操作系统加固

实验报告

姓名：蔡欣彤

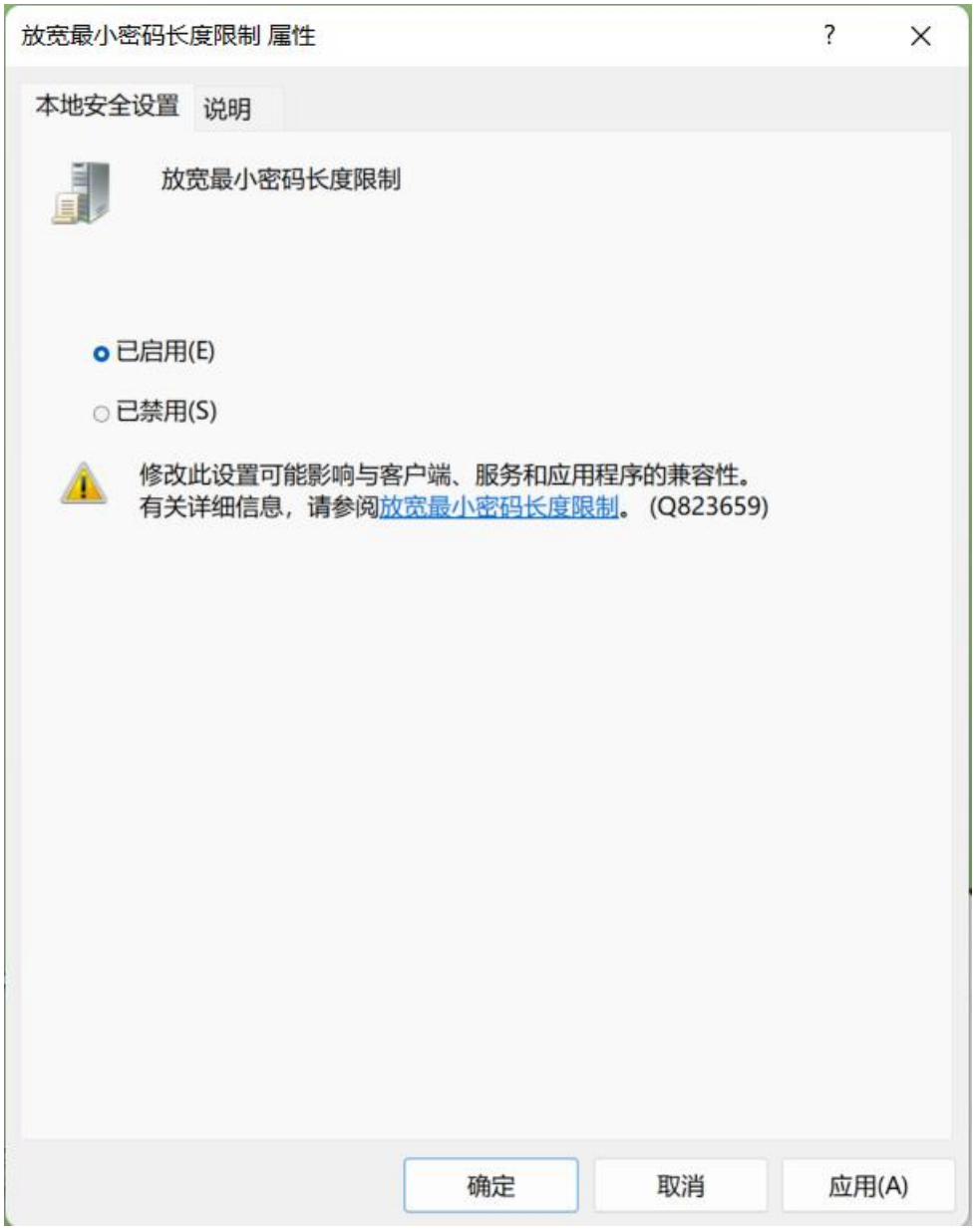
日期：2023.7.7

一、 实验内容

例题 1. 设置最短密码长度为 15

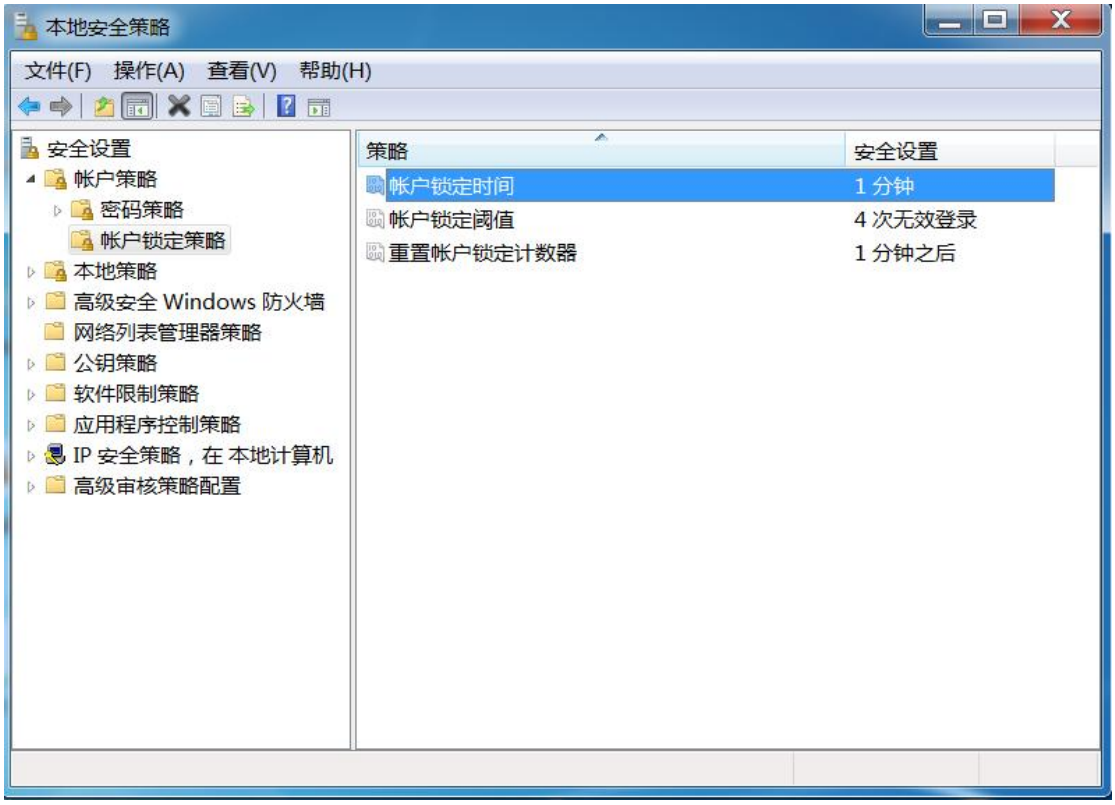
本地安全策略-->账户策略-->密码策略（win11）

因密码只能在 0-14 个字符，必须先放宽最小密码长度限制



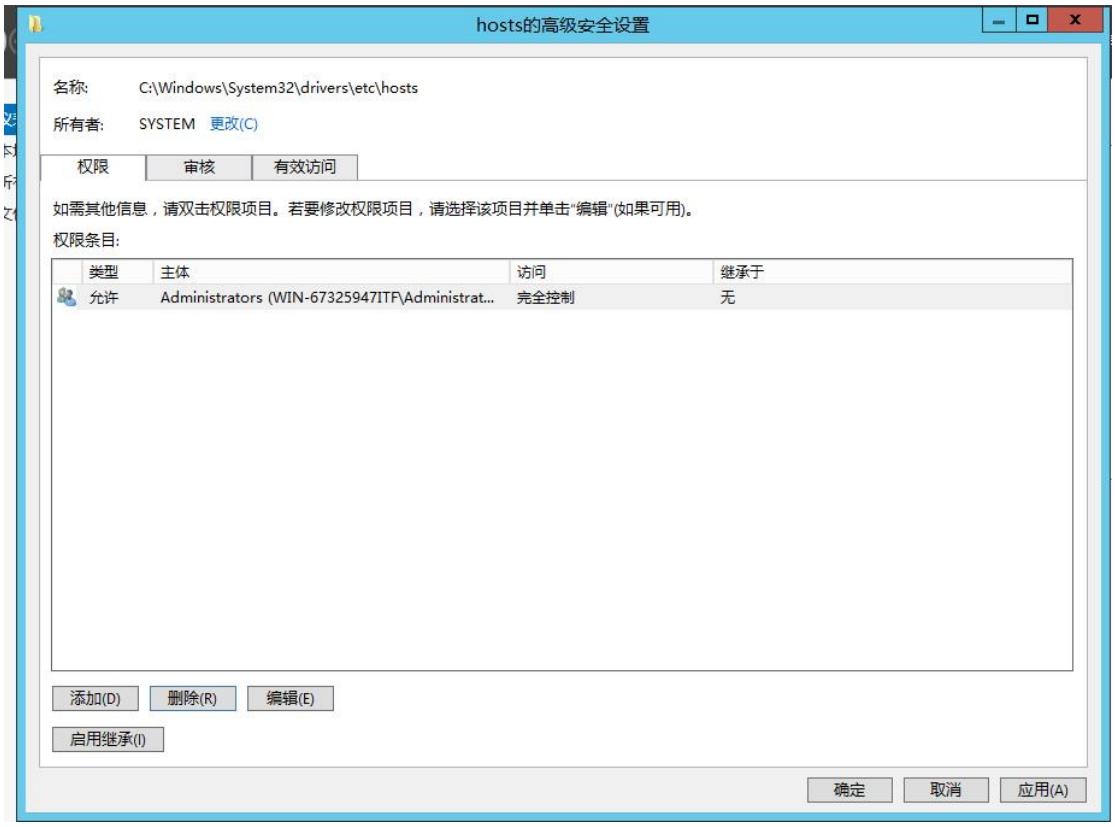
例题 2. 一分钟内仅允许 4 次登录失败，超过 4 次，登录帐号锁定 1 分钟

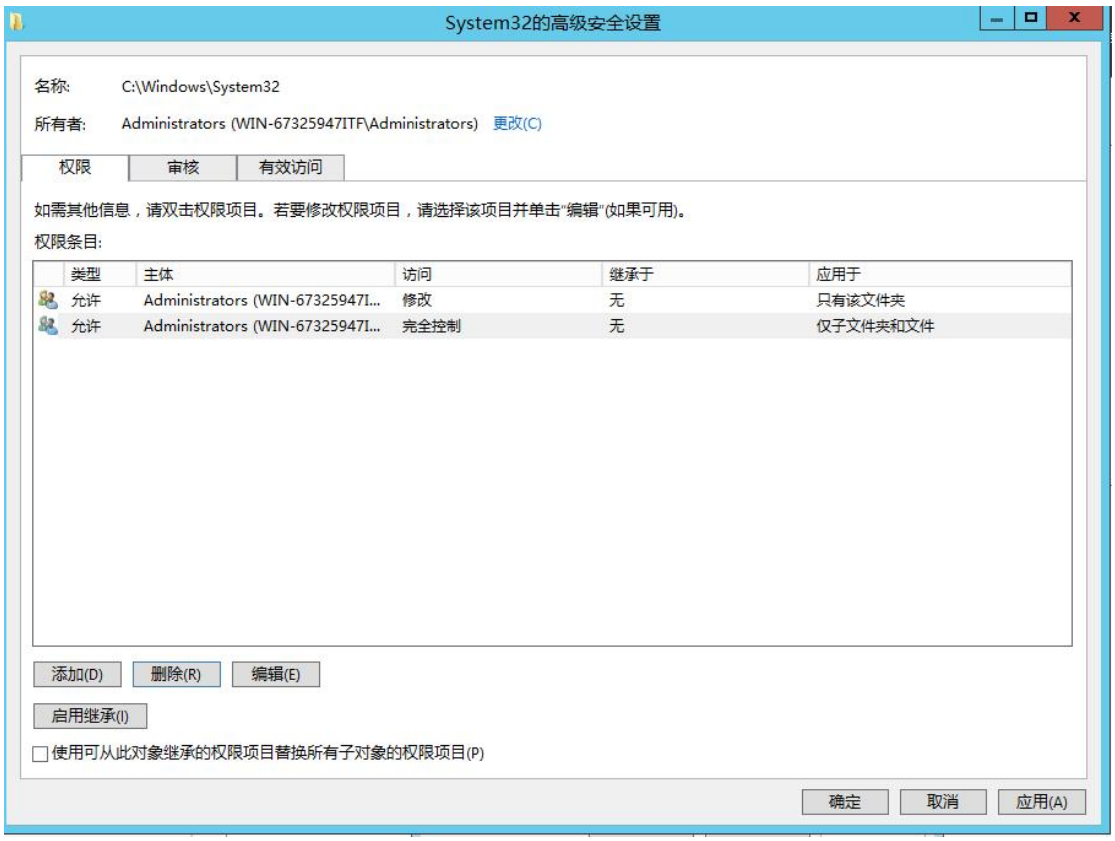
Win7



例题 3. 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）

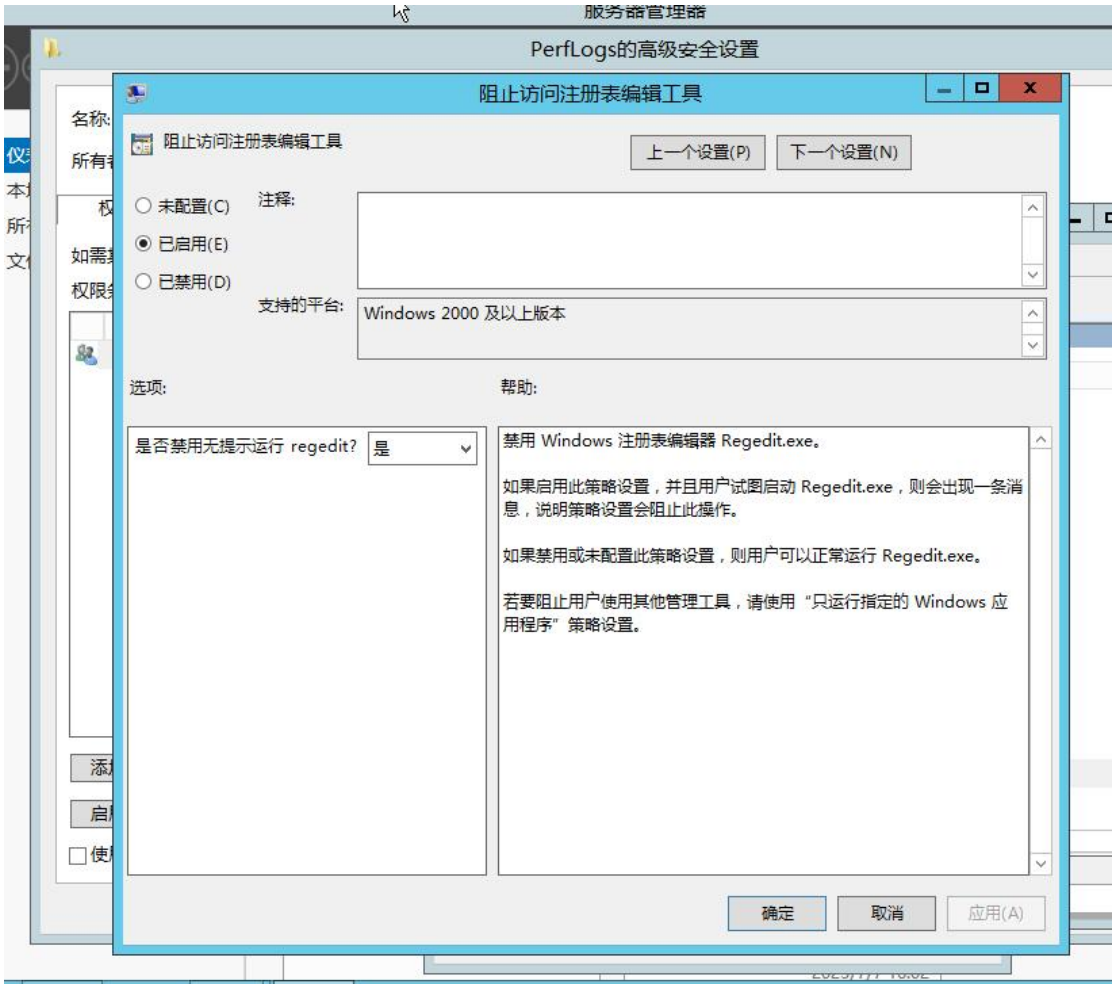
找到该文件的位置，然后将其他组删除


hosts的高级安全设置
名称: C:\Windows\System32\drivers\etc\hosts
所有者: SYSTEM 更改(C)
权限
审核
有效访问
如需其他信息，请双击权限项目。若要修改权限项目，请选择该项目并单击"编辑"(如果可用)。
权限条目:
类型
主体
访问
继承于
允许
Administrators (WIN-67325947ITF\Administrat...
完全控制
无
添加(D)
删除(R)
编辑(E)
启用继承(I)
确定
取消
应用(A)

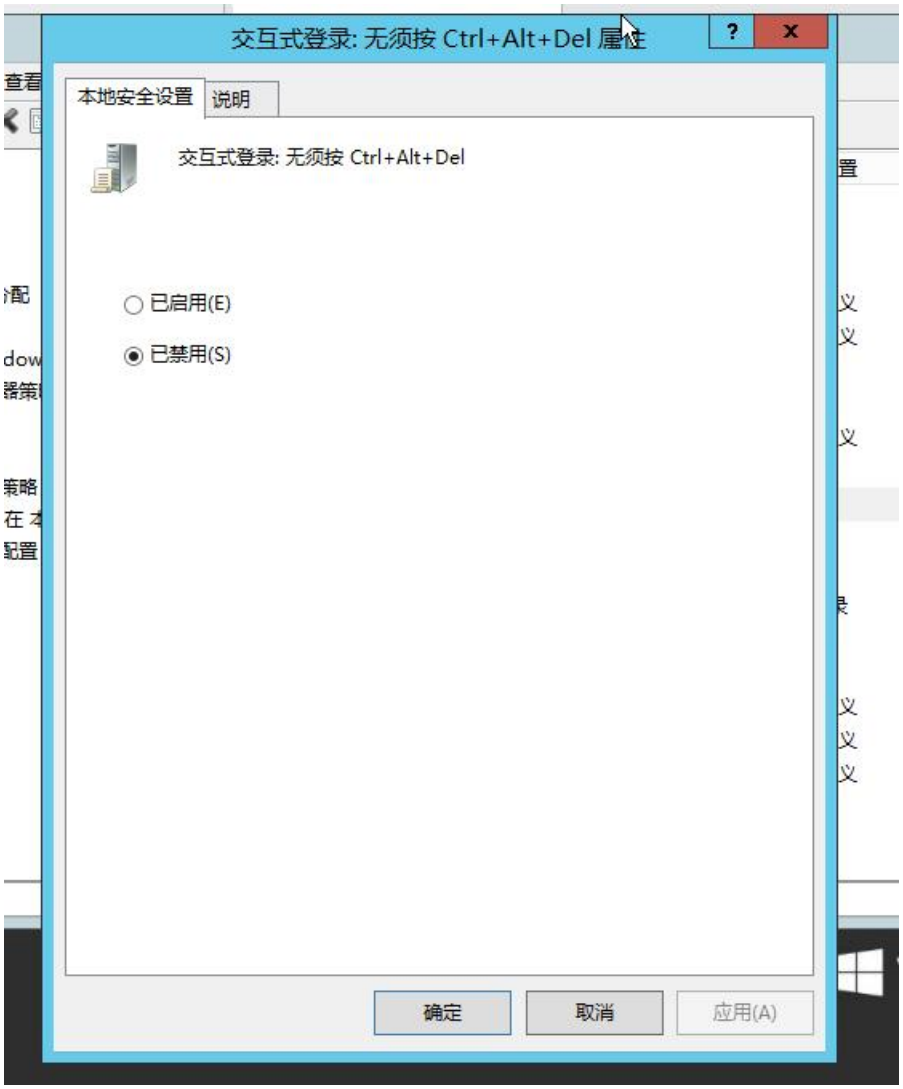

System32的高级安全设置
名称: C:\Windows\System32
所有者: Administrators (WIN-67325947ITF\Administrators) 更改(C)
权限
审核
有效访问
如需其他信息，请双击权限项目。若要修改权限项目，请选择该项目并单击"编辑"(如果可用)。
权限条目:
类型
主体
访问
继承于
应用于
允许
Administrators (WIN-67325947I...
修改
无
只有该文件夹
允许
Administrators (WIN-67325947I...
完全控制
无
仅子文件夹和文件
添加(D)
删除(R)
编辑(E)
启用继承(I)
使用可从此对象继承的权限项目替换所有子对象的权限项目(P)
确定
取消
应用(A)

例题 4. 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

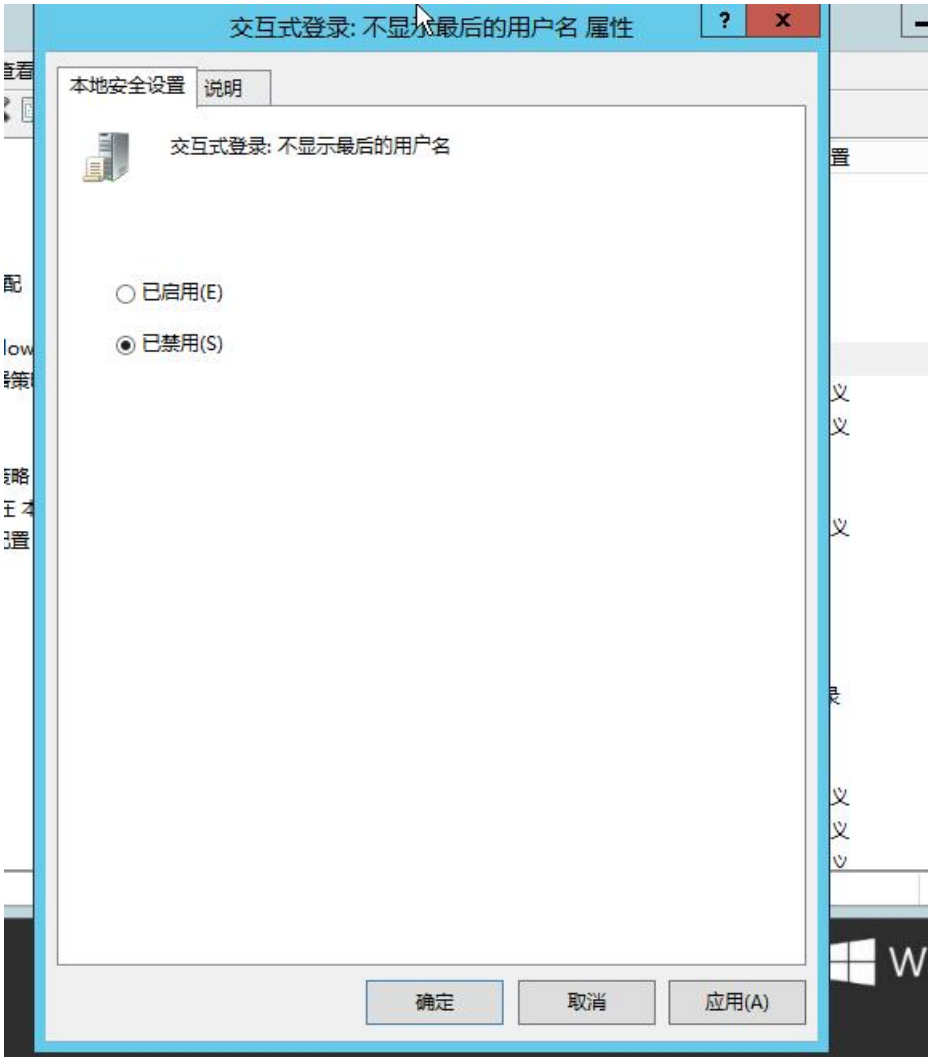


win+r 输入 secpol,msc>本地策略>安全选项>找到 Ctrl+Alt+Del



例题 5. 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

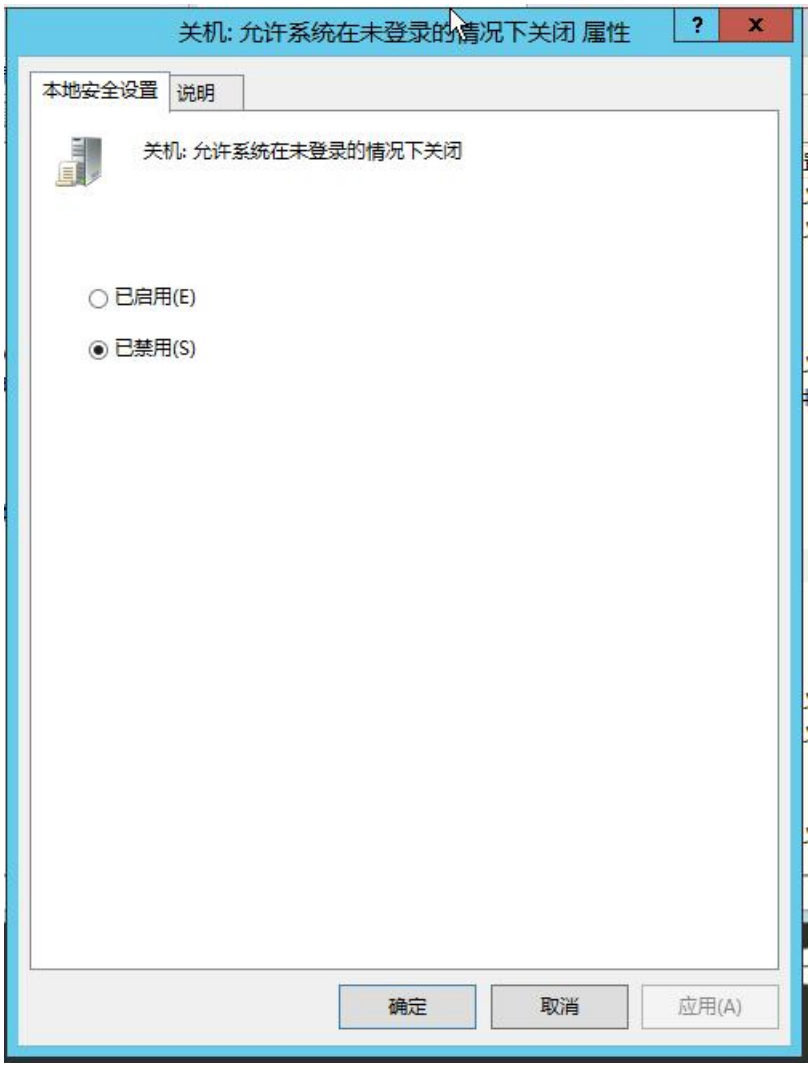


例题 6. 禁止匿名枚举 SAM 帐户

Win+r 输入 secpol.msc>本地策略>安全选项>

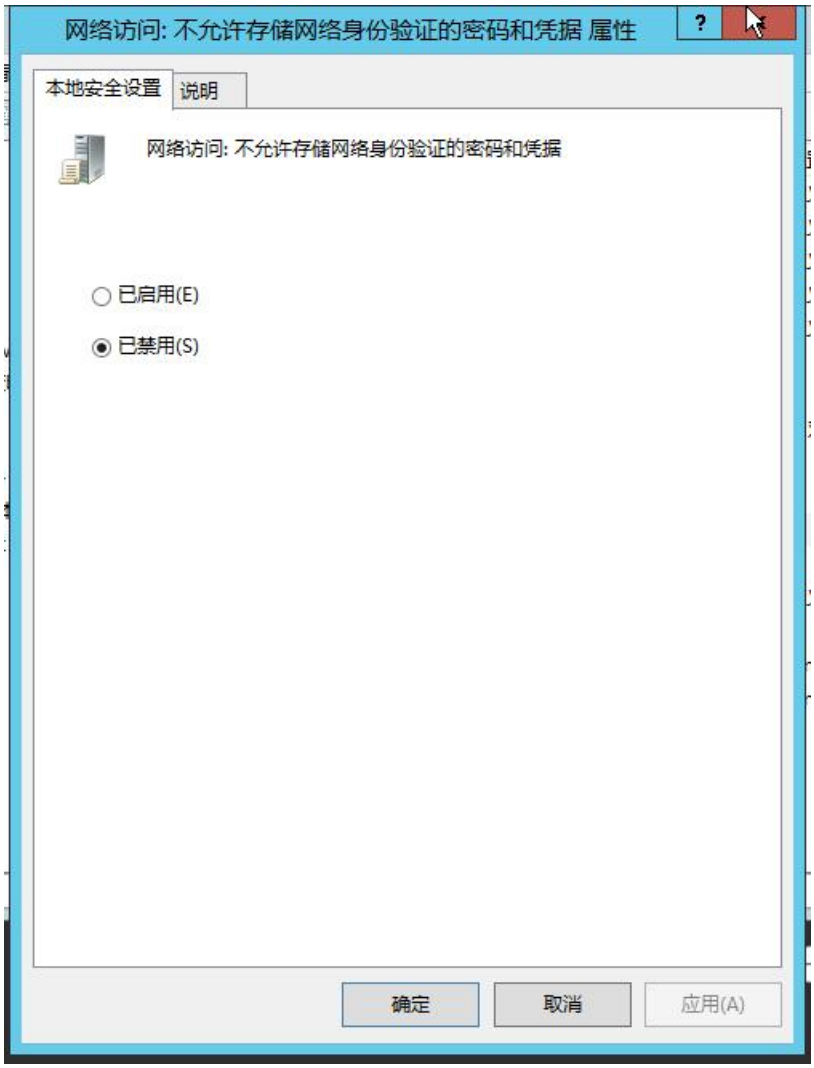
例题 7. 禁止系统在未登录的情况下关闭

Win+r 输入 secpol.msc>本地策略>安全选项>



例题 8. 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>



例题 9. 将服务器开启审核策略

登录事件 成功/失败；

特权使用 成功；

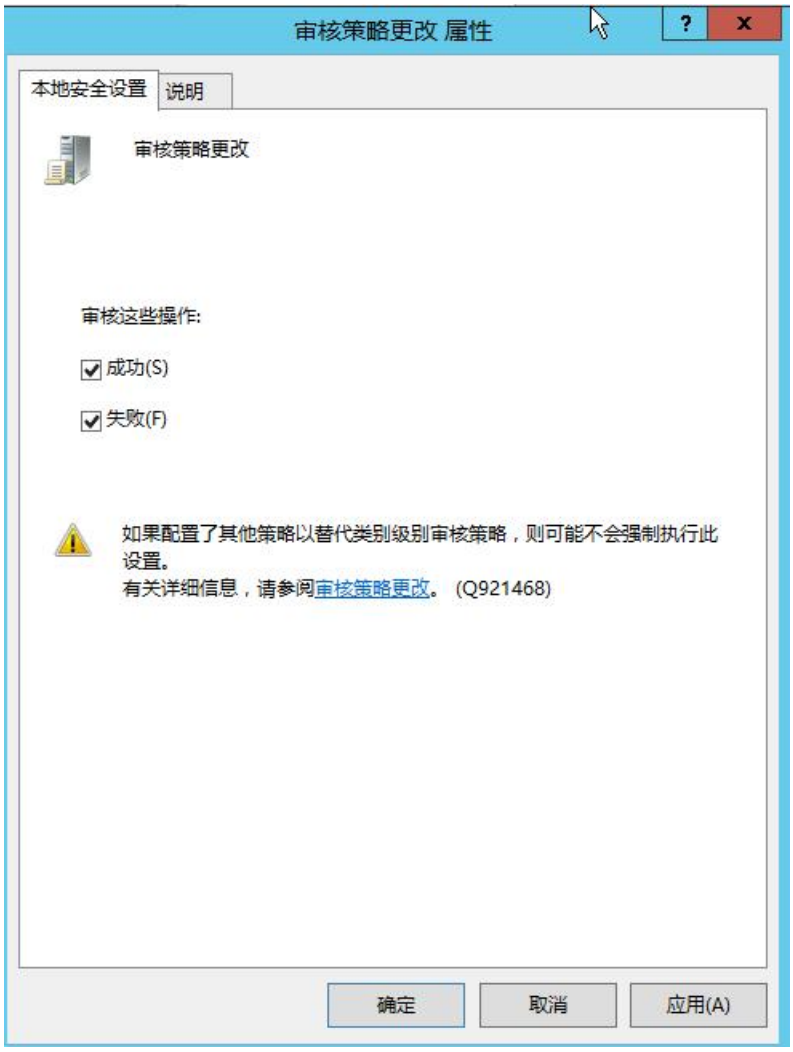
策略更改 成功/失败；

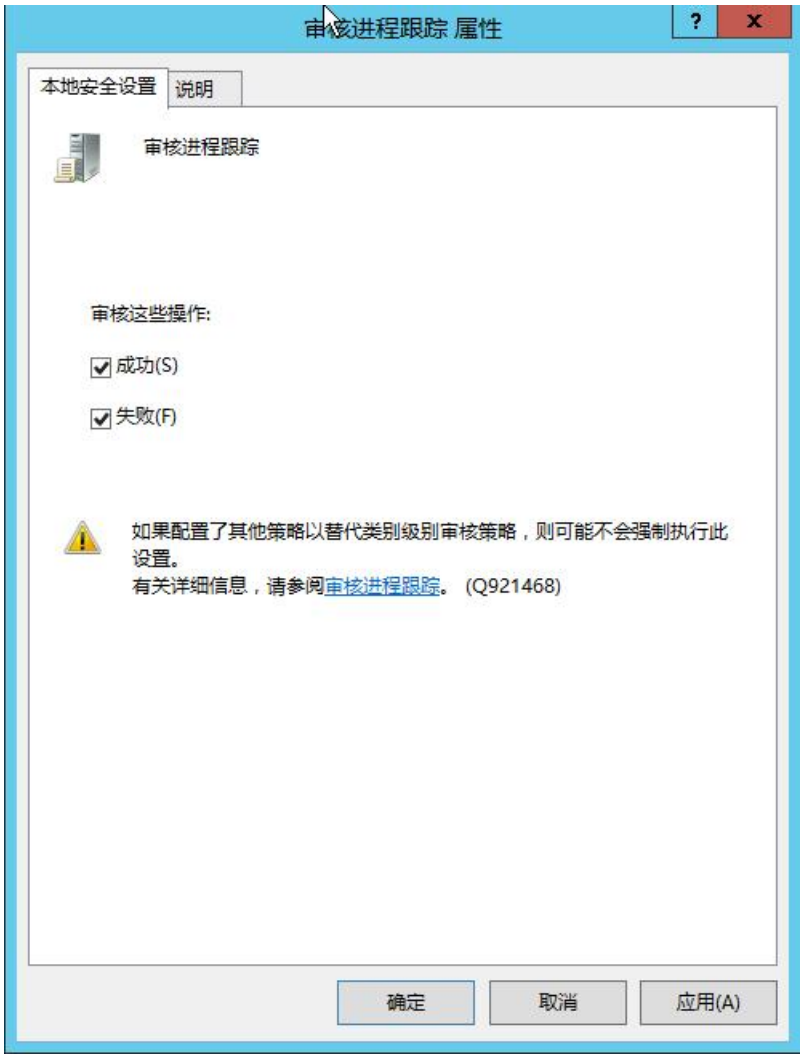
进程跟踪 成功/失败

Win+r 输入 secpol.msc>本地策略>审核策略


审核登录事件 属性
本地安全设置
说明
审核登录事件
审核这些操作:
成功(S)
失败(F)
如果配置了其他策略以替代类别级别审核策略，则可能不会强制执行此设置。
有关详细信息，请参阅审核登录事件。 (Q921468)
确定
取消
应用(A)

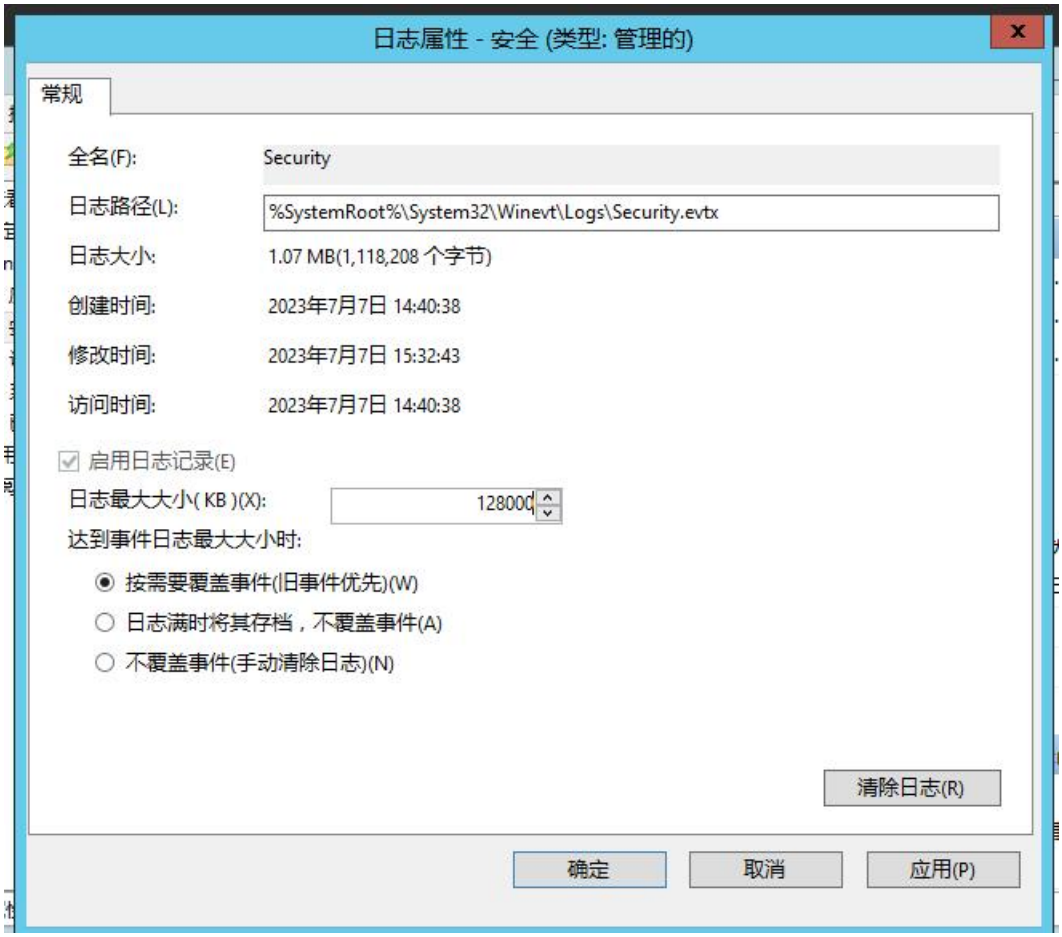

审核特权使用 属性
本地安全设置
说明
审核特权使用
审核这些操作:
成功(S)
失败(F)
如果配置了其他策略以替代类别级别审核策略，则可能不会强制执行此设置。
有关详细信息，请参阅审核特权使用。 (Q921468)
确定
取消
应用(A)


审核策略更改 属性
本地安全设置
说明
审核策略更改
审核这些操作:
成功(S)
失败(F)
如果配置了其他策略以替代类别级别审核策略，则可能不会强制执行此设置。
有关详细信息，请参阅审核策略更改。 (Q921468)
确定
取消
应用(A)



例题 10.　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



例题 11.　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

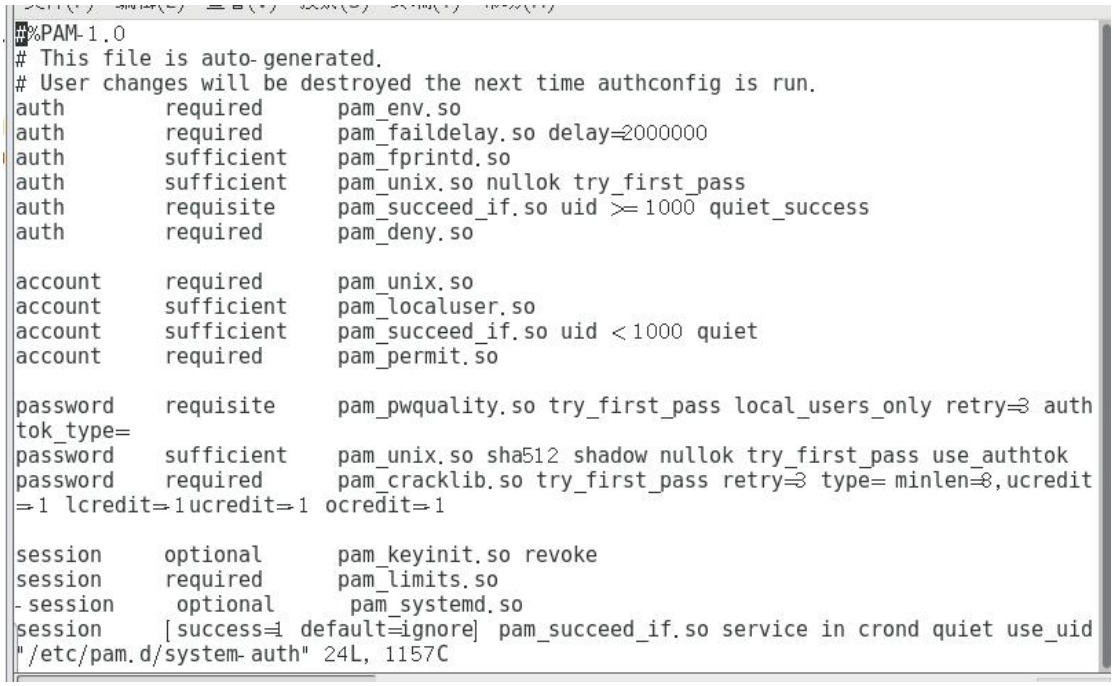
PASS_WARN_AGE 14 新建用户的密码到期提前提醒 天数

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

```
#       PASS_WARN_AGE   Number of days warning g
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    15
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in
#
UID MIN                 1000
```

例题 12.　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



```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 auth
tok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_cracklib.so try_first_pass retry=3 type= minlen=8,ucredit
=1 lcredit=1ucredit=1 ocredit=1

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
"/etc/pam.d/system-auth" 24L, 1157C
```

二、 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