|  |
| --- |
| **老男孩信息系统安全配置基线**  **Linux 操作系统分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408348019)  [1.1适用范围 4](#_Toc408348020)  [1.2规范依据 4](#_Toc408348021)  [1.3实施策略 4](#_Toc408348022)  [二. 安全配置基线标准 6](#_Toc408348023)  [2.1身份鉴别 6](#_Toc408348024)  [2.1.1配置口令复杂度 6](#_Toc408348025)  [2.1.2设置口令认证失败锁定次数 6](#_Toc408348026)  [2.1.3配置口令生存期 7](#_Toc408348027)  [2.1.4配置使用SSH方式远程访问 8](#_Toc408348028)  [2.1.5配置历史口令使用策略 8](#_Toc408348029)  [2.2访问控制 9](#_Toc408348030)  [2.2.1禁用共享账户 9](#_Toc408348031)  [2.2.2锁定无关账户 10](#_Toc408348032)  [2.2.3清除UID为0的非root账户 11](#_Toc408348033)  [2.2.4设置umask值 11](#_Toc408348034)  [2.2.5配置重要目录与文件的权限 12](#_Toc408348035)  [2.2.6控制未授权的SUID/SGID 13](#_Toc408348036)  [2.2.7控制任何人都有写权限的目录 14](#_Toc408348037)  [2.2.8控制任何人都有写权限的文件 14](#_Toc408348038)  [2.2.9删除没有属主的文件 15](#_Toc408348039)  [2.2.10控制异常或隐含文件 16](#_Toc408348040)  [2.2.11禁止 Ctrl+Alt+Del 16](#_Toc408348041)  [2.3安全审计 17](#_Toc408348042)  [2.3.1配置syslog.conf 17](#_Toc408348043)  [2.3.2配置认证日志 18](#_Toc408348044)  [2.3.3配置使用NTP 18](#_Toc408348045)  [2.3.4配置远程日志服务器 19](#_Toc408348046)  [2.3.5配置安全日志 20](#_Toc408348047)  [2.4入侵防范 21](#_Toc408348048)  [2.4.1关闭不需要的服务 21](#_Toc408348049)  [2.5资源控制 22](#_Toc408348050)  [2.5.1配置登录超时 22](#_Toc408348051)  [2.5.2设置登录超时 22](#_Toc408348052)  [2.5.3配置增强被远程访问的安全性 23](#_Toc408348053)  [2.5.4限制root账户远程登录 24](#_Toc408348054)  [2.6其它安全项 24](#_Toc408348055)  [2.6.1关闭系统core dump状态 24](#_Toc408348056)  [三. 评审与修订 25](#_Toc408348057)   1. 概述 |

* 1. 适用范围

本配置基线适用于老男孩的Linux系列操作系统，主要涉及Linux操作系统安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行的Linux系列操作系统。

该文档参照标准Linux操作系统编写，但在实际情况中，不同厂家、版本的Linux存在不同程度的订制和阉割，请依据自身实际安全需求，参照对应的制度、标准或要求进行检查。

* 1. 规范依据

根据老男孩目前Linux操作系统的安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 配置口令复杂度 | 必须实施 |
| 2 | 身份鉴别 | 设置口令认证失败锁定次数 | 必须实施 |
| 3 | 身份鉴别 | 配置口令生存期 | 必须实施 |
| 4 | 身份鉴别 | 配置使用SSH方式远程访问 | 必须实施 |
| 5 | 身份鉴别 | 配置历史口令使用策略 | 建议实施 |
| 6 | 访问控制 | 禁用共享账户 | 必须实施 |
| 7 | 访问控制 | 锁定无关账户 | 必须实施 |
| 8 | 访问控制 | 清除UID为0的非root账户 | 必须实施 |
| 9 | 访问控制 | 设置umask值 | 必须实施 |
| 10 | 访问控制 | 配置重要目录与文件的权限 | 建议实施 |
| 11 | 访问控制 | 控制未授权的SUID/SGID | 建议实施 |
| 12 | 访问控制 | 控制任何人都有写权限的目录 | 建议实施 |
| 13 | 访问控制 | 控制任何人都有写权限的文件 | 建议实施 |
| 14 | 访问控制 | 删除没有属主的文件 | 建议实施 |
| 15 | 访问控制 | 控制异常或隐含文件 | 建议实施 |
| 16 | 访问控制 | 禁止Ctrl+Alt+Del | 建议实施 |
| 17 | 安全审计 | 配置syslog.conf | 必须实施 |
| 18 | 安全审计 | 配置认证日志 | 必须实施 |
| 19 | 安全审计 | 配置使用NTP | 必须实施 |
| 20 | 安全审计 | 配置远程日志服务器 | 建议实施 |
| 21 | 安全审计 | 配置安全日志 | 按需实施 |
| 22 | 入侵防范 | 关闭不需要的服务 | 必须实施 |
| 23 | 资源控制 | 配置登录超时 | 必须实施 |
| 24 | 资源控制 | 设置登录超时 | 必须实施 |
| 25 | 资源控制 | 配置增强被远程访问的安全性 | 必须实施 |
| 26 | 资源控制 | 限制root账户远程登录 | 按需实施 |
| 27 | 其它安全项 | 关闭系统core dump状态 | 建议实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 配置口令复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置口令复杂度（必须实施） |
| **安全基线编号** | 操作系统-Linux-1 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号4类中至少2类。 |
| **配置方法** | /etc/pam.d/system-auth文件中是否对pam\_cracklib.so的参数进行了正确设置。  建议在/etc/pam.d/system-auth 文件中配置：  password requisite pam\_cracklib.so difok=3 minlen=8 ucredit=-1 lcredit=-1 dcredit=1 |
| **检查方法** | 参考配置方法。至少8位，包含一位大写字母，一位小写字母和一位数字。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 设置口令认证失败锁定次数

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置口令认证失败锁定次数（必须实施） |
| **安全基线编号** | 操作系统-Linux-2 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次，锁定该用户使用的帐号。 |
| **配置方法** | 以root身份登录Linux系统，检查/etc/pam.d/system-auth文件中是否对pam\_tally.so的参数进行了正确设置。命令如下：  More /etc/pam.d/system-auth  设置连续输错10次密码，帐号锁定5分钟，使用命令“vi /etc/pam.d/system-auth”修改配置文件，添加auth required pam\_tally.so onerr=fail deny=10 unlock\_time=300  注：解锁用户faillog -u<用户名>-r |
| **检查方法** | 参见配置方法，可在合适的时间对某一（登录）影响较弱的账户进行测试。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），d）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。 |
| **备注** | 根据实际需求进行配置。 |

* + 1. 配置口令生存期

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置口令生存期（必须实施） |
| **安全基线编号** | 操作系统-Linux-3 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，账户口令的生存期不长于90天。 |
| **配置方法** | 1、询问管理员是否存在如下类似的简单用户密码配置，比如：  root/root, test/test, root/root1234  2、执行：more /etc/login.defs，检查PASS\_MAX\_DAYS/ PASS\_MIN\_DAYS/PASS\_WARN\_AGE参数  3、执行：awk -F: '($2 == "") { print $1 }' /etc/shadow, 检查是否存在空口令帐号 |
| **检查方法** | 建议在/etc/login.defs文件中配置：  PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数  PASS\_MIN\_DAYS 0#新建用户的密码最短使用天数PASS\_WARN\_AGE 7#新建用户的密码到期提前提醒天数  过期口令登录不成功。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 配置使用SSH方式远程访问

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置使用SSH方式远程访问（必须实施） |
| **安全基线编号** | 操作系统-Linux-4 |
| **安全基线项说明** | 远程访问服务器时，建议使用SSH（安全）方式。 |
| **配置方法** | 登录服务器，使用root权限执行下列命令  查看SSH服务状态：  # service ssh status  若返回的结果为  查看telnet服务状态：  # service telnet status |
| **检查方法** | SSH服务状态查看结果为：running  telnet服务状态查看结果为：not running/unrecognized |
| **依据** | 7.1.3.1 主机：身份鉴别（A3），e) 主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当通过互联网对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听； |
| **备注** |  |

* + 1. 配置历史口令使用策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置历史口令使用策略（建议实施） |
| **安全基线编号** | 操作系统-Linux-5 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近5次（含5次）内已使用的口令。 |
| **配置方法** | 登录系统，并使用root账户权限。  Debian / Ubuntu系统修改文件如下文件  # vi /etc/pam.d/common-password （需要修改参数见下面）  CentOS / RHEL / RedHat / Fedora 修改文件如下文件  # vi /etc/pam.d/system-auth （需要修改参数见下面）  上述均在password sufficient pam\_unix.so use\_authtok md5 shadow remember=5  在相应行的后面添加 remember=10，而不是添加一行！  SUSE比较恶心，找了半天才找到。man pw\_check  在/etc/security/pam\_pwcheck文件中添加remember=5  passwd: nullok use\_cracklib remember=5 |
| **检查方法** | 见配置方法，查看passed文件内的参数显示“HISTORY＝5”。  或在挑选合适的时间，选用适当的账户（不影响登录）进行测试。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令。 |
| **备注** |  |

* 1. 访问控制
     1. 禁用共享账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁用共享账户（必须实施） |
| **安全基线编号** | 操作系统-Linux-6 |
| **安全基线项说明** | 系统需按照实际用户分配账户，避免不同用户间使用共享账户（同一个账户）进行操作；  避免“用户账户”和服务器间通信使用的账户共享。 |
| **配置方法** | 此项为问询项，需要与系统、应用管理员确认是否有共享账户存在。  可以查看如下配置文件进行检查，以root权限登录后进行检查：  cat /etc/passwd  cat/etc/shadow  cat /etc/group  ----------------------------------------------------------------------------------------------  如需建立用户，参考如下：  #useradd username //创建账户  #passwd username //设置密码  使用该命令为不同的用户分配不同的账户，设置不同的口令及权限信息等。 |
| **检查方法** | 以root账户登录Linux系统  #cat /etc/passwd  输出所有用户信息后，与管理员确认是否有共享账户情况存在。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），e) 应及时删除多余的、过期的帐户，避免共享帐户的存在； |
| **备注** |  |

* + 1. 锁定无关账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 锁定无关账户（必须实施） |
| **安全基线编号** | 操作系统-Linux-7 |
| **安全基线项说明** | 应该锁定与设备运行、维护等工作无关的账户。 |
| **配置方法** | 锁定用户方法一：  修改/etc/passwd文件，将需要锁定的账户的shell域后添加nologin；  #vi /etc/passwd  test:x:1000:100:SUSE-LINUX:/home/test:/bin/bash/**nologin**  锁定用户方法二：  在超级权限的账户下使用”passwd”命令  #passwd –l username //锁定账户；  #passwd –d username//解锁用户；  解锁用户后需重新设置密码，且/etc/passwd文件内容不会发生变化。该操作比较麻烦，不推荐使用。  一般情况下，需要锁定的用户：lp,nuucp,hpdb,sync,adm |
| **检查方法** | 以root账户登录Linux系统  # cat /etc/password  查看多余账户的shell域为nologin为符合；  例如：  test:x:1000:100:SUSE-LINUX:/home/test:/bin/bash/nologin |
| **依据** | 7.1.3.2 主机：访问控制（S3），e) 应及时删除多余的、过期的帐户，避免共享帐户的存在； |
| **备注** |  |

* + 1. 清除UID为0的非root账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 清除UID为0的非root账户（用户）（必须实施） |
| **安全基线编号** | 操作系统-Linux-8 |
| **安全基线项说明** | 因为UID为0的任何用户都拥有系统的最高特权，保证只有root用户的UID为0。需要检查是否存在除root之外UID为0的用户 |
| **配置方法** | 执行：awk -F: '($3 == 0) { print $1 }' /etc/passwd |
| **检查方法** | 返回值包括“root”以外的条目，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），e）应及时删除多余的、过期的账户，避免共享账户的存在。 |
| **备注** |  |

* + 1. 设置umask值

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置umask值（必须实施） |
| **安全基线编号** | 操作系统-Linux-9 |
| **安全基线项说明** | umask设置了用户创建文件的默认权限，建议修改，确保创建的文件具有所希望的缺省权限。 |
| **配置方法** | 一般可在/etc/profile、/etc/bashrc、$ [HOME]/.bash\_profile、$[HOME]/.profile或$[HOME]/.bashrc中设置umask值，但具体看Linux的发型版本。  执行：  more /etc/profile  more /etc/csh.login  more /etc/csh.cshrc  more /etc/bashrc  检查是否包含umask值且umask=027。  若umask值为默认，则低于安全要求，建议修改为027 |
| **检查方法** | 见配置方法，检查上述提到的四个配置文件内umask值为027则满足要求。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** | umask 027－提供中等文件保护，(740)－w（组），rwx（其他用户）；  umask 026－提供稍严格的文件保护，(741)－w（组），rw（其他用户）；  umask 077－提供完整的文件保护，(700)－组或其他用户无权访问； |

* + 1. 配置重要目录与文件的权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置重要目录与文件的权限（建议实施） |
| **安全基线编号** | 操作系统-Linux-10 |
| **安全基线项说明** | 检查、配置系统中重要目录（如：/etc/rc.d）、文件（如：/etc/passwd）的访问权限，避免随意访问。 |
| **配置方法** | 登录系统，以root权限执行以下命令检查目录和文件的权限设置情况：  ls –l /etc/  ls –l /etc/rc.d/init.d/  ls –l /tmp  ls –l /etc/inetd.conf  ls –l /etc/passwd  ls –l /etc/shadow  ls –l /etc/group  ls –l /etc/security  ls –l /etc/services  ls -l /etc/rc\*.d  对于重要目录，建议执行如下类似操作：  # chmod -R 750 /etc/rc.d/init.d/\*  这样只有root可以读、写和执行这个目录下的脚本。 |
| **检查方法** | 若权限过低，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 控制未授权的SUID/SGID

|  |  |
| --- | --- |
| **安全基线项目名称** | 控制未授权的SUID/SGID（建议实施） |
| **安全基线编号** | 操作系统-Linux-11 |
| **安全基线项说明** | 检查是否有文件或文件夹的SUID/SGID权限配置错误或不当，若有应该对其进行控制（禁止或修改）避免权限过度。 |
| **配置方法** | 用下面的命令查找系统中所有的SUID和SGID程序，执行：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find $PART \( -perm -04000 -o -perm -02000 \) -type f -xdev -print  Done  建议经常性的对比suid/sgid文件列表，以便能够及时发现可疑的后门程序 |
| **检查方法** | 若存在未授权的文件，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 控制任何人都有写权限的目录

|  |  |
| --- | --- |
| **安全基线项目名称** | 控制任何人都有写权限的目录（建议实施） |
| **安全基线编号** | 操作系统-Linux-12 |
| **安全基线项说明** | 检查是否存在任何人都有写权限的目录，理论上不应存在，反之则需确保这些目录在受控的范围内。 |
| **配置方法** | 在系统中定位任何人都有写权限的目录用下面的命令：  for PART in `awk '($3 == "ext2" || $3 == "ext3") \  { print $2 }' /etc/fstab`; do  find $PART -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print  Done |
| **检查方法** | 若返回值非空，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 控制任何人都有写权限的文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 控制任何人都有写权限的文件（建议实施） |
| **安全基线编号** | 操作系统-Linux-13 |
| **安全基线项说明** | 检查是否存在任何人都有写权限的文件，理论上不应存在，反之则需确保这些文件在受控的范围内。 |
| **配置方法** | 在系统中定位任何人都有写权限的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find $PART -xdev -type f \( -perm -0002 -a ! -perm -1000 \) -print  Done |
| **检查方法** | 若返回值非空，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 删除没有属主的文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除没有属主的文件（建议实施） |
| **安全基线编号** | 操作系统-Linux-14 |
| **安全基线项说明** | 避免存在没有属主（未标记）的文件 |
| **配置方法** | 定位系统中没有属主的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find $PART -nouser -o -nogroup -print  done  注意：不用管“/dev”目录下的那些文件。 |
| **检查方法** | 若返回值非空，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 控制异常或隐含文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 控制异常或隐含文件（建议实施） |
| **安全基线编号** | 操作系统-Linux-15 |
| **安全基线项说明** | 对异常和隐含文件进行检查，控制（禁用或删除）这些文件。 |
| **配置方法** | 用“find”程序可以查找到这些隐含文件。例如：  # find / -name ".. \*" -print –xdev  # find / -name "…\*" -print -xdev | cat -v  同时也要注意象“.xx”和“.mail”这样的文件名的。（这些文件名看起来都很象正常的文件名） |
| **检查方法** | 若返回值非空，则低于安全要求； |
| **依据** | 7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 禁止 Ctrl+Alt+Del

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止Ctr+Alt+Del（建议实施） |
| **安全基线编号** | 操作系统-Linux-16 |
| **安全基线项说明** | 禁止执行Ctrl-Alt-Delete键盘命令，使得在控制台直接按ctl-alt-del不能直接重新启动计算机。 |
| **配置方法** | 以root账户登录Linux系统  在“/etc/inittab” 文件中注释掉下面这行（使用#）：ca::ctrlaltdel:/sbin/shutdown -t3 -r now 改为：#ca::ctrlaltdel:/sbin/shutdown -t3 -r now  输入如下命令使改动生效：# /sbin/init q |
| **检查方法** | 以root账户登录Linux系统  #cat /etc/inittab确认如下行是否被注释：  #ca::ctrlaltdel:/sbin/shutdown -t3 -r now |
| **依据** | 7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* 1. 安全审计
     1. 配置syslog.conf

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置syslog.conf（必须实施） |
| **安全基线编号** | 操作系统-Linux-17 |
| **安全基线项说明** | syslog.conf是syslogd进程的配置文件，而syslog保存了系统中所发生事件的详细记录,这些记录可以查阅、确定系统当前状态,观察入侵者踪迹,寻找某特定程序(或事件)相关的数据，建议开启并合理配置。 |
| **配置方法** | 执行：more /etc/syslog.conf，查看是否设置了下列项：  kern.warning;\*.err;authpriv.none\t@loghost  \*.info;mail.none;authpriv.none;cron.none\t@loghost  \*.emerg\t@loghost  local7.\*\t@loghost  建议配置专门的日志服务器，加强日志信息的异地同步备份 |
| **检查方法** | 若未设置，则低于安全要求； |
| **依据** | 7.1.3.3 主机：安全审计（G3），a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。  7.1.3.3 主机：安全审计（G3），b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账户的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内。  7.1.3.3 主机：安全审计（G3），c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。 |
| **备注** |  |

* + 1. 配置认证日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置认证日志（必须实施） |
| **安全基线编号** | 操作系统-Linux-18 |
| **安全基线项说明** | 应该对登录（认证）进行审计。 |
| **配置方法** | 执行命令：more /etc/syslog.conf  查看参数authpriv值 |
| **检查方法** | 若未对所有登录事件都记录，则低于安全要求； |
| **依据** | 7.1.3.3 主机：安全审计（G3），a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。  7.1.3.3 主机：安全审计（G3），b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账户的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内。  7.1.3.3 主机：安全审计（G3），c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。 |
| **备注** |  |

* + 1. 配置使用NTP

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置使用NTP（必须实施） |
| **安全基线编号** | 操作系统-Linux-19 |
| **安全基线项说明** | 为了保证日志记录时间的准确性，建议配置NTP服务器，并与NTP服务器时间同步 |
| **配置方法** | 以root账户登录Linux系统  在/etc/ntp.conf文件中配置时间服务器。  #vi /etc/ntp.conf  在配置文件末尾可见如下行：  server 127.0.0.1 local clock  fudge 127.0.0.1 stratum 10  在如上两行下添加NTP服务器IP  server x.x.x.x minpoll 4 maxpoll 4  保存退出后，执行开机自启动命令。  # chkconfig xntpd on  利用date命令查看系统当前时间，与监控终端时间比较，若相差超过1000s，利用ntpdate命令与时间服务器强制同步。  #ntpdate x.x.x.x  配置完成后，启动ntp服务。  # /etc/init.d/xntpd start |
| **检查方法** | 以root账户登录Linux系统  查看NTP进程是否启动；  # ps –ef | grep xntp  在/etc/ntp.conf中查看是否配置NTP服务器  #cat /etc/ntp.conf  server x.x.x.x minpoll4 maxpoll 4 |
| **依据** |  |
| **备注** | 请将配置范例中的x.x.x.x替换为实际网络环境中的NTP服务器IP |

* + 1. 配置远程日志服务器

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置远程日志服务器（建议实施） |
| **安全基线编号** | 操作系统-Linux-20 |
| **安全基线项说明** | 建议系统配置远程日志功能，将需要重点关注的日志内容传输到日志服务器进行备份。 |
| **配置方法** | 以root账户登录Linux系统  修改配置文件  #vi /etc/audisp/plugins.d/syslog.conf，  增加syslog服务器配置：  \*.\* @logserver  保存退出后重新启动syslog服务：  # service syslog restart |
| **检查方法** | 以root账户登录Linux系统  查看syslog.conf中是否配置了远程日志服务器  #cat /etc/audisp/plugins.d/syslog.conf  \*.\* @ logserver |
| **依据** | 7.1.3.3 主机：安全审计（G3），f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。 |
| **备注** |  |

* + 1. 配置安全日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置安全日志（按需实施） |
| **安全基线编号** | 操作系统-Linux-21 |
| **安全基线项说明** | 系统应配置完备日志记录，记录对与系统相关的安全事件。 |
| **配置方法** | 以root账户登录 Linux系统  修改配置文件，记录与设备相关的安全事件  #vi /etc/audisp/plugins.d/syslog.conf。  配置如下类似语句：  \*.err /var/log/errors  authpriv.info /var/log/authpriv\_info  \*.info /var/log/info  auth.none /var/log/auth\_none  修改配置文件，记录用户登录信息  #vi /etc/login.defs  修改LASTLOG\_ENAB的属性：  LASTLOG\_ENAB yes  开启系统记账功能  通过设置日志文件可以对每个用户的每一条命令进行纪录，这一功能默认是不开放的，为了打开它，需要执行/usr/lib/acct目录下的accton文件，格式如下  #/usr/lib/acct/accton /var/adm/pact  开启acct服务：  #chkconfig acct on  执行读取命令  #lastcomm [user name] |
| **检查方法** | 确认已配置设备安全日志  #cat /etc/audisp/plugins.d/syslog.conf  确认已配置记录用户登录信息  #cat /etc/login.defs |　grep LASTLOG\_ENAB  确认开启系统记账功能  #chkconfig --list | grep acct |
| **依据** | 7.1.3.3 主机：安全审计（G3），a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。  7.1.3.3 主机：安全审计（G3），b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账户的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内。  7.1.3.3 主机：安全审计（G3），c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。 |
| **备注** | 可根据实际要求配置。太大量的日志审计有可能影响本地硬盘I/O |

* 1. 入侵防范
     1. 关闭不需要的服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 关闭不需要的服务（必须实施） |
| **安全基线编号** | 操作系统-Linux-22 |
| **安全基线项说明** | 基于最小安装原则，关闭不必要的服务。 |
| **配置方法** | 使用命令“who -r”查看当前init级别  使用命令“chkconfig --list <服务名>”查看所有服务的状态 |
| **检查方法** | 若有不必要的系统在当前级别下为on，则低于安全要求 |
| **依据** | 7.1.3.5 主机：入侵防范（G3），c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新; |
| **备注** | 需要手工检查。  使用命令“chkconfig --level <init级别><服务名> on|off|reset”设置服务在个init级别下开机是否启动 |

* 1. 资源控制
     1. 配置登录超时

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置登录超时（必须实施） |
| **安全基线编号** | 操作系统-Linux-23 |
| **安全基线项说明** | 帐号与口令-检查登录超时设置 |
| **配置方法** | 使用命令“vi /etc/profile”修改配置文件，添加“TMOUT=”行开头的注释，建议设置为“TMOUT=180”，即超时时间为3分钟。 |
| **检查方法** | 返回值为空或值低于180，则低于安全要求 |
| **依据** | 7.1.3.7 主机：资源控制（G3），b) 应根据安全策略设置登录终端的操作超时锁定。 |
| **备注** |  |

* + 1. 设置登录超时

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置登录超时（必须实施） |
| **安全基线编号** | 操作系统-Linux-24 |
| **安全基线项说明** | 对于具备字符交互界面的系统，应配置账户超时策略，超时时间为300秒。 |
| **配置方法** | 以root账户登录Linux系统  针对全局的设置：  在/etc/profile中增加export TMOUT=300 /\*\*部分Linux发行版此参数或为“TMOUT”（不需要export）请留意测试 \*\*/  #vi /etc/profile  export TMOUT=300 /\*\*此参数的单位为“秒”\*\*/  针对特定用户的设置：  在特定用户的$home/.profile文件中增加export TMOUT=300  # vi $home/.profile  export TMOUT=300 |
| **检查方法** | 以root账户登录SUSE Linux系统  检查在/etc/profile中是否存在TMOUT=300  或者选择合适的时间，使用对系统（登录）影响最小的用户进行测试。 |
| **依据** | 7.1.3.7 主机：资源控制（S3），b) 应根据安全策略设置登录终端的操作超时锁定； |
| **备注** |  |

* + 1. 配置增强被远程访问的安全性

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置增强被远程访问的安全性（必须实施） |
| **安全基线编号** | 操作系统-Linux-25 |
| **安全基线项说明** | .rhosts在用户目录内指定了远程用户的名字，其远程用户使用本地用户账户执行rcp、rlogin和rsh等命令时不必提供口令；  .netrc提供了ftp和REXEC命令所需的信息，可自动连接主机而不必提供口令，该文件也放在用户本地目录中。  如无必要，无需对上述两个文件内的参数进行设置，建议删除这两个文件 |
| **配置方法** | 执行：find / -name .netrc，检查系统中是否存在.netrc文件，  执行：find / -name .rhosts ，检查系统中是否存在.rhosts文件  若存在，建议删除。 |
| **检查方法** | 见配置方法。 |
| **依据** | 7.1.3.7 主机：资源控制（A3），a）应通过设定终端接入方式、网络地址范围等条件限制终端登录。 |
| **备注** | 如无必要，删除这两个文件 |

* + 1. 限制root账户远程登录

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制Root账户远程登录（按需实施） |
| **安全基线编号** | 操作系统-Linux-26 |
| **安全基线项说明** | 对SSH服务进行安全检查,禁止root账户直接登录。 |
| **配置方法** | 使用命令“cat /etc/ssh/sshd\_config”查看配置文件  （1）检查是否允许root直接登录  检查“PermitRootLogin ”的值是否为no  （2）检查SSH使用的协议版本  检查“Protocol”的值 |
| **检查方法** | 使用命令“vi /etc/ssh/sshd\_config”编辑配置文件  （1）不允许root直接登录  设置“PermitRootLogin ”的值为no  （2）修改SSH使用的协议版本  设置“Protocol”的版本为2 |
| **依据** | 7.1.3.7 主机：资源控制（A3），a）应通过设定终端接入方式、网络地址范围等条件限制终端登录。 |
| **备注** | root用户需要使用普通用户远程登录后su进行系统管理 |

* 1. 其它安全项
     1. 关闭系统core dump状态

|  |  |
| --- | --- |
| **安全基线项目名称** | 关闭系统core dump 状态（建议实施） |
| **安全基线编号** | 操作系统-Linux-27 |
| **安全基线项说明** | coredump包含了程序运行时的内存、寄存器状态、堆栈指针、内存管理等信息，当系统或应用运行出错时，coredump信息有助于快速定位、处理、解决问题。但信息中可能包括系统信息，易被入侵者利用，建议关闭。 |
| **配置方法** | 执行：more /etc/security/limits.conf 检查是否包含下列项：  \* soft core 0  \* hard core 0  core dump |
| **检查方法** | 若不存在，则低于安全要求 |
| **依据** | 7.1.3.4主机：剩余信息保护（S3），a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。