Linux 主机加固

2010 年 9 月

目 录

本文档是 Linux 操作系统的对于 Linux 操作系统设备账号认证、日志、协议、补丁升级、文件系统管理等方面的安全配置要求，共 45 项，对系统的安全配置审计、加固操作起到指导性作用。

1 账号管理、认证授权

1.1 账号

1.1.1 SHG-Linux-01-01-01

编号	SHG-Linux-01-01-01
名称	为不同的管理员分配不同的账号
实施目的	根据不同类型用途设置不同的帐户账号，提高系统安全。
问题影响	账号混淆，权限不明确，存在用户越权使用的可能。
系统当前状态	cat /etc/passwd 记录当前用户列表
实施步骤	**1、参考配置操作** 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 755 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。

回退方案	删除新增加的帐户
判断依据	标记用户用途，定期建立用户列表，比较是否有非法用户
实施风险	高
重要等级	★★★
备注	

1.1.2 SHG-Linux-01-01-02

编号	SHG-Linux-01-01-02
名称	去除不需要的帐号、修改默认帐号的 shell 变量
实施目的	删除系统不需要的默认帐号、更改危险帐号缺省的 shell 变量
问题影响	允许非法利用系统默认账号
系统当前状态	cat /etc/passwd 记录当前用户列表， cat /etc/shadow 记录当前密码配置
实施步骤	**1、参考配置操作** # userdel lp # groupdel lp 如果下面这些系统默认帐号不需要的话，建议删除。 lp, sync, shutdown, halt, news, uucp, operator, games, gopher 修改一些系统帐号的 shell 变量，例如 uucp,ftp 和 news 等，还有一些仅仅需要 FTP 功能的帐号，一定不要给他们设置/bin/bash 或者/bin/sh 等 Shell 变量。可以在/etc/passwd 中将它们的 shell 变量设为/bin/false 或者/dev/null 等，也可以使用 usermod -s /dev/null username 命令来更改 username 的 shell 为/dev/null。
回退方案	恢复账号或者 SHELL

判断依据	如上述用户不需要，则锁定。
实施风险	高
重要等级	★★★
备注	

1.1.3 SHG-Linux-01-01-03

编号	SHG-Linux-01-01-03
名称	限制超级管理员远程登录
实施目的	限制具备超级管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账。
问题影响	允许 root 远程非法登陆
系统当前状态	cat /etc/ssh/sshd_config cat /etc/securetty
实施步骤	**1、 参考配置操作** SSH: #vi /etc/ssh/sshd_config 把 PermitRootLogin yes 改为 PermitRootLogin no 重启 sshd 服务

	#service sshd restart CONSOLE: 在/etc/securetty文件中配置：CONSOLE = /dev/tty01
回退方案	还原配置文件 /etc/ssh/sshd_config
判断依据	/etc/ssh/sshd_config 中 PermitRootLogin no
实施风险	高
重要等级	★★★
备注	

1.1.4 SHG-Linux-01-01-04

编号	SHG-Linux-01-01-04
名称	对系统账号进行登录限制
实施目的	对系统账号进行登录限制，确保系统账号仅被守护进程和服务使用。
问题影响	可能利用系统进程默认账号登陆，账号越权使用
系统当前状态	cat /etc/passwd 查看各账号状态。
实施步骤	**1、 参考配置操作** Vi /etc/passwd 例如修改 lynn:x:500:500::/home/lynn:/sbin/bash 更改为： lynn:x:500:500::/home/lynn:/sbin/nologin 该用户就无法登录了。

	禁止所有用户登录。 touch /etc/nologin 除 root 以外的用户不能登录了。 **2、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
回退方案	还原/etc/passwd 文件配置
判断依据	/etc/passwd 中的禁止登陆账号的 shell 是 /sbin/nologin
实施风险	高
重要等级	★
备注	

1.1.5 SHG-Linux-01-01-05

编号	SHG-Linux-01-01-05
名称	为空口令用户设置密码
实施目的	禁止空口令用户，存在空口令是很危险的，用户不用口令认证就能进入系统。
问题影响	用户被非法利用
系统当前状态	cat /etc/passwd awk -F: '($2 == ""){print $1}' /etc/passwd
实施步骤	awk -F: '($2 == ""){print $1}' /etc/passwd 用 root 用户登陆 Linux 系统，执行 passwd 命令，给用户增加口令。

	例如：passwd test test。
回退方案	Root 身份设置用户口令，取消口令 如做了口令策略则失败
判断依据	登陆系统判断 Cat /etc/passwd
实施风险	高
重要等级	★
备注	

1.1.6 SHG-Linux-01-01-06

编号	SHG-Linux-01-01-06
名称	除 root 之外 UID 为 0 的用户
实施目的	帐号与口令-检查是否存在除 root 之外 UID 为 0 的用户
问题影响	账号权限过大，容易被非法利用
系统当前状态	awk -F: '($3 == 0) { print $1 }' /etc/passwd
实施步骤	删除 处 root 以外的 UID 为 0 的用户。
回退方案	无
判断依据	返回值包括“root”以外的条目，则低于安全要求；
实施风险	高

重要等级	★
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

1.2 口令

1.2.1 SHG-Linux-01-02-01

编号	SHG-Linux-01-02-01
名称	缺省密码长度限制
实施目的	防止系统弱口令的存在，减少安全隐患。对于采用静态口令认证技术的设备，口令长度至少 8 位。
问题影响	增加密码被暴力破解的成功率
系统当前状态	cat /etc/login.defs
实施步骤	**1、参考配置操作** # vi /etc/login.defs 把下面这行 PASS_MIN_LEN 5　改为 PASS_MIN_LEN 8
回退方案	vi /etc/login.defs ，修改设置到系统加固前状态。
判断依据	PASS_MIN_LEN 8
实施风险	低
重要等级	★★★
备注	

1.2.2 SHG-Linux-01-02-02

编号	SHG-Linux-01-02-02
名称	缺省密码生存周期限制
实施目的	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，减少口令安全隐患。
问题影响	密码被非法利用，并且难以管理
系统当前状态	运行 cat /etc/login.defs 查看状态，并记录。
实施步骤	**1、参考配置操作** PASS_MAX_DAYS 90 PASS_MIN_DAYS 0
回退方案	Vi /etc/login.defs ，修改设置到系统加固前状态。
判断依据	PASS_MAX_DAYS 90
实施风险	低
重要等级	★★★
备注	

1.2.3 SHG-Linux-01-02-03

编号	SHG-Linux-01-02-03
名称	口令过期提醒
实施目的	口令到期前多少天开始通知用户口令即将到期
问题影响	密码被非法利用，并且难以管理
系统当前状态	运行 cat /etc/login.defs 查看状态，并记录。

实施步骤	**1、参考配置操作** PASS_WARN_AGE 7
回退方案	Vi /etc/login.defs ，修改设置到系统加固前状态。
判断依据	PASS_WARN_AGE 7
实施风险	低
重要等级	★★★
备注	

1.3 文件与授权

1.3.1 SHG-Linux-01-03-01

编号	SHG-Linux-01-03-01
名称	设置关键目录的权限
实施目的	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
问题影响	非法访问文件
系统当前状态	运行 ls -al /etc/ 记录关键目录的权限
实施步骤	**1、参考配置操作** 通过 chmod 命令对目录的权限进行实际设置。 **2、补充操作说明** etc/passwd 必须所有用户都可读，root 用户可写 -rw-r—r— /etc/shadow 只有 root 可读 -r--------

	/etc/group 必须所有用户都可读，root 用户可写 -rw-r—r— 使用如下命令设置： chmod 644 /etc/passwd chmod 600 /etc/shadow chmod 644 /etc/group 如果是有写权限，就需移去组及其它用户对/etc 的写权限（特殊情况除外） 执行命令#chmod -R go-w /etc
回退方案	通过 chmod 命令还原目录权限到加固前状态。
判断依据	[root@localhost sysconfig]# ls -al /etc/passwd | grep '^...-.--.--' -rw-r--r-- 1 root 1647 3ÔÂ 7 19:05 /etc/passwd [root@localhost sysconfig]# ls -al /etc/group | grep '^...-.--.--' -rw-r--r-- 1 root 624 3ÔÂ 7 19:04 /etc/group [root@localhost sysconfig]# ls -al /etc/shadow | grep '^...-------' -r-------- 1 root 1140 3ÔÂ 7 19:06 /etc/shadow
实施风险	高
重要等级	★★★
备注	

1.3.2 SHG-Linux-01-03-02

编号	SHG-Linux-01-03-02
名称	修改 umask 值
实施目的	控制用户缺省访问权限，当在创建新文件或目录时，屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其

	它用户及别的组的用户修改该用户的文件或更高限制。
问题影响	非法访问目录
系统当前状态	more /etc/profile more /etc/csh.login more /etc/csh.cshrc more /etc/bashrc 检查是否包含 umask 值
实施步骤	**1、参考配置操作** 设置默认权限： vi /etc/profile vi /etc/csh.login vi /etc/csh.cshrc vi /etc/bashrc 在末尾增加 umask 027 修改文件或目录的权限，操作举例如下： #chmod 444 dir ；#修改目录 dir 的权限为所有人都为只读。 根据实际情况设置权限； **2、补充操作说明** 如果用户需要使用一个不同于默认全局系统设置的 umask，可以在需要的时候通过命令行设置，或者在用户的 shell 启动文件中配置 **3、补充说明** umask 的默认设置一般为 022，这给新创建的文件默认权限 755（777-022=755），这会给文件所有者读、写权限，但只给组成员和其他用户读权限。 umask 的计算： umask 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。

回退方案	修改 more /etc/profile more /etc/csh.login more /etc/csh.cshrc more /etc/bashrc 文件到加固前状态。
判断依据	umask 027
实施风险	高
重要等级	★
备注	

1.3.3 SHG-Linux-01-03-03

编号	SHG-Linux-01-03-03
名称	资源限制
实施目的	限制用户对系统资源的使用，可以避免拒绝服务（如：创建很多进程、消耗系统的内存，等等）这种攻击方式。这些限制必须在用户登录之前设定。
问题影响	拒绝服务攻击
系统当前状态	Cat /etc/security/limits.conf Cat /etc/pam.d/login
实施步骤	**1、参考配置操作** ✧ 第一步 编辑“limits.conf”文件 （vi /etc/security/limits.conf），加入或改变下面这些行：

	* soft core 0 * hard core 0 * hard rss 5000 * hard nproc 20 如果限制 limitu 用户组对主机资源的使用， 加入： @limitu soft core 0 @limitu hard nproc 30 @limitu - maxlogins 5 这些行的的意思是：“core 0”表示禁止创建 core 文件；“nproc 20”把最多进程数限制到 20；“rss 5000”表示除了 root 之外，其他用户都最多只能用 5M 内存。上面这些都只对登录到系统中的用户有效。通过上面这些限制，就能更好地控制系统中的用户对进程、core 文件和内存的使用情况。星号“*”表示的是所有登录到系统中的用户。 ✧ 第二步 必须编辑“/etc/pam.d/login”文件，在文件末尾加入下面这一行： session required /lib/security/pam_limits.so **补充说明：** 加入这一行后“/etc/pam.d/login”文件是这样的： #%PAM-1.0 auth required /lib/security/pam_securetty.so auth required /lib/security/pam_pwdb.so shadow nullok auth required /lib/security/pam_nologin.so account required /lib/security/pam_pwdb.so password required /lib/security/pam_cracklib.so password required /lib/security/pam_pwdb.so nullok use_authtok md5 shadow

	session required /lib/security/pam_pwdb.so session required /lib/security/pam_limits.so #session optional /lib/security/pam_console.sodaemon 统计进程数量 ps ax | grep httpd | wc -l
回退方案	/etc/security/limits.conf /etc/pam.d/login 恢复加固前状态
判断依据	/etc/security/limits.conf 中包含 hard core 0 * hard rss 5000 * hard nproc 20 的定义 /etc/pam.d/login 中包含 session required /lib/security/pam_limits.so
实施风险	高
重要等级	★
备注	

1.3.4 SHG-Linux-01-03-04

编号	SHG-Linux-01-03-04
名称	设置目录权限
实施目的	设置目录权限，防止非法访问目录。
问题影响	非法访问目录

系统当前状态	查看重要文件和目录权限：ls -l 并记录。
实施步骤	**1、参考配置操作** 查看重要文件和目录权限：ls -l 更改权限： 对于重要目录，建议执行如下类似操作： # chmod -R 750 /etc/init.d/* 这样只有 root 可以读、写和执行这个目录下的脚本。
回退方案	使用 chmod 命令还原被修改权限的目录。
判断依据	判断 /etc/init.d/* 下的文件权限 750 以下
实施风险	高
重要等级	★
备注	

1.3.5 SHG-Linux-01-03-05

编号	SHG-Linux-01-03-05
名称	设置关键文件的属性
实施目的	增强关键文件的属性，减少安全隐患。 使 messages 文件只可追加。 使轮循的 messages 文件不可更改。
问题影响	非法访问目录,或者删除日志
系统当前状态	# lsattr /var/log/messages # lsattr /var/log/messages.* # lsattr /etc/shadow # lsattr /etc/passwd # lsattr /etc/group

实施步骤	1、参考配置操作 # chattr +a /var/log/messages # chattr +i /var/log/messages.* # chattr +i /etc/shadow # chattr +i /etc/passwd # chattr +i /etc/group 建议管理员对关键文件进行特殊设置（不可更改或只能追加等）。
回退方案	使用 chattr 命令还原被修改权限的目录。
判断依据	# lsattr /var/log/messages # lsattr /var/log/messages.* # lsattr /etc/shadow # lsattr /etc/passwd # lsattr /etc/group 判断属性
实施风险	高
重要等级	★★
备注	

1.3.6 SHG-Linux-01-03-06

编号	SHG-Linux-01-03-06
名称	对 root 为 ls、rm 设置别名
实施目的	为 ls 设置别名使得 root 可以清楚的查看文件的属性（包括不可更改等特殊属性）。 为 rm 设置别名使得 root 在删除文件时进行确认，避免误操作。

问题影响	非法执行指令
系统当前状态	查看当前 shell： # echo $SHELL 如果是 csh： # vi ~/.cshrc 如果是 bash： # vi ~/.bashrc
实施步骤	**1、参考配置操作** 查看当前 shell： # echo $SHELL 如果是 csh： # vi ~/.cshrc 如果是 bash： # vi ~/.bashrc 加入 alias ls　ls -aol alias rm　rm -i 重新登录之后查看是否生效。
回退方案	通过 chmod 命令还原目录权限到加固前状态。
判断依据	alias ls　ls -aol alias rm =’rm –i’ 类似的定义
实施风险	低
重要等级	★★
备注	

1.3.7 SHG-Linux-01-03-07

编号	SHG-Linux-01-03-07
名称	使用 PAM 禁止任何人 su 为 root
实施目的	避免任何人可以 su 为 root，减少安全隐患。
问题影响	用户提权
系统当前状态	cat /etc/pam.d/su
实施步骤	**1、参考配置操作** 编辑 su 文件(vi /etc/pam.d/su)，在开头添加下面两行： auth sufficient /lib/security/pam_rootok.so auth required /lib/security/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： # chmod –G10 username
回退方案	恢复/etc/pam.d/su 到加固前状态。
判断依据	Cat /etc/pam.d/su
实施风险	高
重要等级	★★★
备注	

1.3.8 SHG-Linux-01-03-08

编号	SHG-Linux-01-03-08
名称	查看/tmp 目录属性
实施目的	开放 tmp 目录的权限

问题影响	用户没有完整进入该目录，去浏览、删除和移动文件的权限
系统当前状态	ls -al / | grep tmp
实施步骤	**1、参考配置操作** Chmod +t /tmp T 或 T（Sticky）：/tmp 和 /var/tmp 目录供所有用户暂时存取文件，亦即每位用户皆拥有完整的权限进入该目录，去浏览、删除和移动文件。
回退方案	Chmod 回复加固之前的状态
判断依据	# ls -al / | grep tmp drwxrwxrwt 7 root 4096 May 11 20:07 tmp/
实施风险	高
重要等级	★★★
备注	

2 日志配置

2.1.1 SHG-Linux-02-01-01

编号	SHG-Linux-02-01-01
名称	启用日志记录功能
实施目的	登陆认证服务记录
问题影响	无法对用户的登陆进行日志记录
系统当前状态	运行 cat /etc/syslog.conf 查看状态，并记录。

实施步骤	**1、 参考配置操作** cat /etc/syslog.conf # The authpriv file has restricted access. authpriv.* /var/log/secure *auth, authpriv:主要认证有关机制,例如 telnet, login, ssh 等需要认证的服务都是使用此一机制
回退方案	vi /etc/syslog.conf ，修改设置到系统加固前状态。
判断依据	authpriv.* /var/log/secure
实施风险	低
重要等级	★★★
备注	

2.1.2 SHG-Linux-02-01-02

编号	SHG-Linux-02-01-02
名称	记录系统安全事件
实施目的	通过设置让系统记录安全事件，方便管理员分析
问题影响	无法记录系统的各种安全事件
系统当前状态	Cat /etc/syslog.conf
实施步骤	**1、参考配置操作** 修改配置文件 vi /etc/syslog.conf， 配置如下类似语句： *.err;kern.debug;daemon.notice; /var/adm/messages 定义为需要保存的设备相关安全事件。
回退方案	vi /etc/syslog.conf，修改设置到系统加固前状态。

判断依据	记录系统安全事件
实施风险	高
重要等级	★
备注	

2.1.3 SHG-Linux-02-01-03

编号	SHG-Linux-02-01-03
名称	对 ssh、su 登录日志进行记录
实施目的	对 ssh、su 尝试进行记录
问题影响	无法记录 ssh 和 su 登陆的操作
系统当前状态	cat /etc/syslog.conf ps –elf | grep syslog cat /var/log/secure
实施步骤	**1、参考配置操作** **1、参考配置操作** # vi /etc/syslog.conf 加入 # The authpriv file has restricted access. authpriv.* /var/log/secure 重新启动 syslogd： # /etc/rc.d/init.d/syslog restart
回退方案	vi /etc/syslog.conf ， 修改设置到系统加固前状态。
判断依据	authpriv.* /var/log/secure

	ps -elf | grep syslog 存在进程
实施风险	低
重要等级	★
备注	

2.1.4 SHG-Linux-02-01-04

编号	SHG-Linux-02-01-04
名称	启用记录 cron 行为日志功能
实施目的	对所有的 cron 行为进行审计。
问题影响	无法记录 cron 服务（计划任务）
系统当前状态	Cat /etc/syslog.conf | grep cron
实施步骤	**1、 参考配置操作** Vi /etc/syslog.conf # Log cron stuff cron.* /var/log/cron
回退方案	vi /etc/syslog.conf ，修改 cron.设置到系统加固前状态。
判断依据	cron.*
实施风险	低
重要等级	★
备注	

2.1.5 SHG-Linux-02-01-05

编号	SHG-Linux-02-01-05
名称	增加 ftpd 审计功能
实施目的	增加 ftpd 审计功能，增强 ftpd 安全性。
问题影响	无法记录 FTPD 服务
系统当前状态	Cat /etc/inetd.conf /etc/syslog.conf
实施步骤	**1、参考配置操作** # vi /etc/inetd.conf ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l -r -A -S 其中： -l 成功/失败的 ftp 会话被 syslog 记录 -r 使 ftpd 为只读模式，任何命令都不能更改文件系统 -A 允许 anonymous 用户登录，/etc/ftpwelcome 是欢迎信息 -S 对 anonymous ftp 传输进行记录 在/etc/syslog.conf 中，增加 ftp.* /var/log/ftpd 使日志产生到/var/log/ftpd 文件 重新启动 inetd 进程： # kill -1 `cat /var/run/inetd.pid`
回退方案	回复 /etc/inetd.conf /etc/syslog.conf 到系统加固前状态。
判断依据	ftpd -l -r -A –S ftp.* /var/log/ftpd
实施风险	低

重要等级	★
备注	

3 通信协议

3.1 IP 协议安全

3.1.1 SHG-Linux-03-01-01

编号	SHG-Linux-03-01-01
名称	使用 ssh 加密传输
实施目的	提高远程管理安全性
问题影响	使用非加密通信，内容易被非法监听
系统当前状态	运行 # ps -elf|grep ssh 查看状态，并记录。
实施步骤	**1、参考配置操作** 从 http://www.openssh.com/下载 SSH 并安装到系统。
回退方案	卸载 SSH、或者停止 SSH 服务
判断依据	有 SSH 进程
实施风险	高
重要等级	★

备注	

3.1.2 SHG-Linux-03-01-02

编号	SHG-Linux-03-01-01
名称	设置访问控制列表
实施目的	设置访问控制列表，使得只有可信主机才能访问服务器在/etc/(x)inetd.conf 中启用的特定网络服务。
问题影响	没有访问控制，系统可能被非法登陆或使用
系统当前状态	查看/etc/hosts.allow 和/etc/hosts.deny 2 个文件的配置状态，并记录。
实施步骤	**1、参考配置操作** 使用 TCP_Wrappers 可以使系统安全面对外部入侵。最好的策略就是阻止所有的主机（在“/etc/hosts.deny”文件中加入“ ALL:ALL@ALL, PARANOID ”），然后再在“/etc/hosts.allow” 文件中加入所有允许访问的主机列表。 第一步： 编辑 hosts.deny 文件（vi /etc/hosts.deny），加入下面该行： # Deny access to everyone. ALL: ALL@ALL, PARANOID 第二步： 编辑 hosts.allow 文件（vi /etc/hosts.allow），加入允许访问的主机列表，比如： ftp: 202.54.15.99 foo.com 202.54.15.99 和 foo.com 是允许访问 ftp 服务的 IP 地址和主机名称。 第三步： tcpdchk 程序是 TCP_Wrapper 设置检查程序。它用来检查你的 TCP_Wrapper 设置，并报告发现的潜在的和真实的问题。设置完后，运行下面这个命令： # tcpdchk

回退方案	修改/etc/hosts.allow 和/etc/hosts.deny 2 个文件的配置到加固之前的状态。
判断依据	配置访问控制 也可在防火墙的 ACL，或者交换的 VLAN 上设置。
实施风险	高
重要等级	★
备注	

3.1.3 SHG-Linux-03-01-03

编号	SHG-Linux-03-01-03
名称	更改主机解析地址的顺序
实施目的	更改主机解析地址的顺序，减少安全隐患。
问题影响	对本机未经许可的 IP 欺骗
系统当前状态	Cat /etc/host.conf
实施步骤	“/etc/host.conf” 说明了如何解析地址。编辑“/etc/host.conf”文件（vi /etc/host.conf），加入下面该行： # Lookup names via DNS first then fall back to /etc/hosts. order bind,hosts # We have machines with multiple IP addresses. multi on # Check for IP address spoofing nospoof on

	第一项设置首先通过 DNS 解析 IP 地址，然后通过 hosts 文件解析。第二项设置检测是否“/etc/hosts”文件中的主机是否拥有多个 IP 地址（比如有多个以太口网卡）。第三项设置说明要注意对本机未经许可的 IP 欺骗。
回退方案	回复/etc/host.conf 配置文件
判断依据	/etc/host.conf order bind,hosts nospoof on
实施风险	高
重要等级	★
备注	

3.1.4 SHG-Linux-03-01-04

编号	SHG-Linux-03-01-04
名称	打开 syncookie
实施目的	打开 syncookie 缓解 syn flood 攻击
问题影响	syn flood 攻击
系统当前状态	Cat /proc/sys/net/ipv4/tcp_syncookies
实施步骤	# echo 1 > /proc/sys/net/ipv4/tcp_syncookies 可以加入/etc/rc.d/rc.local 中。
回退方案	echo 0 > /proc/sys/net/ipv4/tcp_syncookies

判断依据	Cat /proc/sys/net/ipv4/tcp_syncookies 值为 1
实施风险	高
重要等级	★
备注	

3.1.5 SHG-Linux-03-01-05

编号	SHG-Linux-03-01-05
名称	不响应 ICMP 请求
实施目的	不响应 ICMP 请求,避免信息泄露
问题影响	信息泄露
系统当前状态	Cat /proc/sys/net/ipv4/icmp_echo_ignore_all
实施步骤	不响应 ICMP 请求： # echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
回退方案	echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all
判断依据	Cat /proc/sys/net/ipv4/icmp_echo_ignore_all 返回 1
实施风险	高
重要等级	★
备注	

3.1.6 SHG-Linux-03-01-06

编号	SHG-Linux-03-01-06
名称	防 syn 攻击优化
实施目的	提高未连接队列大小
问题影响	SYN flood attack
系统当前状态	sysctl net.ipv4.tcp_max_syn_backlog
实施步骤	**1、参考配置操作** sysctl -w net.ipv4.tcp_max_syn_backlog="2048"
回退方案	sysctl -w net.ipv4.tcp_max_syn_backlog= 恢复加固之前的值
判断依据	sysctl net.ipv4.tcp_max_syn_backlog 值为 2048
实施风险	高
重要等级	★
备注	

4 设备其他安全配置要求

4.1 补丁管理

4.1.1 SHG-Linux-04-01-01

编号	SHG-Linux-04-01-01
名称	补丁装载
实施目的	可以使系统版本为最新并解决安全问题
问题影响	系统存在严重的安全漏洞
系统当前状态	Uname -a Rpm -qa cat /proc/version
实施步骤	**1、参考配置操作** 补丁地址： http://www.redhat.com/corp/support/errata/ RPM 包： # rpm -Fvh [文件名] 请慎重对系统打补丁，补丁安装应当先在测试机上完成。补丁安装可能导致系统或某些服务无法工作正常。 在下载补丁包时，一定要对签名进行核实，防止执行特洛伊木马。
回退方案	patchrm
判断依据	查看 http://www.redhat.com/corp/support/errata/ 比较补丁修复情况
实施风险	高

重要等级	★★
备注	

4.2 服务进程和启动

4.2.1 SHG-Linux-04-02-01

编号	SHG-Linux-04-02-01
名称	关闭无效服务
实施目的	关闭无效的服务，提高系统性能，增加系统安全性。
问题影响	不用的服务会带来很多安全隐患
系统当前状态	Cat /etc/inetd.conf 查看并记录当前的配置
实施步骤	**1、参考配置操作** 取消所有不需要的服务，编辑“/etc/inetd.conf”文件，通过注释取消所有你不需要的服务（在该服务项目之前加一个“#”）。 第一步： 更改“/etc/inetd.conf”权限为 600，只允许 root 来读写该文件。 # chmod 600 /etc/inetd.conf 第二步： 确定“/etc/inetd.conf”文件所有者为 root。 # chown root /etc/inetd.conf 第三步： 编辑 /etc/inetd.conf 文件（vi /etc/inetd.conf），取消不需要的服务，如：ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth 等等。把不需要的服务关闭可以使系统的危险性降低很多。 第四步： 给 inetd 进程发送一个 HUP 信号： # killall -HUP inetd 第五步： 用 chattr 命令把/ec/inetd.conf 文件设为不可修改。

	# chattr +i /etc/inetd.conf /etc/inetd.conf 文件中只开放需要的服务。 对于启用的网络服务，使用 TCP Wrapper 增强访问控制和日志审计功能。 建议使用 xinetd 代替 inetd，前者在访问控制和日志审计方面有较大的增强。 *这样可以防止对inetd.conf的任何修改（以外或其他原因）。唯一可以取消这个属性的只有root。如果要修改inetd.conf文件，首先要取消不可修改属性：* *# chattr -i /etc/inetd.conf* portmap（如果启动使用 nfs 等需要 rpc 的服务，建议关闭 portmap 服务 cups 服务（Common Unix Printing Service，用于打印，建议关闭） named 服务（除非主机是 dns 服务器，否则关闭 named 服务） apache（http）服务 xfs（X Font Service）服务 vsftpd lpd linuxconf identd smb
回退方案	还原/etc/inetd.conf 文件到加固前的状态。
判断依据	在/etc/inetd.conf文件中禁止下列不必要的基本网络服务。 ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth, sendmail, nfs 标记用户用途，定期建立用户列表，比较是否有非法用户

实施风险	高
重要等级	★
备注	

4.2.2 SHG-Linux-04-02-02

编号	SHG-Linux-04-02-02
名称	关闭无效服务和进程自动启
实施目的	禁止系统不需要启动的服务，减少安全隐患。防止黑客获取更多的系统信息。
问题影响	黑客获取更多的系统信息
系统当前状态	列举并记录/etc/rc.d/rc[0-9].d 脚本目录下的文件 find /etc/rc?.d/ -name "S*"
实施步骤	**1、参考配置操作** 进入相应目录，将脚本开头大写 S 改为小写 s 即可。 如： # cd /etc/rc.d/rc6.d # mv S45dhcpd s45dhcpd
回退方案	还原/etc/rc.d/rc[0-9].d 下的脚本文件名到加固前的状态。
判断依据	判断/etc/rc.d/rc[0-9].d 下脚本文件名的状态
实施风险	高
重要等级	★
备注	

4.2.3 SHG-Linux-04-02-03

编号	SHG-Linux-04-02-03
名称	禁止/etc/rc.d/init.d 下某些脚本的执行
实施目的	禁止系统开机时不需要启动的服务，减少安全隐患。防止黑客获取更多的系统信息。
问题影响	不用的服务会带来很多安全隐患
系统当前状态	cat /etc/rc.d/init.d/* 查看并记录当前的配置
实施步骤	**1、参考配置操作** # cd /etc/rc.d/init.d 在不需要开机自动运行的脚本第一行写入 exit 0。 则开机时该脚本 exit 0 之后的内容不会执行。 需要更改的服务包括： identd lpd linuxconf netfs portmap routed rstatd rwalld rwhod sendmail ypbind yppasswdd ypserv 具体操作时根据主机的角色请于管理员确认后再实施。
回退方案	还原/etc/rc.d/init.d 文件到加固前的状态。
判断依据	停止不需要的服务的启动脚本
实施风险	高
重要等级	★
备注	

4.2.4 SHG-Linux-04-02-04

编号	SHG-Linux-04-02-04
名称	加固 snmp 服务
实施目的	减少安全隐患避免信息泄露
问题影响	信息泄露
系统当前状态	Ps –elf | grep snmp Cat /etc/snmp/snmpd.conf
实施步骤	**1、参考配置操作** chkconfig snmpd off chkconfig snmptrapd off /etc/rc.d/init.d/snmpd stop /etc/rc.d/init.d/snmptrapd stop **如果需要 SNMP 服务** 如下方式修改/etc/snmp/snmpd.conf 文件 A、修改默认的 community string com2sec notConfigUser default public 将 public 修改为你才知道的字符串 B、把下面的#号去掉 #view mib2 included .iso.org.dod.internet.mgmt.mib-2 fc C、把下面的语句 access notConfigGroup "" any noauth exact systemview none none 改成： access notConfigGroup "" any noauth exact mib2 none none 3、重启 snmpd 服务 #/etc/rc.d/init.d/snmpd restart

回退方案	/etc/snmp/snmpd.conf 回复加固前状态 停止 snmp 服务/etc/rc.d/init.d/snmpd stop
判断依据	/etc/snmp/snmpd.conf 中 com2sec notConfigUser default xxxxx view mib2 included .iso.org.dod.internet.mgmt.mib-2 fc access notConfigGroup "" any noauth exact mib2 none none ps -elf | grep snmp 查看是否有服务
实施风险	高
重要等级	★
备注	

4.2.5 SHG-Linux-04-02-05

编号	SHG-Linux-04-02-05
名称	修改 ssh 端口
实施目的	隐藏 ssh 信息
问题影响	信息泄露，会带来 SSH 的各种尝试威胁
系统当前状态	Cat /etc/ssh/sshd_config
实施步骤	Vi /etc/ssh/sshd_config 修改 Port 22 修改成其他端口，迷惑非法试探者 Linux 下 SSH 默认的端口是 22,为了安全考虑，现修改 SSH 的端口为 1433,修改方法如下 ：

	/usr/sbin/sshd -p 1433
回退方案	修改/etc/ssh/sshd_config 到加固前状态
判断依据	Cat /etc/ssh/sshd_config 判断 port 字段
实施风险	中
重要等级	★
备注	

4.3 Banner 与屏幕保护

4.3.1 SHG-Linux-04-03-01

编号	SHG-Linux-04-03-01
名称	隐藏系统提示信息
实施目的	减少系统提示信息，降低安全隐患。
问题影响	信息泄露
系统当前状态	Cat /etc/rc.d/rc.local Cat /etc/issue
实施步骤	**1、参考配置操作** 在缺省情况下，当你登录到 linux 系统，它会告诉你该 linux 发行版的名称、版本、内核版本、服务器的名称。应该尽可能的隐藏系统信息。 首先编辑“/etc/rc.d/rc.local” 文件，在下面显示的这

	些行前加一个“#”，把输出信息的命令注释掉。 # This will overwrite /etc/issue at every boot. So, make any changes you want to make to /etc/issue here or you will lose them when you reboot. #echo "" > /etc/issue #echo "$R" >> /etc/issue #echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue #cp -f /etc/issue /etc/issue.net #echo >> /etc/issue 其次删除"/etc"目录下的 isue.net 和 issue 文件： # mv /etc/issue /etc/issue.bak # mv /etc/issue.net /etc/issue.net.bak
回退方案	恢复 /etc/rc.d/rc.local /etc/issue /etc/issue.net
判断依据	Cat /etc/rc.d/rc.local 注释住处信息
实施风险	中
重要等级	★
备注	

4.3.2 SHG-Linux-04-03-02

编号	SHG-Linux-04-03-02
名称	设置登录超时时间
实施目的	对于具备字符交互界面的设备，应配置定时帐户自动登出。

问题影响	管理员忘记退出被非法利用
系统当前状态	查看/etc/profile 文件的配置状态，并记录。
实施步骤	**1、参考配置操作** 在 unix 系统中 root 账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销 root 账户，那将会带来很大的安全隐患，应该让系统自动注销。通过修改账户中“TMOUT”参数，可以实现此功能。TMOUT 按秒计算。编辑 profile 文件（vi /etc/profile），在“HISTFILESIZE=”后面加入下面这行： TMOUT=180 表示 180 秒，也就是表示 3 分钟。这样，如果系统中登录的用户在 3 分钟内都没有动作,那么系统会自动注销这个账户。也可以在个别用户的“.bashrc”文件中添加该值，以便系统对该用户实行特殊的自动注销时间。 改变这项设置后，必须先注销用户，再用该用户登录才能激活这个功能。
回退方案	修改/etc/profile 的配置到加固之前的状态。
判断依据	TMOUT=180
实施风险	中
重要等级	★
备注	

4.3.3 SHG-Linux-04-03-03

编号	SHG-Linux-04-03-03
名称	启动 LILO 时需要密码

实施目的	password 用于系统启动时应当输入密码； restricted 用于命令行启动系统时（如：进入单用户模式）需要输入密码。
问题影响	管理员忘记退出被非法利用
系统当前状态	Cat /etc/lilo.conf Ls -al /etc/lilo.conf Lsattr /etc/lilo.conf
实施步骤	**1、参考配置操作** 第一步：编辑 lilo.conf 文件（vi /etc/lilo.conf），加入或改变这三个参数（加#的部分）： boot=/dev/hda prompt *timeout=00* # 把该行改为 00，系统启动时将不再等待，而直接启动 LINUX message=/boot/message linear default=linux *restricted* # 加入该行 *password= lilopassforbocotest* # 加入该行并设置自己的密码（明文） image=/boot/vmlinuz-2.4.18 label=linux root=/dev/hda6 read-only 第二步：因为“/etc/lilo.conf”文件中包含明文密码，所以要把它设置为 root 权限读取。 # chmod 0600 /etc/lilo.conf 第三步：更新系统，以便对“/etc/lilo.conf”文件做的修改起作用。

	# /sbin/lilo -v 第四步：使用“chattr”命令使“/etc/lilo.conf”文件不可改变。 # chattr +i /etc/lilo.conf 这样可以在一定程度上防止对“/etc/lilo.conf”任何改变（意外或其他原因） 最后将/etc/lilo.conf 文件权限改为 600 # chmod 600 /etc/lilo.conf **补充说明** 通过对“/etc/lilo.conf”加 i 属性使文件不可更改。如果要对文件作修改的话，先去掉 i 属性，即 # chattr -i /etc/lilo.conf 为 LILO 设置密码不能防止黑客从软盘、CD-ROM 启动系统、加载根分区，需要在 BIOS 中设置密码。
回退方案	Chattr -I /etc/lilo.conf 恢复/etc/lilo.conf 到加固前状态和权限
判断依据	判断 /etc/lilo.conf *password= lilopassforbocotest*
实施风险	中
重要等级	★
备注	

4.4 可疑文件

4.4.1 SHG-Linux-04-04-01

编号	SHG-Linux-04-04-01
名称	查找 SUID/SGID 程序
实施目的	去除不必要的 SUID/SGID 权限
问题影响	非法提权
系统当前状态	find / -perm -04000 -type f -ls find / -perm -02000 -type f -ls 或者 find / -type f \(-perm -04000 -o -perm -02000 \) -ls
实施步骤	**1、 参考配置操作** 给文件加 SUID 和 SUID 的命令如下： chmod u+s filename 设置 SUID 位 chmod u-s filename 去掉 SUID 设置 chmod g+s filename 设置 SGID 位 chmod g-s filename 去掉 SGID 设置 **2、 补充说明** suid 是 4000，sgid 是 2000，sticky 是 1000 比如 rwsr-xr-x 就是 4755 SUID 是 Set User ID, SGID 是 Set Group ID 的意思。SUID 的程序在运行时，将有效用户 ID 改变为该程序的所有者 ID，使得进程在很大程度上拥有了该程序的所有者的特权。如果被设置为 SUID root，那么这个进程将拥有超级用户的特权(当然，一些较新版本的 UNIX 系统加强了这一方面的安全检测，一定程度上降低了安全隐患)。当进程结束时，又恢复为原来的状态。
回退方案	chmod u+s filename 设置 SUID 位

	chmod g+s filename 设置 SGID 位
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.2 SHG-Linux-04-04-02

编号	SHG-Linux-04-04-02
名称	查找/dev 下的非设备文件
实施目的	查找/dev 下的非设备文件
问题影响	可疑文件隐藏
系统当前状态	find /dev -type f -exec ls -l {} \;
实施步骤	**1、参考配置操作** find /dev -type f -exec ls -l {} \; 记录可以文件
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.3 SHG-Linux-04-04-03

编号	SHG-Linux-04-04-03
名称	查找非/dev 下的设备文件
实施目的	查找非/dev 下的设备文件
问题影响	可以文件隐藏
系统当前状态	find / -type b -print | grep -v '^/dev/' find / -type c -print | grep -v '^/dev/'
实施步骤	**1、参考配置操作** find / -type b -print | grep -v '^/dev/' find / -type c -print | grep -v '^/dev/'
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.4 SHG-Linux-04-04-04

编号	SHG-Linux-04-04-04
名称	查找所有人可写的文件
实施目的	查找所有人可写的文件
问题影响	文件越权使用
系统当前状态	find / -perm -2 ! -type l -ls 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 执行：echo $PATH \| egrep '(^\|:)(\.\|:\|$)'，检查是否包含父目录，
实施步骤	**1、参考配置操作** find / -perm -2 ! -type l -ls find / -type d \(-perm -002 -o -perm -020 \) -ls
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.5 SHG-Linux-04-04-05

编号	SHG-Linux-04-04-05
名称	查找没有属主的文件
实施目的	查找没有属主的文件
问题影响	危险可以文件检查
系统当前状态	find / -nouser -o -nogroup -print

实施步骤	**1、参考配置操作** find / -nouser -o -nogroup -print
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.6 SHG-Linux-04-04-06

编号	SHG-Linux-04-04-06
名称	查找 rhosts 文件
实施目的	查找 rhosts 文件
问题影响	不带密码的登陆
系统当前状态	find / -name .rhosts ，检查系统中是否有.rhosts 文件
实施步骤	**1、参考配置操作** find / -name .rhosts -print **3、 补充说明** 远程登录（rlogin）是一个 UNIX 命令，它允许授权用户进入网络中的其它 UNIX 机器并且就像用户在现场操作一样。一旦进入主机，用户可以操作主机允许的任何事情，比如：读文件、编辑文件或删除文件等。 rlogin 设计的初衷是方便同名的用户从一台机器直接登录到另一台机器.

	比如机器 A 上有用户 test1，机器 B 上该用户也有一个同名账号 test1, 如果机器 B 上设置好.rhosts 的话就 test1 就可以从机器 A 上直接登录机器 B. 通常在配 HA 的时候，会将+放进/.rhosts，因为这样做同步的时候就会比较方便，但记得在配置完的时候，把这个+去掉
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.7 SHG-Linux-04-04-07

编号	SHG-Linux-04-04-07
名称	查找 netrc 文件
实施目的	查找 netrc 文件
问题影响	密码外泄
系统当前状态	find / -name .netrc，检查系统中是否有.netrc 文件
实施步骤	**1、参考配置操作** find / -name .netrc -print **4、 补充说明** 有些 命令通过检查 $HOME/.netrc 文件（包含远程主机上使用的用户名和密码）来提供自动登录的功能。 如果没有远程主机的 $HOME/.netrc 文件中的有效项，将提

	示输入登录标识和密码。
回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	高
重要等级	★
备注	

4.4.8 SHG-Linux-04-04-08

编号	SHG-Linux-04-04-08
名称	文件系统-检查异常隐含文件
实施目的	文件系统-检查异常隐含文件
问题影响	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）
系统当前状态	find / -name ".. *" -print
实施步骤	rm [filename] **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）。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。

回退方案	无
判断依据	和管理员确定该文件的正确性，建立信息库，定期比对
实施风险	中
重要等级	★★
备注	