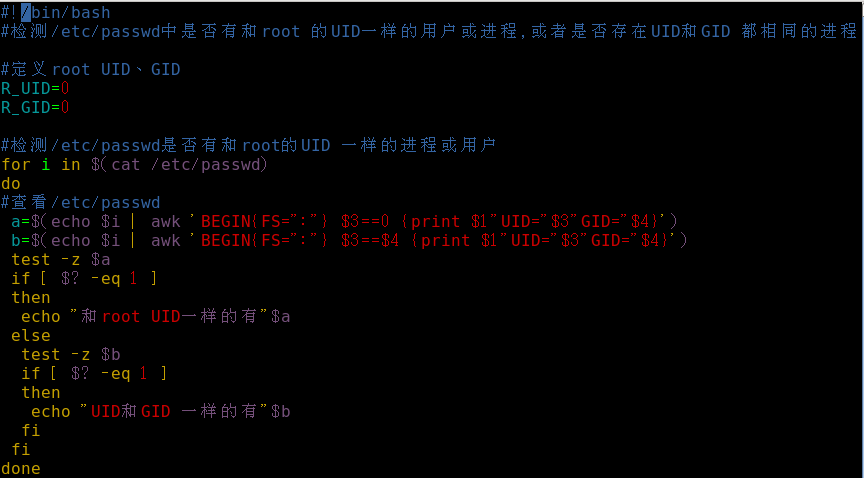
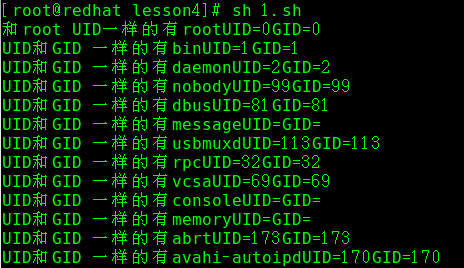
1. root 用户的UID=0，GID=0，检测/etc/passwd 是否有和root 的UID一样，或者是否同时存在两个用户的UID，GID一样

编写脚本



执行结果



1. 检测root密码脚本占位符（X） 是否被改动，不是X说明被修改

编写脚本



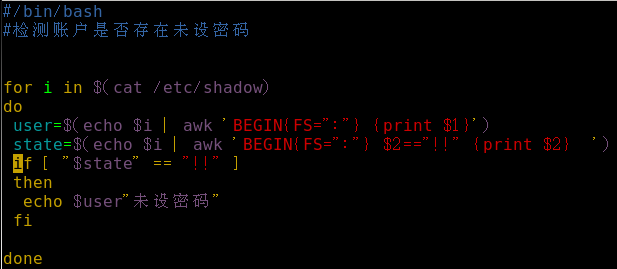
运行结果



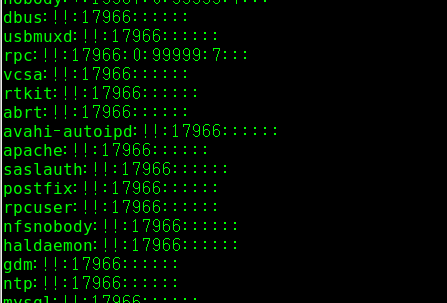
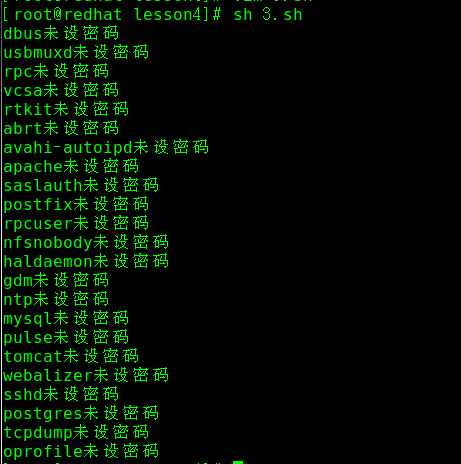


3.检测账户是否存在未设密码（！！ 表示未设密码）

脚本编写

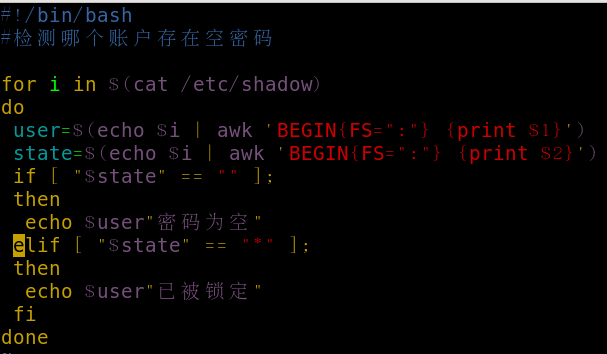


运行结果

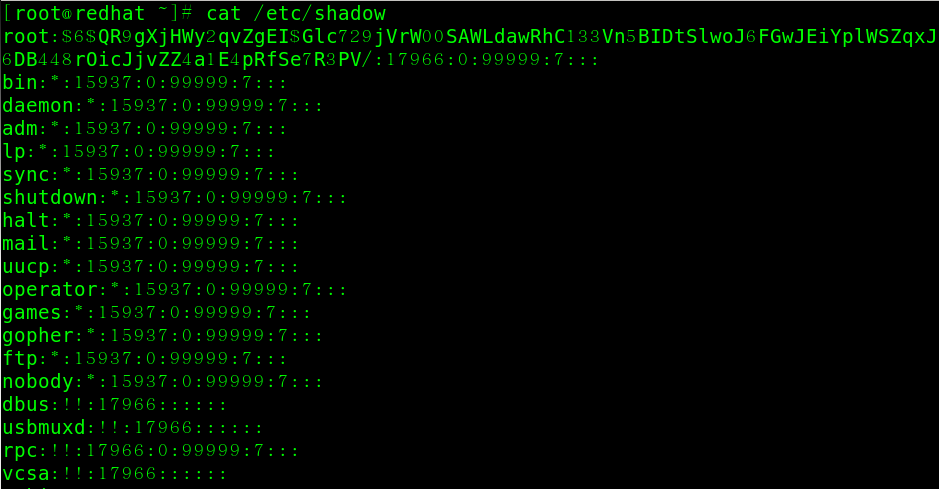
 

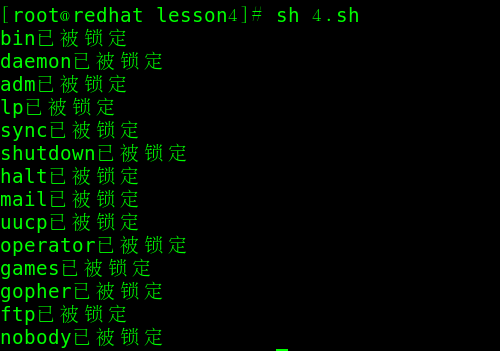
1. 检测到提示哪个账户密码为空或哪些账号被锁定 （”” ：密码为空，“\*” 被锁定）

脚本编写



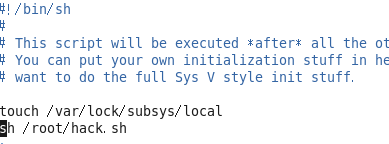
执行结果



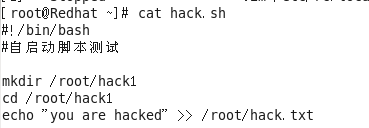


1. rc.local 操作系统自动执行

在rc.local中添加一下运行hack.sh脚本的语句



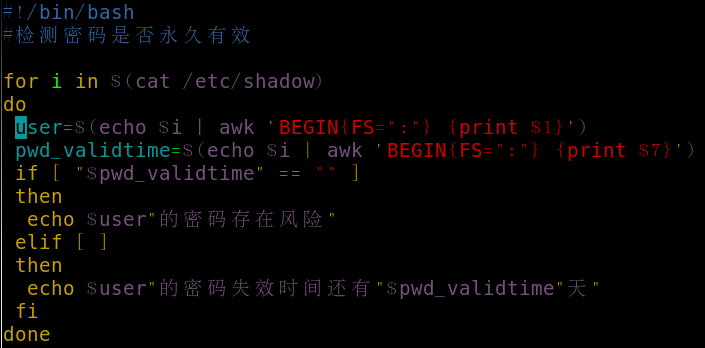
hack.sh 脚本内容如下：在root目录下创建一个hack1文件夹，然后再/root目录下写入一个文件，内容为“you are hacked”

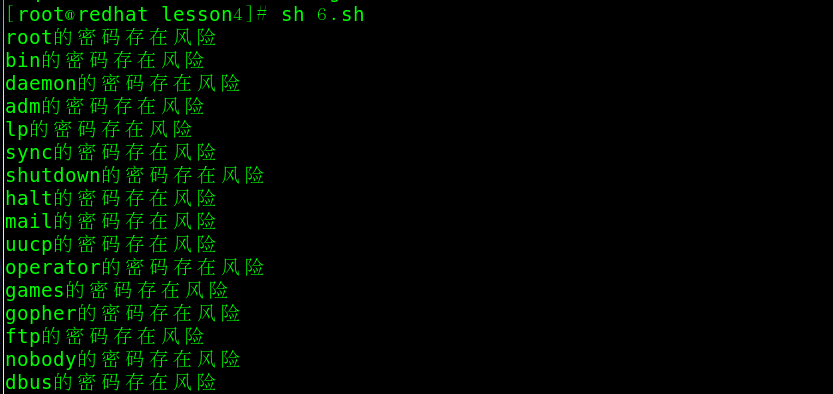


重启测试



1. 检测失效时间，如果为空，则说明密码存在风险





7．检测密码是否永久有效，如果是99999，说明存在风险

脚本编写



运行效果

