目录

[第1章 概述 3](" \l "_Toc87876562)

[1.1 简介 3](" \l "_Toc87876563)

[1.2 适用范围 3](" \l "_Toc87876564)

[1.3 适用版本 3](" \l "_Toc87876565)

[第2章 账号口令 3](" \l "_Toc87876566)

[2.1 检查是否已设置口令生存周期 3](" \l "_Toc87876567)

[2.2 检查口令最小长度 4](" \l "_Toc87876568)

[2.3 检查是否设置口令过期警告天数 4](" \l "_Toc87876569)

[2.4 检查设备密码复杂度策略 5](" \l "_Toc87876570)

[2.5 检查是否存在空口令账号 5](" \l "_Toc87876571)

[2.6 检查是否设置除root之外UID为0的用户 6](" \l "_Toc87876572)

[第3章 认证授权 6](" \l "_Toc87876573)

[3.1 检查用户umask设置 6](" \l "_Toc87876574)

[3.2 检查重要目录或文件权限设置 7](" \l "_Toc87876575)

[3.3 检查重要文件属性设置-需重启 9](" \l "_Toc87876576)

[3.4 检查用户目录缺省访问权限设置 11](" \l "_Toc87876577)

[3.5 检查是否设置ssh登录前警告Banner 11](" \l "_Toc87876578)

[第4章 日志审计 12](" \l "_Toc87876579)

[4.1 检查是否配置远程日志功能 12](" \l "_Toc87876580)

[4.2 检查安全事件日志配置 13](" \l "_Toc87876581)

[4.3 检查日志文件是否非全局可写 14](" \l "_Toc87876582)

[4.4 检查是否对登录进行日志记录 15](" \l "_Toc87876583)

[4.5 检查是否配置su命令使用情况记录 16](" \l "_Toc87876584)

[第5章 协议安全 17](" \l "_Toc87876585)

[5.1 检查系统openssh安全配置 17](" \l "_Toc87876586)

[5.2 检查是否已修改snmp默认团体字 17](" \l "_Toc87876587)

[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 18](" \l "_Toc87876588)

[5.4 检查是否禁止root用户登录ftp 18](" \l "_Toc87876589)

[5.5 检查是否禁止匿名用户登录FTP 19](" \l "_Toc87876590)

[第6章 其他配置操作 20](" \l "_Toc87876591)

[6.1 检查是否设置命令行界面超时退出-需重启 20](" \l "_Toc87876592)

[6.2 检查是否设置系统引导管理器密码 20](" \l "_Toc87876593)

[6.3 检查系统core dump设置 21](" \l "_Toc87876594)

[6.4 检查历史命令设置 21](" \l "_Toc87876595)

[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 22](" \l "_Toc87876596)

[6.6 检查是否对系统账户进行登录限制 22](" \l "_Toc87876597)

[6.7 检查密码重复使用次数限制 23](" \l "_Toc87876598)

[6.8 检查用户认证失败次数限制 24](" \l "_Toc87876599)

[6.9 检查是否关闭绑定多ip功能 25](" \l "_Toc87876600)

[6.10 检查是否限制远程登录ip范围 25](" \l "_Toc87876601)

[6.11 检查别名文件/etc/aliases(或/etc/mail/aliases)配置 26](" \l "_Toc87876602)

[6.12 检查拥有suid和sgid权限的文件 28](" \l "_Toc87876603)

[6.13 检查是否配置定时自动屏幕锁定（适用于具备图形界面的设备） 28](" \l "_Toc87876604)

[6.14 检查系统内核参数配置 30](" \l "_Toc87876605)

[6.15 检查是否按组进行账号管理 31](" \l "_Toc87876606)

[6.16 检查是否按用户分配账号 32](" \l "_Toc87876607)

[6.17 检查root用户的path环境变量 32](" \l "_Toc87876608)

[6.18 检查系统是否禁用ctrl+alt+del组合键-需重启 33](" \l "_Toc87876609)

[6.19 检查是否关闭系统信任机制 33](" \l "_Toc87876610)

[6.20 检查系统磁盘分区使用率 34](" \l "_Toc87876611)

[6.21 检查是否删除了潜在危险文件 34](" \l "_Toc87876612)

[6.22 检查是否删除与设备运行，维护等工作无关的账号 35](" \l "_Toc87876613)

[6.23 检查是否配置用户所需最小权限 36](" \l "_Toc87876614)

[6.24 检查是否关闭数据包转发功能（适用于不做路由功能的系统）-对于集群系统或者需要数据包转发的系统不做该配置 37](" \l "_Toc87876615)

[6.25 检查是否禁用不必要的系统服务 37](" \l "_Toc87876616)

[6.26 检查是否使用NTP（网络时间协议）保持时间同步 38](" \l "_Toc87876617)

[6.27 检查NFS（网络文件系统）服务设置 39](" \l "_Toc87876618)

[6.28 检查是否安装OS补丁 39](" \l "_Toc87876619)

[6.29 检查是否设置ssh成功登陆后Banner 40](" \l "_Toc87876620)

[6.30 检查FTP用户上传的文件所具有的权限 40](" \l "_Toc87876621)

[6.31 检查FTP Banner设置 41](" \l "_Toc87876622)

[6.32 检查/usr/bin/目录下可执行文件的拥有者属性 42](" \l "_Toc87876623)

[6.33 检查telnet Banner设置 42](" \l "_Toc87876624)

[6.34 检查是否限制FTP用户登录后能访问的目录 43](" \l "_Toc87876625)

[6.35 检查是否关闭不必要的服务和端口-需重启 44](" \l "_Toc87876626)

# 概述

## 简介

本文规定了LINUX操作系统主机应当遵循的操作系统安全性设置标准，本文档旨在指导系统管理人员或安全检查人员进行LINUX 操作系统的安全合规性检查和配置。

服务器安全基线是指为满足安全规范要求，考虑到信息安全管理的三+四个特性：保密性、完整性、可用性、可审计性、可靠性、抗抵赖性。服务器安全配置必须达到的标准，一般通过检查安全配置参数是否符合安全标准或公司标准来度量。主要包括了账号配置安全、口令配置安全、授权配置、日志配置、IP通信配置等方面内容，这些安全配置直接反映了系统自身的安全脆弱性。

## 适用范围

本配置标准的使用者包括：服务器系统管理员、安全管理员和相关使用人员。

本配置标准适用的范围包括： Linux服务器。

## 适用版本

适用于Linux服务器。

# 账号口令

## 检查是否已设置口令生存周期

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查口令生存周期 |
| **安全基线项说明** | 长期不修改密码会提高密码暴露风险，所以为了提高保密性，检查是否设置口令生存周期 |
| **检测操作步骤** | 在文件/etc/login.defs中设置 PASS\_MAX\_DAYS 不大于标准值  检查语句：  cat /etc/login.defs | grep PASS\_MAX\_DAYS |
| **基线符合性判定依据** | 推荐值<=90  根据等保要求，推荐口令生存周期为不大于3个月的时间 |
| **备注** | 等级：重要 / 评分：7 |

## 检查口令最小长度

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查口令最小长度 |
| **安全基线项说明** | 长度小的口令存在被爆破出的风险，所以为了保证密码的安全，提高保密性  需要检查口令最小长度 |
| **检测操作步骤** | 在文件/etc/login.defs中设置 PASS\_MIN\_LEN 不小于标准值  检查语句：  cat /etc/login.defs | grep PASS\_MIN\_LEN |
| **基线符合性判定依据** | >=8  根据等保要求，口令最小长度不小于8位。 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否设置口令过期警告天数

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查口令过期前警告天数 |
| **安全基线项说明** | 为了防止口令过期而不知道，提高可用性。所以需要去检查设置口令过期警告天数。 |
| **检测操作步骤** | 在文件/etc/login.defs中设置 PASS\_WARN\_AGE 不小于标准值  检查语句：  cat /etc/login.defs | grep PASS\_WARN\_AGE |
| **基线符合性判定依据** | >=30  根据等保要求，一般设置过期警告天数为提前一个月告知。 |
| **备注** | 等级：重要 / 评分：7 |

## 检查设备密码复杂度策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查密码复杂度策略中设置的大写字母个数  检查密码复杂度策略中设置的数字个数  检查密码复杂度策略中设置的特殊字符个数  检查密码复杂度策略中设置的小写字母个数 |
| **安全基线项说明** | 口令过于简单会有被爆破出的风险，所以为了防止爆破风险，提高密码的保密性，需要检查设备的密码复杂度策略 |
| **检测操作步骤** | Redhat系统：修改/etc/pam.d/system-auth文件,  Suse9：修改/etc/pam.d/passwd文件，  Suse10,Suse11：修改/etc/pam.d/common-password文件，  在ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选3种，追加到password requisite pam\_cracklib.so后面，添加到配置文件中。  例如：password requisite pam\_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数 |
| **基线符合性判定依据** | 根据等保要求，至少有一个大写字母、小写字母、数字 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否存在空口令账号

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否存在空口令账号 |
| **安全基线项说明** | 空口令会让攻击者可以不需要口令进入系统，危险性很大。所以需要检查是否存在空口令账号 |
| **检测操作步骤** | 按照密码设置策略设置非空密码 命令： passwd [OPTION...] <accountName>  检查语句：cat /etc/shadow | awk -F: ‘($2 == “”)’ |
| **基线符合性判定依据** | 不存在空口令账号 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否设置除root之外UID为0的用户

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否存在除root之外UID为0的用户 |
| **安全基线项说明** | 不可设置除了root之外，第二个具有root权限的账号。为了提高可靠性，需要检查是否设置除了root之外UID为0的用户。 |
| **检测操作步骤** | 文件/etc/passwd中除root所在行外所有行第二个与第三个冒号之间UID不应设置为0  检查语句： cat/etc/passwd | awk -F: ‘($3 == 0 ){ print $1 }’ |
| **基线符合性判定依据** | 没有除root之外UID为0的用户 |
| **备注** | 等级：一般 / 评分：5 |

# 认证授权

## 检查用户umask设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查文件/etc/csh.cshrc中umask设置  检查文件/etc/bashrc（或/etc/bash.bashrc）中umask设置  检查文件/etc/profile中umask设置 |
| **安全基线项说明** | 介绍：umask指文件权限的掩码。它是从权限中“拿走”相应的“位”（即bit）,且用户创建时不能赋予执行权限  --- = 000 = 0 --x = 001 = 1 -w- = 010 = 2 -wx = 011 = 3 r-- = 100 = 4 r-x = 101 = 5 rw- = 110 = 6 rwx = 111 = 7  简单来说就是umask配置好后，创建系统用户时所赋予的权限为最高权限减去umask设置的权限。如umask：077，则创建用户时的用户权限为700. |
| **检测操作步骤** | 在文件/etc/csh.cshrc中设置 umask 077或UMASK 077  在文件/etc/csh.login中设置 umask 077或UMASK 077  检查文件/etc/bashrc（或/etc/bash.bashrc）中设置 umask 077或UMASK 077  在文件/etc/profile中设置umask 077或UMASK 077 |
| **基线符合性判定依据** | =077 |
| **备注** | 等级：一般 / 评分：5 |

## 检查重要目录或文件权限设置

|  |  |
| --- | --- |
| **安全基线项目名称** | /etc/xinetd.conf文件权限是否符合规范  /etc/group文件权限是否符合规范  /etc/shadow文件权限是否符合规范  /etc/services文件权限是否符合规范  /etc/security目录权限是否符合规范  /etc/passwd文件权限是否符合规范  /etc/rc6.d文件权限是否符合规范  /etc/tmp文件权限是否符合规范  /etc/rc0.d文件权限是否符合规范  /etc/rc1.d/文件权限是否符合规范  /etc/rc2.d文件权限是否符合规范  /etc/目录权限是否符合规范 -----设置影响gnome桌面自启动，系统重启时无法自启动gnome桌面。故使用gnome图形化的系统不设置该项。  /etc/rc4.d文件权限是否符合规范  /etc/rc5.d文件权限是否符合规范  /etc/rc3.d文件权限是否符合规范  /etc/rc.d/init.d/文件权限是否符合规范  检查系统引导器配置文件权限 |
| **安全基线项说明** | /etc/xinetd.d目录 在Linux系统中有一个超级服务程序inetd，大部分的网络服务都是由它启动的，如chargen、echo、finger、talk、telnet、wu-ftpd等…，在旧版本它的设置是在/etc/inetd.conf中配置的。 在新版本，它就改成了一个xinetd.d目录  /etc/group文件是有关于系统管理员对用户和用户组管理的文件,linux用户组的所有信息都存放在/etc/group文件中  /etc/shadow 文件，用于存储 Linux 系统中用户的密码信息，又称为“影子文件  /etc/services文件是记录网络服务名和它们对应使用的端口号及协议  inux资源限制配置文件是/etc/security/limits.conf；限制用户进程的数量对于linux系统的稳定性非常重要  /etc/passwd文件目录存储的是操作系统用户信息, 该文件为所有用户可见  这个目录存放的是一些脚本，一般是Linux以rpm包安装时设定的一些服务的启动/关闭脚本。系统在安装时装了好多rpm包，这里面就有很多对应的脚本。执行这些脚本可以用来启动、停止、重启这些服务  /tmp文件夹是存放linux临时文件的地方  /etc/rc0.d - /etc/rc5.d 是各启动级别的启动脚本  init.d 启动脚本存放目录  上面介绍了相关目录文件的意思、其重要性。为了安全性提高可靠性需要检查重要目录或文件的权限设置 |
| **检测操作步骤** | chmod 600 /etc/xinetd.conf  chmod 644 /etc/group  chmod 400 /etc/shadow  chmod 644 /etc/services  chmod 600 /etc/security  chmod 644 /etc/passwd  chmod 750 /etc/rc6.d  chmod 750 /tmp  chmod 750 /etc/rc0.d/  chmod 750 /etc/rc1.d/  chmod 750 /etc/rc2.d/  chmod 750 /etc/ -----设置影响gnome桌面自启动，系统重启时无法自启动gnome桌面。故使用gnome图形化的系统不设置该项。  chmod 750 /etc/rc4.d  chmod 750 /etc/rc5.d/  chmod 750 /etc/rc3.d  chmod 750 /etc/rc.d/init.d/  如果/etc/grub.conf文件存在，且非链接文件，则执行chmod 600 /etc/grub.conf;  如果/boot/grub/grub.conf文件存在，则执行chmod 600 /boot/grub/grub.conf;  如果/etc/lilo.conf文件存在，则执行chmod 600 /etc/lilo.conf。  检查语句：  stat -c %a /etc/passwd |
| **基线符合性判定依据** | 查看检测步骤中的标准值  根据等保要求设置，如etc/shadow只给400权限，表示只读权限 |
| **备注** | 等级：一般 / 评分：5 |

## 检查重要文件属性设置-需重启

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/etc/passwd文件属性  检查/etc/shadow文件属性  检查/etc/group文件属性  检查/etc/gshadow文件属性 |
| **安全基线项说明** | 为了提高完整性、可用性、可靠性。需要检查重要文件的属性设置  下面是对属性值的说明：  a，如果对文件设置a属性，那么只能在文件中增加数据，也不能删除和修改数据，如果对目录设置a属性，那么只允许在目录中建立和修改文件，但不允许删除文件，多用于服务器日志文件安全。  i，如果对文件设置i属性，那么不允许对文件进行删除，改名，也不能添加和修改数据，如果对目录设置i属性，那么只能修改目录下文件的数据，但不允许建立和删除文件  若配置该项，则无法在创建用户，若要创建用户，需要root权限取消设置的i属性：chattr -i /etc/passwd |
| **检测操作步骤** | 执行chattr +i /etc/passwd  如果不支持chattr,编辑/etc/fstab  在相应的reiserfs系统的选项中添加"user\_xattr,attrs"这两个选项，然后重启主机。  执行chattr +i /etc/shadow  如果不支持chattr,编辑/etc/fstab  在相应的reiserfs系统的选项中添加"user\_xattr,attrs"这两个选项，然后重启主机  执行chattr +i /etc/group  如果不支持chattr,编辑/etc/fstab  在相应的reiserfs系统的选项中添加"user\_xattr,attrs"这两个选项，然后重启主机。  执行chattr +i /etc/gshadow  如果不支持chattr,编辑/etc/fstab  在相应的reiserfs系统的选项中添加"user\_xattr,attrs"这两个选项，然后重启主机。  检查语句：  lsattr /etc/passwd |
| **基线符合性判定依据** | 符合依据参考检测步骤中的操作值 |
| **备注** | 等级：一般 / 评分：5 |

## 检查用户目录缺省访问权限设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查用户目录缺省访问权限设置 |
| **安全基线项说明** | 为了满足信息安全要求的保密性，需要检查用户目录缺省访问权限设置  如设置缺省权限为027 ，则用户默认的目录访问权限为750，即rwx rx- ---权限。 |
| **检测操作步骤** | 设置默认权限：  vi /etc/login.defs，  在末尾增加umask 027或UMASK 027 |
| **基线符合性判定依据** | 027  根据等保要求，建议设置目录缺省访问权限值设置为207 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否设置ssh登录前警告Banner

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否设置ssh登录前警告Banner |
| **安全基线项说明** | 为了保证信息安全抗抵赖性，可靠性。需检查是否设置ssh登录前的警告Banner信息，警示登录系统的人员。 |
| **检测操作步骤** | 执行如下命令创建ssh banner信息文件：  #touch /etc/ssh\_banner  #chown bin:bin /etc/ssh\_banner  #chmod 644 /etc/ssh\_banner  #echo " Authorized only. All activity will be monitored and reported " > /etc/ssh\_banner  可根据实际需要修改该文件的内容。  2. 修改/etc/ssh/sshd\_config文件，添加如下行：  Banner /etc/ssh\_banner  3.重启sshd服务：  #/etc/init.d/sshd restart或者  /bin/systemctl restart sshd.service  检查语句：  cat /etc/ssh/sshd\_config | grep Banner |
| **基线符合性判定依据** | 已设置ssh登录前的Banner信息 |
| **备注** | 等级：可选 / 评分：3 |

# 日志审计

## 检查是否配置远程日志功能

|  |  |
| --- | --- |
| **安全基线项目名称** | syslog-ng是否配置远程日志功能  rsyslog是否配置远程日志功能  syslog是否配置远程日志功能 |
| **安全基线项说明** | 为了保证信息安全的可审计性，抗抵赖性，需要检查是否配置远程日志功能。 |
| **检测操作步骤** | 在/etc/syslog-ng/syslog-ng.conf中配置destination logserver { udp("10.10.10.10" port(514)); };  log { source(src); destination(logserver); };  可以将此处10.10.10.10替换为实际的IP  修改配置文件vi /etc/rsyslog.conf，  加上这一行：  \*.\* @192.168.0.1  可以将"\*.\*"替换为你实际需要的日志信息。比如：kern.\* ; mail.\* 等等。  可以将此处192.168.0.1替换为实际的IP或域名(域名格式形如：[www.nsfocus.com,根据具体情况填写)。](http://www.nsfocus.com,根据具体情况填写)。)  修改配置文件vi /etc/syslog.conf，  加上这一行：  \*.\* @192.168.0.1  可以将"\*.\*"替换为你实际需要的日志信息。比如：kern.\* ; mail.\* 等等。  可以将此处192.168.0.1替换为实际的IP或域名(域名格式形如：www.nsfocus.com,根据具体情况填写)。 |
| **基线符合性判定依据** | 符合依据参考检测步骤内容 |
| **备注** | 等级：可选 / 评分：1 |

## 检查安全事件日志配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查syslog-ng是否配置安全事件日志  检查rsyslog是否配置安全事件日志  检查syslog是否配置安全事件日志 |
| **安全基线项说明** | 为了保证信息安全的可审计性，需要检查安全事件日志配置情况。 |
| **检测操作步骤** | 编辑/etc/syslog-ng/syslog-ng.conf  配置：  filter f\_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); };  destination msgs { file("/var/adm/msgs"); };  log { source(src); filter(f\_msgs); destination(msgs); };  其中/var/adm/msgs为日志文件。  如果该文件不存在，则创建该文件，命令为：  touch /var/adm/msgs，并修改权限为666.命令为：chmod 666 /var/adm/msgs.  重启日志服务：  #/etc/init.d/syslog restart  编辑/etc/rsyslog.conf  配置：  \*.err;kern.debug;daemon.notice /var/adm/messages  其中/var/adm/messages为日志文件。  如果该文件不存在，则创建该文件，命令为：  touch /var/adm/messages，并修改权限为666.命令为：chmod 666 /var/adm/messages.  重启日志服务：  #/etc/init.d/rsyslog restart  编辑/etc/syslog.conf  配置：  \*.err;kern.debug;daemon.notice /var/adm/messages  其中/var/adm/messages为日志文件。  如果该文件不存在，则创建该文件，命令为：  touch /var/adm/messages，并修改权限为666.命令为：chmod 666 /var/adm/messages.  重启日志服务：  #/etc/init.d/syslog restart |
| **基线符合性判定依据** | 符合依据请参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查日志文件是否非全局可写

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/var/log/cron日志文件是否other用户不可写  检查/var/log/secure文件是否other用户不可写  检查/var/log/messages文件是否不可被其他用户修改  检查/var/log/boot.log是否是否other用户不可写  检查/var/log/mail文件是否other用户不可写  检查/var/log/localmessages文件是否other用户不可写  检查/var/log/spooler文件是否other用户不可写  检查/var/log/maillog文件是否other用户不可写 |
| **安全基线项说明** | 为了保证信息安全的可审计性，和完整性。需要检查日志文件是否非全局可写。 |
| **检测操作步骤** | 执行命令：chmod 775 /var/log/cron  执行命令：chmod 775 /var/log/secure  执行命令：chmod 775 /var/log/boot.log  执行命令：chmod 755 /var/log/messages  执行命令：chmod 775 /var/log/mail  执行命令：chmod 775 /var/log/localmessages  执行命令：chmod 775 /var/log/spooler  执行命令：chmod 775 /var/log/maillog  检查语句：  ll /var/log/cron |
| **基线符合性判定依据** | 符合依据参考检测操作步骤，根据等保要求，建议非同组的其他用户不可写 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否对登录进行日志记录

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否记录成功登陆日志 |
| **安全基线项说明** | 为了保证信息安全的可审计性、抗抵赖性，需要检查是否对登录进行日志记录。 |
| **检测操作步骤** | 登录日志文件为/var/log/wtmp,/var/log/utmp.这2个文件中记录着所有登录过主机的用户，时间，来源等内容，这个文件不具可读性，可用last命令来看。  如果命令无结果，请联系管理员。 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否配置su命令使用情况记录

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否配置su命令使用情况记录 |
| **安全基线项说明** | Linux su（英文全拼：swith user）命令用于变更为其他使用者的身份，除 root 外，需要键入该使用者的密码。  使用权限：所有使用者  为了保证信息安全的可审计性、抗抵赖性，需要检查是否配置su命令使用情况记录 |
| **检测操作步骤** | 1.  Redhat5.x之前(包括5.x):编辑/etc/syslog.conf,  Redhat 6.x:编辑/etc/rsyslog.conf,  Suse 9:编辑/etc/syslog.conf,  配置:  authpriv.\* /var/log/secure  2.  Suse10, 11:  编辑:/etc/syslog-ng/syslog-ng.conf。  配置:  filter f\_secure { facility(authpriv); };  destination priverr { file("/var/log/secure"); };  log { source(src); filter(f\_secure); destination(priverr); };  3.  创建/var/log/secure文件  touch /var/log/secure  4.  重启syslog服务  #/etc/init.d/syslog restart |
| **基线符合性判定依据** | 参考操作标准 |
| **备注** | 等级：可选 / 评分：1 |

# 协议安全

d

## 检查系统openssh安全配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查系统openssh安全配置 |
| **安全基线项说明** | Openssh是使用加密的远程登录实现，可以有效保护登录及数据的安全，为了保证信息安全的保密性、可靠性，需要检查系统openssh安全配置。  注意该配置需要有多个账号，而不是只有一个root账号。 |
| **检测操作步骤** | 确保/etc/ssh/sshd\_config或/etc/ssh2/sshd2\_config文件存在。如果不存在，则忽略下面配置步骤。  在sshd\_config或sshd2\_config中配置：Protocol 2 -设置协议版本为ssh2，ssh1有安全漏洞 /bin/systemctl restart sshd.service |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 检查是否已修改snmp默认团体字

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否安装snmp服务  检查snmp团体字是否未使用private  检查配置文件/etc/snmp/snmpd.conf是否存在。  检查snmp团体字是否未使用public |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否已修改snmp默认团体字  Snmp的默认团体字存在安全漏洞，导致服务器信息泄露 |
| **检测操作步骤** | 如果系统未安装snmp服务，则认为合规。  编辑/etc/snmp/snmpd.conf，修改private默认团体字为用户自定义团体字。  如果系统安装了snmp服务，请确保该文件存在。如果不存在，则在/etc/snmp/目录下创建该文件  编辑/etc/snmp/snmpd.conf，修改public默认团体字为用户自定义团体字。 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 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

|  |  |
| --- | --- |
| **安全基线项目名称** | 对于使用IP协议进行远程维护的设备,应配置使用SSH协议  对于使用IP协议进行远程维护的设备,应禁止使用telnet协议 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查使用ip协议远程维护的设备是否配置ssh协议，禁用telnet协议。  Telnet协议明文传输，安全性低。容易被嗅探泄露信息 |
| **检测操作步骤** | 在网站上免费获取OpenSSH <http://www.openssh.com/,并根据安装文件说明执行安装步骤>  在/etc/services文件中，注释掉 telnet 23/tcp 一行(如不生效重启telnetd服务或xinetd服务或系统，例如，Red Hat 上重启xinetd：service xinetd restart，根据实际情况操作) |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否禁止root用户登录ftp

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止root登录VSFTP  禁止root登录WU-FTP |
| **安全基线项说明** | 为了保证信息安全的可用性、需要检查是否禁止root用户登录ftp  Root用户权限过大，容易导致系统文件误删除 |
| **检测操作步骤** | 编辑/etc/ftpusers(或/etc/vsftpd/ftpusers)文件  在/etc/ftpusers文件中加入下列行  root  检查语句：  cat /etc/vsftpd/ftpusers | grep root | grep -v ^# |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 检查是否禁止匿名用户登录FTP

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止匿名WU-FTP用户登录  禁止匿名VSFTP用户登录 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否禁止匿名用户登录FTP  匿名用户多被黑客用来进入ftp |
| **检测操作步骤** | 在/etc/passwd文件中，删除ftp用户  编辑/etc/vsftpd.conf(或/etc/vsftpd/vsftpd.conf)文件，设置：anonymous\_enable=NO  检查语句：  cat /etc/vsftpd/vsftpd.conf | grep "anonymous\_enable=NO" | grep -v ^# |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

# 其他配置操作

## 检查是否设置命令行界面超时退出-需重启

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查命令行界面超时时间 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否设置命令行界面超时退出 |
| **检测操作步骤** | 以root账户执行，vi /etc/profile末尾增加 export TMOUT=600(单位：秒，可根据具体情况设定超时退出时间，要求不小于600秒),注销用户，再用该用户登录激活该功能 |
| **基线符合性判定依据** | <=600  根据等保要求，建议设置超时时间不大于600秒 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否设置系统引导管理器密码

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否设置grub密码  检查是否设置lilo密码 |
| **安全基线项说明** | 为了保证信息安全的保密性、可靠性，需要检查是否设置系统引导管理器密码。 |
| **检测操作步骤** | 1.1请确认系统引导器的类型为grub,如果不为grub,则忽略此检查点。  1.2.如果/boot/grub/menu.lst文件存在，编辑/boot/grub/menu.lst文件,设置password=\*（\*为需要设置的密码。  1.3.如果不存在，请检查grub是否正确安装，或/boot/grub/menu.lst文件是否被更名。  检查语句：  cat /boot/grub/menu.lst | grep password  2.1.请确认系统引导器的类型为lilo,如果不为lilo,则忽略此检查点。  2.2.如果/etc/lilo.conf文件存在，编辑/etc/lilo.conf文件,设置password=\*（\*为需要设置的密码。  2.3.如果不存在，请检查lilo是否正确安装，或/etc/lilo.conf文件是否被更名。  检查语句：  cat /etc/lilo.conf | grep password |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：3 |

## 检查系统core dump设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/etc/security/limits.conf是否设置\* hard core 0  检查/etc/security/limits.conf是否设置\* soft core 0 |
| **安全基线项说明** | 当程序运行的过程中异常终止或崩溃，操作系统会将程序当时的内存状态记录下来，保存在一个文件中，这种行为就叫做Core Dump（中文有的翻译成“核心转储”)  为了保证信息安全的保密性，需要检查系统cire dump设置 |
| **检测操作步骤** | 在文件/etc/security/limits.conf中配置\* hard core 0  在文件/etc/security/limits.conf中配置\* soft core 0 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 检查历史命令设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查保留历史命令的记录文件大小  检查保留历史命令的条数 |
| **安全基线项说明** | 为了保证信息安全的可审计行、抗抵赖性，需要检查历史命令设置 |
| **检测操作步骤** | 编辑文件/etc/profile，  配置  HISTFILESIZE=5  编辑文件/etc/profile，将HISTSIZE 值修改为5 |
| **基线符合性判定依据** | 根据等保要求，符合依据为操作步骤设置值 |
| **备注** | 等级：可选 / 评分：3 |

## 检查是否使用PAM认证模块禁止wheel组之外的用户su为root

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否使用PAM认证模块禁止wheel组之外的用户su为root |
| **安全基线项说明** | Linux-PAM（即linux可插入认证模块）是一套共享库,使本地系统管理员可以随意选择程序的认证方式  为了保证信息安全的保密性，需要检查是否使用PAM认证模块禁止whell组之外的用户su为root |
| **检测操作步骤** | 编辑su文件(vi /etc/pam.d/su)，在开头添加下面两行：  auth sufficient pam\_rootok.so 和  auth required pam\_wheel.so group=wheel 这表明只有wheel组的成员可以使用su命令成为root用户。  你可以把用户添加到wheel组，以使它可以使用su命令成为root用户。  添加方法为：usermod –G wheel username |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否对系统账户进行登录限制

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止系统账号进行交互式登录 |
| **安全基线项说明** | 为了保证信息安全的可靠性、保密性。需要检查是否对系统账户进行登录限制 |
| **检测操作步骤** | 参考配置操作  禁止账号交互式登录：  修改/etc/shadow文件，用户名后密码列为两个感叹号“！！”；  删除账号：#userdel username;  补充操作说明  禁止交互登录的系统账号，比如daemon,bin,sys、adm、lp、uucp、nuucp、smmsp等等 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查密码重复使用次数限制

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查密码重复使用次数限制 |
| **安全基线项说明** | 为了保证信息安全的保密性、可用性、可靠性，需要检测密码重复使用次数  密码重复使用有被猜测爆破的风险 |
| **检测操作步骤** | Redhat:编辑/etc/pam.d/system-auth文件，  Suse9:编辑/etc/pam.d/passwd文件，  Suse10,Suse11:编辑/etc/pam.d/common-password文件，  修改设置如下  password sufficient pam\_unix.so md5 shadow nullok try\_first\_pass use\_authtok remember=5  补充操作说明  只需在password sufficient这一行加上remember=5即可  NIS系统无法生效，非NIS系统或NIS+系统能够生效。 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：4 |

## 检查用户认证失败次数限制

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否配置账户认证失败次数限制  检查是否配置SSH方式账户认证失败次数限制 |
| **安全基线项说明** | 为了保证信息安全的可靠性、保密性，需要检查用户认证失败次数限制。  不限制存在爆破的风险 |
| **检测操作步骤** | Redhat:  编辑/etc/pam.d/system-auth文件  配置:  auth required pam\_tally.so deny=5  account required pam\_tally.so   Suse9:  编辑/etc/pam.d/passwd文件  配置:  auth required pam\_tally.so deny=5  account required pam\_tally.so   Suse10，Suse11:  编辑/etc/pam.d/common-auth文件  配置:auth required pam\_tally.so deny=5 unlock\_time=600 no\_lock\_time  编辑/etc/pam.d/common-account文件  配置:account required pam\_tally.so   参数说明：  deny #连续认证失败次数超过的次数  unlock\_time #锁定的时间，单位为秒  编辑/etc/pam.d/sshd文件  在auth行下方添加：  auth required pam\_tally.so deny=5 unlock\_time=600 no\_lock\_time  在account行下方添加：  account required pam\_tally.so  参数说明：  deny #连续认证失败次数超过的次数  unlock\_time #锁定的时间，单位为秒 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否关闭绑定多ip功能

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否配置关闭多IP绑定 |
| **安全基线项说明** |  |
| **检测操作步骤** | 编辑/etc/host.conf文件：  multi off #关闭多IP绑定  补充操作说明  Redhat 默认没有/etc/host.conf文件，要先新建一个host.conf文件 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否限制远程登录ip范围

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/etc/hosts.allow配置  检查/etc/hosts.deny配置 |
| **安全基线项说明** | 为了提高信息安全可靠性，需要检查是否限制远程登录ip范围 |
| **检测操作步骤** | 编辑/etc/hosts.allow  增加一行 <service>: 允许访问的IP；举例如下：  all:192.168.4.44:allow #允许单个IP；  sshd:192.168.1.:allow #允许192.168.1的整个网段的PC通过SSH来访问本机  重启进程：  #/etc/init.d/xinetd restart  编辑/etc/hosts.deny  增加一行 all:all  重启进程：  #/etc/init.d/xinetd restart |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查别名文件/etc/aliases(或/etc/mail/aliases)配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/etc/aliases是否禁用不必要的别名  检查/etc/mail/aliases是否禁用不必要的别名 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查别名文件配置  /etc/aliases是linux系统下的一种配置文件，作用是将使用者名称进行转换。 |
| **检测操作步骤** | 参考配置操作  编辑别名文件vi /etc/aliases，删除或注释掉下面的行  #games: root  #ingres: root  #system: root  #toor: root  #uucp: root  #manager: root  #dumper: root  #operator: root  #decode: root  #root: marc  补充操作说明  更新后运行/usr/bin/newaliases，使改变生效  或者/usr/bin/alias   1. 编辑别名文件vi /etc/mail/aliases，删除或注释掉下面的行  #games: root  #ingres: root  #system: root  #toor: root  #uucp: root  #manager: root  #dumper: root  #operator: root  #decode: root  #root: marc  2.修改后运行命令：/usr/bin/newaliases，使改变生效   或者/usr/bin/alias  没有则不需要配置 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选/ 评分：1 |

## 检查拥有suid和sgid权限的文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查重要文件是否存在suid和sgid权限 |
| **安全基线项说明** | 为了保证信息安全的可靠性、需要检查拥有suid和sgid权限的文件  这两个权限很大，为了安全性，需要做出调整。 |
| **检测操作步骤** | 执行命令:  find /usr/bin/chage /usr/bin/gpasswd /usr/bin/wall /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp /usr/bin/write /usr/sbin/usernetctl /usr/sbin/traceroute /bin/mount /bin/umount /bin/ping /sbin/netreport -type f -perm +6000 2>/dev/null  如果存在输出结果，则使用chmod 755 文件名 命令修改文件的权限。  例如：chmod a-s /usr/bin/chage |
| **基线符合性判定依据** | 符合性依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否配置定时自动屏幕锁定（适用于具备图形界面的设备）

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用空闲激活  启用屏幕锁定  启用屏保  启用空闲激活时间 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否配置定时自动屏幕锁定 |
| **检测操作步骤** | 在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”；  或用命令方式：  gconftool-2 --direct \ 此处为回车换行  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行  --type bool \ 此处为回车换行  --set /apps/gnome-screensaver/idle\_activation\_enabled true  在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”；  或使用命令：  gconftool-2 --direct \ 此处为回车换行  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行  --type bool \ 此处为回车换行  --set /apps/gnome-screensaver/lock\_enabled true  在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”；  或使用命令：  gconftool-2 --direct \ 此处为回车换行  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行  --type string \ 此处为回车换行  --set /apps/gnome-screensaver/mode blank-only  在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”；  或使用命令：  gconftool-2 --direct \ 此处为回车换行  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行  --type int \ 此处为回车换行  --set /apps/gnome-screensaver/idle\_delay 15 根据具体情况设置时间 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查系统内核参数配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否禁止icmp源路由  是否禁止icmp重定向报文  检查send\_redirects配置  检查ip\_forward配置  检查icmp\_echo\_ignore\_broadcasts配置 |
| **安全基线项说明** | 为了保证信息安全的可靠性、可用性，需要检查系统内核参数配置  该检查项主要为了缓解拒绝服务攻击而做的。 |
| **检测操作步骤** | 1.备份配置文件  #cp -p /proc/sys/net/ipv4/conf/all/accept\_source\_route/proc/sys/net/ipv4/conf/all/accept\_source\_route.bak  2.执行命令  #**sysctl -w net.ipv4.conf.all.accept\_source\_route="0"**  并修改/proc/sys/net/ipv4/conf/all/accept\_source\_route的值为0  1.备份配置文件  #cp -p /proc/sys/net/ipv4/conf/all/accept\_redirects /proc/sys/net/ipv4/conf/all/accept\_redirects.bak  2.执行命令  #**sysctl -w net.ipv4.conf.all.accept\_redirects="0"**  并修改/proc/sys/net/ipv4/conf/all/accept\_redirects的值为0  1.备份配置文件  #cp -p /proc/sys/net/ipv4/conf/all/send\_redirects /proc/sys/net/ipv4/conf/all/send\_redirects.bak  2.执行命令  #**sysctl -w net.ipv4.conf.all.send\_redirects="0"**  并修改/proc/sys/net/ipv4/conf/all/send\_redirects的值为0  1.备份配置文件  #cp -p /proc/sys/net/ipv4/ip\_forward /proc/sys/net/ipv4/ip\_forward.bak  2.执行命令  #**sysctl -w net.ipv4.ip\_forward="0"**  并修改/proc/sys/net/ipv4/ip\_forward的值为0  1.备份配置文件  #cp -p /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts.bak  2.执行命令  #**sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts="1"**  并修改/proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts的值为1 |
| **基线符合性判定依据** | 符合性依据请参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：4 |

## 检查是否按组进行账号管理

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否按组进行账号管理 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否按组进行账号管理 |
| **检测操作步骤** | 1.执行备份：  #cp -p /etc/group /etc/group.bak  2.创建新的用户组  #groupadd 组名  #usermod -g 组名 -d 用户目录 -m 用户名  把用户添加进入某个组(s)或参考usermod --help说明进行设置 |
| **基线符合性判定依据** | 符合性依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否按用户分配账号

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否按用户分配账号 |
| **安全基线项说明** | 为了保证信息安全的保密性、可靠性，需要检查是否按用户分配账号 |
| **检测操作步骤** | 为用户创建账号：  #useradd username #创建账号  #passwd username #设置密码  修改权限：  #chmod 750 directory #其中750为设置的权限，可根据实际情况设置相应的权限，directory是要更改权限的目录)  使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：3 |

## 检查root用户的path环境变量

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查root用户的path环境变量内容 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查root用户的path环境变量 |
| **检测操作步骤** | 修改文件/etc/profile或/root/.bash\_profile 在环境变量$PATH中删除包含（.和..）的路径 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 检查系统是否禁用ctrl+alt+del组合键-需重启

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查系统是否禁用ctrl+alt+del组合键 |
| **安全基线项说明** | 检查系统是否禁用ctrl+alt+del组合键 |
| **检测操作步骤** | 编辑/etc/inittab，注释如下行ca::ctrlaltdel:/sbin/shutdown\*\*\*，之后重启系统  Centos7.x: vi /usr/lib/systemd/system/ctrl-alt-del.target。  找到下面行并注释掉：  Alias=ctrl-alt-del.target  Centos5.x: vi /etc/inittab  找到下面行并注释掉：  ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now  Centos6.x: /etc/init/control-alt-delete.conf  找到下面行并注释掉：  start on control-alt-delete  Ubuntu：vi /etc/init/contro;-alt-delete.conf  找到下面行并注释：  exec shutdown -r now "Control-Alt-Delete pressed" |
| **基线符合性判定依据** | 符合性依据参考检测操作步骤 |
| **备注** | 等级：一般 / 评分：5 |

## 检查是否关闭系统信任机制

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否存在equiv文件  检查是否存在rhosts文件 |
| **安全基线项说明** | 为了保证信息安全的保密性、可靠性，所以需要检查是狗关闭系统信任机制  在信任地址列表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，如 rexec，rcp，rlogin 等等 |
| **检测操作步骤** | 1.执行命令find / -maxdepth 2 -name hosts.equiv  2.进入到. hosts.equiv文件存在的目录  3.执行命令：mv hosts.equiv hosts.equiv.bak  1.执行命令find / -maxdepth 3 -type f -name .rhosts 2>/dev/null  2.进入到.rhosts文件存在的目录  3.执行命令：mv .rhosts .rhosts.bak |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查系统磁盘分区使用率

|  |  |
| --- | --- |
| **安全基线项目名称** | 检测系统磁盘根分区已使用空间是否维持在80%以下 |
| **安全基线项说明** | 为了保证信息安全的可用性，需要检查系统磁盘分区使用率 |
| **检测操作步骤** | 如果磁盘动态分区空间不足，建议管理员扩充磁盘容量  命令：df -h |
| **基线符合性判定依据** | <=80 |
| **备注** | 等级：可选 / 评分：3 |

## 检查是否删除了潜在危险文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否删除hosts.equiv文件  是否删除.rhosts 文件  是否删除.netrc 文件 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否删除了潜在危险文件  下面对文件的介绍：  /etc/hosts.equiv 文件包含远程系统的可信主机列表，每行列示一台主机。如果用户尝试从此文件中列出的主机之一远程登录（使用 rlogin 命令），并且如果远程系统可以访问用户的口令项，则远程系统允许用户在不使用口令的情况下登录。  .rhosts 文件是 /etc/hosts.equiv 文件的用户等效文件。此文件包含主机-用户组合列表，而不包含一般意义的主机。如果此文件中列出了主机-用户组合，则指定用户将被授予从指定主机登录而不必提供口令的权限。  文件”~/.netrc”用于设置自动登录时所需要的帐号信息。 |
| **检测操作步骤** | 1.执行命令find / -maxdepth 3 -name hosts.equiv 2>/dev/null  2.进入到hosts.equiv文件存在的目录  3.执行命令：mv hosts.equiv hosts.equiv.bak  1.执行命令find / -maxdepth 3 -name .rhosts 2>/dev/null  2.进入到.rhosts文件存在的目录  3.执行命令：mv .rhosts .rhosts.bak  1.执行命令find / -maxdepth 3 -name .netrc 2>/dev/null  2.进入到.netrc文件存在的目录  3.执行命令：mv .netrc .netrc.bak |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否删除与设备运行，维护等工作无关的账号

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否删除与设备运行、维护等工作无关的账号 |
| **安全基线项说明** | 为了保证信息安全的保密性、可靠性，需要检查是否删除与设备运行，维护等工作无关的账户 |
| **检测操作步骤** | 删除用户:#userdel username;  锁定用户：  #usermod -L username  只有具备超级用户权限的使用者方可使用.  #usermod –U username可以解锁。  补充操作说明  需要锁定的用户：adm,lp,mail,uucp,operator,games,gopher,ftp,nobody,nobody4,noaccess,listen,webservd,rpm,dbus,avahi,mailnull,smmsp,nscd,vcsa,rpc,rpcuser,nfs,sshd,pcap,ntp,haldaemon,distcache,apache,webalizer,squid,xfs,gdm,sabayon,named。 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否配置用户所需最小权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/etc/passwd文件权限  检查/etc/group文件权限  检查/etc/shadow文件权限 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否配置用户所需最小权限 |
| **检测操作步骤** | chmod 644 /etc/passwd  chmod 644 /etc/group  chmod 600 /etc/shadow |
| **基线符合性判定依据** | 参考操作步骤标准 |
| **备注** | 等级：一般 / 评分：4 |

## 检查是否关闭数据包转发功能（适用于不做路由功能的系统）-对于集群系统或者需要数据包转发的系统不做该配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 对于不做路由功能的系统，检查是否关闭数据包转发功能 |
| **安全基线项说明** | 为了保证信息安全的保密性，需要检查是否关闭数据包转发功能  如果系统存在集群或者需要数据包转发则不做该基线配置 |
| **检测操作步骤** | Redhat 默认已经关闭了数据包转发功能。  可通过以下命令来查看数据包转发功能是否关闭：  # cat /proc/sys/net/ipv4/ip\_forward  如果返回值为0，说明数据包转发功能已经关闭，为1则开启。  关闭数据包转发功能：  命令： #sysctl -w net.ipv4.ip\_forward=0 |
| **基线符合性判定依据** | =0 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否禁用不必要的系统服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 列出所需要服务的列表(包括所需的系统服务)，不在此列表的服务需关闭。 |
| **安全基线项说明** | 为了保证信息安全的可靠性，检查是否禁用不必要的系统服务  不必要的服务不要开启，既消耗系统内存，又存在安全隐患 |
| **检测操作步骤** | 查看所有开启的服务：  #ps aux  禁用xinetd.d 目录中不用的服务：  #vi /etc/xinetd.d/servicename  将服务文件里面的disable设置为disable=yes重启xinetd服务,即可。  要直接关闭某个服务，如sshd可用如下命令:  # /etc/init.d/sshd stop #关闭正在运行的sshd服务  补充操作说明  关闭下列不必要的基本网络服务。  chargen-dgram daytime-stream echo-streamklogin tcpmux-server chargen-stream discard-dgram eklogin krb5-telnet tftp cvs discard-stream ekrb5-telnet kshell time-dgram daytime-dgram echo-dgram gssftp rsync time-stream |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否使用NTP（网络时间协议）保持时间同步

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否配置NTP服务器地址  检查ntp服务是否开启 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否使用NTP保持时间同步，若未开启则无需配置该基线 |
| **检测操作步骤** | 编辑ntp 的配置文件：  #vi /etc/ntp.conf,  配置：server IP地址（提供ntp服务的机器）  如：server 192.168.1.1  开启ntp服务：  redhat为：/etc/init.d/ntpd start  suse9为：/etc/init.d/xntpd start  suse10,11为：/etc/init.d/ntp start。  如果ntp服务未开启，开启ntp服务：  redhat为：/etc/init.d/ntpd start  suse9为：/etc/init.d/xntpd start  suse10,11为：/etc/init.d/ntp start |
| **基线符合性判定依据** | 符合依据草靠检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查NFS（网络文件系统）服务设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 如果需要NFS服务，需要限制能够访问NFS服务的IP范围  如果没有必要，需要停止NFS服务 |
| **安全基线项说明** | 为了保证信息安全的保密性、可靠性，需要检查NFS服务设置 |
| **检测操作步骤** | 限制能够访问NFS服务的IP范围：  编辑文件：vi /etc/hosts.allow  增加一行:portmap: 允许访问的IP  停止nfs服务：  Suse系统：/etc/init.d/nfsserver stop  Redhat系统：/etc/init.d/nfs stop |
| **基线符合性判定依据** | 符合依据检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否安装OS补丁

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否安装OS补丁 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否安装os补丁 |
| **检测操作步骤** | 可以使用OnlineUpdate或Patch CD Update等方式升级系统补丁 |
| **基线符合性判定依据** | 系统已安装最新补丁 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否设置ssh成功登陆后Banner

|  |  |
| --- | --- |
| **安全基线项目名称** | 是否设置ssh成功登录后Banner信息 |
| **安全基线项说明** | 为了保证信息安全的抗抵赖性，需要检查是否设置ssh成功登录后Banner |
| **检测操作步骤** | 1.修改文件/etc/motd的内容，如没有该文件，则创建它。  #echo "Login success. All activity will be monitored and reported " > /etc/motd根据实际需要修改该文件的内容 |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：2 |

## 检查FTP用户上传的文件所具有的权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制FTP用户登录后上传文件的属性 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查FTP用户上传的文件所具有的权限。 |
| **检测操作步骤** | 如果系统使用vsftp：  修改/etc/vsftpd.conf（或者为/etc/vsftpd/vsftpd.conf）  # vi /etc/vsftpd.conf  确保以下行未被注释掉，如果没有该行，请添加：  write\_enable=YES //允许上传。如果不需要上传权限，此项可不进行更改。  ls\_recurse\_enable=YES  local\_umask=022 //设置用户上传文件的属性为755  anon\_umask=022 //匿名用户上传文件(包括目录)的 umask  重启网络服务  # /etc/init.d/vsftpd restart  如果系统使用pure-ftp  修改/etc/pure-ftpd/pure-ftpd.conf  # vi /etc/pure-ftpd/pure-ftpd.conf  确保以下行未被注释掉，如果没有该行，请添加：  Umask 177:077  重启ftp服务  #/etc/init.d/pure-ftpd restart |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：3 |

## 检查FTP Banner设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否更改默认的ftp登陆警告Banner |
| **安全基线项说明** | 为了保障信息安全的抗抵赖性，需要检查FTP Banner设置 |
| **检测操作步骤** | 1.修改vsftp回显信息  # vi /etc/vsftpd.conf(或/etc/vsftpd/vsftpd.conf)  ftpd\_banner=” Authorized users only. All activity will be monitored and reported.”  可根据实际需要修改该文件内容。  重启服务：  # /etc/init.d/vsftpd restart  2.修改pure-ftp配置文件：  #vi /etc/pure-ftpd/pure-ftpd.conf  找到以下行，确保该行未被注释。  FortunesFile /usr/share/fortune/zippy  编辑/usr/share/fortune/zippy文件（如没有fortune文件夹或者zippy文件，则新建该文件夹或该文件）：  #vi /usr/share/fortune/zippy  将自定义BANNER写入其中。  重启服务：  # /etc/init.d/pure-ftpd restart |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查/usr/bin/目录下可执行文件的拥有者属性

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查/usr/bin/目录下的可执行文件的拥有者属性，当可执行文件设置s属性时，执行时可以获取其拥有者的权限。 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要减产可执行文件的拥有者属性  s属性在运行时可以获得拥有者的权限，所以为了安全需要，需要做出修改 |
| **检测操作步骤** | 找出系统中所有含有“s”属性的文件，把不必要的“s”属性去掉，或者把不用的直接删除。 自行判断 # find /usr/bin -type f \( -perm -04000 -o -perm -02000 \) -exec ls -lg {} \;  # chmod a-s filename |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：3 |

## 检查telnet Banner设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否更改默认的telnet登录警告Banner |
| **安全基线项说明** | 为了保证信息安全的抗抵赖性，需要检擦telnet Banner设置 |
| **检测操作步骤** | 1.修改telnet回显信息  修改文件/etc/issue 和/etc/issue.net中的内容：  #echo " Authorized users only. All activity may be monitored and reported " > /etc/issue  #echo " Authorized users only. All activity may be monitored and reported " > /etc/issue.net  可根据实际需要修改该文件的内容,但是不要出现系统敏感信息,如redhat,suse等。  2.重启服务：  # /etc/init.d/xinetd restart |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否限制FTP用户登录后能访问的目录

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否限制FTP用户登录后能访问的目录 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否限制FTP用户登录后能访问的目录 |
| **检测操作步骤** | 1.vsftp  修改/etc/vsftpd.conf(或者/etc/vsfptd/vsftpd.conf)  #vi /etc/vsftpd.conf  确保以下行未被注释掉，如果没有该行，请添加：  chroot\_local\_user=YES  重启网络服务  #/etc/init.d/vsftpd restart   2.pure-ftp  修改/etc/pure-ftpd/pure-ftpd.conf  #vi /etc/pure-ftpd/pure-ftpd.conf  确保以下行未被注释掉（并且值为以下值），如果没有该行，请添加：  ChrootEveryone yes  AllowUserFXP no  AllowAnonymousFXP no  重启ftp服务  #/etc/init.d/pure-ftpd restart |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：可选 / 评分：2 |

## 检查是否关闭不必要的服务和端口-需重启

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否关闭kshell服务  检查是否关闭time服务  检查是否关闭ntalk服务  检查是否关闭lpd服务  检查是否关闭sendmail服务  检查是否关闭printer服务  检查是否关闭klogin服务  检查是否关闭nfslock服务  检查是否关闭echo服务  检查是否关闭discard服务  检查是否关闭chargen服务  检查是否关闭bootps服务  检查是否关闭tftp服务  检查是否关闭nfs服务  检查是否关闭ypbind服务  检查是否关闭ident服务  检查是否关闭daytime服务 |
| **安全基线项说明** | 为了保证信息安全的可靠性，需要检查是否关闭不必要的端端口和服务  不必要的端口和服务会扩大系统的被攻击面  下面介绍相关服务信息：  Shell 服务  time服务正在运行，该服务会泄露服务器当前时钟  服务器聊天  Lpd打印机服务  Sendmail邮件服务  Printer打印服务  Kerberos rlogin连接到该计算机  nfslock：一个可选的服务，用于启动相应的RPC进程，允许NFS客户端在服务器上对文件加锁  echo服务是一种非常有用的用于调试和检测的工具。该协议接收到什么原样发回，类似于日常生活中的“回声”  discard服务由于连接的空服务  CHARGEN字符发生器协议（Character Generator Protocol）是一种简单网络协议，设计的目的是用来调试TCP或UDP协议程序、测量连接的带宽或进行QoS的微调等。它的默认端口为19，分为基于TCP和UDP两种方式  bootps引导程序协议  TFTP是TrivialFileTransferProtocol的简称，翻译汉语意思就是：简单文件传输协议。TFTP协议是TCP/IP协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，其默认端口号为69  Nfs 网络文件系统  Nis管理-NIS， 表示网络信息服务 (Network Information Services)。ypbind-“绑定(bind)” NIS 客户机到它的 NIS 服务器上。 这样， 它将从系统中获取 NIS 域名， 并使用 RPC 连接到服务器上。 ypbind 是 NIS 环境中， 客户机-服务器通讯的核心； 如果客户机上的 ypbind 死掉的话， 它将无法访问 NIS 服务器  认证协bai议(ident protocol)在RFC1413中的描述：du每个类unix的操作系统都带有一个默zhi认监听dao113端口的身份服zhuan务器。身份服务器能够提供本机某发起TCP连接进程的用户名  DAYTIME协议是基于TCP的应用，是一种有用的调试工具，它的作用是返回当前时间和日期，格式是字符串格式 |
| **检测操作步骤** | chkconfig [--level levels] kshell off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] time off  chkconfig [--level levels] time-udp off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] ntalk off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] lpd off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] printer off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] klogin off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] nfslock off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] echo off  chkconfig [--level levels] echo-udp off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] discard off  chkconfig [--level levels] discard-udp off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] chargen off  chkconfig [--level levels] chargen-udp off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] bootps off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] tftp off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] nfs off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] ypbind off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] ident off  注:levels为运行级别,需要重启机器  chkconfig [--level levels] daytime off  注:levels为运行级别,需要重启机器  chkconfig --level 345 atd off ##和cron很相似的定时运行程序的服务  注：以上chkcofig 命令中的3和5是系统启动的类型，以下为数字代表意思  0:开机(请不要切换到此等级)  1:单人使用者模式的文字界面  2:多人使用者模式的文字界面,不具有网络档案系统(NFS)功能  3:多人使用者模式的文字界面,具有网络档案系统(NFS)功能  4:某些发行版的linux使用此等级进入x windows system  5:某些发行版的linux使用此等级进入x windows system  6:重新启动  检查语句：  Chkconfig --list |
| **基线符合性判定依据** | 符合依据参考检测操作步骤 |
| **备注** | 等级：重要 / 评分：7 |

## 检查内核版本是否处于CVE-2021-43267漏洞影响版本

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查内核版本是否处于CVE-2021-43267漏洞影响版本 |
| **安全基线项说明** | CVE-2021-43267漏洞是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漏洞。  漏洞影响Linux内核范围：  5.10-rc1 < Linux kernel < 5.14.16 |
| **检测操作步骤** | 输入命令 uname –r即可查看Linux内核版本是否在5.10-5.14.16之间。 |
| **基线符合性判定依据** | 内核版本不在5.10-rc1和5.14.16之间。 |
| **备注** | 等级：重要 / 评分：7 |