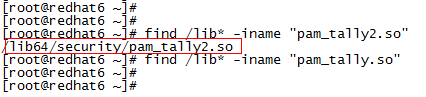
使用下面命令，查看系统是否含有pam\_tally2.so 模块，如果没有，就需要使用pam\_tally.so 模块，两个模块的使用方法不太一样，需要区分开来。



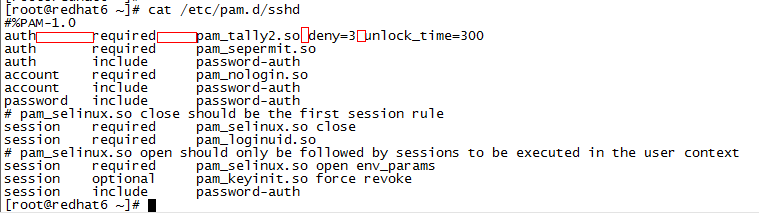
2.使用pam\_tally2.so 模块限制用户登录失败N次锁定用户（几分钟后自动解锁）

Linux有一个pam\_tally2.so的PAM模块，来限定用户的登录失败次数，如果次数达到设置的阈值，则锁定用户。

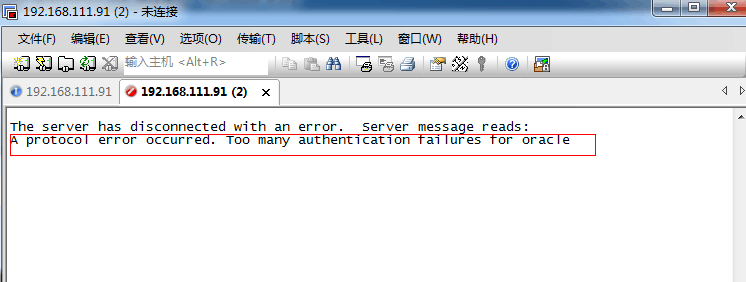
2.1.远程ssh登录限制方法（常用）

如果想限制远程登录，需要改SSHD文件（可以只限制远程登录而不限制tty登录即只对sshd

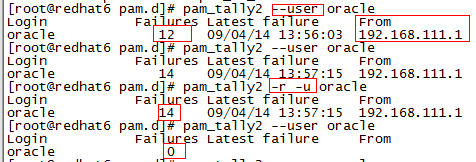
文件增加此限制），在#%PAM-1.0的下面，即第二行，添加内容，一定要写在前面，如果写在后面，虽然用户被锁定，但是只要用户输入正确的密码，还是可以登录的！



失败效果（远程ssh登录；这个远程ssh的时候，没有提示，我用的是Xshell，不知道其它终端有没提示，只要超过设定的值，输入正确的密码也是登陆不了的！）如下：



也可以直接在system-auth 文件中直接添加这些命令，修改完成后，凡是调用system-auth 文件的服务，都会生效。因为有自动解锁时间，所以，不用担心全部限制后，会出现永远无法登陆的“尴尬”情况。

查看用户登录失败的次数并解锁命令2.2.

2.3.Suse Linux 多次登录失败锁定用户及解锁

在服务器端以root用户登录

执行命令：

# faillog –a ////查看用户登录错误次数

如果超过三次的话，用户不能登录并且此后登录用户错误登录次数还是会增加。

在登录错误次数不满三次时，登录成功后，则这个用户登录错误值将清零，退出后重新telnet 登录将采用新的计数。

# faillog -u user –r ////清空指定用户user的错误登录次数

# faillog –r ////清空所有用户错误登录次数

/var/log/faillog会自动生成，里边记录用户登录失败次数等信息

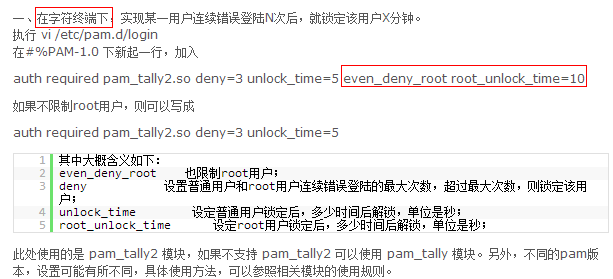
2.4.手动锁定用户禁止使用

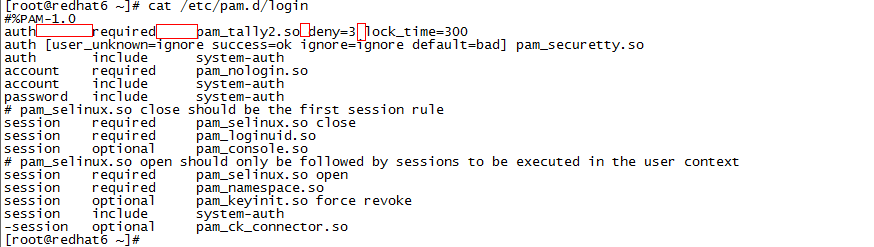
可以用usermod命令来锁定用户密码，使密码无效，该用户名将不能使用。

锁定命令：usermod -L 用户名

解锁命令：usermod -U 用户名

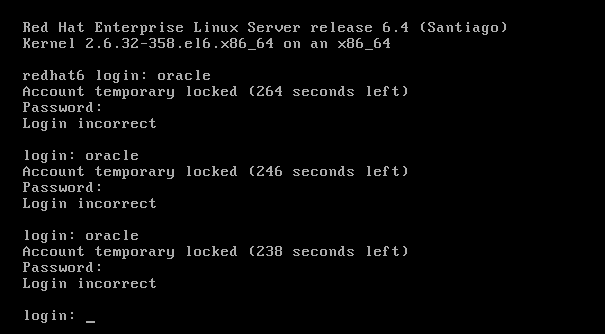
2.5.本地字符终端登录限制方法（不常用）

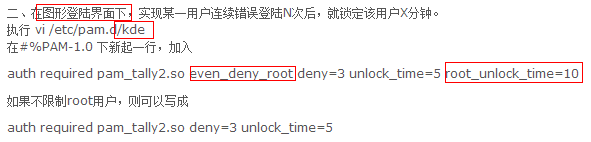




在#%PAM-1.0的下面，即第二行，添加内容，一定要写在前面，如果写在后面，虽然用户被锁定，但是只要用户输入正确的密码，还是可以登录的！

失败效果（tty登录）如下图：



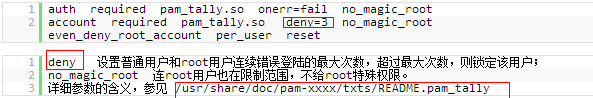
2.6.本地图形登录限制方法（不常用）

3.使用pam\_tally.so 模块限制用户登录失败N次锁定用户（几分钟后自动解锁）

4.1.如果想在所有登陆方式上，限制所有用户

可以在/etc/pam.d/system-auth 中增加2行

如果不想限制root用户，可以将even\_deny\_root\_account 取消掉。



4.2.只在本地文本终端上做限制

可以编辑如下文件，添加的内容和上方一样。

vi /etc/pam.d/login

4.3.只在图形化登陆界面上做限制，

可以编辑如下文件，添加的内容和上方也一样。

vi /etc/pam.d/kde

4.4.只在远程telnet、ssh登陆上做限制

可以编辑如下文件，添加的内容和上方也一样。

vi /etc/pam.d/remote

vi /etc/pam.d/sshd

4.5.3、手动解除锁定：

查看某一用户错误登陆次数：

查看work用户的错误登陆次数：

pam\_tally –user work

清空某一用户错误登陆次数：

清空work 用户的错误登陆次数，

pam\_tally –user work –reset

faillog -r 命令亦可。

4.6.pam\_tally没有自动解锁功能

因为pam\_tally没有自动解锁的功能，所以，在设置限制时，要多加注意，万一全做了限制，而root用户又被锁定了，就只能够进单用户模式解锁了，当然，也可以添加crontab任务，达到定时自动解锁的功能，但需要注意的是，如果在/etc/pam.d/system-auth 文件中添加了pam\_tally的话，当root被锁定后，crontab任务会失效，所以，最好不要在system-auth 文件中添加pam\_tally。

4.7.添加crontab任务（达到定时自动解锁的功能）

root用户执行crontab -e 命令，添加如下内容



意思是，每1分钟，将所有用户登陆失败的次数清空，并将所有用户解锁。