Linux 操作系统配置安全基线标准与操作指南

南京农业大学图书与信息中心

2018 年 6 月

目　录

第 1 章 概述

1.1 安全基线概念

安全基线是指满足最小安全保证的基本要求。

1.2 文档编制目的

本文档针对安装运行 Linux 系列操作系统的计算机主机所应当遵循的基本安全设置要求提供了参考建议，供校园网用户在安装使用 Linux 操作系统过程中进行安全配置合规性自查、检查、加固提供标准依据与操作指导。

1.3 文档适用范围

本文档适用于 Linux 系列操作系统的各类版本，部分操作系统或版本的特定配置与操作见括号内说明。文档使用人员包括系统管理员及终端计算机用户。

1.4 文档修订

本文档的解释权和修改权属于南京农业大学图书与信息中心，欢迎校园网用户提供意见或建议，请发送至 security@njau.edu.cn。

第 2 章 账号管理、认证授权

2.1 账号

2.1.1 用户口令设置

安全基线项目名称	操作系统用户口令安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-01-01
安全基线项说明	用户帐号口令设置
设置操作步骤	1、执行：# awk -F: '($2 == "") { print $1 }' /etc/shadow，检查是否存在空口令账号,以 root 用户登录,执行# passwd 用户名 密码，设置密码。 2、执行：# vi/etc/login.defs，检查以下参数 PASS_MAX_DAYS 密码最长过期天数 参考值 90 PASS_MIN_DAYS 密码最小过期天数 参考值 80 PASS_MIN_LEN 密码最小长度 参考值 8 PASS_W ARN_AGE 密码过期警告天数 参考值 7
基线符合性判定依据	密码设置符合策略，不存在空口令账号
备注	#为系统操作提示符。

2.1.2 root 用户远程登录限制

安全基线项目名称	操作系统 root 用户远程登录安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-01-02
安全基线项说明	root 用户远程登录限制
设置操作步骤	1、新建用户，执行：#Useradd 用户名，#Passwd 密码; 2、授权新用户拥有 root 用户管理权限，执行#vi /etc/sudoers，在“## Allow root torun any commands anywhere root ALL=(ALL) ALL”下添加“新用户 ALL=(ALL) ALL” 3、修改 sshd_Config 文件，执行 vi /etc/ssh/sshd_config 找到 PermitRootLogin,删除前面的#号并且修改为 no，重启 sshd 服务,执行# service sshd restart。
基线符合性判定依据	查看配置：cat /etc/ssh/sshd_config，PermitRootLogin no 符合，或尝试以 root 远程登录应不成功。
备注	以新用户身份登录系统后，执行 sudo 命令可获取 root 操作权

	限。root 用户拥有系统最高权限,权限远高于 Windows 系统中的 administrator 用户。一旦 root 用户信息被泄露,对于服务器来说将是极为致命的威胁。所以禁止 root 用户通过 ssh 的方式进行远程登录,这样可以极大的提高服务器的安全性,即使是 root 用户密码泄露出去也能够保障服务器的安全。

2.1.3 检查是否存在除 root 之外 UID 为 0 的用户

安全基线项目名称	操作系统超级用户策略安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-01-03
安全基线项说明	检查是否存在除 root 之外 UID 为 0 的用户
设置操作步骤	1、执行：#awk -F: '($3 == 0) { print $1 }' /etc/passwd，返回值包括“root”以外的条目，则存在； 2、删除非法帐户
基线符合性判定依据	返回值应只有“root”条目
备注	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

2.1.4 root 用户环境变量的安全性

安全基线项目名称	操作系统超级用户环境变量安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-01-04
安全基线项说明	root 用户环境变量的安全性
设置操作步骤	1、执行： echo $PATH \| egrep '(^\|:)(\.\|:\|$)' ，检查是否包含父目录， 2、执行： find `echo $PATH | tr ':' ' '` -type d \(-perm -002 -o -perm -020 \) -ls ，检查是否包含组目录权限为 777 的目录
基线符合性判定依据	返回值无则安全
备注	确保 root 用户的系统路径中不包含父目录，在非必要的情况下，不应包含组权限为 777 的目录

2.2 认证

2.2.1 远程连接的安全性配置

安全基线项目名称	操作系统远程连接安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-01
安全基线项说明	远程连接的安全性配置
设置操作步骤	1、执行： find / -name .netrc，检查系统中是否有.netrc 文件； 2、执行： find / -name .rhosts ，检查系统中是否有.rhosts 文件； 3、删除这两个文件
基线符合性判定依据	返回值无，则安全。
备注	

2.2.2 用户的 umask 安全配置

安全基线项目名称	操作系统用户 umask 安全基线要求项
安全基线编号	用户的 umask 安全配置
安全基线项说明	NJAUSBL-Linux-V01-02-02-02
设置操作步骤	执行：#more /etc/profile #more /etc/csh.login #more /etc/csh.cshrc #more /etc/bashrc，检查是否包含 umask 值
基线符合性判定依据	如有 umask 值且不是默认的，则安全。
备注	建议设置用户的 umask=077

2.2.3 重要目录和文件的权限设置

安全基线项目名称	操作系统目录文件权限安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-03
安全基线项说明	重要目录和文件的权限设置
设置操作步骤	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 建议按如下命令设置：# chmod -R 750 /etc/rc.d/init.d/*，使 root 可以读、写和执行这个目录下的脚本。
基线符合性判定依据	若权限设置过低则系统用户无法进入文件目录或操作文件，不符合。
备注	

2.2.4 查找未授权的 SUID/SGID 文件

安全基线项目名称	操作系统 SUID/SGID 文件安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-04
安全基线项说明	查找未授权的 SUID/SGID
设置操作步骤	用下面的命令查找系统中所有的 SUID 和 SGID 程序，执行： #find . -perm -04000;#find . -perm -02000
基线符合性判定依据	若存在未授权的文件，则不安全。
备注	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

2.2.5 检查任何人都有写权限的目录

安全基线项目名称	操作系统 Linux 目录写权限安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-05
安全基线项说明	文件系统-检查任何人都有写权限的目录
设置操作步骤	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
基线符合性判定依据	若返回值非空，则低于安全要求；

备注	

2.2.6 查找任何人都有写权限的文件

安全基线项目名称	操作系统 Linux 文件写权限安全基线要求项
安全基线编号	NJAUSBL-Linux-02-02-06
安全基线项说明	文件系统-查找任何人都有写权限的文件
设置操作步骤	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
基线符合性判定依据	若返回值非空，则低于安全要求；
备注	

2.2.7 检查没有属主的文件

安全基线项目名称	操作系统 Linux 文件所有权安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-07
安全基线项说明	文件系统-检查没有属主的文件
设置操作步骤	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。
基线符合性判定依据	若返回值非空，则低于安全要求；
备注	补充操作说明 发现没有属主的文件往往就意味着有黑客入侵你的系统了。不能允许没有主人的文件存在。如果在系统中发现了没有主人的文件或目录，先查看它的完整性，如果一切正常，给它一个主人。有时候卸载程序可能会出现一些没有主人的文件或目录，在这种情况下可以把这些文件和目录删除掉。

2.2.8 检查异常隐含文件

安全基线项目名称	操作系统 Linux 隐含文件安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-02-02-08
安全基线项说明	文件系统-检查异常隐含文件
设置操作步骤	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）
基线符合性判定依据	若返回值非空，则低于安全要求;
备注	补充操作说明 在系统的每个地方都要查看一下有没有异常隐含文件（点号是起始字符的，用“ ls”命令看不到的文件） ，因为这些文件可能是隐藏的黑客工具或者其它一些信息（口令破解程序、其它系统的口令文件，等等） 。在 UNIX 下，一个常用的技术就是用一些特殊的名，如: “, ” 、“.. ”（点点空格） 或“..^G”（点点 control-G ），来隐含文件或目录。

第 3 章 日志审计

3.1 日志

3.1.1 syslog 登录事件记录

安全基线项目名称	操作系统 Linux 登录审计安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-03-01-01
安全基线项说明	日志审计-syslog 登录事件记录
设置操作步骤	执行命令: more /etc/syslog.conf 查看参数 authpriv 值
基线符合性判定依据	若未对所有登录事件都记录，则低于安全要求;
备注	

3.2 审计

3.2.1 Syslog.conf 的配置审核

安全基线项目名称	操作系统 Linux 配置审计安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-03-02-01
安全基线项说明	日志审计-Syslog.conf 的配置审核
设置操作步骤	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
基线符合性判定依据	若未设置，则低于安全要求；
备注	补充操作说明 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

第 4 章 系统文件

4.1 系统状态

4.1.1 系统 core dump 状态

安全基线项目名称	操作系统 Linux core dump 状态安全基线要求项
安全基线编号	NJAUSBL-Linux-V01-04-01-01
安全基线项说明	系统文件 -系统 core dump 状态
设置操作步骤	执行： more /etc/security/limits.conf 检查是否包含下列项： * soft core 0 * hard core 0
基线符合性判定依据	若不存在，则低于安全要求
备注	补充操作说明 core dump 中可能包括系统信息，易被入侵者利用，建议关闭