Linux 操作系统安全

1 Linux 简述

Linux 是一套免费使用和自由传播的类 Unix 操作系统，是一个基于 POSIX 和 UNIX 的多用户、多任务、支持多线程和多 CPU 的操作系统。它能运行主要的 UNIX 工具软件、应用程序和网络协议。它支持 32 位和 64 位硬件。Linux 继承了 Unix 以网络为核心的设计思想，是一个性能稳定的多用户网络操作系统。

Linux 操作系统诞生于 1991 年 10 月 5 日。Linux 存在着许多不同的 Linux 版本，但它们都使用了 Linux 内核。Linux 可安装在各种计算机硬件设备中，比如手机、平板电脑、路由器、视频游戏控制台、台式计算机、大型机和超级计算机。

因为 Linux 的灵活、安全、稳定、开源的特性，Linux 在生产环境中占据了大量份额，安全问题也引起人们的重视，下面我们从用户、文件、进程、网络、日志五个方面介绍 Linux 的安全加固基线，学习本节前应先对主流 Linux 系统较为熟悉。

2 用户管理

用户与组 sudoer 密码 失效时间 强制修改等 本地与远程登陆

安全基线项目名称	操作系统 Linux 用户口令设置安全基线要求项
安全基线项说明	对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天。
检测操作步骤	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
基线符合性判定依据	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 不存在空口令帐号
备注	

安全基线项目名称	操作系统 Linux 登录超时设置
安全基线项说明	检查登录超时设置
检测操作步骤	使用命令“ cat /etc/profile |grep TMOUT”查看 TMOUT 是否被设置
基线符合性判定依据	返回值为空或值低于 180，则低于安全要求
备注	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

安全基线项目名称	操作系统 Linux SSH 安全连接要求
安全基线项说明	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议。
检测操作步骤	查看 SSH 服务状态： # service ssh status 查看 telnet 服务状态： # service telnet status
基线符合性判定依据	SSH 服务状态查看结果为： running

安全基线项目名称	操作系统 Linux 超级用户登录设置
安全基线项说明	对 SSH 服务进行安全检查
检测操作步骤	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
基线符合性判定依据	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
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

安全基线项目名称	操作系统 Linux 用户口令强度安全基线要求项
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、特殊符号四类中至少两类
检测操作步骤	/etc/pam.d/system-auth 文件中是否对 pam_cracklib.so 的参数进行了正确设置。
基线符合性判定依据	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 至少 8 位，包含一位大写字母，一位小写字母和一位数字

安全基线项目名称	操作系统 Linux 用户口令锁定策略安全基线要求项
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。
检测操作步骤	/etc/pam.d/system-auth 文件中是否对 pam_tally.so 的参数进行了正确设置。
基线符合性判定依据	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

安全基线项目名称	操作系统 Linux 远程登录安全基线要求项
安全基线项说明	root 用户远程登录限制
检测操作步骤	执行： more /etc/securetty，检查 Console 参数
基线符合性判定依据	建议在/etc/securetty 文件中配置： CONSOLE = /dev/tty01

安全基线项目名称	操作系统 Linux 超级用户策略安全基线要求项
安全基线项说明	检查是否存在除 root 之外 UID 为 0 的用户
检测操作步骤	执行： awk -F: '($3 == 0) { print $1 }' /etc/passwd
基线符合性判定依据	返回值包括“ root”以外的条目，则低于安全要求；
备注	补充操作说明 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

安全基线项目名称	操作系统 Linux 超级用户环境变量安全基线要求项
安全基线项说明	root 用户环境变量的安全性
检测操作步骤	执行： echo $PATH \| egrep '(^\|:)(\.\|:\|$)'，检查是否包含父目录， 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	返回值包含以上条件，则低于安全要求；
备注	补充操作说明 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

安全基线项目名称	操作系统 Linux 远程连接安全基线要求项
安全基线项说明	远程连接的安全性配置
检测操作步骤	执行： find / -name .netrc，检查系统中是否有.netrc 文件， 执行： find / -name .rhosts ，检查系统中是否有.rhosts 文件
基线符合性判定依据	返回值包含以上条件，则低于安全要求；
备注	补充操作说明 如无必要，删除这两个文件

安全基线项目名称	操作系统 Linux 用户 umask 安全基线要求项
安全基线项说明	用户的 umask 安全配置
检测操作步骤	执行： more /etc/profile more /etc/csh.login more /etc/csh.cshrc more /etc/bashrc 检查是否包含 umask 值且 umask=027
基线符合性判定依据	umask 值是默认的，则低于安全要求
备注	补充操作说明 建议设置用户的默认 umask=027

安全基线项目名称	操作系统 Linux 用户 sudoer 安全基线要求项
安全基线项说明	用户的 sudoer 安全配置
检测操作步骤	执行：cat /etc/sudoer 查看是否有不合规的 sudoer 用户
基线符合性判定依据	含有不合规用户，则低于安全要求

3 文件管理

文件权限 特殊权限 FACL

安全基线项目名称	操作系统 Linux 目录文件权限安全基线要求项
安全基线项说明	重要目录和文件的权限设置
检测操作步骤	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
基线符合性	若权限过低，则低于安全要求；

判定依据	
备注	补充操作说明 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。

安全基线项目名称	操作系统 Linux SUID/SGID 文件安全基线要求项
安全基线项说明	查找未授权的 SUID/SGID 文件
检测操作步骤	用下面的命令查找系统中所有的 SUID 和 SGID 程序，执行： 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
基线符合性判定依据	若存在未授权的文件，则低于安全要求；

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
安全基线项说明	检查任何人都有写权限的目录
检测操作步骤	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；

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
安全基线项说明	查找任何人都有写权限的文件
检测操作步骤	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；

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
安全基线项说明	检查没有属主的文件
检测操作步骤	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。

安全基线项目名称	操作系统 Linux 隐含文件安全基线要求项
安全基线项说明	检查异常隐含文件
检测操作步骤	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。

4 进程管理

计划任务 自启动

安全基线项目名称	操作系统 Linux 关闭不必要的服务
安全基线项说明	关闭不必要的服务
检测操作步骤	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
基线符合性判定依据	若有不必要的系统在当前级别下为 on，则低于安全要求
备注	使用命令“ chkconfig --level <init 级别> <服务名> on|off|reset”设置服务在 init 级别下开机是否启动

安全基线项目名称	操作系统 Linux 关闭不必要的计划任务
安全基线项说明	关闭不必要的计划任务
检测操作步骤	使用命令“ crontab -l”查看当前计划任务 或使用命令“ vim /var/spool/cron/crontabs/”查看所有计划任务
基线符合性判定依据	若有不必要的计划任务在当前列表，则低于安全要求

5 网络管理

端口 防火墙

安全基线项目名称	操作系统 Linux 防火墙安全基线要求项
安全基线项说明	iptables 或 ufw 防火墙安全基线
检测操作步骤	执行命令：chkconfig --list 服务名 查看防火墙的运行状态
基线符合性判定依据	若防火墙未运行，则低于安全要求；

安全基线项目名称	操作系统 Linux 防火墙配置信息安全基线要求项
安全基线项说明	iptables 或 ufw 防火墙配置信息安全基线
检测操作步骤	执行命令： iptables -L 或 vim /etc/ufw 服务名 查看防火墙的配置规则
基线符合性判定依据	若配置规则不达标，则低于安全要求；
备注	iptables 限制进入连接 iptables -A INPUT -i eth0 -s 192.168.10.0/24 -p tcp --dport 22 -j ACCEPT iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT iptables -A INPUT -i eth0 -p tcp --dport 22 -j DROP 限制外发连接 iptables -A OUTPUT -o eth0 -p tcp --syn -j DROP iptables -A OUTPUT -o eth0 -p udp -j DROP

6 日志管理

日志配置与审计

安全基线项目名称	操作系统 Linux 登录审计安全基线要求项
安全基线项说明	syslog 登录事件记录
检测操作步骤	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；

安全基线项目名称	操作系统 Linux 配置审计安全基线要求项
安全基线项说明	Syslog.conf 的配置审核
检测操作步骤	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

安全基线项目名称	操作系统 Linux core dump 状态安全基线要求项
安全基线项说明	系统 core dump 状态
检测操作步骤	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

参考资料：
1.https://wenku.baidu.com/view/7e0adcc78bd63186bcebbcd7.html