**操作系统加固**

**实验报告**

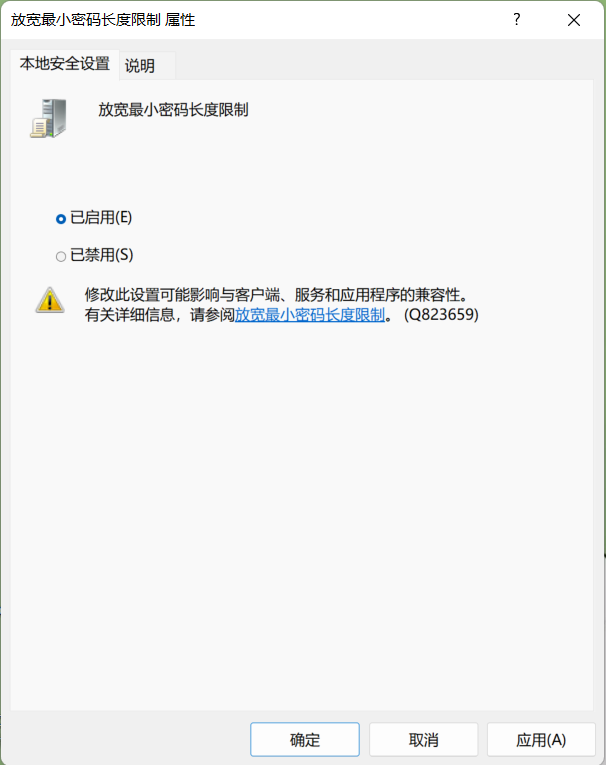
姓名： 蔡欣彤

日期： 2023.7.7

1. **实验内容**
   * 1. 设置最短密码长度为15

本地安全策略-->账户策略-->密码策略（win11）

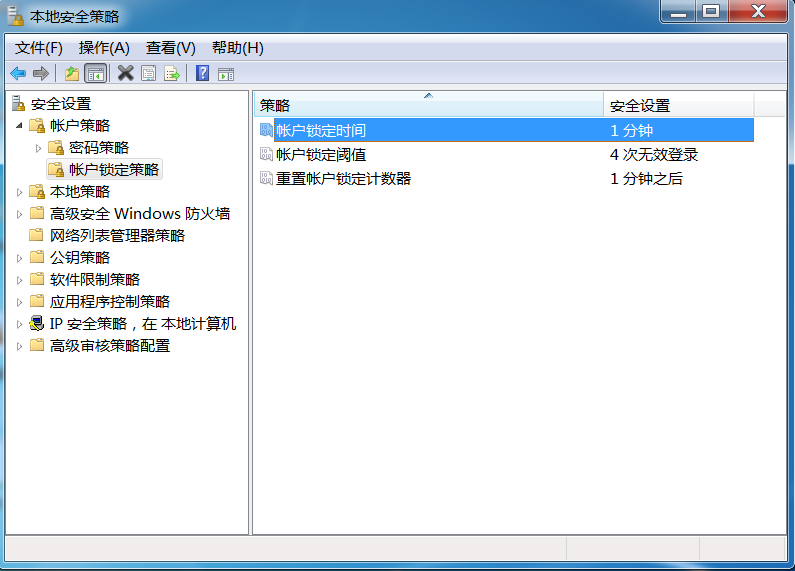
因密码只能在0-14个字符，必须先放宽最小密码长度限制





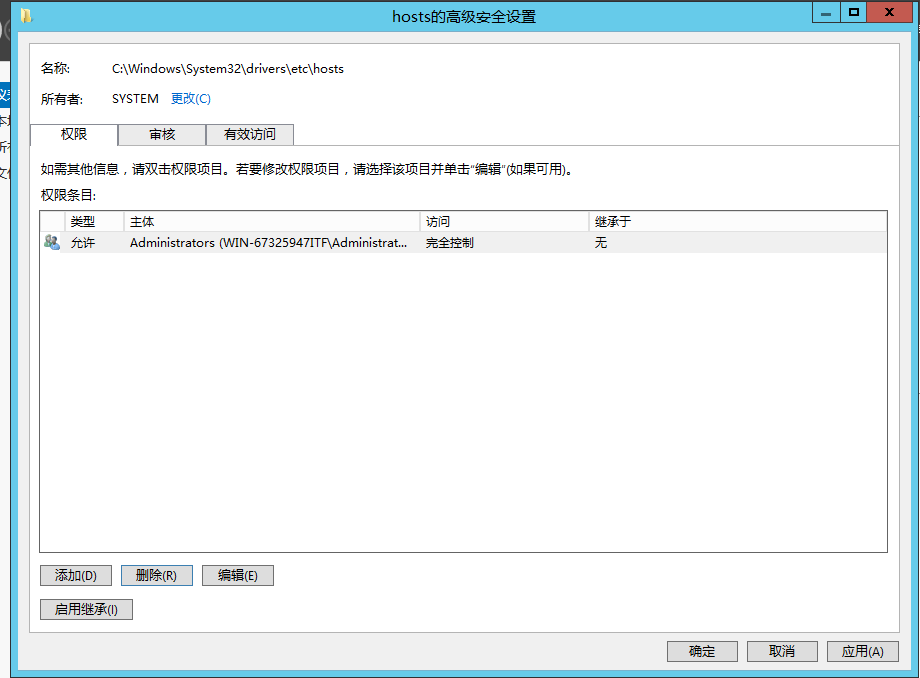
* + 1. 一分钟内仅允许4次登录失败，超过4次，登录帐号锁定1分钟

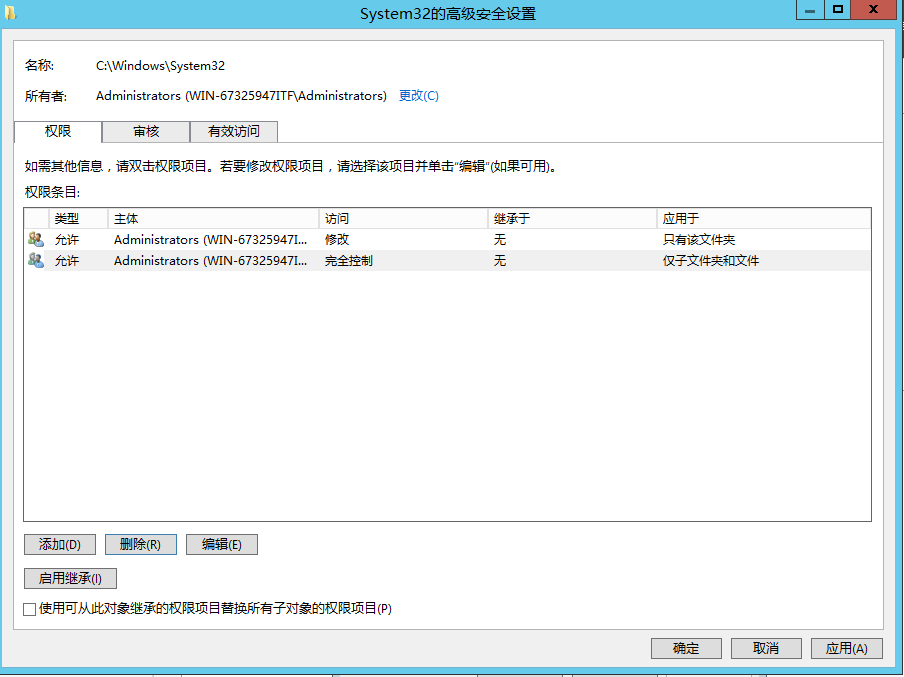
Win7

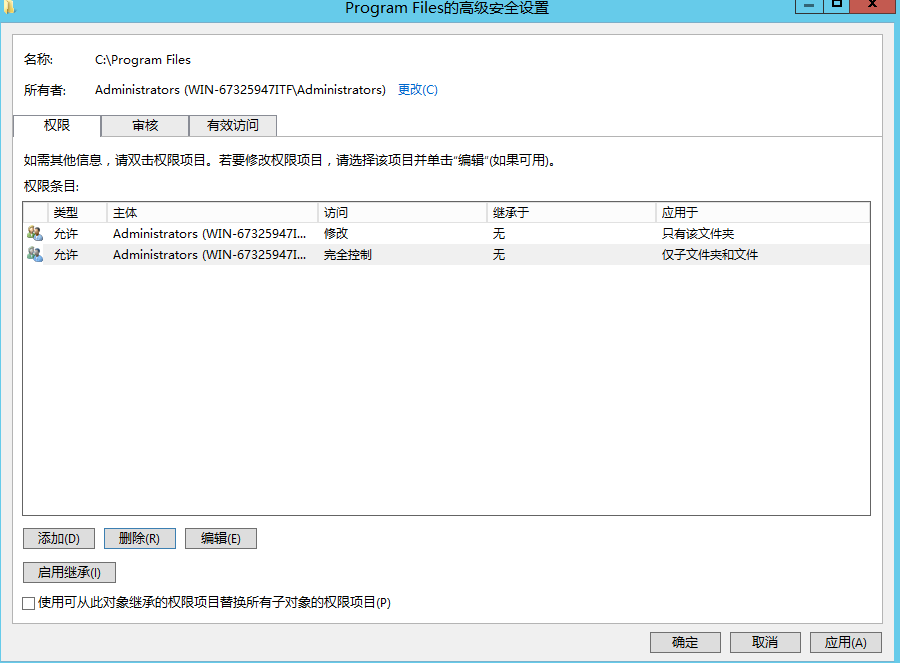


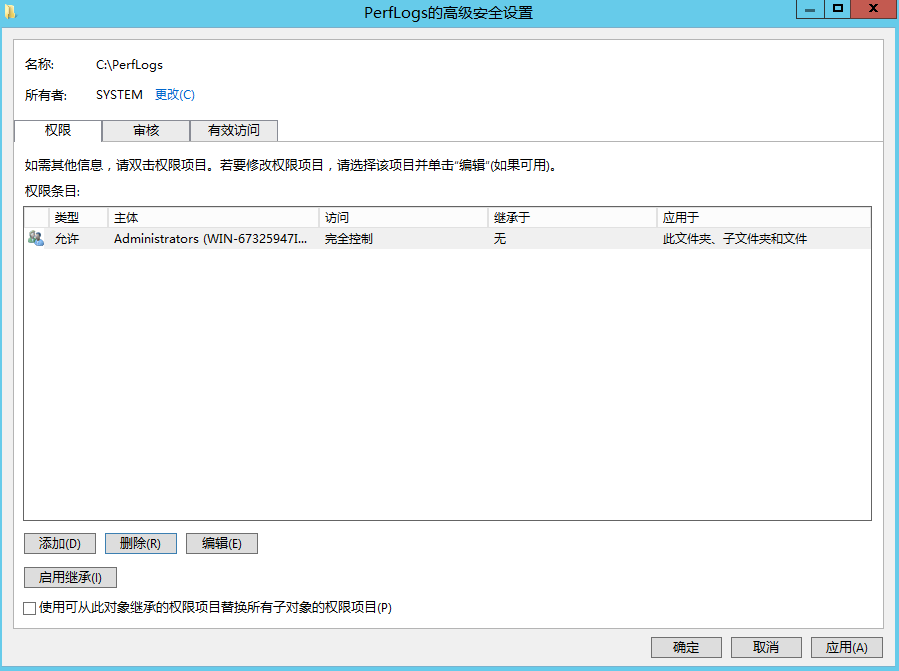
* + 1. 设置操作系统中的关键目录（system32、hosts、Program Files、Perflogs）的权限为最优状态，即仅允许管理员用户进行读取及运行.（Windows server 2012）

找到该文件的位置，然后将其他组删除



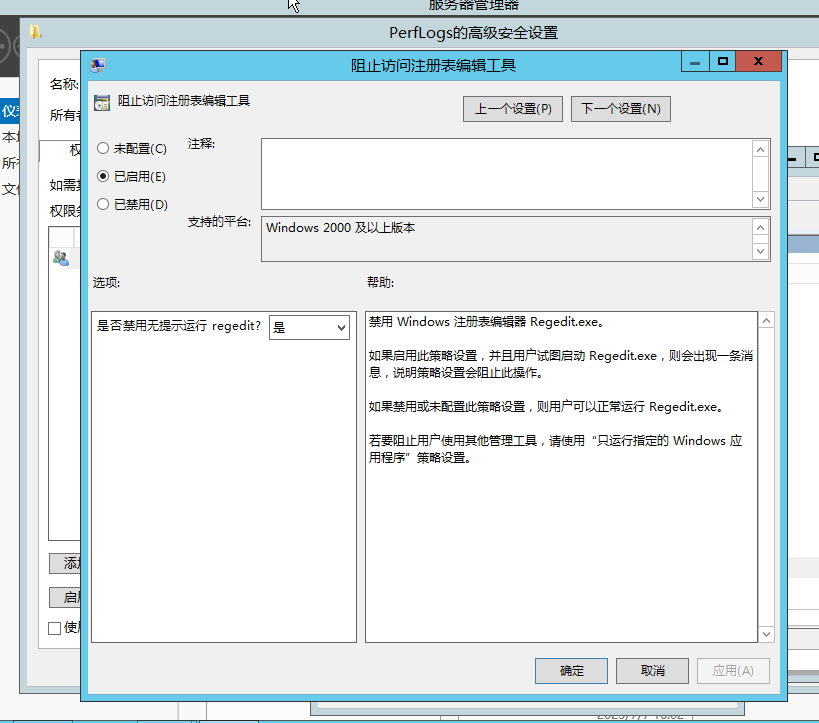




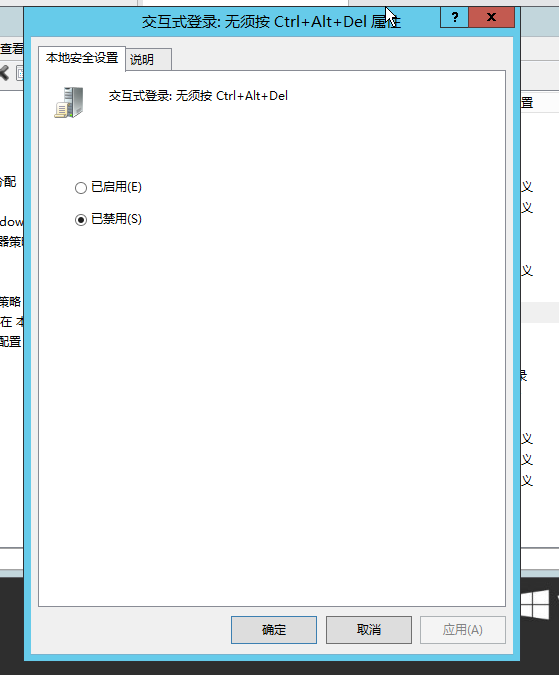


* + 1. 禁止普通用户使用注册表编辑工具以及Ctrl+Alt+Del

Win+r输入gpedit.msc>用户配置>管理模板>系统>防止访问注册表编辑工具

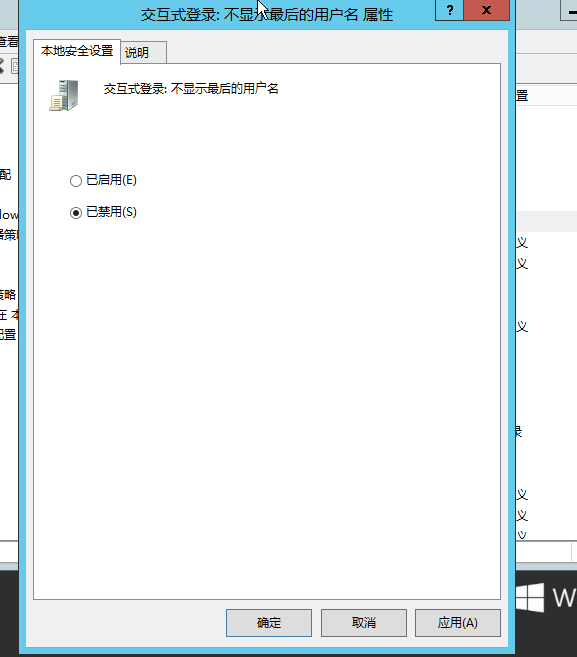


win+r输入secpol,msc>本地策略>安全选项>找到Ctrl+Alt+Del



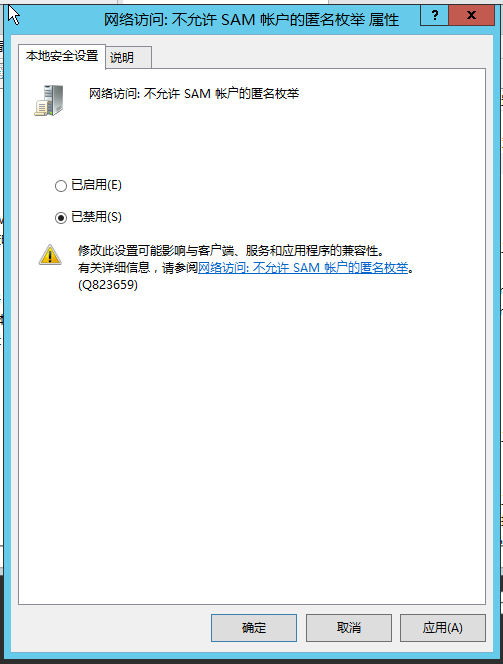
* + 1. 交互式登录时不显示用户名

Win+r输入secpol.msc>本地策略>安全选项>找到图中内容即可



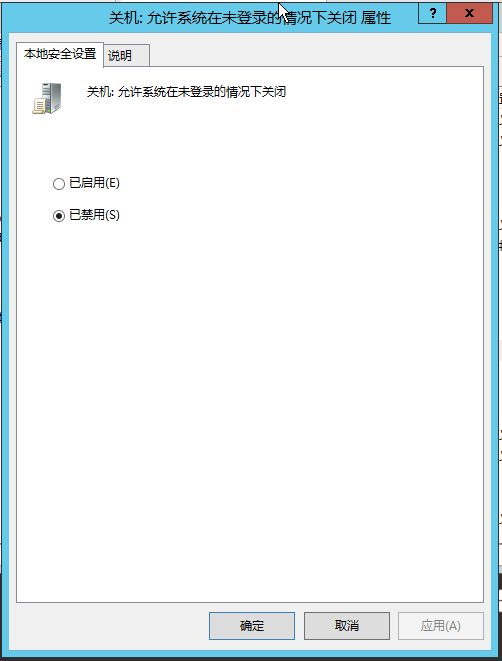
* + 1. 禁止匿名枚举SAM帐户

Win+r输入secpol.msc>本地策略>安全选项>



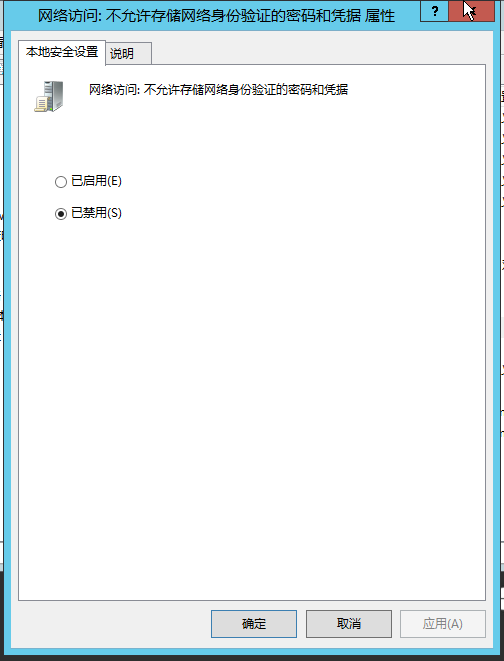
* + 1. 禁止系统在未登录的情况下关闭

Win+r输入secpol.msc>本地策略>安全选项>



* + 1. 禁止存储网络身份验证的密码和凭据

Win+r输入secpol.msc>本地策略>安全选项>



* + 1. 将服务器开启审核策略

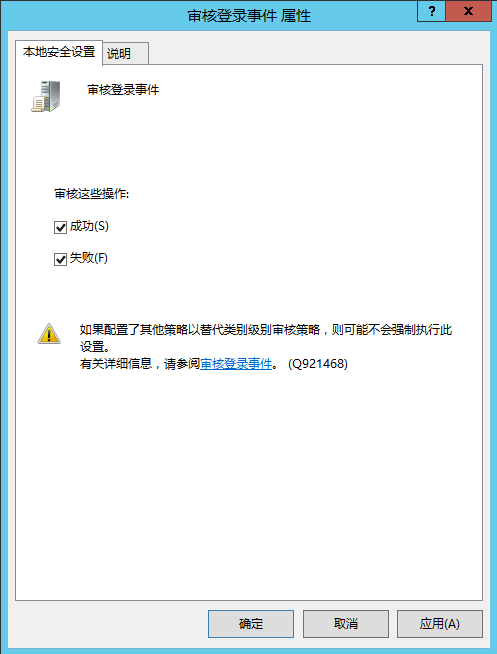
登录事件 成功/失败；

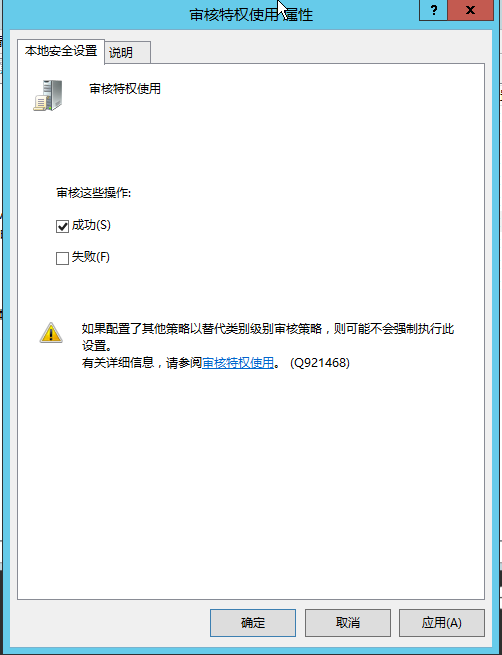
特权使用 成功；

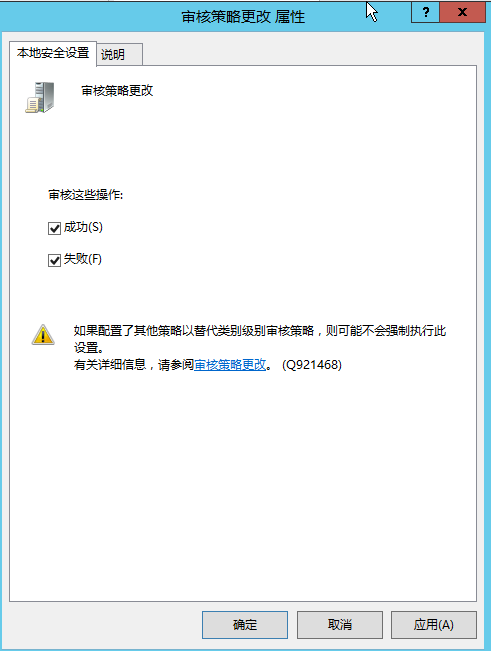
策略更改 成功/失败；

进程跟踪 成功/失败

Win+r输入secpol.msc>本地策略>审核策略



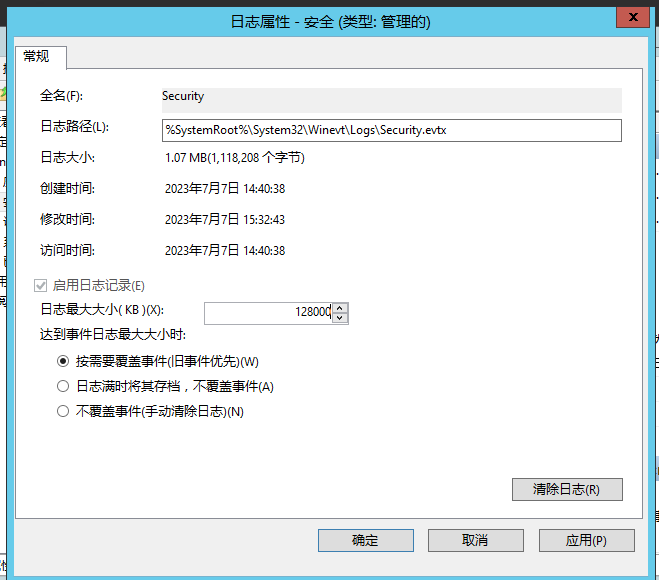






* + 1. 安全日志文件大小至少为128MB，设置当达到最大的日志大小上限时，覆盖早于30天的日志

Win+r输入eventvwr.msc>windows日志>点击安全属性修改日志大小



* + 1. 设置最短密码长度为15

命令：vi /etc/login.defs 设置参数：

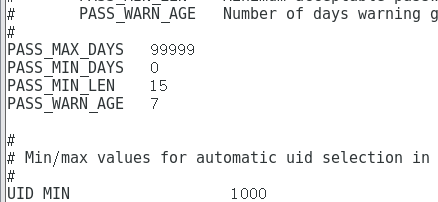
PASS\_MAX\_DAYS 90 新建用户的密码最长使用天数

PASS\_MIN\_DAYS 3 新建用户的密码最短使用天数

PASS\_MIN\_LEN 14 新建用户密码最小长度

PASS\_WARN\_AGE 14 新建用户的密码到期提前提醒 天数

命令： chage --maxdays 90 root 同时执行命令设置 root 密码失效时间



* + 1. 密码策略必须同时满足大小写字母、数字、特殊字符,将密码必须符合复杂性要求的属性



1. **实验总结**

（在实验中遇到的问题及解决方法、收获是什么）

学会了操作系统加固的流程