ubunru18.04-????????????

序号	检查项分类	配置检查项	检查内容	加固建议	风险等级	处理方法
1	入侵防范	检查历史命令设置	检查保留历史命令的条数	可以通过两种方式进行配置: 1、编辑文件 /etc/profile，根据实际需求，配置 HISTSIZE=实际需求数值，系统默认值为 1000，编辑完成后使用命令 source /etc/profile 使其生效，最后使用命令 echo $HISTSIZE 进行检查; 2、编辑 ~/.bashrc，根据实际需求，配置 HISTSIZE=实际需求数值，系统默认值为 1000，编辑完成后使用命令 source ~/.bashrc 使其生效，最后使用命令 echo $HISTSIZE 进行检查	高风险	无需处理

2	入侵防范	检查历史命令设置	检查保留历史命令的记录文件大小	可以通过两种方式进行配置： 1、编辑文件 /etc/profile，根据实际需求，配置 HISTFILESIZE=实际需求数值，系统默认值为 1000，编辑完成后使用命令 source /etc/profile 使其生效，最后使用命令 echo $HISTFILESIZE 进行检查； 2、编辑 ~/.bashrc，根据实际需求，配置 HISTFILESIZE=实际需求数值，系统默认值为 1000，编辑完成后使用命令 source ~/.bashrc 使其生效，最后使用命令 echo $HISTFILESIZE 进行检查	高风险	无需处理
3	身份鉴别	检查口令最小长度	在 /etc/login.defs 中设置口令最小长度	在文件 /etc/login.defs 中设置 PASS_MIN_LEN 不小于标准值	高风险	

4	安全审计	检查安全事件日志配置	检查 rsyslog 是否配置安全事件日志	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 或者 service rsyslog restart	高风险	mkdir -p /var/adm touch /var/adm/messages chmod 666 /var/adm/messages cat >> /etc/rsyslog.conf << EOF *.err;kern.debug;daemon.notice /var/adm/messages EOF service rsyslog restart

5	身份鉴别	检查密码重复使用次数限制	检查密码重复使用次数限制	Redhat,CentOS,Fedora:编辑 /etc/pam.d/system-auth 文件，Suse9:编辑 /etc/pam.d/passwd文件，Ubuntu,Suse10,Suse11,Suse12: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。	高风险	vi /etc/pam.d/common-password 找到这一行: plaintext password [success=1 default=ignore] pam_unix.so obscure sha512 在行尾追加 remember=5 ，修改完成后: plaintext password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5
6	安全审计	检查是否启用 cron 行为日志功能	rsyslog 是否启用记录 cron 行为日志功能	编辑 /etc/rsyslog.conf文件，配置: cron.* /var/log/cron ，其中 /var/log/cron 为日志文件。如果该文件不存在，则创建该文件，命令为: touch /var/log/cron ，并修改权限为 775.命令为: chmod 775 /var/log/cron.	高风险	touch /var/log/cron chmod 775 /var/log/cron cat >> /etc/rsyslog.conf << EOF cron.* /var/log/cron EOF rsyslogd -N1 systemctl restart rsyslog

7	安全审计	检查是否对登录进行日志记录	检查是否记录成功登陆日志	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。	高风险	cat >> /etc/pam.d/common-session << EOF session required pam_lastlog.so showfailed session optional pam_utmp.so EOF cat >> /etc/rsyslog.conf << EOF auth,authpriv.* /var/log/auth.log EOF systemctl restart rsyslog
8	身份鉴别	检查是否设置口令更改最小间隔天数	检查口令更改最小间隔天数	在文件 /etc/login.defs 中设置 PASS_MIN_DAYS 不小于标准值	高风险	vi /etc/login.defs 定位到 PASS_MIN_DAYS 0 改为 PASS_MIN_DAYS 6
9	身份鉴别	检查是否设置口令生存周期	检查口令生存周期	在文件 /etc/login.defs 中设置 PASS_MAX_DAYS 不大于标准值,PASS_MAX_DAYS 90，如果该文件不存在，则创建并按照要求进行编辑	高风险	vi /etc/login.defs 定位到 PASS_MAX_DAYS 99999 改为 PASS_MAX_DAYS 90
10	身份鉴别	检查是否设置口令过期前警告天数	检查口令过期前警告天数	在文件 /etc/login.defs 中设置 PASS_WARN_AGE 不小于标准值	高风险	vi /etc/login.defs 定位到 PASS_WARN_AGE 7 改为 PASS_WARN_AGE 30

11	身份鉴别	检查是否设置命令行界面超时退出	检查命令行界面超时时间	以 root 账户执行，vi /etc/profile, 增加 export TMOUT=600(单位：秒，可根据具体情况设定超时退出时间，要求不大于 600 秒), 注销用户，再用该用户登录激活该功能	高风险	cat >> /etc/profile << EOF export TMOUT=600 EOF source /etc/profile echo $TMOUT

12	安全审计	检查是否配置命令使用情况记录	su	检查是否配置命令使用情况记录	su	1. Suse 9, Redhat 5.x, CentOS 5.x 之前 (包括 5.x): 编辑 //etc//syslog.conf, Suse12, Ubuntu, Fedora, Redhat 6.x之后 (包括 6.x), CentOS 6.x 之后 (包括 6.x): 编辑 /etc/rsyslog.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 或者 service syslog restart	高风险	cat >> /etc/rsyslog.conf << EOF authpriv.* /var/log/secure EOF touch /var/log/secure chmod 600 /var/log/secure systemctl restart rsyslog

13	安全审计	检查是否配置远程日志功能	rsyslog 是否配置远程日志功能	编辑 /etc/rsyslog.conf 配置文件，添加日志转发规则。
				例如:
				# 使用 TCP 协议将所有日志转发到远程服务器
				. @@10.10.10.10:514
				# 或使用 UDP 协议
				. @10.10.10.10:514
				可以将此处 10.10.10.10 替换为实际的 IP
					高风险	192.168.6.55 做为日志接收服务器
						cat >> /etc/rsyslog.conf << EOF
						# TCP 接收
						module(load="imtcp")
						input(type="imtcp" port="514")
						
						# UDP 接收
						module(load="imudp")
						input(type="imudp" port="514")
						EOF
						systemctl restart rsyslog
						
						其他服务器
						cat >> /etc/rsyslog.conf << EOF
						# TCP 方式（更可靠，推荐）
						. @@192.168.6.55:514
						EOF
						systemctl restart rsyslog

14	入侵防范	检查是否限制远程登录 IP范围	检查 /etc/hosts.deny 配置	编辑 /etc/hosts.deny 增加一行 all:all	高风险	cat >> /etc/hosts.deny << EOF all:all EOF

15	入侵防范	检查是否限制远程登录 IP范围	检查 /etc/hosts.allow配置	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 或者 service xinetd restart	高风险	cat >> /etc/hosts.allow << EOF ALL: 127.0.0.1,192.168.6.0/24 EOF

16	身份鉴别	检查设备密码复杂度策略	检查密码复杂度策略中设置的小写字母个数	Redhat,CentOS,Fedora系统：修改/etc/pam.d/system-auth文件，Suse9：修改/etc/pam.d/paswd文件，Ubuntu,Suse10,Suse11,Suse12：修改/etc/pam.d/common-password文件，要求密码复杂度必须包含大小写字母、数字以及特殊字符，配置如下：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 现代系统(RHEL7+/CentOS7+/Fedora20+/Ubuntu16.04+/SUSE12+)：修改/etc/security/pwquality.conf文件，配置如下：ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=4 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；minclass：必须包含的字符类别数（4表示需包含全部四类字符）	高风险	sudo apt update
						sudo apt install libpam-pwquality -y
						vi /etc/security/pwquality.conf 无此文件
						# 至少 1个大写字母
						ucredit = -1
						# 至少 1个小写字母
						lcredit = -1
						# 至少 1个数字
						dcredit = -1
						# 至少 1个特殊符号
						ocredit = -1
						# 必须满足 4种字符类型（大小写、数字、特殊字符全部要有）
						minclass = 4
						# 同时搭配最小密码长度（基线通用 8位）
						minlen = 8
						vi /etc/pam.d/common-password 找到 pam_unix.so 上方的密码校验行，确保存在 pam_pwquality.so 模块，标准配置如下：
						password requisite pam_pwquality.so retry=3

17	身份鉴别	检查设备密码复杂度策略	检查密码复杂度策略中设置的数字个数	Redhat,CentOS,Fedora系统: 修改/etc/pam.d/system-auth文件 , Suse9: 修改/etc/pam.d/passwd文件, Ubuntu,Suse10,Suse11,Suse12: 修改/etc/pam.d/common-password文件, 要求密码复杂度必须包含大小写字母、数字以及特殊字符, 配置如下: password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 现代系统(RHEL7+/CentOS7+/Fedora20+/Ubuntu16.04+/SUSE12+): 修改/etc/security/pwquality.conf文件, 配置如下: ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=4 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; minclass: 必须包含的字符类别数 (4表示需包含全部四类字符)	高风险

18	身份鉴别	检查设备密码复杂度策略	检查密码复杂度策略中设置的特殊字符个数	Redhat,CentOS,Fedora系统: 修改/etc/pam.d/system-auth文件 , Suse9: 修改/etc/pam.d/passwd文件, Ubuntu,Suse10,Suse11,Suse12: 修改/etc/pam.d/common-password文件, 要求密码复杂度必须包含大小写字母、数字以及特殊字符，配置如下: password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 现代系统(RHEL7+/CentOS7+/Fedora20+/Ubuntu16.04+/SUSE12+): 修改/etc/security/pwquality.conf文件, 配置如下: ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=4 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; minclass: 必须包含的字符类别数 (4表示需包含全部四类字符)	高风险

19	身份鉴别	检查设备密码复杂度策略	检查密码复杂度策略中设置的大写字母个数	Redhat,CentOS,Fedora系统: 修改/etc/pam.d/system-auth文件 , Suse9: 修改/etc/pam.d/passwd文件, Ubuntu,Suse10,Suse11,Suse12: 修改/etc/pam.d/common-password文件, 要求密码复杂度必须包含大小写字母、数字以及特殊字符, 配置如下: password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 现代系统(RHEL7+/CentOS7+/Fedora20+/Ubuntu16.04+/SUSE12+): 修改/etc/security/pwquality.conf文件, 配置如下: ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=4 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; minclass: 必须包含的字符类别数(4表示需包含全部四类字符)	高风险

20	身份鉴别	检查账户认证失败次数限制	检查是否配置账户认证失败次数限制	请注意：修改配置文件为高风险操作，以下步骤仅供参考。 如果操作不当导致用户不能登录，那么建议进入单用户模式恢复配置。 Redhat,CentOS,Fedora: 编辑 /etc/pam.d/system-auth文件 注意 ： pam_tally.so 适用于低版本，高版本使用 pam_tally2.so 配置 ： auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Suse9: 编辑 /etc/pam.d/passwd文件 配置 ： auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Ubuntu,Suse10,Suse11,Suse12: 编辑 /etc/pam.d/common-auth 文件 注意 ： pam_tally.so 适用于低版本，高版本使用 pam_faillock.so 配置 :auth required pam_tally.so deny=5 unlock_time=600	高风险	sudo cp /etc/pam.d/common-auth /etc/pam.d/common-auth.bak.$(date +%F) sudo cp /etc/pam.d/common-account /etc/pam.d/common-account.bak.$(date +%F) sudo vi /etc/pam.d/common-auth 找到 `auth` 开头的行区域，在靠近顶部（`pam_unix.so` 之前）添加一行 auth required pam_tally2.so deny=5 unlock_time=600 even_deny_root audit sudo vi /etc/pam.d/common-account 在倒数第 2 行添加 account required pam_tally2.so # 故意用错误密码登录 5 次 ssh shuncom@localhost # 查看锁定状态 sudo pam_tally2 --user=shuncom # 手动解锁（如果需要） sudo pam_tally2 --user=shuncom --reset

21	身份鉴别	检查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	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 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 如果系统版大于等于 centos 6 在 auth 行下方添加： auth required pam_tally2.so deny=5 unlock_time=600 在 account 行下方添加： account required pam_tally2.so	高风险
22	访问控制	检查是否禁止root用户远程登录	检查是否禁止root用户远程ssh登录	修改/etc/ssh/sshd_config文件，配置PermitRootLogin no。重启服务，/etc/init.d/sshd restart 或者 service sshd restart	中风险

23	访问控制	检查是否禁止root用户远程登录	检查是否禁止root用户远程telnet登录	编辑/etc/pam.d/login文件，配置auth required pam_securetty.so 或: auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so	中风险	vi /etc/pam.d/logn auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
24	访问控制	检查是否配置用户所需最小权限	检查/etc/shadow文件权限	chmod 400 /etc/shadow	中风险	
25	访问控制	检查重要文件属性设置	检查 /etc/group 文件属性	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。	中风险	chattr +i /etc/group lsattr /etc/group 输出出现 ----i-------- 代表锁定成功
26	访问控制	检查重要文件属性设置	检查/etc/gshadow文件属性	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。	中风险	chattr +i /etc/gshadow lsattr /etc/gshadow 输出出现 ----i-------- 代表锁定成功

27	访问控制	检查重要文件属性设置	检查 /etc/passwd 文件属性	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。	中风险	chattr +i /etc/passwd lsattr /etc/passwd 输出出现 ----i-------- 代表锁定成功
28	访问控制	检查重要目录或文件权限设置	/etc/rc.d/init.d/ 或 /etc/init.d/ 目录权限是否符合规范	1. 对于 RedHat/CentOS系统: chmod 750 /etc/rc.d/init.d 2. 对于 Debian/Ubuntu系统: chmod 750 /etc/init.d	中风险	chmod 750 /etc/init.d
29	访问控制	检查重要目录或文件权限设置	/etc/security 目录权限是否符合规范	chmod 600 /etc/security	中风险	chmod 600 /etc/security
30	访问控制	检查重要目录或文件权限设置	/etc/shadow 文件权限是否符合规范	chmod 400 /etc/shadow	中风险	chmod 400 /etc/shadow
31	身份鉴别	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	对于使用 IP 协议进行远程维护的设备，应禁止使用 telnet协议	利用命令 rpm -qa |grep telnet 查看是否安装 telnet 和 telnet server 如果安装的话 1、编辑 /etc/xinetd.d/telnet, 修改 disable = yes。 2.激活 xinetd 服务。命令如下: # service xinetd restart 如果没安装则说明禁用 telnet 服务	高风险	

32	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭ntalk服务	Centos6: chkconfig [--level levels] ntalk off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable ntalk 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop ntalk	高风险
33	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭sendmail服务	Centos6: chkconfig [--level levels] sendmail off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable sendmail 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop sendmail	高风险
34	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭printer服务	Centos6: chkconfig [--level levels] printer off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable printer 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop printer	高风险

35	入侵防范	检查是否关闭不必要的服务和端	检查是否关闭bootps服务	Centos6: chkconfig [--level levels] bootps off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable bootps 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop bootps	高风险
36	入侵防范	检查是否关闭不必要的服务和端	检查是否关闭nfslock服务	Centos6: chkconfig [--level levels] nfslock off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable nfslock 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop nfslock	高风险
37	入侵防范	检查是否关闭不必要的服务和端	检查是否关闭ident服务	Centos6: chkconfig [--level levels] ident off 注 :levels 为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable ident 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop ident	高风险

38	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭tftp服务	Centos6: chkconfig [--level levels] tftp off 注 :levels为运行级别 ,需要重启机器 Centos7, Debian等 systemctl disable tftp 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop tftp	高风险
39	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭time服务	Centos6: chkconfig [--level levels] time off chkconfig [--level levels] time-udp off 注 :levels为运行级别 ,需要重启机器 Centos7, Debian等 systemctl disable time 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop time	高风险
40	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭lpd服务	Centos6: chkconfig [--level levels] lpd off 注 :levels为运行级别 ,需要重启机器 Centos7, Debian等 systemctl disable lpd 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop lpd	高风险

41	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭chargen服务	Centos6: chkconfig [--level levels] chargen off chkconfig [--level levels] chargen-udp off 注 :levels为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable chargen 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop chargen	高风险
42	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭nfs服务	Centos6: chkconfig [--level levels] nfs off 注 :levels为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable nfs 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop nfs	高风险

43	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭daytime服务	Centos6: chkconfig [--level levels] daytime off 注 :levels为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable daytime 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop daytime	高风险
44	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭echo服务	Centos6: chkconfig [--level levels] echo off chkconfig [--level levels] echo-udp off 注 :levels为运行级别 , 需要重启机器 Centos7, Debian等 systemctl disable echo 注 :, 需要重启机器 , 如需立刻关闭服务, 可 systemctl stop echo	高风险

45	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭discard服务	Centos6: chkconfig [--level levels] discard off chkconfig [--level levels] discard-udp off 注 :levels为运行级别 ,需要重启机器 Centos7,Debian等 systemctl disable discard 注 :,需要重启机器 ,如需立刻关闭服务, 可 systemctl stop discard	高风险
46	入侵防范	检查是否关闭不必要的服务和端口	检查是否关闭kshell服务	Centos6: chkconfig [--level levels] discard off chkconfig [--level levels] discard-udp off 注 :levels为运行级别 ,需要重启机器 Centos7,Debian等 systemctl disable kshell 注 :,需要重启机器 ,如需立刻关闭服务, 可 systemctl stop kshell	高风险
47	身份鉴别	检查是否存在空口令账号	是否存在空口令账号	按照密码设置策略设置非空密码 命令: passwd [OPTION...] <accountName>	高风险
48	入侵防范	检查是否安装OS补丁	检查是否安装OS补丁	可以使用OnlineUpdate或 Patch CD Update等方式升级系统补丁	高风险

49	访问控制	检查拥有suid和sgid权限的文件	检查重要文件是否存在suid和sgid权限	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	中风险
50	访问控制	检查日志文件是否非全局可写	检查/var/log/messages文件是否不可被其他用户修改	执行命令: chmod 775 /var/log/messages	中风险
51	访问控制	检查日志文件是否非全局可写	检查/var/log/localmessages文件是否other用户不可写	执行命令: chmod 775 /var/log/localmessages	中风险
52	访问控制	检查日志文件是否非全局可写	检查/var/log/secure文件是否other用户不可写	执行命令: chmod 775 /var/log/secure	中风险
53	访问控制	检查日志文件是否非全局可写	检查/var/log/cron日志文件是否other用户不可写	执行命令: chmod 775 /var/log/cron	中风险
54	访问控制	检查日志文件是否非全局可写	检查/var/log/mail文件是否other用户不可写	执行命令: chmod 775 /var/log/mail	中风险

55	访问控制	检查是否按用户分配账号	检查是否按用户分配账号	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。	中风险
56	访问控制	检查是否禁止root用户登录 FTP	禁止 root登录 VSFTP	1.编辑/etc/ftpusers(或/etc/vsftpd/ftpusers)文件 2.添加 root	中风险
57	访问控制	检查是否禁止root用户登录 FTP	禁止 root登录 WU-FTP	在 /etc/ftpusers 文件中加入下列行 root	中风险
58	访问控制	检查是否禁止匿名用户登录 FTP	禁止匿名 WU-FTP用户登录	在 /etc/passwd 文件中，删除 ftp 用户	中风险
59	访问控制	检查是否禁止匿名用户登录 FTP	禁止匿名 VSFTP 用户登录	编辑/etc/vsftpd.conf(或/etc/vsftpd/vsftpd.conf)文件，设置： anonymous_enable=NO	中风险

60	入侵防范	检查是否禁用不必要的系统服务	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。	检查是否关闭不必要的系统服务，以关闭 tftp 服务为例: 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。 直接关闭某个服务，如 tftp 可用如下命令： # /etc/init.d/tftp stop # 关闭正在运行的 tftp服务 补充操作说明 请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	中风险
61	访问控制	检查是否配置用户所需最小权限	检查 /etc/group 文件权限	chmod 644 /etc/group	中风险

62	访问控制	检查是否配置用户所需最小权限	检查/etc/passwd文件权限	chmod 644 /etc/passwd	中风险
63	访问控制	检查是否限制FTP用户登录后能访问的目录	检查是否限制FTP用户登录后能访问的目录	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	中风险
64	访问控制	检查重要目录或文件权限设置	/etc/passwd文件权限是否符合规范	chmod 644 /etc/passwd	中风险

65	访问控制	检查重要目录或文件权限设置	/etc/xinetd.conf文件权限是否符合规范	chmod 600 /etc/xinetd.conf 补充说明：低版本的 Linux 系统采用 inetd.conf 配置文件，执行命令 :chmod 600 /etc/inetd.conf	中风险
66	访问控制	检查重要目录或文件权限设置	/etc/services 文件权限是否符合规范	chmod 644 /etc/services	中风险
67	访问控制	检查重要目录或文件权限设置	/etc/group 文件权限是否符合规范	chmod 644 /etc/group	中风险

Revision #2
Created 3 July 2026 06:34:35 by Admin
Updated 3 July 2026 06:38:00 by Admin