**Linux 安全应用（[China Mobile](https://www.baidu.com/link?url=z-9KwXPL1t0TgsTr12nqyvY4PszHuLicydF-bmI0EOb-otdgFpH0r4V6ek74vywz-GBbnVRakHm8K31-UxRzeh5_5kWsLuxbWv08NGvaD2yTo1XqX7qABDEsJU_qpQm1&wd=&eqid=863d67630000af56000000035c00f0b8" \t "https://www.baidu.com/_blank)）**

目录

[禁止UID为0的用户存在多个 5](#_Toc4745)

[判定方式： 5](#_Toc1128)

[原始结果： 6](#_Toc7239)

[操作方式： 6](#_Toc31840)

[删除无关账号 6](#_Toc21607)

[判定方式： 6](#_Toc21776)

[原始结果： 7](#_Toc9161)

[操作方式： 7](#_Toc17581)

[设置账户组 8](#_Toc32073)

[判定方式： 8](#_Toc31313)

[原始结果： 8](#_Toc25746)

[操作方式： 8](#_Toc16368)

[禁止存在空密码的账户 9](#_Toc25823)

[判断依据 9](#_Toc171)

[原始结果 9](#_Toc15984)

[操作方式 9](#_Toc32469)

[避免账号共享 9](#_Toc2299)

[判断依据 9](#_Toc7990)

[原始结构 10](#_Toc14955)

[操作方法 10](#_Toc6988)

[口令锁定策略 10](#_Toc15513)

[判断依据 10](#_Toc14996)

[原始结果 11](#_Toc20976)

[操作方式 11](#_Toc29476)

[口令存活期 12](#_Toc18461)

[判定依据 12](#_Toc5156)

[原始结果 12](#_Toc12591)

[操作方式 12](#_Toc28892)

[口令复杂度 13](#_Toc24283)

[判断依据 13](#_Toc31096)

[原始结果 13](#_Toc30913)

[操作方法 14](#_Toc22198)

[口令重复次数限制 14](#_Toc3548)

[判断依据 14](#_Toc2058)

[原始结果 14](#_Toc17038)

[操作方法 15](#_Toc16396)

[使用PAM认证模块禁止wheel组之外的用户su为root 15](#_Toc2015)

[判断依据 15](#_Toc22826)

[原始结果 16](#_Toc28142)

[操作方式 16](#_Toc19687)

[限制root用户ssh远程登录 16](#_Toc29343)

[判断依据 16](#_Toc10811)

[原始结果 17](#_Toc30478)

[操作方法 17](#_Toc11214)

[使用SSH协议进行远程维护 18](#_Toc6484)

[判断依据 18](#_Toc21791)

[原始结果 18](#_Toc23958)

[操作方法 18](#_Toc30172)

[限制root用户TELNET远程登录 19](#_Toc10364)

[判断依据 19](#_Toc11504)

[原始结果 19](#_Toc24200)

[操作方法 20](#_Toc4374)

[修改SSH的Banner的信息 20](#_Toc22235)

[判断依据 20](#_Toc4849)

[原始结果 20](#_Toc1387)

[操作方法 21](#_Toc3323)

[修改SSH的Banner的警告信息 21](#_Toc8129)

[判断依据 21](#_Toc22468)

[原始结果 21](#_Toc22698)

[操作方法 22](#_Toc11612)

[配置NFS服务限制 22](#_Toc29323)

[判断依据 22](#_Toc15581)

[原始结果 23](#_Toc9527)

[操作方法 23](#_Toc5997)

[配置NTP 23](#_Toc31596)

[判断依据 23](#_Toc10806)

[原始结果 24](#_Toc11635)

[操作方法 25](#_Toc21789)

[修改FTP的Banner信息 25](#_Toc26990)

[判断依据 25](#_Toc27716)

[原始结果 26](#_Toc16210)

[操作方法 29](#_Toc8867)

[修改SNMP的默认Community 30](#_Toc21939)

[判断依据 30](#_Toc3627)

[原始结果 30](#_Toc30138)

[操作方法 31](#_Toc14937)

[用户FTP访问安全配置 31](#_Toc12289)

[判断依据 31](#_Toc9262)

[原始数据 32](#_Toc10541)

[操作方法 33](#_Toc4814)

[关闭不必要启动项 34](#_Toc21630)

[判断依据 34](#_Toc6761)

[原始结果 34](#_Toc21416)

[操作方法 34](#_Toc17174)

[禁止root用户登录FTP 34](#_Toc11959)

[判断依据 34](#_Toc23490)

[原始结果 35](#_Toc27595)

[操作方法 38](#_Toc357)

[限制FTP用户登录后能访问的目录 39](#_Toc3559)

[判断依据 39](#_Toc25885)

[原始结果 39](#_Toc31545)

[操作方法 41](#_Toc28637)

[关闭不必要的服务和端口 42](#_Toc3703)

[判断依据 42](#_Toc6351)

[原始结果 42](#_Toc29762)

[操作方法 44](#_Toc11171)

[禁止匿名FTP 45](#_Toc15553)

[判断依据 45](#_Toc26197)

[原始结果 45](#_Toc2752)

[操作方法 47](#_Toc21048)

[修改TELNET的Banner信息 48](#_Toc21785)

[判断依据 48](#_Toc6727)

[原始结果 48](#_Toc5182)

[操作方法 49](#_Toc28935)

[文件与目录缺省权限控制 50](#_Toc17678)

[判断依据 50](#_Toc27271)

[原始结果 50](#_Toc13152)

[操作方法 50](#_Toc4922)

[账号文件权限设置 50](#_Toc20973)

[判断依据 50](#_Toc4798)

[原始结果 51](#_Toc21119)

[操作方法 51](#_Toc25042)

[配置用户最小授权 51](#_Toc2183)

[判断依据 51](#_Toc5385)

[原始结果 52](#_Toc12691)

[操作方法 52](#_Toc2551)

[禁止ICMP重定向 53](#_Toc23092)

[判断依据 53](#_Toc29423)

[原始结果 53](#_Toc2902)

[操作方法 53](#_Toc23948)

[日志文件安全 53](#_Toc2840)

[判断依据 53](#_Toc29335)

[原始结果 54](#_Toc5542)

[操作方法 55](#_Toc25095)

[启用远程日志功能 55](#_Toc21925)

[判断依据 55](#_Toc17463)

[原始结果 55](#_Toc24875)

[操作方法 56](#_Toc16768)

[记录安全事件日志 56](#_Toc26465)

[判断依据 56](#_Toc7120)

[原始结果 56](#_Toc23611)

[操作方法 57](#_Toc20999)

[记录账户登录日志 58](#_Toc6890)

[判断依据 58](#_Toc4889)

[原始结果 59](#_Toc31994)

[操作方法 59](#_Toc10043)

[配置su命令使用情况记录 60](#_Toc4919)

[判断依据 60](#_Toc26552)

[原始结果 60](#_Toc22214)

[操作方法 61](#_Toc25113)

[记录cron行为日志 62](#_Toc7200)

[判断依据 62](#_Toc27064)

[原始结果 62](#_Toc7890)

[操作方法 63](#_Toc13073)

[禁止IP路由转发 64](#_Toc29729)

[判断依据 64](#_Toc11832)

[原始结果 64](#_Toc25616)

[操作方法 64](#_Toc16991)

[控制远程访问的IP地址 64](#_Toc25435)

[判断依据 64](#_Toc23136)

[原始结果 65](#_Toc32341)

[操作方法 65](#_Toc29336)

[禁止IP源路由 65](#_Toc17371)

[判断依据 65](#_Toc6810)

[原始结果 65](#_Toc30904)

[操作方法 66](#_Toc12675)

[更改主机解析地址的顺序 66](#_Toc24351)

[判断依据 66](#_Toc6654)

[原始结果 66](#_Toc31547)

[操作方法 66](#_Toc19243)

[系统core dump状态 67](#_Toc17622)

[判断依据 67](#_Toc3597)

[原始结果 67](#_Toc30637)

[操作方法 67](#_Toc29490)

[打开syncookie缓解syn flood攻击 68](#_Toc32488)

[判断依据 68](#_Toc10915)

[原始结果 68](#_Toc7630)

[操作方法 68](#_Toc30824)

[禁止存在心血漏洞 68](#_Toc18102)

[判断依据 68](#_Toc4647)

[原始结果 69](#_Toc23221)

[操作方法 69](#_Toc22172)

[禁止存在bash安全漏洞 69](#_Toc8099)

[判断依据 69](#_Toc5637)

[原始结果 69](#_Toc26479)

[操作方法 69](#_Toc6835)

[登录超时时间设置 70](#_Toc31443)

[判断依据 70](#_Toc23390)

[原始结果 70](#_Toc10985)

[操作方法 70](#_Toc19703)

[Root用户环境变量的安全性 70](#_Toc18483)

[判断依据 70](#_Toc14334)

[原始结果 70](#_Toc29455)

[操作方法 71](#_Toc21937)

[禁止组合键关机 71](#_Toc6329)

[判断依据 71](#_Toc23438)

[原始结果 71](#_Toc18742)

[操作方法 71](#_Toc4089)

[设置屏幕锁定 72](#_Toc13805)

[判断依据 72](#_Toc6410)

[原始结果 72](#_Toc26039)

[操作方法 72](#_Toc32461)

[设置关键文件的属性 73](#_Toc21160)

[判断依据 73](#_Toc25718)

[原始结果 73](#_Toc1757)

[操作方法 73](#_Toc22625)

[历史命令设置 73](#_Toc14619)

[判断依据 73](#_Toc22733)

[原始数据 74](#_Toc12034)

[操作方法 74](#_Toc23478)

[对root为ls、rm设置别名 74](#_Toc6676)

[判断依据 74](#_Toc23099)

[原始数据 75](#_Toc3572)

[操作方法 75](#_Toc9326)

# 禁止UID为0的用户存在多个

## 判定方式：

通过如下命令查看/etc/passwd文件中UID为0的账号:

#awk -F: '($3 == 0) { print $1 }' /etc/passwd

判定依据

不存在root用户外的其他用户UID为0则合规，否则不合规

## 原始结果：

awk -F: '($3 == 0) { print $1 }' /etc/passwd

echo "result="`awk -F: '($3 == 0) { print $1 }' /etc/passwd | grep -v "^[[:space:]]\*#" |grep -v root|wc -l`

root

result=0

## 操作方式：

参考配置操作

1、执行配置文件备份：

#cp –p /etc/passwd /etc/passwd\_bak

#cp –p /etc/shadow /etc/shadow\_bak

#cp –p /etc/group /etc/group\_bak

2、查询UID为0的账号信息

#awk -F: '($3 == 0) { print $1 }' /etc/passwd

如果命令的输出存在非root账号，则使用如下命令删除该账户(切记不要删除root用户)。

#userdel username

# 删除无关账号

## 判定方式：

检测方法

1、查看/etc/shadow文件，确认以下用户(lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody)的密码列字段是否以\*或者!!开头：

#egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:" /etc/shadow|awk -F: '($2!~/^\*/) && ($2!~/^!!/) {print $1":"}'

2、查看/etc/passwd文件确认以下用户(lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody)的shell域字段值是否为/bin/false

#egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:" /etc/passwd|awk -F: '($7!~/bin\/false/) {print $1":"$7}'

判定依据

1、lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody用户不存在或/etc/shadow文件中对应密码字段以\*或者!!开头

2、lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody用户不存在或者/etc/passwd文件中对应shell域为/bin/false

## 原始结果：

cat /etc/shadow|sed '/^\s\*#/d'|awk -F: '($2!~/^\*/) && ($2!~/^!!/) {print $1":"}'|egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:"

egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:" /etc/passwd|awk -F: '($7!~/bin\/false/) {print $1":"$7}'

echo "result\_pw="`cat /etc/shadow|sed '/^\s\*#/d'|awk -F: '($2!~/^\*/) && ($2!~/^!!/) {print $1}'|egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:"|wc -l`

echo "result\_shell="`egrep "^lp:|^sync:|^halt:|^news:|^uucp:|^operator:|^games:|^gopher:|^smmsp:|^nfsnobody:|^nobody:" /etc/passwd|awk -F: '($7!~/bin\/false/) {print $1":"$7}'|wc -l`

lp:/sbin/nologin

sync:/bin/sync

halt:/sbin/halt

uucp:/sbin/nologin

operator:/sbin/nologin

games:/sbin/nologin

gopher:/sbin/nologin

nobody:/sbin/nologin

nfsnobody:/sbin/nologin

result\_pw=0

result\_shell=9

## 操作方式：

参考配置操作

1、如果以下用户(lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody)没有被删除或锁定，可以使用如下命令对其进行操作：

（1）、删除用户：

#userdel username

（2）、锁定用户：

#passwd -l username #锁定用户，只有具备超级用户权限的使用者方可使用。

#passwd –d username #解锁用户，解锁后原有密码失效,登录设置新密码才能登录。

#passwd -u username #解锁用户后，原密码仍然有效。

（3）、修改用户shell域为/bin/false

#usermod -s /bin/false username #命令来更改相应用户的shell为/bin/false，其中[name]为要修改的具体用户名。

# 设置账户组

## 判定方式：

检测方法

1、使用如下命令查看文件/etc/login.defs，确认文件中变量GID\_MIN和GID\_MAX的值：

#grep -v ^# /etc/login.defs |grep "^GID\_MIN"|awk '($1="GID\_MIN") {print $2}'

#grep -v ^# /etc/login.defs |grep "^GID\_MAX"|awk '($1="GID\_MAX") {print $2}'

2、使用以下命令查看系统中是否存在用户id>=GID\_MIN且<=GID\_MAX的用户：

#UP\_GIDMIN=`(grep -v ^# /etc/login.defs |grep "^GID\_MIN"|awk '($1="GID\_MIN") {print $2}')`

#UP\_GIDMAX=`(grep -v ^# /etc/login.defs |grep "^GID\_MAX"|awk '($1="GID\_MAX") {print $2}')`

#egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($4>='$UP\_GIDMIN' && $4<='$UP\_GIDMAX') {print $1":"$3":"$4}'

判定依据

存在组id>=GID\_MIN且<=GID\_MAX的用户则合规，否则不合规。

## 原始结果：

UP\_GIDMIN=`(grep -v ^# /etc/login.defs |grep "^GID\_MIN"|awk '($1="GID\_MIN") {print $2}')`

UP\_GIDMAX=`(grep -v ^# /etc/login.defs |grep "^GID\_MAX"|awk '($1="GID\_MAX") {print $2}')`

egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($4>='$UP\_GIDMIN' && $4<='$UP\_GIDMAX') {print $1":"$3":"$4}'

echo $UP\_GIDMIN $UP\_GIDMAX

echo "result="`egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($4>='$UP\_GIDMIN' && $4<='$UP\_GIDMAX') {print $1":"$3":"$4}'|wc -l`

unset UP\_GIDMIN UP\_GIDMAX

mysql:500:500

routine:501:501

bjwebwh:502:502

bjwebwhl:503:503

500 60000

result=4

## 操作方式：

参考配置操作

1、创建用户组

#cp -p /etc/group /etc/group\_bak #备份文件

#groupadd groupname #创建一个组

#usermod –g group username #将用户username分配到group组中

# 禁止存在空密码的账户

## 判断依据

检测方法

执行以下命令查看系统中是否存在空口令账号

#awk -F: '( $2 == "" ) { print $1 }' /etc/shadow

判定依据

系统中口令为空的账号个数为0则合规，否则不合规。

## 原始结果

awk -F: '( $2 == "" ) { print $1 }' /etc/shadow

echo "result="`awk -F: '( $2 == "" ) { print $1 }' /etc/shadow |wc -l`

result=0

## 操作方式

参考配置操作

1、执行备份：

#cp -p /etc/passwd /etc/passwd\_bak

#cp -p /etc/shadow /etc/shadow\_bak

2、为帐户设置满足密码复杂度的密码：

#passwd username

# 避免账号共享

## 判断依据

检测方法

1、使用如下命令查看文件/etc/login.defs，确认文件中变量UID\_MIN和UID\_MAX的值：

#grep -v ^# /etc/login.defs |grep "^UID\_MIN"|awk '($1="UID\_MIN"){print $2}'

#grep -v ^# /etc/login.defs |grep "^UID\_MAX"|awk '($1="UID\_MAX"){print $2}'

2、使用以下命令查看系统中是否存在用户id>=UID\_MIN且<=UID\_MAX的用户：

#up\_uidmin=`(grep -v ^# /etc/login.defs |grep "^UID\_MIN"|awk '($1="UID\_MIN"){print $2}')`

#up\_uidmax=`(grep -v ^# /etc/login.defs |grep "^UID\_MAX"|awk '($1="UID\_MAX"){print $2}')`

#egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($3>='$up\_uidmin' && $3<='$up\_uidmax') {print $1":"$3}'

判定依据

存在用户id>=UID\_MIN且<=UID\_MAX的用户则合规，否则不合规

## 原始结构

up\_uidmin=`(grep -v ^# /etc/login.defs |grep "^UID\_MIN"|awk '($1="UID\_MIN"){print $2}')`

up\_uidmax=`(grep -v ^# /etc/login.defs |grep "^UID\_MAX"|awk '($1="UID\_MAX"){print $2}')`

egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($3>='$up\_uidmin' && $3<='$up\_uidmax') {print $1":"$3}'

echo "result="`egrep -v "oracle|sybase|postgres" /etc/passwd|awk -F: '($3>='$up\_uidmin' && $3<='$up\_uidmax') {print $1":"$3}'|wc -l`

unset up\_uidmin up\_uidmax

mysql:500

routine:501

bjwebwh:502

bjwebwhl:503

result=4

## 操作方法

参考配置操作

1、创建用户

#useradd username #创建账号

#passwd username #设置密码修改权限

# 口令锁定策略

## 判断依据

检测方法

（1）redhat5以上系统编辑文件/etc/pam.d/system-auth

（2）suse9以上编辑/etc/pam.d/common-auth查看是否存在如下内容：

auth required pam\_tally2.so deny=5 onerr=fail no\_magic\_root unlock\_time=180

account required pam\_tally2.so

(redhat5.1以下版本及suse只支持pam\_tally.so)

判定依据

用户连续认证失败次数设置为5则合规，否则不合规。

## 原始结果

if [ -f /etc/redhat-release ];then

if [ -n "`cat /etc/redhat-release 2>/dev/null |grep "Red Hat"`" ];then

linux\_version=`cat /etc/redhat-release |awk '{print$7}'|awk -F. '{print$1}'`

elif [ -n "`cat /etc/redhat-release 2>/dev/null |grep "CentOS"`" ];then

linux\_version=`cat /etc/redhat-release|awk '{print$3}'|awk -F. '{print$1}'`

fi

if [ "$linux\_version" -ge 5 ];then

cat /etc/pam.d/system-auth|sed '/^#/d'|sed '/^$/d'|egrep -i "auth[[:space:]]\*required[[:space:]]\*pam\_tally.so|auth[[:space:]]\*required[[:space:]]\*pam\_tally2.so|account[[:space:]]\*required[[:space:]]\*pam\_tally.so|account[[:space:]]\*required[[:space:]]\*pam\_tally2.so"

fi

elif [ -f /etc/SuSE-release ];then

suse\_version=`cat /etc/SuSE-release 2>/dev/null |grep -i "VERSION"|awk '{print $3}'`

if [ "$suse\_version" -ge 9 ];then

cat /etc/pam.d/common-auth|grep -v '^#'|egrep -i "auth[[:space:]]\*required[[:space:]]\*pam\_tally.so|auth[[:space:]]\*required[[:space:]]\*pam\_tally2.so|account[[:space:]]\*required[[:space:]]\*pam\_tally.so|account[[:space:]]\*required[[:space:]]\*pam\_tally2.so"

fi

fi

unset linux\_version suse\_version

## 操作方式

参考配置操作

Redhat系统（5.x版本之后）

（1）执行备份：

#cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth\_bak

（2）修改配置（vi /etc/pam.d/system-auth）

auth required pam\_tally2.so deny=5 unlock\_time=300 even\_deny\_root root\_unlock\_time=10

account required pam\_tally2.so

解释：deny：认证失败次数

unlock\_time：锁定时间

even\_deny\_root：限制root用户

root\_unlock\_time：root用户锁定时间

SUSE系统（9版本之后）

（1）执行备份

#cp -p /etc/pam.d/common-auth /etc/pam.d/common-auth.bak

（2）修改配置（vi /etc/pam.d/common-auth）

auth required pam\_tally2.so onerr=fail audit silent deny=5 unlock\_time=900

account required pam\_tally2.so

解释：onerr：当意外发生时，返加PAM\_SUCCESS或pam错误代码，一般该项不进行配置。

audit：如果登录的用户不存在，则将访问信息写入系统日志。

silent：静默模式，不输出任何日志信息。

# 口令存活期

## 判定依据

检测方法

查看文件/etc/login.defs( more /etc/login.defs)，检查如下参数值是否满足要求：

PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数不大于90

PASS\_MIN\_DAYS 10 #新建用户的密码最短使用天数为10

PASS\_WARN\_AGE 7 #新建用户的密码到期提前提醒天数为7

判定依据

PASS\_MAX\_DAYS不大于90，PASS\_MIN\_DAYS等于10，PASS\_WARN\_AGE等于7则合规，否则不合规。

## 原始结果

cat /etc/login.defs |grep -v "^[[:space:]]\*#"|grep -E '^\s\*PASS\_MAX\_DAYS|^\s\*PASS\_MIN\_DAYS|^\s\*PASS\_WARN\_AGE'

PASS\_MAX\_DAYS 99999

PASS\_MIN\_DAYS 0

PASS\_WARN\_AGE 7

## 操作方式

参考配置操作

1、文件备份：

#cp -p /etc/login.defs /etc/login.defs\_bak

2、修改策略设置，编辑文件/etc/login.defs(vi /etc/login.defs)，在文件中加入如下内容(如果存在则修改，不存在则添加)：

PASS\_MAX\_DAYS 90

PASS\_MIN\_DAYS 10

PASS\_WARN\_AGE 7

# 口令复杂度

## 判断依据

检测方法

1、 redhat系统编辑文件/etc/pam.d/system-auth，是否存在如下配置：

password requisite pam\_cracklib.so try\_first\_pass retry=3 dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1 minlen=8

2、suse9以上编辑/etc/pam.d/common-password是否存在如下配置：

password required pam\_pwcheck.so nullok

password requisite pam\_cracklib.so minlen=8 lcredit=-1 ocredit=-1 ucredit=-1 dcredit=-4 use\_authtok

password required pam\_unix2.so nullok use\_first\_pass use\_authtok

判定依据

设置了口令复杂度则合规，否则不合规。

## 原始结果

Calculate ()

{

DCREDIT=`cat $FILE|egrep -v "^#|^$"|grep -w "dcredit"|sed 's/^.\*dcredit=//g'|sed 's/\s.\*$//g'`;

LCREDIT=`cat $FILE|egrep -v "^#|^$"|grep -w "lcredit"|sed 's/^.\*lcredit=//g'|sed 's/\s.\*$//g'`;

UCREDIT=`cat $FILE|egrep -v "^#|^$"|grep -w "ucredit"|sed 's/^.\*ucredit=//g'|sed 's/\s.\*$//g'`;

OCREDIT=`cat $FILE|egrep -v "^#|^$"|grep -w "ocredit"|sed 's/^.\*ocredit=//g'|sed 's/\s.\*$//g'`;

MINLEN=`cat $FILE|egrep -v "^#|^$"|grep "minlen"|sed 's/^.\*minlen=//g'|sed 's/\s.\*$//g'`;

echo "DCREDIT=$DCREDIT";

echo "LCREDIT=$LCREDIT";

echo "UCREDIT=$UCREDIT";

echo "OCREDIT=$OCREDIT";

echo "MINCLASS=$MINLEN";

unset DCREDIT LCREDIT UCREDIT OCREDIT MINLEN;

}

if ([ -f /etc/redhat-release ] && [ -f /etc/pam.d/system-auth ]);

then

FILE=/etc/pam.d/system-auth;

Calculate;

fi

if ([ -f /etc/SuSE-release ] && [ -f /etc/pam.d/common-password ])

then

FILE=/etc/pam.d/common-password

Calculate;

fi

unset FILE suse\_version;

DCREDIT=

LCREDIT=

UCREDIT=

OCREDIT=

MINCLASS=

## 操作方法

参考配置操作

1、redhat系统

编辑文件/etc/pam.d/system-auth，在文件中找到如下内容：

password requisite pam\_cracklib.so，将其修改为：

password requisite pam\_cracklib.so try\_first\_pass retry=3 dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1 minlen=8 #至少包含一个数字、一个小写字母、一个大写字母、一个特殊字符、且密码长度>=8

# 口令重复次数限制

## 判断依据

检测方法

1、redhat系统编辑文件/etc/pam.d/system-auth，

2、suse9编辑检查文件/etc/pam.d/passwd，

3、suse10以上编辑/etc/pam.d/common-password，查看类似password sufficient pam\_unix.so所在行是否存在remember=5，如果没有则新增，例如：

password sufficient pam\_unix.so md5 shadow nullok try\_first\_pass use\_authtok remember=5

判定依据

文件/etc/pam.d/system-auth(SUSE9:/etc/pam.d/passwd、SUSE10以上/etc/pam.d/common-password)中包含类似如下内容则合规，否则不合规：

password sufficient pam\_unix.so md5 shadow nullok try\_first\_pass use\_authtok remember=5

## 原始结果

if ([ -f /etc/redhat-release ] && [ -f /etc/pam.d/system-auth ]);

then FILE=/etc/pam.d/system-auth

cat $FILE |sed '/^#/d'|sed '/^$/d'|grep password

fi

suse\_version=`cat /etc/SuSE-release 2>/dev/null|grep -i "VERSION"|awk '{print $3}'`

if ([ "x$suse\_version" = x10 ] || [ "x$suse\_version" = x11 ])

then

FILE=/etc/pam.d/common-password

cat $FILE|grep -v '^#'|grep -v '^$'|grep password

else

if [ -f /etc/SuSE-release ]

then

FILE=/etc/pam.d/passwd

cat $FILE|grep -v '^#'|grep -v '^$'|grep password

fi

fi

unset suse\_version FILE;

password requisite pam\_cracklib.so try\_first\_pass retry=3 type=

password sufficient pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok

password required pam\_deny.so

## 操作方法

参考配置操作

1、执行备份

#cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth.bak

#cp -p /etc/pam.d/passwd /etc/pam.d/passwd.bak

#cp -p /etc/pam.d/common-password /etc/pam.d/common-password.bak

2、创建文件/etc/security/opasswd用于存储旧密码，并设置权限。

#touch /etc/security/opasswd

#chown root:root /etc/security/opasswd

#chmod 600 /etc/security/opasswd

3、修改策略设置

#vi /etc/pam.d/system-auth((SUSE9:/etc/pam.d/passwd、SUSE10以上/etc/pam.d/common-password)在类似password sufficient pam\_unix.so所在行末尾增加remember=5，中间以空格隔开.如果没有则新增，例如:

password sufficient pam\_unix.so md5 shadow nullok try\_first\_pass use\_authtok remember=5

# 使用PAM认证模块禁止wheel组之外的用户su为root

## 判断依据

检测方法

执行命令cat /etc/pam.d/su，查看文件中是否存在如下配置：

auth sufficient pam\_rootok.so

auth required pam\_wheel.so group=wheel

判定依据

使用pam\_rootok.so认证模块认证且配置了只允许wheel组的用户才能su为root则合规，否则不合规。

## 原始结果

cat /etc/pam.d/su|grep -v "^[[:space:]]\*#"|grep -v "^$"|grep "^auth"

auth sufficient pam\_rootok.so

auth include system-auth

## 操作方式

参考配置操作

1、编辑文件(vi /etc/pam.d/su)

（1）redhat4.x(32位)在文件开头加入如下两行(有则修改,没有则添加):

auth sufficient /lib/security/$ISA/pam\_rootok.so

auth required /lib/security/$ISA/pam\_wheel.so use\_uid

#注意auth与sufficient之间由两个tab建隔开,sufficient与动态库路径之间使用一个tab建隔开

（2）redhat4.x(64位)在文件开头加入如下两行(有则修改,没有则添加):

auth sufficient /lib64/security/$ISA/pam\_rootok.so

auth required /lib64/security/$ISA/pam\_wheel.so use\_uid

#注意auth与sufficient之间由两个tab建隔开,sufficient与动态库路径之间使用一个tab建隔开

（3）redhat5.x版本之后以及SUSE系统在文件开头加入如下两行(有则修改,没有则添加):

auth sufficient pam\_rootok.so

auth required pam\_wheel.so use\_uid

#注意auth与sufficient之间由两个tab建隔开，sufficient与动态库路径之间使用一个tab建隔开

说明：(这表明只有wheel组中的用户可以使用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:

#usermod -G wheel username #username为需要添加至wheel组的账户名称。

# 限制root用户ssh远程登录

## 判断依据

检测方法

1、执行以下命令查看配置文件/etc/ssh/sshd\_config是否配置拒绝root用户通过ssh协议远程登录：

#grep -v "^[[:space:]]\*#" /etc/ssh/sshd\_config|grep "PermitRootLogin no"

2、执行以下命令查看ssh协议版本是否为2：

#grep -v "^[[:space:]]\*#" /etc/ssh/sshd\_config|egrep "^protocol\s\*2|^Protocol\s\*2"

判定依据

/etc/ssh/sshd\_config文件存在PermitRootLogin no(表示禁止root用户通过ssh协议远程登录)且ssh协议为protocol 2(表示ssh协议版本为2)则合规，否则不合规

## 原始结果

if grep -v "^[[:space:]]\*#" /etc/ssh/sshd\_config|grep -i "PermitRootLogin no"

then echo "This device does not permit root to ssh login,check result:true";

else

echo "This device permits root to ssh login,check result:false";

fi

if grep -v "^[[:space:]]\*#" /etc/ssh/sshd\_config|egrep "^protocol[[:space:]]\*2|^Protocol[[:space:]]\*2"

then echo "SSH protocol version is 2,check result:true"

else

echo "SSH protocol version is not 2,check result:false"

fi

This device permits root to ssh login,check result:false

Protocol 2

SSH protocol version is 2,check result:true

## 操作方法

参考配置操作

1、执行备份：

#cp -p /etc/ssh/sshd\_config /etc/ssh/sshd\_config\_bak

2、新建一个普通用户并设置高强度密码(防止设备上只存在root用户可用时，无法远程访问)：

#useradd username

#passwd username

3、禁止root用户远程登录系统

（1）、编辑文件/etc/ssh/sshd\_config(vi /etc/ssh/sshd\_config)，修改PermitRootLogin值为no并去掉注释。

PermitRootLogin no #则禁止了root从ssh登录。

（2）、重启SSH服务

#/etc/init.d/sshd restart

4、修改SSH协议版本

（1）、编辑文件/etc/ssh/sshd\_config(vi /etc/ssh/sshd\_config)，修改Protocol的值为2并去掉注释。

Protocol 2

（2）、重启ssh服务

#/etc/init.d/sshd restart

# 使用SSH协议进行远程维护

## 判断依据

检测方法

（1）redhat7以下版本及SUSE系统使用以下命令查看telnet和ssh服务状态：

#chkconfig --list |grep -E '(telnet|ssh)'

（2）redhat7版本使用以下版本查看telnet和ssh服务状态

#systemctl|grep -E '(telnet|ssh)'

判定条件

输出ssh服务启用，telnet服务关闭则合规，否则不合规。

## 原始结果

if [[ `cat /etc/redhat-release 2>/dev/null|cut -b 22` -eq 7 ]] || [[ `cat /etc/redhat-release 2>/dev/null|cut -b 41` -eq 7 ]];then

echo "telnet\_status="`systemctl|grep telnet|grep active|wc -l`

echo "ssh\_status="`ps -ef|grep "sshd"|grep -v "grep"|wc -l`

else

echo "telnet\_status="`chkconfig --list |egrep "\*.telnet"|egrep -i "on|启用"|wc -l`

echo "ssh\_status="`ps -ef|grep "sshd"|grep -v "grep"|wc -l`

fi

unset telnet\_status ssh\_status

telnet\_status=0

ssh\_status=3

## 操作方法

参考配置操作

redhat7以下版本及SUSE系统

1、关闭TELNET服务(如果设备安装了TELNET服务则执行以下操作关闭，否则无需操作)：

（1）备份

#cp -p /etc/xinetd.d/telnet /etc/xinetd.d/telnet\_bak

（2）编辑文件/etc/xinetd.d/telnet(vi /etc/xinetd.d/telnet)，把disable项改为yes，即disable = yes。

（3）执行以下命令重启xinetd服务。

#service xinetd restart

2、开启SSH服务：

（1）安装SSH软件包。

（2）通过以下命令启动ssh服务：

#/etc/init.d/sshd start

redhat7版本

1、关闭telnet服务

#systemctl stop telnet.socket

#systemctl disable telnet.socket

#systemctl restart xinetd

2、开启sshd服务

（1）安装sshd服务

（2）开启sshd服务

#systemctl start sshd.service

开机自启

#systemctl enable sshd.service

# 限制root用户TELNET远程登录

## 判断依据

检测方法

1、使用命令chkconfig --list |egrep "telnet"查看TELNET服务是否开启。

（1）redhat7以下版本及SUSE系统

#chkconfig --list |egrep "telnet"

（2）redhat7版本

#systemctl|grep "telnet.socket"

2、使用以下命令查看文件/etc/securetty中是否有配置有(pts/\*)这样的内容：

#cat /etc/securetty|grep -v "^[[:space:]]\*#"|grep "pts/\*"

判定依据

如果TELNET服务未开启，则合规；或者TELNET服务开启，但文件/etc/securetty中不存在pts/\* 也合规，否者不合规。(\*为数字)。

## 原始结果

if [[ `cat /etc/redhat-release 2>/dev/null|cut -b 22` -eq 7 ]] || [[ `cat /etc/redhat-release 2>/dev/null|cut -b 41` -eq 7 ]];then

telnet\_status=`systemctl|grep "telnet.socket"|wc -l`

else

telnet\_status=`chkconfig --list|egrep "telnet.\*"|egrep "on|启用"|wc -l`

fi

if [ $telnet\_status -ge 1 ];then

echo "pts\_count="`cat /etc/securetty|grep -v "^[[:space:]]\*#"|grep "pts/\*"|wc -l`

else

echo "Telnet process is not open"

fi

unset telnet\_status

Telnet process is not open

## 操作方法

参考配置操作

1、编辑文件/etc/securetty(vi /etc/securetty)注释掉pts/\*这样的内容并保存。

# 修改SSH的Banner的信息

## 判断依据

检测方法

1、执行以下命令验证SSH服务是否开启

#/etc/init.d/sshd status

2、如果SSH服务开启,请查看文件/etc/motd中是否设置banner信息。

判定依据

1、SSH服务未开启

2、SSH开启，且文件/etc/motd不为空

二者满足其一则合规，否则不合规。

## 原始结果

ssh\_status=`ps -ef|grep "sshd"|grep -v "grep"|wc -l`;

if ([ $ssh\_status != 0 ] && [ -s /etc/motd ]);

then

echo "sshd is running,banner is not null,check result:true";

else

if [ $ssh\_status -ge 1 ];

then

echo "sshd is running,banner is null,check result:false";

else

if [ -s /etc/motd ];

then

echo "sshd is not running,banner is not null,check result:true";

else

echo "sshd is not running,banner is null,check result:true";

fi;

fi;

fi;

unset ssh\_status;

sshd is running,banner is null,check result:false

## 操作方法

参考配置操作

1、修改文件/etc/motd的内容，如没有该文件，则创建它：

#touch /etc/motd

2、使用如下命令在文件/etc/motd中添加banner信息。

#echo " Authorized users only. All activity may be monitored and reported " > /etc/motd

可根据实际需要修改该文件的内容。

# 修改SSH的Banner的警告信息

## 判断依据

检查方法

1、执行以下命令验证SSH服务是否开启

#/etc/init.d/sshd status

2、如果SSH服务开启，请查看文件/etc/ssh/sshd\_config文件，是否配置如下内容：

Banner /etc/sshbanner

查看对应的/etc/sshbanner文件中是否配置警告标示：

"Authorized users only. All activity may be monitored and reported "

判定依据

1、SSH服务未开启

2、SSH服务开启，且设置了变量Banner的值，并且Banner对应的文件不为空。

二者满足其一则合规，否则不合规。

## 原始结果

ssh\_banner=`cat /etc/ssh/sshd\_config | grep -v '^[[:space:]]\*#' | grep -i Banner|awk '{print $2}'`;

ssh\_status=`netstat -antp|grep -i listen|grep ":22\>"|wc -l`;

if ([ "$ssh\_status" != 0 ] && [ -s "$ssh\_banner" ]);

then

echo "sshd is running.sshd banner is not null.sshd banner check result:true";

else

if [ "$ssh\_status" != 0 ];

then

echo "sshd is running.sshd banner is null.sshd banner check result:false";

else

echo "sshd is not running.sshd banner check result:true";

fi;

fi;

unset ssh\_banner ssh\_status;

sshd is not running.sshd banner check result:true

## 操作方法

参考配置操作

1、如果此项检查不合规，执行以下步骤进行修复。

执行如下命令创建ssh banner信息文件：

#touch /etc/ssh\_banner

#chown bin:bin /etc/ssh\_banner

#chmod 644 /etc/ssh\_banner

#echo " Authorized only. All activity will be monitored and reported " > /etc/ssh\_banner

可根据实际需要修改该文件的内容。

2、修改/etc/ssh/sshd\_config文件，添加如下行：

Banner /etc/ssh\_banner

3、重启sshd服务:

#/etc/init.d/sshd restart

# 配置NFS服务限制

## 判断依据

检测方法

1、查看系统是否存在如下NFS守护进程:rpc.lockd， rpc.nfsd， rpc.statd， rpc.mountd

2、查看NFS服务状态：

# chkconfig --list |grep nfs

nfs 0:off 1:off 2:off 3:off 4:off 5:off 6:off

nfslock 0:off 1:off 2:off 3:on 4:on 5:on 6:off

3、查看是否对NFS服务访问做限制：

#more /etc/hosts.allow

#more /etc/hosts.deny

判定依据

1、不存在与NFS有关的守护进程

2、如果存在NFS守护进程，但/etc/hosts.allow设置了允许访问nfs的远程地址且/etc/hosts.deny设置了拒绝所有访问NFS的远程地址。

二者满足其中之一则合规，否则不合规。

## 原始结果

ps -ef |egrep "nfs|rpc.mountd|rpc.nfsd|rpc.lockd|rpc.statd"|egrep -v "egrep|grep"|grep -v kblockd

NFSSTATUS=`ps -ef |egrep "nfs|rpc.mountd|rpc.nfsd|rpc.lockd|rpc.statd"|egrep -v "egrep|grep"|grep -v kblockd|wc -l`

NFSAllowNo=`egrep -i "nfs" /etc/hosts.allow |sed '/^#/d'|sed '/^$/d'|wc -l`

NFSDenyNo=`egrep -i "nfs:all|all:all" /etc/hosts.deny |sed '/^#/d'|sed '/^$/d'|wc -l`

if [ $NFSSTATUS = 0 ];

then

echo "NFS daemon not running";

else

if ([ $NFSAllowNo != 0 ] && [ $NFSDenyNo != 0 ])

then

echo "NFS daemon running.check result:true";

else

echo "NFS daemon running.check result:false";

fi;

fi;

unset NFSSTATUS NFSAllowNo;

rpcuser 3886 1 0 Nov15 ? 00:00:00 rpc.statd

NFS daemon running.check result:false

## 操作方法

参考配置操作

1、杀掉如下NFS进程：rpc.lockd， rpc.nfsd， rpc.statd， rpc.mountd

2、禁用NFS

#chkconfig --level 235 nfs off

3、如需要nfs服务,设置限制能够访问NFS服务的IP范围：

编辑文件/etc/hosts.allow增加一行：

nfs:允许访问的IP

编辑文件/etc/hosts.deny增加一行：

nfs:all或者all:all

# 配置NTP

## 判断依据

检测方法

1、检查时间服务是否开启

（1）在Redhat5/6系统及SUSE9/10/11系统查看NTP服务是否开启

#ps -ef|grep ntpd

（2）在Redhat7系统上查看chrony服务是否开启

#ps -ef|grep chronyd

2、查看配置文件是否配置时间同步服务器

（1）在Redhat5/6系统及SUSE9/10/11系统查看/etc/ntp.conf文件

#cat /etc/ntp.conf|grep "^server"

（2）在Redhat7系统上查看/etc/chrony.conf文件

#cat /etc/chrony.conf|grep "^server"

判定依据

1、时间服务进程存在

2、相应配置文件里时间同步服务器配置存在

1和2同时满足则合规；否则不合规。

## 原始结果

redhat\_version=`cat /etc/redhat-release 2>/dev/null|awk -F"release" '{print $2}'|awk -F\. '{print $1}'|sed 's/\s\*//g'|awk -F. '{print$1}'`

suse\_version=`cat /etc/SuSE-release 2>/dev/null|grep -i "VERSION"|awk -F'=' '{print $2}'|sed 's/[[:space:]]//g'|awk -F. '{print$1}'`

if [ -n "$suse\_version" ] || [ "$redhat\_version" -lt 7 ];then

if [ -n "`ps -ef|grep ntp|grep -v grep`" ];then

echo "Process is running";

grep "^server" /etc/ntp.conf|grep -v "127.127.1.0"|grep -v "127.0.0.1";

echo "ntpserver1="`grep "^server" /etc/ntp.conf|grep -v "127.127.1.0"|grep -v "127.0.0.1"|wc -l`;

else

echo "Process is not running";

crontab -l 2>/dev/null|grep -v "^#"|grep ntp;

echo "ntpserver2="`crontab -l 2>/dev/null|grep -v "^#"|grep ntp|wc -l`;

fi

elif [ "$redhat\_version" -eq 7 ];then

if [ -n "`ps -ef|grep chrony|grep -v grep`" ];then

echo "Process is running"

grep "^server" /etc/chrony.conf|grep -v "127.127.1.0"|grep -v "127.0.0.1";

echo "ntpserver1="`grep "^server" /etc/chrony.conf|grep -v "127.127.1.0"|grep -v "127.0.0.1"|wc -l`;

else

echo "Process is not running"

crontab -l 2>/dev/null|grep -v "^#"|grep ntp;

echo "ntpserver2="`crontab -l 2>/dev/null|grep -v "^#"|grep ntp|wc -l`;

fi

fi

unset redhat\_version suse\_version

Process is running

server 192.168.10.24 prefer

server 192.168.10.25

ntpserver1=2

## 操作方法

参考配置操作

1、配置时间同步服务器

（1）Redhat5/6和SUSE9/10/11系统

文件备份：

#cp /etc/ntp.conf /etc/ntp.conf.bak

编辑/etc/ntp.conf文件

#vi /etc/ntp.conf

添加内容：

server [时间服务器域名或IP]

（2）Redhat7系统

文件备份：

#cp /etc/chrony.conf /etc/chrony.conf.bak

编辑/etc/chrony.conf文件

#vi /etc/chrony.conf

添加内容：

server [时间服务器域名或IP]

2、开启时间服务

（1）Redhat5/6系统

#/etc/init.d/ntpd start

（2）Redhat7系统

#systemctl start chronyd.service

（3）SUSE9系统

#/etc/init.d/xntpd start

（4）SUSE10/11系统

#/etc/init.d/ntp start

# 修改FTP的Banner信息

## 判断依据

检测方法

1、如果是vsftp服务器，查看如下配置文件/etc/vsftpd.conf(或者/etc/vsftpd/vsftpd.conf)。

2、如果是pure-ftp服务器，查看如下配置文件pure-ftpd.conf。

3、如果是wu-ftp服务器，查看如下配置文件ftpaccess。

4、如果是proftpd服务器，查看如下配置文件proftpd.conf。

判定依据

1、FTP进程不存在

2、vsftp服务器，查看/etc/vsftpd.conf(/etc/vsftpd/vsftpd.conf)是否存在如下内容：

ftpd\_banner=” Authorized users only. All activity may be monitored and reported.”

3、wu-ftp服务器，如果ftpaccess文件中存在类似如下内容：

banner /etc/ftpd/banner.msg

且/etc/ftpd/banner.msg内容非空。

4、pure-ftp服务器，查看pure-ftpd.conf文件中是否存在如下内容：

FortunesFile <file>

且<file>内容非空。

5、proftpd服务器，查看proftpd.conf文件中是否存在如下内容：

DisplayConnect <file>

且<file>内容为非空。

以上5个条件满足其一则合规，否则不合规

## 原始结果

FTPSTATUS=`ps -ef|grep ftpd|grep -v grep|wc -l`

Check\_ftp ()

{

if [ -f /etc/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd.conf";

else

if [ -f /etc/vsftpd/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd/vsftpd.conf";

fi;

fi;

if [ -f "$FTPCONF" ]

then

if [ `grep -v "^[[:space:]]\*#" $FTPCONF|grep -i "ftpd\_banner"|wc -l` -ne 0 ];

then

echo "vsftpd is running.Banner in $FTPCONF is recommended.FTP check result:true";

else

echo "vsftpd is running.Banner in $FTPCONF is not recommended.FTP check result:false";

fi;

fi;

if [ -f /etc/pure-ftpd/pure-ftpd.conf ];

then

if [ `cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "FortunesFile"|wc -l` -eq 0 ]

then

echo "pure-ftpd is running.banner in pure-ftpd.conf is not recommended.FTP check result:false.";

else

if [ -s "`cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "FortunesFile"|awk '{print $2}'`" ];

then

echo "pure-ftpd is running.Banner in pure-ftpd.conf is recommended.FTP check result:true.";

else

echo "pure-ftpd is running.Banner in pure-ftpd.conf is not recommended.FTP check result:false.";

fi;

fi;

else

if [ -f /etc/pure-ftpd.conf ]

then

if [ `cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "FortunesFile"|wc -l` -eq 0 ]

then

echo "pure-ftpd is running.banner in pure-ftpd.conf is not recommended.FTP check result:false.";

else

if [ -s "`cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "FortunesFile"|awk '{print $2}'`" ];

then

echo "pure-ftpd is running.Banner in pure-ftpd.conf is recommended.FTP check result:true.";

else

echo "pure-ftpd is running.Banner in pure-ftpd.conf is not recommended.FTP check result:false.";

fi;

fi

fi;

fi;

if [ -f /etc/ftpaccess ];

then

if [ `cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*banner"|wc -l` -eq 0 ]

then

echo "wu-ftpd is running.banner in wu-ftpd.conf is not recommended.FTP check result:false.";

else

if [ -s "`cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*banner"|awk '{print $2}'`" ];

then

echo "wu-ftpd is running.Banner in wu-ftpd.conf is recommended.FTP check result:true.";

else

echo "wu-ftpd is running.Banner in wu-ftpd.conf is not recommended.FTP check result:false.";

fi;

fi;

else

if [ -f /etc/ftpd/ftpaccess ]

then

if [ `cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*banner"|wc -l` -eq 0 ]

then

echo "wu-ftpd is running.banner in wu-ftpd.conf is not recommended.FTP check result:false.";

else

if [ -s "`cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*banner"|awk '{print $2}'`" ];

then

echo "wu-ftpd is running.Banner in wu-ftpd.conf is recommended.FTP check result:true.";

else

echo "wu-ftpd is running.Banner in wu-ftpd.conf is not recommended.FTP check result:false.";

fi;

fi;

fi;

fi;

if [ -f /etc/proftpd.conf ];

then

if [ -s "`cat /etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed '/<Anonymous.\*>/,/<\/Anonymous>/d'|grep -i "DisplayConnect"|awk '{print $2}'`" ]

then

echo "proftpd is running.banner in proftpd.conf is recommended.FTP check result:true.";

else

echo "proftpd is running.banner in proftpd.conf is not recommended.FTP check result:false.";

fi;

else

if [ -f /etc/proftpd/proftpd.conf ];

then

if [ -s "`cat /etc/proftpd/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed '/<Anonymous.\*>/,/<\/Anonymous>/d'|grep -i "DisplayConnect"|awk '{print $2}'`" ]

then

echo "proftpd is running.banner in proftpd.conf is recommended.FTP check result:true.";

else

echo "proftpd is running.banner in proftpd.conf is not recommended.FTP check result:false.";

fi;

else

if [ -f /usr/local/proftpd/etc/proftpd.conf ]

then

if [ -s "`cat /usr/local/proftpd/etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed '/<Anonymous.\*>/,/<\/Anonymous>/d'|grep -i "DisplayConnect"|awk '{print $2}'`" ]

then

echo "proftpd is running.banner in proftpd.conf is recommended.FTP check result:true.";

else

echo "proftpd is running.banner in proftpd.conf is not recommended.FTP check result:false.";

fi;

fi;

fi;

fi;

unset FTPCONF;

}

if [ $FTPSTATUS -eq 0 ];

then

echo "FTP is not running.FTP check result:true"

else

Check\_ftp;

fi;

unset FTPSTATUS;

FTP is not running.FTP check result:true

## 操作方法

参考配置操作

1、vsftp

修改vsftp回显信息

#vi /etc/vsftpd.conf (或者/etc/vsftpd/vsftpd.conf)

修改ftpd\_banner的值为ftpd\_banner=” Authorized users only. All activity may be monitored and reported.”

可根据实际需要修改该文件内容

2、pure-ftp

修改Pure-FTP回显信息Pure-ftp回显信息分为两种：

自带回显信息：

Pure-ftp自带回显信息没法通过更改配置来更改，只能在安装的时候选择withoutbanner选项去掉自带BANNER信息。

自定义回显信息:Pure-ftp还有自定义回显信息，配置方法如下：

(1)、修改pure-ftp配置文件：

#vi /etc/pure-ftpd/pure-ftpd.conf找到以下行，确保该行未被注释。

FortunesFile <file>

(2)、编辑/usr/share/fortune/zippy文件(如没有fortune文件夹或者zippy文件，则新建该文件夹或该文件):

#vi /usr/share/fortune/zippy将自定义BANNER写入其中。

3、wu-ftp

(1)、#vi /etc/ftpd/ftpaccess(/etc/ftpaccess)，找到以下行，确保该行未被注释：

banner /etc/ftpd/banner.msg

(2)、编辑文件/etc/ftpd/banner.msg(如果没有则新建):

#vi /etc/ftpd/banner.msg将自定义BANNER写入其中。

4、proftpd

(1)、#vi /usr/local/etc/proftpd.conf找到以下行，查看Banner信息文件是否存在：

DisplayConnect <file> #Banner信息文件

(2)、如果Banner文件不存在则新建：

#touch <file>

#vi <file> #编辑该文件并添加自定义Banner信息

5、重启FTP服务

# 修改SNMP的默认Community

## 判断依据

检测方法

1、查看snmpd服务状态：

#chkconfig snmpd

2、查看SNMP共同体字符串配置：

（1）、SUSE9：

#cat /etc/snmpd.conf

（2）、SUSE 10：

#cat /etc/snmp/snmpd.conf

（3）、linux：

#cat /etc/snmp/snmpd.conf

判定依据

1、SNMP服务未开启

2、SNMP服务开启，且修改了默认团体名称

两个条件满足其中一个则合规，否则不合规。

## 原始结果

SNMPD\_STATUS=`ps -ef|grep snmpd|egrep -v "grep"|wc -l`;

Check\_SNMPD ()

{

if [ -f /etc/snmp/snmpd.conf ];

then SNMPD\_CONF=/etc/snmp/snmpd.conf;

else SNMPD\_CONF=/etc/snmpd.conf;

fi;

grep -v "^#" $SNMPD\_CONF|egrep "community";

if [ `grep -v "^#" $SNMPD\_CONF|egrep "rocommunity|rwcommunity"|egrep "public|private"|wc -l` -eq 0 ];

then echo "SNMPD is running.SNMP check result:true";

else echo "SNMPD is running.SNMP check result:false";

fi;

}

if [ "$SNMPD\_STATUS" -ge 1 ];

then Check\_SNMPD;

else echo "SNMPD is not running.SNMP check result:true";

fi

unset SNMPD\_STATUS SNMPD\_CONF;

SNMPD is not running.SNMP check result:true

## 操作方法

参考配置操作

1、SUSE 9步骤：

（1）、修改snmp配置文件 /etc/snmpd.conf找到以rocommunity或rwcommunity开头的行，如:rocommunity public 127.0.0.1其中的第二个字段(public)即为团体名，用新的团体名称替换该字段:rocommunity community\_name 127.0.0.1

（2）、重启snmp服务：

#rcsnmpd restartb

2、SUSE 10\linux步骤

（1）、修改snmp配置文件/etc/snmp/snmpd.conf找到以rocommunity或rwcommunity开头的行，如:rocommunity public 127.0.0.1其中的第二个字段(public)即为团体名，用新的团体名称替换该字段：

rocommunity community\_name 127.0.0.1

（2）、重启snmp服务：

#service snmpd restart

# 用户FTP访问安全配置

## 判断依据

检测方法

1、如果是vsftp服务器,查看如下配置文件/etc/vsftpd.conf(或者/etc/vsftpd/vsftpd.conf)。

2、如果是pure-ftp服务器,查看如下配置文件pure-ftpd.conf。

3、如果是wu-ftp服务器,查看如下配置文件ftpaccess。

4、如果是proftp服务器,查看如下配置文件proftpd.conf。

判定依据

1、FTP进程不存在。

2、vsftp服务器，查看/etc/vsftpd.conf(/etc/vsftpd/vsftpd.conf)是否存在如下内容:

ls\_recurse\_enable=YES

local\_umask=022 //设置用户上传文件的属性为755

anon\_umask=022 //匿名用户上传文件(包括目录)的 umask

3、proftp服务器，查看proftpd.conf是否存在如下内容：

Umask 022

4、wu-ftp服务器，如果ftpaccess文件中存在类似如下内容：

upload /home/ftpd /incoming yes real guest anonymous 0644 dirs

其文件上载权限必须为0644

5、pure-ftp服务器，查看pure-ftpd.conf文件中是否存在如下配置：

Umask 177:077

以上5个条件满足其一则合规，否则不合规。

## 原始数据

FTPSTATUS=`ps -ef|grep ftpd|grep -v grep|wc -l`;

Check\_ftp ()

{

if [ -f /etc/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd.conf";

else

if [ -f /etc/vsftpd/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd/vsftpd.conf";

fi;

fi;

if [ -f "$FTPCONF" ]

then

cat $FTPCONF|grep -v "^[[:space:]]\*#"|grep "ls\_recurse\_enable";

cat $FTPCONF|grep -v "^[[:space:]]\*#"|grep "local\_umask";

cat $FTPCONF|grep -v "^[[:space:]]\*#"|grep "anon\_umask";

fi;

if [ -f /etc/pure-ftpd/pure-ftpd.conf ];

then

echo "pureftp\_umask="`cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*Umask"`;

else

if [ -f /etc/pure-ftpd.conf ]

then

echo "pureftp\_umask="`cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*Umask"`;

fi;

fi;

if [ -f /etc/proftpd.conf ];

then

echo "proftp\_umask="`cat /etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*Umask"`;

else

if [ -f /etc/proftpd/proftpd.conf ];

then

echo "proftp\_umask="`cat /etc/proftpd/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*Umask"`;

else

if [ -f /usr/local/proftpd/etc/proftpd.conf ];

then

echo "proftp\_umask="`cat /usr/local/proftpd/etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*Umask"`;

fi;

fi;

fi;

if [ -f /etc/ftpaccess ];

then

cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*upload";

else

if [ -f /etc/ftpd/ftpaccess ]

then

cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "^[[:space:]]\*upload";

fi;

fi;

unset FTPCONF;

}

if [ $FTPSTATUS -eq 0 ];

then echo "FTP is not running.FTP check result:true.";

else

Check\_ftp;

fi

unset FTPSTATUS;

FTP is not running.FTP check result:true.

## 操作方法

参考配置操作

1、vsftp

修改/etc/vsftpd.conf(或者为/etc/vsftpd/vsftpd.conf)，确保以下行未被注释掉，如果没有该行，请添加:

ls\_recurse\_enable=YES

local\_umask=022 //设置用户上传文件的属性为755

anon\_umask=022 //匿名用户上传文件(包括目录)的 umask

2、pure-ftp

编辑配置文件pure-ftpd.conf，查看是否存在如下设置

Umask 177:077 #此权限限制比较苛刻，如果配置后影响使用请通过系统自定义策略参数修改其值为133:022

3、proftp

编辑配置文件proftpd.conf，查看是否存在如下配置

Umask 022

4、wu-ftp

编辑配置文件ftpaccess，如果文件中存在类似如下配置:

upload /home/ftpd /incoming yes real guest anonymous 0644 dirs

确保其上载的文件权限为0644

5、重启FTP服务器

# 关闭不必要启动项

## 判断依据

检测方法

以下脚本如果以S开头，需要修改:lp|rpc|snmpdx|keyserv|nscd|Volmgt|uucp|dmi|sendmail|autoinstall

使用命令检查/etc/rc2.d、/etc/rc3.d、/etc/rc4.d、/etc/rc5.d目录下的所有"S"打头的脚本文件，将以上启动不必要服务的脚本文件改名确认新文件名不以"S"打头。

# ls /etc/rc2.d/\* /etc/rc3.d/\* /etc/rc4.d/\* /etc/rc5.d/\*|egrep "lp|rpc|snmpdx|keyserv|nscd|Volmgt|uucp|dmi|sendmail|autoinstall"|grep "^S\*"

判定依据

系统中不存以上名称以S开头的脚本文件则合规，否则不合规。

## 原始结果

ls /etc/rc2.d/\* /etc/rc3.d/\* /etc/rc4.d/\* /etc/rc5.d/\* 2>/dev/null|egrep "lp|rpc|snmpdx|keyserv|nscd|Volmgt|uucp|dmi|sendmail|autoinstall"|grep "^S"

echo "result="` ls /etc/rc2.d/\* /etc/rc3.d/\* /etc/rc4.d/\* /etc/rc5.d/\* 2>/dev/null|egrep "lp|rpc|snmpdx|keyserv|nscd|Volmgt|uucp|dmi|sendmail|autoinstall"|grep "^S"|wc -l`

result=0

## 操作方法

参考配置操作

此项扫描不合规，请将那些启动不必要服务的脚本文件改名，确认新文件名不以"S"打头，修改前切记要进行备份。

# 禁止root用户登录FTP

## 判断依据

检测方法

1、如果是vsftp服务器，查看如下配置文件/etc/pam.d/vsftpd、/etc/vsftpd/vsftpd.conf(/etc/vsftpd.conf)。

2、如果是pure-ftp服务器，查看如下配置文件pure-ftpd.conf。

3、如果是wu-ftp服务器，查看如下配置文件/etc/ftpd/ftpusers(/etc/ftpusers)。

4、如果是proftp服务器，查看如下配置文件proftpd.conf。

判定依据

1、FTP进程不存在

2、vsftp服务器，/etc/pam.d/vsftpd中指定了ftpusers，且对应的ftpusers中存在root用户或者在配置文件/etc/vsftpd/vsftpd.conf(/etc/vsftpd.conf)配置了userlist\_enable=YES、userlist\_deny=NO、userlist\_file=<file path>，且<file path>中不存在root用户。

3、pure-ftp服务器，pure-ftpd.conf文件中设置了MinUID 100，限制了uid<=100的用户登录FTP。

4、wu-ftp服务器，/etc/ftpd/ftpusers(/etc/ftpusers)文件中存在root用户。

5、proftp服务器，proftpd.conf文件中不存在如下配置：

RootLogin on

以上五个条件满足其一则合规，否则不合规。

## 原始结果

FTPSTATUS=`ps -ef|grep ftpd|grep -v "grep ftpd"|wc -l`;

Check\_ftp2 ()

{

if [ -f /etc/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd.conf";

FTPUSER=`cat $FTPCONF|grep -v "^#"|grep userlist\_file|cut -d= -f2`;

Check\_vsftpconf;

else

if [ -f /etc/vsftpd/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd/vsftpd.conf";

FTPUSER=`cat $FTPCONF|grep -v "^#"|grep userlist\_file|cut -d= -f2`;

Check\_vsftpconf;

fi;

fi;

}

Check\_vsftpconf ()

{

userlist\_enable=`grep -v "^#" $FTPCONF|grep -i "userlist\_enable=YES"|wc -l`;

userlist\_deny=`grep -v "^#" $FTPCONF|grep -i "userlist\_deny=NO"|wc -l`;

if [ $userlist\_enable = 1 -a $userlist\_deny = 1 ];

then

if [ -n "$FTPUSER" ]

then

if [ `grep -v "^#" $FTPUSER|egrep "^root$"|wc -l` = 0 ];

then

echo "FTP is running.FTP user config $ftpusers\_pam is not recommended.FTP user config "$FTPUSER" is recommended.FTP check result:true";

else

echo "FTP is running.FTP user config $ftpusers\_pam is not recommended.FTP user config "$FTPUSER" is not recommended.FTP check result:false";

fi;

else

echo "FTP is running.FTP user config $ftpusers\_pam is not recommended.FTP user config "$FTPUSER" does not exist.FTP check result:false";

fi;

else

echo "FTP is running.FTP user config $ftpusers\_pam is not recommended.userlist\_enable and userlist\_deny is not recommended.FTP check result:false";

fi;

}

Check\_ftp1 ()

{

if [ -f /etc/pam.d/vsftpd ];

then

ftpusers\_pam=`grep "file" /etc/pam.d/vsftpd|egrep -v "^#"|sed 's/^.\*file=//g'|awk '{print $1}'`

if [ -n "$ftpusers\_pam" ]

then

if [ `grep -v "^#" $ftpusers\_pam|egrep "^root$"|wc -l` -ge 1 ];

then

echo "FTP is running.FTP user config $ftpusers\_pam is recommended.FTP check result:true";

else

Check\_ftp2;

fi

else

Check\_ftp2;

fi

else

echo "/etc/pam.d/vsftpd is not exist,scripts exit now";

Check\_ftp2;

fi

if [ -f /etc/proftpd.conf ];

then

if [ `cat /etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "RootLogin[[:space:]]\*on|wc -l` -eq 0 ]

then

echo "proftpd is running.FTP check result:true";

else

echo "proftpd is running.FTP check result:false";

fi;

else

if [ -f /etc/proftpd/proftpd.conf ];

then

if [ `cat /etc/proftpd/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "RootLogin[[:space:]]\*on|wc -l` -eq 0 ]

then

echo "proftpd is running.FTP check result:true";

else

echo "proftpd is running.FTP check result:false";

fi;

else

if [ -f /usr/local/proftpd/etc/proftpd.conf ];

then

if [ `cat /usr/local/proftpd/etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "RootLogin[[:space:]]\*on|wc -l` -eq 0 ]

then

echo "proftpd is running.FTP check result:true";

else

echo "proftpd is running.FTP check result:false";

fi;

fi;

fi;

fi;

if [ -f /etc/ftpusers ];

then

echo "wu-ftp\_users="`cat /etc/ftpusers|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^root"`;

else

if [ -f /etc/ftpd/ftpusers ];

then

echo "wu-ftp\_users="`cat /etc/ftpd/ftpusers|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^root"`;

fi;

fi;

if [ -f /etc/pure-ftpd/pure-ftpd.conf ];

then

cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "MinUID";

else

if [ -f /etc/pure-ftpd.conf ];

then

cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "MinUID";

fi;

fi;

}

if [ $FTPSTATUS -eq 0 ];

then echo "FTP is not running.FTP check result:true";

else Check\_ftp1;

fi

unset FTPSTATUS FTPCONF FTPUSER ftpusers\_pam

FTP is not running.FTP check result:true

## 操作方法

参考配置操作

1、vsftp

（1）、修改ftpusers文件，增加不能通过FTP登录的用户

1）、首先需确定ftpusers文件位置，可以通过以下命令知道

#cat /etc/pam.d/vsftpd

auth required pam\_listfile.so item=user sense=deny file=/etc/vsftpd.ftpusers onerr=succeed

#其中file=/etc/vsftpd/ftpusers即为当前系统上的ftpusers文件.

2）、修改file对应的文件在文件中增加以下用户，则该用户均不允许通过FTP登录(每隔用户占一行):

root

daemon

bin

sys

adm

lp

uucp

nuucp

listen

nobody

noaccess

nobody4

（2）、配置vsftpd.conf文件，设定只允许特定用户通过FTP登录:

1）、vsftpd.conf文件路径一般为/etc/vsftpd.conf或者/etc/vsftpd/vsftpd.conf。

修改其中内容：

userlist\_enable=YES #此选项被激活后，VSFTPD将读取userlist\_file参数所指定的文件中的用户列表。

userlist\_deny=NO #决定禁止还是只允许由userlist\_file指定文件中的用户登录FTP服务器，YES默认值，禁止文件中的用户登录，同时也不向这些用户发出输入口令的提示，NO只允许在文件中的用户登录FTP服务器.

userlist\_file=/etc/vsftpd/user\_list

2）、编辑userlist\_file对应的文件去掉root.

2、wu-ftp

编辑/etc/ftpusers或者/etc/ftpd/ftpusers，在文件中另取一行录入root，例如：

root

venustech

说明:ftpusers文件中用户将禁止登录FTP

3、proftp

编辑配置文件proftpd.conf，在文件中查看是否存在如下内容，存在则将其注释掉：

RootLogin on

4、pure-ftp

编辑配置文件pure-ftpd.conf，在文件中查看是否存在如下内容，没有则新增:

MinUID 100 #即禁止uid<=100的用户登录FTP

5、重启FTP服务

# 限制FTP用户登录后能访问的目录

## 判断依据

检测方法

1、如果是vsftp服务器，查看如下配置文件/etc/vsftpd.conf(或者/etc/vsftpd/vsftpd.conf)。

2、如果是pure-ftp服务器，查看如下配置文件pure-ftpd.conf。

3、如果是wu-ftp服务器，查看如下配置文件ftpaccess。

4、如果是proftp服务器，查看如下配置文件proftpd.conf。

判定依据

1、FTP进程不存在

2、vsftp服务器,配置文件中存在如下内容：

chroot\_list\_enable=YES

chroot\_local\_user=NO

chroot\_list\_file=/etc/vsftpd/chroot\_list

3、pure-ftp服务器，配置文件中存在ChrootEveryone的值为yes

4、proftp服务器，配置文件中存在DefaultRoot ~.

5、wu-ftp服务器，配置文件中存在restricted-uid \*

以上四个条件满足其一则合规，否则不合规。

## 原始结果

FTPSTATUS=`ps -ef|grep -v grep|grep -i ftpd|wc -l`

Check\_ftp ()

{

if [ -f /etc/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd.conf";

else

if [ -f /etc/vsftpd/vsftpd.conf ];

then

FTPCONF="/etc/vsftpd/vsftpd.conf";

fi;

fi;

if [ -f "$FTPCONF" ];

then

if ([ `grep -v "^#" $FTPCONF|grep -i "chroot\_list\_enable=YES"|wc -l` -eq 1 ] && [ `grep -v "^#" /etc/vsftpd/vsftpd.conf|grep -i "chroot\_local\_user=YES"|wc -l` -eq 0 ]);

then

if [ -s "`grep -v "^#" /etc/vsftpd/vsftpd.conf|grep -i "chroot\_list\_file"|cut -d\= -f2`" ]

then

echo "FTP is running.FTP check result:true"

else

echo "FTP is running.FTP check result:false"

fi

else

echo "FTP is running.FTP check result:false"

fi

fi

if [ -f /etc/pure-ftpd/pure-ftpd.conf ];

then

cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "ChrootEveryone";

else

if [ -f /etc/pure-ftpd.conf ];

then

cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "ChrootEveryone";

fi;

fi;

if [ -f /etc/proftpd.conf ];

then

cat /etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "DefaultRoot";

else

if [ -f /etc/proftpd/proftpd.conf ];

then

cat /etc/proftpd/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "DefaultRoot";

else

if [ -f /usr/local/proftpd/etc/proftpd.conf ];

then

cat /usr/local/proftpd/etc/proftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|egrep -i "DefaultRoot";

fi;

fi;

fi;

if [ -f /etc/ftpaccess ];

then

cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "restricted-uid";

else

if [ -f /etc/ftpd/ftpaccess ];

then

cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "restricted-uid";

fi;

fi;

unset FTPCONF;

}

if [ $FTPSTATUS -eq 0 ];

then

echo "FTP is not running.FTP check result:true";

else

Check\_ftp;

fi

unset FTPSTATUS;

FTP is not running.FTP check result:true

## 操作方法

参考配置操作

1、vsftp

（1）、编辑文件/etc/vsftpd.conf或/etc/vsftpd/vsftpd.conf

如果存在chroot\_list\_enable，去掉前面的注释符，修改其值等于YES。不存在则手工增加一行：

chroot\_list\_enable=YES

注释掉chroot\_local\_user或者修改其值等于NO。

如果存在chroot\_list\_file，去掉前面的注释符，不存在则手工增加一行，例如:

chroot\_list\_file=/etc/vsftpd/chroot\_list

（2）、创建chroot\_list\_file对应的文件

例如:

#touch /etc/vsftpd/chroot\_list

#chmod 750 /etc/vsftpd/chroot\_list

（3）、在文件/etc/vsftpd/chroot\_list里添加用户，里面的用户登录后，只能活动在其家目录，无法切换目录，每个用户占一行。例如:

test

test1

2、pure-ftp

编辑配置文件pure-ftpd.conf，在文件中找到如下行，修改ChrootEveryone的值为yes(没有则添加)

ChrootEveryone yes #启用chroot，所有用户登录后，只能在自己的家目录里活动。

3、wu-ftp

编辑配置文件ftpaccess，如果文件中存在类似如下行:

restricted-uid \* #为\*代表所有用户，也可以为具体的用户名。

4、proftp

编辑配置文件proftpd.conf，查看文件中是否存在如下行:

DefaultRoot ~ #将用户限制在自己的目录下

或者

DefaultRoot ~ group1,!group2 #将用户限制在自己的目录下，对group1有效，对group2无效。

5、重启FTP服务

# 关闭不必要的服务和端口

## 判断依据

检测方法

1、查看服务列表：

（1）redhat7以下及SUSE系统执行以下命令查看服务列表：

#chkconfig --list

（2）redhat7执行以下命令查看服务列表：

#systemctl |grep active

查看所有服务的开启关闭列表检查基本的网络服务的开启或禁止情况，根据实际情况关闭不必要的服务。

2、查看开放的端口列表：

#netstat -an

3、编辑文件/etc/service，查看服务与端口对应表 。

判定依据

手工判断

## 原始结果

if [[ `cat /etc/redhat-release 2>/dev/null|cut -b 22` -eq 7 ]] || [[ `cat /etc/redhat-release 2>/dev/null|cut -b 41` -eq 7 ]];then

systemctl|grep active

else

chkconfig --list

fi

netstat -an|awk '{if( $2==0 ){print$0}}'

NetworkManager 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

abrt-ccpp 0:关闭 1:关闭 2:关闭 3:启用 4:关闭 5:启用 6:关闭

abrtd 0:关闭 1:关闭 2:关闭 3:启用 4:关闭 5:启用 6:关闭

acpid 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

atd 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

auditd 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

autofs 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

blk-availability 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭

bluetooth 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

certmonger 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

cpuspeed 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭

crond 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

cups 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

dnsmasq 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

firstboot 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

haldaemon 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

htcacheclean 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

httpd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

ip6tables 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

iptables 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

irqbalance 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

kdump 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

lvm2-monitor 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭

mdmonitor 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

messagebus 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

netconsole 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

netfs 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

network 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

nfs 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

nfs-rdma 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

nfslock 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

ntpd 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

ntpdate 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

oddjobd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

portreserve 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

postfix 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

pppoe-server 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

psacct 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

quota\_nld 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

rdisc 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

rdma 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

restorecond 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

rngd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

rpcbind 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

rpcgssd 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭

rpcsvcgssd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

rsyslog 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

saslauthd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

smartd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

spice-vdagentd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:启用 6:关闭

sshd 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

sssd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

sysstat 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭

udev-post 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭

wdaemon 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

winbind 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

wpa\_supplicant 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

ypbind 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

tcp 0 0 0.0.0.0:59230 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:23456 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN

tcp 0 0 127.0.0.1:631 0.0.0.0:\* LISTEN

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN

tcp 0 0 192.168.10.2:37823 192.168.10.24:23456 ESTABLISHED

tcp 0 0 192.168.10.2:23456 192.168.10.25:40487 ESTABLISHED

tcp 0 0 192.168.10.2:52983 192.168.10.6:23456 ESTABLISHED

tcp 0 0 192.168.10.2:23456 192.168.10.6:50133 ESTABLISHED

tcp 0 0 :::23456 :::\* LISTEN

tcp 0 0 :::2181 :::\* LISTEN

tcp 0 0 :::59853 :::\* LISTEN

tcp 0 0 :::111 :::\* LISTEN

tcp 0 0 ::ffff:192.168.10.2:3888 :::\* LISTEN

tcp 0 0 ::1:631 :::\* LISTEN

tcp 0 0 :::60568 :::\* LISTEN

tcp 0 0 ::1:25 :::\* LISTEN

tcp 0 0 ::ffff:192.168.10.2:3888 ::ffff:192.168.10.3:33594 ESTABLISHED

tcp 0 0 ::ffff:192.168.10.2:51799 ::ffff:192.168.10.3:2888 ESTABLISHED

udp 0 0 0.0.0.0:53794 0.0.0.0:\*

udp 0 0 127.0.0.1:703 0.0.0.0:\*

udp 0 0 0.0.0.0:111 0.0.0.0:\*

udp 0 0 0.0.0.0:627 0.0.0.0:\*

udp 0 0 0.0.0.0:631 0.0.0.0:\*

udp 0 0 192.168.10.2:123 0.0.0.0:\*

udp 0 0 172.31.6.170:123 0.0.0.0:\*

udp 0 0 127.0.0.1:123 0.0.0.0:\*

udp 0 0 0.0.0.0:123 0.0.0.0:\*

udp 0 0 :::39234 :::\*

udp 0 0 :::111 :::\*

udp 0 0 :::627 :::\*

udp 0 0 fe80::9618:82ff:fe74:ff9:123 :::\*

udp 0 0 fe80::9618:82ff:fe74:ff9:123 :::\*

udp 0 0 ::1:123 :::\*

udp 0 0 :::123 :::\*

## 操作方法

参考配置操作

1、禁止非必要服务

（1）redhat7以下版本及SUSE系统

#/etc/init.d/[service] stop

#chkconfig [service] off

（2）redhat7版本

#systemctl stop [service]

#systemctl disable [service]

2、编辑文件 /etc/services

在文件中找到对应服务的端口，注释掉改行内容。

# 禁止匿名FTP

## 判断依据

检测步骤:

一、如果是vsftp服务器,查看如下配置文件/etc/vsftpd.conf(或者/etc/vsftpd/vsftpd.conf).

二、如果是pure-ftp服务器,查看如下配置文件pure-ftpd.conf.

三、如果是wu-ftp服务器,查看如下配置文件ftpaccess.

四、如果是proftp服务器,查看如下配置文件proftpd.conf.

判定条件:

1)ftp进程不存在

2)vsftp服务器,配置文件中存在anonymous\_enable的值为NO

3)pure-ftp服务器,配置文件中存在NoAnonymous的值为yes

4)proftp服务器,配置文件中将匿名用户配置注释掉或者匿名用户配置中存在AnonRequirePassword的值为on.

5)wu-ftp服务器,配置文件中不存在class <class\_name> [guest|anonymous] <ip\_address>

以上四个条件满足其一则合规,否则不合规

## 原始结果

if [ `ps -ef|grep ftpd|grep -v "grep"|wc -l` -ge 1 ];

then

if [ -f /etc/vsftpd.conf ];

then

cat /etc/vsftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "anonymous\_enable";

else

if [ -f /etc/vsftpd/vsftpd.conf ];

then

cat /etc/vsftpd/vsftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "anonymous\_enable";

fi

fi;

if [ -f /etc/ftpaccess ];

then

if ([ `cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^class\s\*[^\s]\{1,\}\s\*.\*guest"|wc -l` -ne 0 ] || [ `cat /etc/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^class\s\*[^\s]\{1,\}\s\*.\*anonymous"|wc -l` -ne 0 ]);

then

echo "wu-ftp There are anonymous logins";

else

echo "wu-ftp There is no anonymous logins";

fi;

else

if [ -f /etc/ftpd/ftpaccess ];

then

if ([ `cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^class\s\*[^\s]\{1,\}\s\*.\*guest"|wc -l` -ne 0 ] || [ `cat /etc/ftpd/ftpaccess|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep "^class\s\*[^\s]\{1,\}\s\*.\*anonymous"|wc -l` -ne 0 ]);

then

echo "wu-ftp There are anonymous logins";

else

echo "wu-ftp There is no anonymous logins";

fi;

fi;

fi;

if [ -f /etc/proftpd.conf ];

then

Anonymous\_1=`cat /etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|grep -i "AnonRequirePassword[[:space:]]\*on"|wc -l`;

Anonymous\_2=`cat /etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|egrep -i "User|Group|UserAlias"|wc -l`;

if ([ $Anonymous\_1 -ge 1 ] || [ $Anonymous\_2 -lt 3 ])

then

echo "proftp There is no anonymous logins";

else

echo "proftp There are anonymous logins";

fi;

else

if [ -f /etc/proftpd/proftpd.conf ];

then

Anonymous\_1=`cat /etc/proftpd/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|grep -i "AnonRequirePassword[[:space:]]\*on"|wc -l`;

Anonymous\_2=`cat /etc/proftpd/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|egrep -i "User|Group|UserAlias"|wc -l`;

if ([ $Anonymous\_1 -ge 1 ] || [ $Anonymous\_2 -lt 3 ])

then

echo "proftp There is no anonymous logins";

else

echo "proftp There are anonymous logins";

fi;

else

if [ -f /usr/local/proftpd/etc/proftpd.conf ];

then

Anonymous\_1=`cat /usr/local/proftpd/etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|grep -i "AnonRequirePassword[[:space:]]\*on"|wc -l`;

Anonymous\_2=`cat /usr/local/proftpd/etc/proftpd.conf|sed '/^\s\*#/d'|sed '/^\s\*$/d'|sed -n '/<Anonymous.\*/,/<\/Anonymous>/p'|egrep -i "User|Group|UserAlias"|wc -l`;

if ([ $Anonymous\_1 -ge 1 ] || [ $Anonymous\_2 -lt 3 ])

then

echo "proftp There is no anonymous logins";

else

echo "proftp There are anonymous logins";

fi;

fi;

fi;

fi;

if [ -f /etc/pure-ftpd/pure-ftpd.conf ];

then

cat /etc/pure-ftpd/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "NoAnonymous";

else

if [ -f /etc/pure-ftpd.conf ];

then

cat /etc/pure-ftpd.conf|grep -v "^[[:space:]]\*#"|grep -v "^[[:space:]]\*$"|grep -i "NoAnonymous";

fi;

fi;

else

echo "ftp is not running,result=true";

fi;

ftp is not running,result=true

## 操作方法

参考配置:

1)vsftp

编辑文件编辑vi /etc/vsftpd.conf(或vi /etc/vsftpd/vsftpd.conf)文件

设置：

anonymous\_enable=NO #如果存在anonymous\_enable则修改,如果不存在则手动增加

2)pure-ftp

编辑配置文件pure-ftpd.conf,在文件中找到如下行,修改NoAnonymous的值为yes(没有则添加)

NoAnonymous yes

3)wu-ftp

编辑配置文件ftpaccess,如果文件中存在类似如下行,则注释掉:

class [类名] [guest/anonymous] [IP地址]

说明:用户类型不能为guest或者anonymous

4)proftp

编辑配置文件proftpd.conf,查看文件中找到如下结构:

<Anonymous ~ftp>

Group ftp

UserAlias anonymous ftp

</Anonymous>

在该结构中添加如下行:

AnonRequirePassword on #启用认证功能,注意AnonRequirePassword后面更得是多个tab符.

或者将<Anonymous ~ftp>....</Anonymous>结构注释掉.

5)重启ftp服务

# 修改TELNET的Banner信息

## 判断依据

检测方法

使用命令查看TELNET默认Banner信息(cat /etc/issue和cat /etc/issue.net)，确认是否不存在如下版本信息内容：

red hat Enterprise Linux Server release 5.5 (Tikanga)

Kernel \r on an \m #Linux

Welcome to SUSE Linux Enterprise Server 10 (i586) - Kernel \r (\l).

dfdfasd #suse

判定依据

1、TELNET服务未开启。

2、TELNET服务开启，但文件/etc/issue和/etc/issue.net不包含系统敏感信息。

二者满足其一则合规，否则不合规。

## 原始结果

redhat\_count=0

suse\_count=0

result=0

telnet\_status=`netstat -an|grep ":23\>"|grep -i listen|wc -l`;

if [ -s /etc/issue ]

then cat /etc/issue

redhat\_count=`cat /etc/issue | grep -i "Red Hat" | wc -l`

suse\_count=`cat /etc/issue | grep -i "suse" | wc -l`

fi

if ([ $redhat\_count -ge 1 ] || [ $suse\_count -ge 1 ])

then result=1

fi

if [ -s /etc/issue.net ]

then cat /etc/issue.net

redhat\_count=`cat /etc/issue.net | grep -i "Red Hat" | wc -l`

suse\_count=`cat /etc/issue.net | grep -i "suse" | wc -l`

fi

if ([ $redhat\_count -ge 1 ] || [ $suse\_count -ge 1 ])

then result=1

fi

if ([ $result = 1 ] && [ $telnet\_status = 1 ]);

then

echo "telnet is running.telnet banner is not valid.telnet banner check result:false";

else

if [ $result = 1 ];

then

echo "telnet is not running.telnet banner is not valid.telnet banner check result:true";

else

if [ $telnet\_status = 1 ];

then

echo "telnet is running.telnet banner is valid.telnet banner check result:true";

else

echo "telnet is not running.telnet banner is valid.telnet banner check result:true";

fi;

fi;

fi;

unset redhat\_count suse\_count result

CentOS release 6.7 (Final)

Kernel \r on an \m

CentOS release 6.7 (Final)

Kernel \r on an \m

telnet is not running.telnet banner is valid.telnet banner check result:true

## 操作方法

参考配置操作

1、修改TELNET回显信息，修改文件/etc/issue 和/etc/issue.net中的内容，执行如下两条命令：

#echo " Authorized users only. All activity may be monitored and reported " > /etc/issue

#echo " Authorized users only. All activity may be monitored and reported " > /etc/issue.net

可根据实际需要修改该文件的内容，但是不要出现系统敏感信息，如redhat，suse等。

2、重启服务：

#/etc/init.d/xinetd restart

# 文件与目录缺省权限控制

## 判断依据

检测方法

查看文件/etc/profile的末尾是否设置umask值：

#awk '{print $1":"$2}' /etc/profile|grep umask|tail -n1

判定依据

/etc/profile文件末尾存在umask 027，则合规，否则为不合规。

## 原始结果

awk '{print $1":"$2}' /etc/profile|grep -v "^[[:space:]]\*#"|grep -i umask|tail -n1

umask:022

## 操作方法

参考配置操作

1、首先对/etc/profile进行备份：

#cp /etc/profile /etc/profile.bak

2、编辑文件/etc/profile，在文件末尾加上如下内容：

umask 027

3、执行以下命令让配置生效：

#source /etc/profile

# 账号文件权限设置

## 判断依据

检测方法

执行以下命令查看用户及组文件权限

#ls -alL /etc/passwd /etc/shadow /etc/group

判定依据

1、/etc/passwd文件的权限<=644 (所有用户必须要有读权限,只有root用户有写的权限)

2、/etc/shadow文件的权限<=600 (只有root用户拥有该文件的读写权限)

3、/etc/group文件的权限<=644 (所有用户必须要有读权限，只有root用户有写的权限)

以上三个条件同时满足则合规，否则不合规。

## 原始结果

ls -alL /etc/passwd /etc/shadow /etc/group

echo "passwd\_total="`ls -alL /etc/passwd 2>/dev/null|grep -v "[r-][w-]-[r-]--[r-]--"|grep "[r-][w-][x-][r-][w-][x-][r-][w-][x-]"|wc -l`

echo "shadow\_total="`ls -alL /etc/shadow 2>/dev/null|grep -v "[r-][w-]-------"|grep "[r-][w-][x-][r-][w-][x-][r-][w-][x-]"|wc -l`

echo "group\_total="`ls -alL /etc/group 2>/dev/null|grep -v "[r-][w-]-[r-]--[r-]--"|grep "[r-][w-][x-][r-][w-][x-][r-][w-][x-]"|wc -l`

-rw-r--r-- 1 root root 852 11月 16 20:40 /etc/group

-rw-r--r-- 1 root root 1750 11月 16 20:40 /etc/passwd

---------- 1 root root 1405 11月 16 20:41 /etc/shadow

passwd\_total=0

shadow\_total=0

group\_total=0

## 操作方法

参考配置操作

1、使用如下命令查看一下文件的权限：

#ls -alL /etc/passwd /etc/shadow /etc/group

2、执行备份:使用cp命令备份需要修改权限的文件或目录。

3、权限修改：

（1）、修改/etc/passwd文件的权限为644

#chmod 644 /etc/passwd (所有用户必须要有读权限，只有root用户有写的权限)。

（2）、修改/etc/shadow文件的权限

#chmod 600 /etc/shadow (只有root用户拥有该文件的读写权限)。

（3）、修改/etc/group文件的权限

#chmod 644 /etc/group (所有用户必须要有读权限，只有root用户有写的权限)。

# 配置用户最小授权

## 判断依据

检测方法

使用以下命令查看如下文件的权限设置：

#ls -lL /etc/passwd 2>/dev/null

#ls -lL /etc/group 2>/dev/null

#ls -lL /etc/services 2>/dev/null

#ls -lL /etc/shadow 2>/dev/null

#ls -lL /etc/xinetd.conf 2>/dev/null

#ls -lLd /etc/security 2>/dev/null

判定依据

1、/etc/passwd文件的权限小于等于644

2、/etc/shadow文件的权限小于等于400

3、/etc/group文件的权限小于等于644

4、/etc/services文件权限小于等于644

5、/etc/xinetd.conf文件权限小于等于600

6、/etc/security目录权限权限小于等于600

以上六者同时满足则合规，否则不合规。

## 原始结果

ls -lL /etc/passwd 2>/dev/null

echo "passwd="`ls -lL /etc/passwd 2>/dev/null|grep -v "[r-][w-]-[r-]--[r-]--"|wc -l`

ls -lL /etc/group 2>/dev/null

echo "group="`ls -lL /etc/group 2>/dev/null|grep -v "[r-][w-]-[r-]--[r-]--"|wc -l`

ls -lL /etc/services 2>/dev/null

echo "services="`ls -lL /etc/services 2>/dev/null|grep -v "[r-][w-]-[r-]--[r-]--"|wc -l`

ls -lL /etc/shadow 2>/dev/null

echo "shadow="`ls -lL /etc/shadow 2>/dev/null|grep -v "[r-]--------"|wc -l`

ls -lL /etc/xinetd.conf 2>/dev/null

echo "xinetd="`ls -lL /etc/xinetd.conf 2>/dev/null|grep -v "[r-][w-]-------"|wc -l`

ls -lLd /etc/security 2>/dev/null

echo "security="`ls -lLd /etc/security 2>/dev/null|grep -v "[r-][w-]-------"|wc -l`

-rw-r--r-- 1 root root 1750 11月 16 20:40 /etc/passwd

passwd=0

-rw-r--r-- 1 root root 852 11月 16 20:40 /etc/group

group=0

-rw-r--r--. 1 root root 641020 10月 2 2013 /etc/services

services=0

---------- 1 root root 1405 11月 16 20:41 /etc/shadow

shadow=0

xinetd=0

drwxr-xr-x. 6 root root 4096 11月 15 07:40 /etc/security

security=1

## 操作方法

参考配置操作

1、赋予用户相关账号文件最小权限

#chmod 644 /etc/passwd

#chmod 400 /etc/shadow

#chmod 644 /etc/group

#chmod 644 /etc/services

#chmod 600 /etc/xinetd.conf

#chmod 600 /etc/security

# 禁止ICMP重定向

## 判断依据

检测方法

使用如下命令查看参数net.ipv4.conf.all.accept\_redirects的值：

#sysctl -n net.ipv4.conf.all.accept\_redirects

判定条件

net.ipv4.conf.all.accept\_redirects的值为0则合规，否则不合规。

## 原始结果

echo "accept\_redirects="`sysctl -n net.ipv4.conf.all.accept\_redirects`

accept\_redirects=1

## 操作方法

参考配置操作

1、备份文件

#cp -p /etc/sysctl.conf /etc/sysctl.conf\_bak

2、编辑文件 /etc/sysctl.conf，有则改之，无则添加以下内容：

net.ipv4.conf.all.accept\_redirects=0

3、使配置生效

#sysctl -p

# 日志文件安全

## 判断依据

检测方法

1、使用以下命令查看日志文件的权限

（1）redhat5.x之前：

#LOGDIR=`if [ -f /etc/syslog.conf ];then cat /etc/syslog.conf| grep -v "^[[:space:]]\*#"|awk '{print $2}'|sed 's/^-//g'|grep '^\s\*\/';fi`;

#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

（2）redhat6.x之后：

#LOGDIR=`cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#"|awk '{print $2}'|sed 's/^-//g'|grep '^\s\*\/'`;

#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

（3）suse：

#LOGDIR=`cat /etc/syslog-ng/syslog-ng.conf|grep -v "^[[:space:]]\*#"|grep "^destination"|grep file|cut -d\" -f2`;

#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

判定依据

不存在权限>640的日志文件则合规，否则不合规。

## 原始结果

unset syslogd\_status syslogng\_status rsyslogd\_status LOGDIR;

syslogd\_status=`ps -ef |grep ' syslogd '|grep -v "grep"|wc -l`;

syslogng\_status=`ps -ef |grep "syslog-ng"|grep -v "grep syslog-ng"|wc -l`;

rsyslogd\_status=`ps -ef | grep "rsyslogd" | grep -v "grep" |wc -l`;

if [ "$syslogd\_status" != 0 ];

then

LOGDIR=`if [ -f /etc/syslog.conf ];then cat /etc/syslog.conf| grep -v "^[[:space:]]\*#"|awk '{print $2}'|sed 's/^-//g'|grep '^\s\*\/';fi`;

ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$7" "$8" "$9}';

else

if [ "$rsyslogd\_status" != 0 ];

then

LOGDIR=`cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#"|awk '{print $2}'|sed 's/^-//g'|grep '^\s\*\/'`;

ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$7" "$8" "$9}';

else

if [ "$syslogng\_status" != 0 ];

then

LOGDIR=`cat /etc/syslog-ng/syslog-ng.conf|grep -v "^[[:space:]]\*#"|grep "^destination"|grep file|cut -d\" -f2`;

ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$7" "$8" "$9}';

else

echo "Process is not running";

fi;

fi;

fi;

unset syslogd\_status syslogng\_status rsyslogd\_status LOGDIR;

-rw-r--r-- 15 09:30 /var/log/boot.log

## 操作方法

参考配置操作

1、对权限大于640的日志文件赋予640权限

#chmod 640 filename

（Redhat系统和SUSE系统做法相同，无版本区分）

# 启用远程日志功能

## 判断依据

检测方法

1、linux

查看文件 /etc/syslog.conf或者/etc/rsyslog.conf存在类似如下语句：

\*.\* @192.168.56.168

2、suse

查看文件/etc/syslog-ng/syslog-ng.conf，存在类似如下内容：

destination logserver { udp("192.168.56.168" port(514)); };

log { source(src); destination(logserver); };

判定依据

步骤1或者步骤2满足其一则合规，否则不合规。

## 原始结果

if [ -f /etc/syslog.conf ];

then

cat /etc/syslog.conf | grep -v "^[[:space:]]\*#" | grep -E '[[:space:]]\*.+@.+';

fi;

if [ -s /etc/syslog-ng/syslog-ng.conf ];

then

ret\_1=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "port(514)"|awk '{print $2}'`;

if [ -n "$ret\_1" ];

then

ret\_2=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "destination($ret\_1)"`;

if [ -n "$ret\_2" ];

then

echo "Set the log server:true";

else

echo "not Set the log server:false";

fi;

fi;

fi;

if [ -f /etc/rsyslog.conf ];

then cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#" | grep -E '[[:space:]]\*.+@.+';

fi

## 操作方法

参考配置操作

1、linux

编辑文件 /etc/syslog.conf或者/etc/rsyslog.conf，增加如下内容：

\*.\* @<日志服务器ip或者域名>

2、suse

编辑文件/etc/syslog-ng/syslog-ng.conf，增加如下内容：

destination logserver { udp("192.168.56.168" port(514)); };

log { source(src); destination(logserver); };

#日志服务器ip视实际情况来确定。

3、重启syslog服务

#/etc/init.d/syslog stop

#/etc/init.d/syslog start

# 记录安全事件日志

## 判断依据

检测方法

1、redhat5.x之前编辑/etc/syslog.conf、redhat6.x之后编辑etc/rsyslog.conf，在文件中加入如下内容：

\*.err;kern.debug;daemon.notice /var/adm/messages

2、SUSE编辑文件/etc/syslog-ng/syslog-ng.conf,在文件中加入如下内容:

filter f\_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); };

destination msgs { file("/var/adm/msgs"); };

log { source(src); filter(f\_msgs); destination(msgs); };

判定依据

配置了记录安全事件日志则合规，否则不合规。

## 原始结果

if [ -f /etc/syslog.conf ];

then

syslog=`cat /etc/syslog.conf | grep -v "^[[:space:]]\*#" | grep "\*.err\;kern\.debug\;daemon\.notice[[:space:]]\*/var/adm/messages"|wc -l`;

if [ $syslog -ge 1 ];

then

echo "syslog check result:true";

else

echo "syslog check result:false";

fi;

fi;

if [ -f /etc/rsyslog.conf ];

then

rsyslog=`cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#" | grep "\*.err\;kern\.debug\;daemon\.notice[[:space:]]\*/var/adm/messages"|wc -l`;

if [ $rsyslog -ge 1 ];

then

echo "rsyslog check result:true";

else

echo "rsyslog check result:false";

fi;

fi;

if [ -s /etc/syslog-ng/syslog-ng.conf ];

then suse\_ret=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice)"`;

if [ -n "$suse\_ret" ];

then suse\_ret2=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep 'file("/var/adm/msgs")'`;

if [ -n "$suse\_ret2" ];

then suse\_ret3=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "destination(msgs)"`;

fi;

fi;

fi;

if [ -n "$suse\_ret3" ];

then echo "suse:valid";

else echo "suse:no value";

fi;

unset suse\_ret suse\_ret2 suse\_ret3 rsyslog syslog;

rsyslog check result:false

suse:no value

## 操作方法

参考配置操作

1、redhat5.x之前编辑/etc/syslog.conf，在文件中加入如下内容:

\*.err;kern.debug;daemon.notice /var/adm/messages，其中/var/adm/messages为日志文件。

（1）如果该文件不存在，则创建该文件，命令为：

#touch /var/adm/messages

（2）修改权限为666，命令为：

#chmod 666 /var/adm/messages

（3）重启日志服务：

#/etc/init.d/syslog restart

2、redhat6.x之后编辑etc/rsyslog.conf，在文件中加入如下内容:

\*.err;kern.debug;daemon.notice /var/adm/messages，其中/var/adm/messages为日志文件。

（1）如果该文件不存在，则创建该文件，命令为：

#touch /var/adm/messages

（2）修改权限为666，命令为:

#chmod 666 /var/adm/messages

（3）重启日志服务：

#/etc/init.d/rsyslog restart

3、SUSE编辑文件/etc/syslog-ng/syslog-ng.conf，在文件中加入如下内容：

filter f\_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); };

destination msgs { file("/var/adm/msgs"); };

log { source(src); filter(f\_msgs); destination(msgs); }; 其中/var/adm/msgs为日志文件。

（1）如果该文件不存在，则创建该文件，命令为:

#touch /var/adm/msgs

（2）修改权限为666，命令为：

#chmod 666 /var/adm/msgs

（3）重启日志服务：

#/etc/init.d/syslog restart

# 记录账户登录日志

## 判断依据

检测方法

1、redhat5.x之前查看文件 /etc/syslog.conf、redhat6.x查看文件/etc/rsyslog.conf存在类似如下语句：

authpriv.\* /var/log/authlog

或者

authpriv.info /var/log/authlog

2、SUSE查看文件/etc/syslog-ng/syslog-ng.conf，存在类似如下内容：

filter f\_auth { facility(auth); };

destination f\_authlog { file("/var/log/authlog"); };

log { source(src); filter(f\_auth); destination(f\_authlog); };

判定依据

步骤1或者步骤2满足其一则合规，否则不合规。

## 原始结果

unset red\_ret suse\_ret suse\_ret2 suse\_ret3

if [ -s /etc/syslog.conf ];

then

cat /etc/syslog.conf | grep -v "^[[:space:]]\*#" | egrep "authpriv\.\\*.\*[[:space:]]\*\/|authpriv\.info.\*[[:space:]]\*\/";

fi;

if [ -s /etc/rsyslog.conf ];

then

cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#" | egrep "authpriv\.\\*.\*[[:space:]]\*\/|authpriv\.info.\*[[:space:]]\*\/";

fi;

if [ -s /etc/syslog-ng/syslog-ng.conf ];

then

suse\_ret=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "facility(auth)" | grep "filter" | awk '{print \$2}'`;

if [ -n "$suse\_ret" ];

then

suse\_ret2=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "destination" | grep "/var/log/authlog"`;

if [ -n "$suse\_ret2" ];

then

suse\_ret3=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "log" | grep "$suse\_ret"`;

fi;

fi;

fi;

if [ -n "$suse\_ret3" ];

then

echo "suse:valid";

else

echo "ret:no value";

fi;

unset suse\_ret suse\_ret2 suse\_ret3;

authpriv.\* /var/log/secure

ret:no value

## 操作方法

参考配置操作

1、redhat5.x之前查看文件 /etc/syslog.conf、redhat6.x查看文件/etc/rsyslog.conf，增加如下内容：

authpriv.\* /var/log/authlog

或者

authpriv.info /var/log/authlog

2、SUSE编辑文件/etc/syslog-ng/syslog-ng.conf，增加如下内容：

filter f\_auth { facility(auth); };

destination f\_authlog { file("/var/log/authlog"); };

log { source(src); filter(f\_auth); destination(f\_authlog); };

3、创建日志文件，并赋予其权限

#touch /var/log/authlog

#chmod 640 /var/log/authlog

4、重启syslog服务

#/etc/init.d/syslog stop

#/etc/init.d/syslog start

# 配置su命令使用情况记录

## 判断依据

检测方法

1、redhat5.x之前查看文件 /etc/syslog.conf、redhat6.x查看文件/etc/rsyslog.conf存在类似如下语句：

authpriv.\* /var/log/secure

2、SUSE查看文件/etc/syslog-ng/syslog-ng.conf，存在类似如下内容：

filter f\_secure { facility(authpriv); };

destination f\_authprive { file("/var/log/secure"); };

log { source(src); filter(f\_secure); destination(f\_secure); };

判定依据

步骤1或者步骤2满足其一则合规，否则不合

## 原始结果

unset red\_ret suse\_ret suse\_ret2 suse\_ret3

if [ -s /etc/syslog.conf ];

then red\_ret=`cat /etc/syslog.conf | grep -v "^[[:space:]]\*#" | grep "authpriv\.\\*[[:space:]]\/\*"`;

fi

if [ -s /etc/rsyslog.conf ];

then red\_ret2=`cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#" | grep "authpriv\.\\*[[:space:]]\/\*"`;

fi

if [ -s /etc/syslog-ng/syslog-ng.conf ];

then

suse\_ret=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "facility(authpriv)" | grep "filter" | awk '{print \$2}'`;

if [ -n "$suse\_ret" ];

then suse\_ret2=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "destination" | grep "/var/log/secure"`;

if [ -n "$suse\_ret2" ];

then suse\_ret3=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "log" | grep "$suse\_ret"`;

fi;

fi;

fi

if [ -n "$red\_ret" ];

then

echo "redhat-suse:valid";

else

if [ -n "$red\_ret2" ];

then

echo "red-hat6:valid";

else

if [ -n "$suse\_ret3" ];

then

echo "suse:valid";

else

echo "ret:no value";

fi

fi;

fi;

unset red\_ret suse\_ret suse\_ret2 suse\_ret3;

red-hat6:valid

## 操作方法

参考配置操作

1、redhat5.x之前查看文件 /etc/syslog.conf，增加如下内容：

authpriv.\* /var/log/secure

2、redhat6.x查看文件/etc/rsyslog.conf，增加如下内容：

authpriv.\* /var/log/secure

3、SUSE编辑文件/etc/syslog-ng/syslog-ng.conf，增加如下内容:

filter f\_secure { facility(authpriv); };

destination f\_authprive { file("/var/log/secure"); };

log { source(src); filter(f\_secure); destination(f\_authprive); };

4、创建日志文件，并赋予其权限

#touch /var/log/secure

#chmod 640 /var/log/secure

5、重启syslog服务

#/etc/init.d/syslog stop

#/etc/init.d/syslog start

# 记录cron行为日志

## 判断依据

检测方法

1、redhat5.x之前查看文件/etc/syslog.conf、redhat6.x查看文件/etc/rsyslog.conf，看文件中是否存在如下配置：

cron.\* /var/log/cron

2、SUSE系统查看文件/etc/syslog-ng/syslog-ng.conf，看文件中是否存在如下内容：

filter f\_cron { facility(cron); };

destination cron { file("/var/log/cron"); };

log { source(src); filter(f\_cron); destination(cron); };

判定依据

1、文件/etc/syslog.conf配置了cron行为日志记录。

2、文件/etc/rsyslog.conf配置了cron行为日志记录。

3、文件/etc/syslog-ng/syslog-ng.conf配置了cron行为日志记录。

三者满足其一则合规，否则不不合规。

## 原始结果

if [ -f /etc/syslog.conf ]

then

echo "syslog="`cat /etc/syslog.conf | grep -v "^[[:space:]]\*#" | grep "cron.\\*"`

fi

if [ -f /etc/rsyslog.conf ]

then

echo "rsyslog="`cat /etc/rsyslog.conf | grep -v "^[[:space:]]\*#" | grep "cron.\\*"`

fi

if [ -s /etc/syslog-ng/syslog-ng.conf ];

then

cron\_1=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "filter[[:space:]]\*.\*[[:space:]]\*{[[:space:]]\*facility(cron);[[:space:]]\*};" | wc -l`;

if [ $cron\_1 -ge 1 ];

then

cron\_2=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "destination[[:space:]]\*.\*[[:space:]]\*{[[:space:]]\*file(\"/var/log/cron\")[[:space:]]\*;[[:space:]]\*};"|awk '{print $2}'`;

if [ -n $cron\_2 ];

then

cron\_3=`cat /etc/syslog-ng/syslog-ng.conf | grep -v "^[[:space:]]\*#" | grep "log[[:space:]]\*{[[:space:]]\*source(src);[[:space:]]\*filter(.\*);[[:space:]]\*destination($cron\_2);[[:space:]]\*};" | wc -l`;

if [ $cron\_3 -ge 1 ]

then

echo "Cron log has been configured,check result:true";

else

echo "No cron log,check result:false";

fi;

fi;

fi;

fi;

rsyslog=cron.\* /var/log/cron

## 操作方法

参考配置操作

1、redhat5.x之前编辑文件/etc/syslog.conf，在文件新增一行(如果存在则无需新增)如下内容：

cron.\* /var/log/cron 其中/var/log/cron为日志文件。

（1）、如果该文件不存在，则创建该文件，命令为:

#touch /var/log/cron

（2）、同时修改其权限为640，命令为:

#chmod 640 /var/log/cron 。

2、redhat6.x编辑文件/etc/syslog.conf，在文件新增一行(如果存在则无需新增)如下内容：

cron.\* /var/log/cron 其中/var/log/cron为日志文件。

（1）、如果该文件不存在，则创建该文件，命令为:

#touch /var/log/cron

（2）、同时修改其权限为640，命令为:

#chmod 640 /var/log/cron 。

3、SUSE系统，编辑文件/etc/syslog-ng/syslog-ng.conf(vi /etc/syslog-ng/syslog-ng.conf)，在文件增加如下内容(如果存在则无需新增)如下内容：

filter f\_cron { facility(cron); };

destination cron { file("/var/log/cron"); };

log { source(src); filter(f\_cron); destination(cron); }; 其中/var/log/cron为日志文件。

（1）、如果该文件不存在，则创建该文件，命令为：

#touch /var/log/cron

（2）、同时修改其权限为640，命令为:

#chmod 640 /var/log/cron 。

# 禁止IP路由转发

## 判断依据

检测方法

使用如下命令查看net.ipv4.ip\_forward的值：

#sysctl -n net.ipv4.ip\_forward

判定依据

net.ipv4.ip\_forward的值为0表示合规，否则不合规。

## 原始结果

echo "ip\_forward="`sysctl -n net.ipv4.ip\_forward`

ip\_forward=0

## 操作方法

参考配置操作

1、备份文件：

#cp -p /etc/sysctl.conf /etc/sysctl.conf\_bak

2、编辑文件sysctl.conf加上

net.ipv4.ip\_forward=0

3、使配置文件生效

#sysctl -p

# 控制远程访问的IP地址

## 判断依据

检测方法

查看/etc/hosts.allow和/etc/hosts.deny两个文件中是否设定了IP范围限制：

#cat /etc/hosts.allow

#cat /etc/hosts.deny

判定依据

1、/etc/hosts.allow中设置了允许访问的IP地址范围。

2、/etc/hosts.deny中设置了拒绝所有远程访问。

两者同时满足则合规，否则不合规。

## 原始结果

at /etc/hosts.allow |sed '/^#/d'|sed '/^$/d'|egrep -i "sshd|telnet|all"

cat /etc/hosts.deny |sed '/^#/d'|sed '/^$/d'|egrep -i "all:all"

echo "allowno="`egrep -i "sshd|telnet|all" /etc/hosts.allow |sed '/^#/d'|sed '/^$/d'|wc -l`

echo "denyno="`egrep -i "sshd|telnet|all" /etc/hosts.deny |sed '/^#/d'|sed '/^$/d'|wc -l`

allowno=0

denyno=0

## 操作方法

参考配置操作

1、执行备份：

#cp -p /etc/hosts.allow /etc/hosts.allow\_bak

#cp -p /etc/hosts.deny /etc/hosts.deny\_bak

2、编辑/etc/hosts.allow文件，增加一行 service: 允许访问的IP(service为服务，例如sshd)，举例如下：all:192.168.4.44:allow #允许单个IP访问所有服务进程

sshd:192.168.1.\*:allow #允许192.168.1.0的整个网段访问SSH服务进程

#编辑文件/etc/hosts.deny增加一行（deny优先级高于allow）

all:all #拒绝一切远程访问配合文件hosts.allow使用。

注：以上内容仅供参考，请根据实际网段和需求进行实施。

# 禁止IP源路由

## 判断依据

检测方法

执行以下命令查看参数accept\_source\_route的值。

#cat /proc/sys/net/ipv4/conf/\*/accept\_source\_route

判定依据

accept\_source\_route的值为0则合规，否则为不合规。

## 原始结果

cat /proc/sys/net/ipv4/conf/\*/accept\_source\_route

0

0

0

0

0

0

0

0

0

0

0

0

## 操作方法

参考配置操作

1、如果此项检查失败,请执行以下命令进行修复：

#for f in /proc/sys/net/ipv4/conf/\*/accept\_source\_route

do

echo 0 > $f

done

加固后系统不可以重启，重启后需要重新加固。

# 更改主机解析地址的顺序

## 判断依据

检测方法

编辑文件/etc/host.conf，看是否存在如下内容：

order hosts，bind

multi on

nospoof on

判定依据

文件/etc/host.conf存在如上配置则合规，否则不合规。

## 原始结果

cat /etc/host.conf|grep -v "^[[:space:]]\*#"|egrep "order[[:space:]]hosts,bind|multi[[:space:]]on|nospoof[[:space:]]on"

multi on

## 操作方法

参考配置操作

1、编辑/etc/host.conf文件

#vi /etc/host.conf，在空白处加入下面三行：

order hosts,bind #第一项设置首先通过DNS解析IP地址,然后通过hosts文件解析。

multi on #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)。

nospoof on #第三项设置说明要注意对本机未经许可的IP欺骗。

# 系统core dump状态

## 判断依据

检测方法

1、查看/etc/security/limits.conf文件中是否配置如下内容：

\* soft core 0

\* hard core 0

2、查看/etc/profile文件中是否存在如下配置，存在则注释掉：

ulimit -S -c 0 > /dev/null 2>&1

判定依据

设置\* soft core、\* hard core为0，且注释掉ulimit -S -c 0 > /dev/null 2>&1行则合规，否则不合规。

## 原始结果

cat /etc/profile|grep -v "^[[:space:]]\*#"|grep "ulimit[[:space:]]\*-S[[:space:]]\*-c[[:space:]]\*0[[:space:]]\*>[[:space:]]\*/dev/null[[:space:]]\*2>&1"

cat /etc/security/limits.conf|grep -v "[[:space:]]\*#"

## 操作方法

参考配置操作

1、编辑文件/etc/security/limits.conf(vi /etc/security/limits.conf)，在文件末尾加入如下两行(存在则修改，不存在则新增)：

\* soft core 0

\* hard core 0

2、编辑文件/etc/profile(vi /etc/profile)注释掉如下行：

#ulimit -S -c 0 > /dev/null 2>&1

# 打开syncookie缓解syn flood攻击

## 判断依据

检测方法

执行以下命令查看参数tcp\_syncookies的值。

#cat /proc/sys/net/ipv4/tcp\_syncookies

判定依据

tcp\_syncookies的值为1则合规，否则为不合规。

## 原始结果

cat /proc/sys/net/ipv4/tcp\_syncookies

1

## 操作方法

参考配置操作

1、方法一

命令行输入如下命令：

#echo 1 > /proc/sys/net/ipv4/tcp\_syncookies

注意：此方法在重启后会失效。

2、方法二

#vi /etc/sysctl.conf

在文件中查找net.ipv4.tcp\_syncookies修改为：

net.ipv4.tcp\_syncookies = 1

如果没找到，则在单独一行添加即可。

3、保存后退出

4、#sysctl -p

此方法在重启后依然有效，网络与服务

# 禁止存在心血漏洞

## 判断依据

检测方法

执行如下命令查看openssl版本。

#openssl version

判定依据

openssl版本不在以下列表的则合规，否则不合规：

1.0.0、1.0.1f、1.0.1e、1.0.1d、1.0.1c、1.0.1b、1.0.1a、1.0.1、1.0.2-beta、1.0.2-beta1

## 原始结果

openssl version

cat /etc/redhat-release 2>/dev/null

OpenSSL 1.0.1e-fips 11 Feb 2013

CentOS release 6.7 (Final)

## 操作方法

参考配置操作

1、请立即升级openssl版本。(本检查项不提供具体升级步骤，请参考相关资料)。

# 禁止存在bash安全漏洞

## 判断依据

检测方法

执行如下命令查看设备是否存在bash安全漏洞。

#env -i X='() { (a)=>\' bash -c '/dev/stdout echo vulnerable' 2>/dev/null

判定依据

如果以上命令的输出为以下内容则不合规：

vulnerable

## 原始结果

env -i X='() { (a)=>\' bash -c '/dev/stdout echo vulnerable' 2>/dev/null

## 操作方法

参考操作步骤:

(1).目前官网已经提供了升级包bash-4.1.2-15.el6\_5.1.x86\_64.rpm,请自行下载升级

# 登录超时时间设置

## 判断依据

检测方法

查看/etc/profile文件中是否配置超时设置：

#cat /etc/profile |grep -i TMOUT

判定依据

输出存在TMOUT，且其值=300秒则合规，否则不合规。

## 原始结果

cat /etc/profile |grep -v "^[[:space:]]\*#"|grep -v "^$"|grep "TMOUT"

## 操作方法

参考配置操作

1、执行备份

#cp -p /etc/profile /etc/profile\_bak

2、在/etc/profile文件增加以下两行(如果存在则修改，否则手工添加)：

#vi /etc/profile

TMOUT=300 #TMOUT按秒计算

export TMOUT

# Root用户环境变量的安全性

## 判断依据

检测方法

使用命令echo $PATH查看PATH环境变量的值，确认PATH环境变量中是否存在.或者..的路径:

.:/usr/bin:..:/usr/sbin

判定依据

$PATH环境变量中不存在.或者..的路径则合规，否则不合规。

## 原始结果

echo $PATH

echo "result=`echo $PATH|egrep "^\.\:|^\.\.\:|\:\.$|\:\.\.$|\:\.\:|\:\.\.\:"|wc -l`"

/usr/local/jdk/bin:/usr/local/jdk/jre/bin:/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin

result=0

## 操作方法

参考配置操作

1、修改文件/etc/profile或/root/.bash\_profile

修改环境变量$PATH，删除环境变量值包含的（.和..）的路径。

# 禁止组合键关机

## 判断依据

检测方法

执行命令查看文件/etc/inittab是否存在如下内容：

#cat /etc/inittab|grep -v "^#"|grep "ctrlaltdel"

ca::ctrlaltdel:/sbin/shutdown -r -t 4 now

判定依据

文件/etc/inittab中不存在如下内容则合规，否则不合规：

ca::ctrlaltdel:/sbin/shutdown -r -t 4 now

## 原始结果

cat /etc/inittab|grep -v "^#"|grep "ctrlaltdel"

## 操作方法

参考配置操作

编辑文件/etc/inittab,将以下行删除、注释,或者将此行：

ca::ctrlaltdel:/sbin/shutdown -r -t 4 now

修改为：

ca::ctrlaltdel:/bin/true

# 设置屏幕锁定

## 判断依据

检测方法

使用如下命令查看屏幕锁定配置：

# gconftool-2 -g /apps/gnome-screensaver/idle\_activation\_enabled

# gconftool-2 -g /apps/gnome-screensaver/lock\_enabled

# gconftool-2 -g /apps/gnome-screensaver/mode

# gconftool-2 -g /apps/gnome-screensaver/idle\_delay

判定依据

1、idle\_activation\_enabled的值为true #启用空闲激活

2、lock\_enabled的值为true #启用屏幕锁定

3、/apps/gnome-screensaver/mode的值为blank-only #屏保模式

4、idle\_delay的值<=15 #空闲激活时间

四个条件同时满足则合规，否则不合规。

## 原始结果

if [ -n "`ps -A | egrep -i "gnome|kde|mate|cinnamon|lx|xfce|jwm"`" ];then

echo "idle\_activation\_enabled="`gconftool-2 -g /apps/gnome-screensaver/idle\_activation\_enabled 2>/dev/null`

echo "lock\_enabled="`gconftool-2 -g /apps/gnome-screensaver/lock\_enabled 2>/dev/null`

echo "mode="`gconftool-2 -g /apps/gnome-screensaver/mode 2>/dev/null`

echo "idle\_delay="`gconftool-2 -g /apps/gnome-screensaver/idle\_delay 2>/dev/null`

else

echo "No desktop installed"

fi

idle\_activation\_enabled=true

lock\_enabled=true

mode=single

idle\_delay=10

## 操作方法

参考配置操作

1、启用空闲激活

#gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/idle\_activation\_enabled true

2、启用屏幕锁定

#gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/lock\_enabled true

3、设置屏保模式

#gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type string --set /apps/gnome-screensaver/mode blank-only

4、设置空闲激活时间

#gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type int --set /apps/gnome-screensaver/idle\_delay 15

# 设置关键文件的属性

## 判断依据

检测方法

使用命令查看/var/log/messages文件是否只可追加不可修改：

#lsattr /var/log/messages

判定依据

/var/log/messages文件的权限第六位为a则合规，否则不合规

## 原始结果

lsattr /var/log/messages 2>/dev/null

-------------e- /var/log/messages

## 操作方法

参考配置操作

1、更改/var/log/messages文件属性

#chattr +a /var/log/messages #如果不存在则忽略

# 历史命令设置

## 判断依据

检测方法

编辑文件/etc/profile查看是否存在如下内容：

HISTFILESIZE=5

HISTSIZE=5

判定依据

HISTFILESIZE和HISTSIZE的值小于等于5则合规，否则不合规。

## 原始数据

cat /etc/profile|grep -v "^[[:space:]]\*#"|grep "HISTFILESIZE"

cat /etc/profile|grep -v "^[[:space:]]\*#"|grep "HISTSIZE"

HISTSIZE=1000

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

## 操作方法

参考配置操作

1、编辑文件/etc/profile，在文件中加入如下两行(存在则修改)：

HISTFILESIZE=5

HISTSIZE=5

2、执行以下命令让配置生效

#source /etc/profile

# 对root为ls、rm设置别名

## 判断依据

检测方法

执行以下操作查看系统是否为root设置rm和ls别名设置：

#echo $SHELL

（1）、如果输出csh：

#vi ~/.cshrc 是否存在如下内容:

alias ls='ls -aol'

alias rm='rm -i'

（2）、如果输出bash：

# vi ~/.bashrc查看是否存在如下内容：

alias ls='ls -aol'

alias rm='rm -i'

判定依据

给root用户设备了ls和rm命令别名则合规，否则不合规。

## 原始数据

if [ `echo $SHELL|egrep "bash|sh"|wc -l` -ge 1 ];then

if [ -f /root/.bashrc ];then

cat /root/.bashrc|grep -v "^[[:space:]]\*#"

else

alias

fi

else

if [ -f /root/.cshrc ];then

cat /root/.cshrc|grep -v "^[[:space:]]\*#"

else

alias

fi

fi

alias rm='rm -i'

alias cp='cp -i'

alias mv='mv -i'

if [ -f /etc/bashrc ]; then

. /etc/bashrc

fi

## 操作方法

参考配置操作

1、#echo $SHELL

（1）、如果输出csh:

#vi ~/.cshrc 在文件末尾增加如下两行

alias ls='ls -aol'

alias rm='rm -i'

（2）、如果输出bash:

# vi ~/.bashrc在文件末尾增加如下两行

alias ls='ls -aol'

alias rm='rm -i'