登录系统
- 6.22检查是否删除与设备运行，维护等工作无关的账号可选建议调整该项配置主要偏向于对系统用户的管理
- 6.23检查是否配置用户所需最小权限一般建议调整权限配置应为满足使用场景的最小化权限
- 6.24检查是否关闭数据包转发功能可选自行判断Linux系统默认是禁止数据包转发的，如非网络设备建议关闭
- 6.25检查是否关闭不必要的服务和端口可选自行判断不必要的服务会消耗系统内存，且存在安全风险
- 6.26检查是否使用NTP(网络时间协议)保持时间同步可选 建议调整应保证windows系统的时间同步
- 6.27检查NFS(网络文件系统)服务配置可选自行判断如果需要NFS服务，需要限制能够访问NFS服务的IP地址
- 6.28检查是否安装OS补丁可选自行判断及时安装操作系统补丁保证系统稳定性，此检查项建议配置为默认值
- 6.29检查是否设置SSH成功登录后Banner可选建议调整检查是否设置ssh成功登录后的Banner
- 6.30检查FTP用户上传的文件所具有的权限可选建议调整限制FTP用户登录后上传文件的属性
- 6.31检查FTPbanner设置可选建议调整检查是否设置ftp成功登录后的Banner信息，提示登录成功
- 6.32检查/usr/bin/目录下可执行文件的拥有者属性可选建议调整可执行文件拥有s属性在运行时可被任意用户执行
- 6.33检查Telnetbanner设置可选建议调整检查是否设置telnet成功登录后的Banner信息，提示登录成功
- 6.34检查是否限制FTP用户登录后能访问的目录可选自行判断限制FTP用户登录后能访问的目录
- 6.35检查是否关闭不必要的服务和端口重要自行判断不必要的端口和服务会扩大系统的被攻击面
- 6.36检查内核版本是否处于CVE-2021-43267漏洞影响范围可选建议调整CVE-2021-43267漏洞影响范围

Summary

全部检测项: 57
通过检测项: 20
失败检测项: 21
手工检测项: 15

扫描时间: 2024年 04月 09日 星期二 18:01:30 CST

或服务器或服务器超管账号分段管理无需配置外，应对服务器密码最长使用期限进行限制。1
业密码管理要求与等级保护标准，口令长度最小值应为8位。此检查项建议调整>=85FAIL
补，应配置密码过期提醒策略防止密码过期无法登陆。此检查项建议调整>=3020FAIL
业密码管理要求与等级保护标准，密码复杂度应包含特殊字符、大小写字母。此检查项建议i
至较大风险。此检查项建议调整不存在空口令账户TRUE
oot权限的账户。此检查项建议调整rootrootTRUE
限减去umask设置的权限，保证所创建用户不可创建其他权限用户。此检查项建议调整umaskC

保障系统安全性，此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置

究安全性。此检查项建议调整参考《Linux系统安全配置基线》对应章节参考子项参考子项

或目录时应屏蔽掉新文件或目录不应有的访问允许权限，防止同属于改组的其他用户及别的
言息，警示登陆系统的人员。此检查项建议调整参考《Linux系统安全配置基线》对应章节MA
周整参考《Linux安全配置基线》对应章节nullMANUAL
整参考《Linux安全配置基线》对应章节*.info;mail.none;authpriv.none;cron.none
改。此检查项建议调整参考《Linux系统安全配置基线》对应章节参考子项参考子项

的完整性。此检查项建议调整参考《Linux系统安全配置基线》对应章节authpriv.*
限命令可审计。此检查项建议调整参考《Linux系统安全配置基线》对应章节authpriv.*

保护登录及数据的安全。此检查项建议调整2FAIL

服务器信息泄漏。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

协议明文传输，安全性低，容易被嗅探泄漏信息。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

误删除。此检查项建议调整null略FAIL

系统文件的保密性和完整性遭到破坏。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

对于600s，此检查项建议系统管理员根据系统情况自行判断<=600FAIL

暴露，此检查项建议调整参考《Linux系统安全配置基线》对应章节FAIL

为5，此检查项建议调整参考《Linux系统安全配置基线》对应章节HISTSIZE=1000，FAIL

用户使用su命令，提高操作系统的完整性。此检查项建议调整s参考《Linux系统安全配置基线》对应章节TRUE

交互式登录。此检查项建议调整参考《Linux系统安全配置基线》对应章节nullMANUAL

爆破的风险。此检查项建议调整>=5FAIL

风险。此检查项建议调整参考《Linux系统安全配置基线》对应章节nullMANUAL

操作责任到人。此检查项建议调整参考《Linux系统安全配置基线》对应章节参考子项参考子项章节FAIL

检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节nullMANUAL

作用是将使用者名称进行转换，此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节TRUE

来踢拳，来放后门控制linux主机。此检查项建议调整TRUE

设备应配置定时自动屏幕锁定。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

建议调整参考《Linux系统安全配置基线》对应章节1TRUE

用户已分组管理，该检查项可以跳过。此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节TRUE

知账号，请及时调整与关闭。此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节TRUE

变量，执行脚本时，输入脚本名字后，系统会在当前的目录下执行该脚本，如脚本有危险命令如rm+Del快捷键，系统有时会重启。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

中的来访用户可不用提供口令就在本地计算机上执行远程命令。此检查项建议调整=0参考子项对应章节TRUE

对应章节TRUE

。此检查项建议系统管理员根据系统情况自行判断<=80略TRUE

系统，存在较大风险。此检查项建议调整参考《Linux系统安全配置基线》对应章节，TRUE

系统用户的管理，如有未知账号，请及时关闭。此项建议整改参考《Linux系统安全配置基线》对应章节TRUE

。此检查项建议调整参考《Linux系统安全配置基线》对应章节644，0，644TRUE

系统需要，请关闭该功能。此检查项建议系统管理员根据系统情况自行判断=00TRUE

安全隐患，此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节TRUE

司同步，提高系统日志的准确性。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

服务的IP范围，如果没有必要，需要停止NFS服务。此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节nullMANUAL

信息，提示登录系统的人员。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

，保证同组用户、其他用户不得有写入权限。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

系统人员。此检查项建议调整参考《Linux系统安全配置基线》对应章节略MANUAL

行时可所以获得拥有者的权限，所以为了安全需要，需要作出修改。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

示登录系统的人员。此检查项建议调整参考《Linux系统安全配置基线》对应章节TRUE

录，防止机密文件非授权访问，此检查项建议系统管理员根据系统情况自行判断参考《Linux系统安全配置基线》对应章节TRUE

击面，此检查项建议系统管理员根据系统情况自行判断nullMANUAL

是Linux内核TIPC模块中的一个堆溢出漏洞，攻击者利用该漏洞可以实现本地或远程代码执行

比检查项建议调整<=9099999FAIL

调整至少有1个大写字母、1个小写字母、1个数字、1个特殊字符nullFAIL

077参考子项目参考子项

'基线》对应章节参考子项参考子项

组的用户修改用户的文件或更高限制。此检查项建议调整027FAIL
NUAL

/var/log/messagesTRUE

/var/log/secureTRUE
/var/log/secureTRUE

配置基线》对应章节nullMANUAL

对应章节FAIL

线》对应章节略FAIL

项

MANUAL

ux系统安全配置基线》对应章节nullMANUAL

节nullMANUAL

《Linux系统安全配置基线》对应章节nullMANUAL

系统安全配置基线》对应章节nullMANUAL

令，将会对系统造成较大影响。此检查项建议调整参考《Linux系统安全配置基线》对应章节
章节Alias=ctrl-alt-del.targetFAIL

项参考子项

线》对应章节nullMANUAL

》对应章节nullMANUAL

节TRUE

自行判断参考《Linux系统安全配置基线》对应章节TRUE

Active: active (running) since 六 2024-03-30 16:33:07 CST; 1 weeks 3 days agoM
基线》对应要求TRUE

《Linux系统安全配置基线》对应章节略FAIL

ix系统安全配置基线》对应章节略FAIL

于漏洞5.10-rc1<Linux kernel <5.14.163.10.0TRUE

TRUE

ANUAL