实验 2 Windows用户组查看与安全策略设置

实验目的

1.掌握在windows中管理组策略的方法。
2.通过管理权限限制和保护本地帐户。

实验内容

1.查看自己的Windows系统用户和组；
2.备份当前计算机安全策略；
3.强制执行远程访问的本地帐户限制；
4.强制实施对远程访问的本地帐户限制；
5.拒绝所有本地管理员帐户的网络登录
6.更改账户登录和密码策略

实验步骤

一.查看自己的Windows系统用户和组

1.本地用户有几个，分别是何种权限？

说明：可以在windows nt下输入 `lusrmgr.msc` 命令查看用户组和用户设置.

2.本地用户组有几个，分别用于何种角色？

3.Windows server提供了不少用户组，你对这些用户组的使用意见是？

二.备份当前windows的本地安全策略和当前注册表。

1.运行 `gpedit.msc` ，打开本地组策略编辑器。

2.找到“本地计算机 策略”-“计算机配置”-“Windows 设置”-“安全设置”

3.右键点击“安全设置”，选择“导出策略”，命名文件名为“默认安全策略备份-日期时间”，后缀名为inf。

> 备份的意义在于后续操作失败或无用时，对系统组策略进行恢复。

4.如果需要恢复，可以使用右键点击“安全设置”，选择导入策略，这时选择刚才备份的“默认安全策略备份”即可。

5.使用 `regedit` 打开注册表编辑器。

6.点击菜单“文件”-“导出...”,文件名可以设置为“注册表备份文件-日期”，后缀名为reg。

7.如需恢复，则可用“导入...”功能。

> 注意，注册表备份是系统管理员所必须熟悉，且每周、设置每日都应执行的操作。有能力的同学可以尝试编写一个shell程序，进行自动备份（可申请加分）。

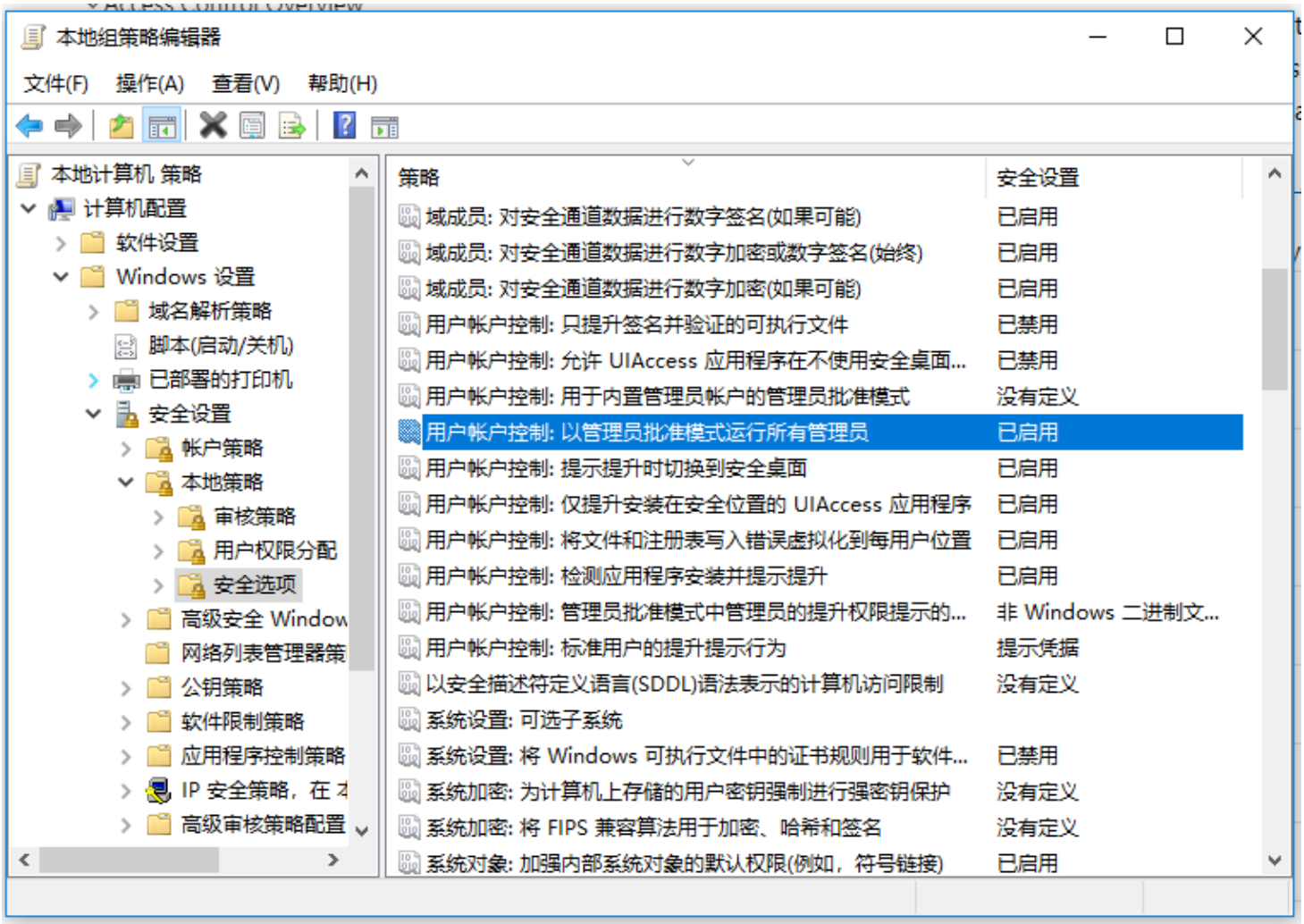
三.强制执行远程访问的本地帐户限制

1.运行 `gpedit.msc` ，打开本地组策略编辑器。

2.找到“本地计算机 策略”-“计算机配置”-“Windows 设置”-“安全设置”。

3.在“安全设置”中，打开“本地策略”-“安全选项”。

4.找到“用户帐户控制: 以管理员批准模式运行所有管理员”，设置为“enable”。



5.请思考，执行此设置的意义是什么？

四.强制实施对远程访问的本地帐户限制

1.使用 `regedit` 打开注册表，然后查看下列位置：

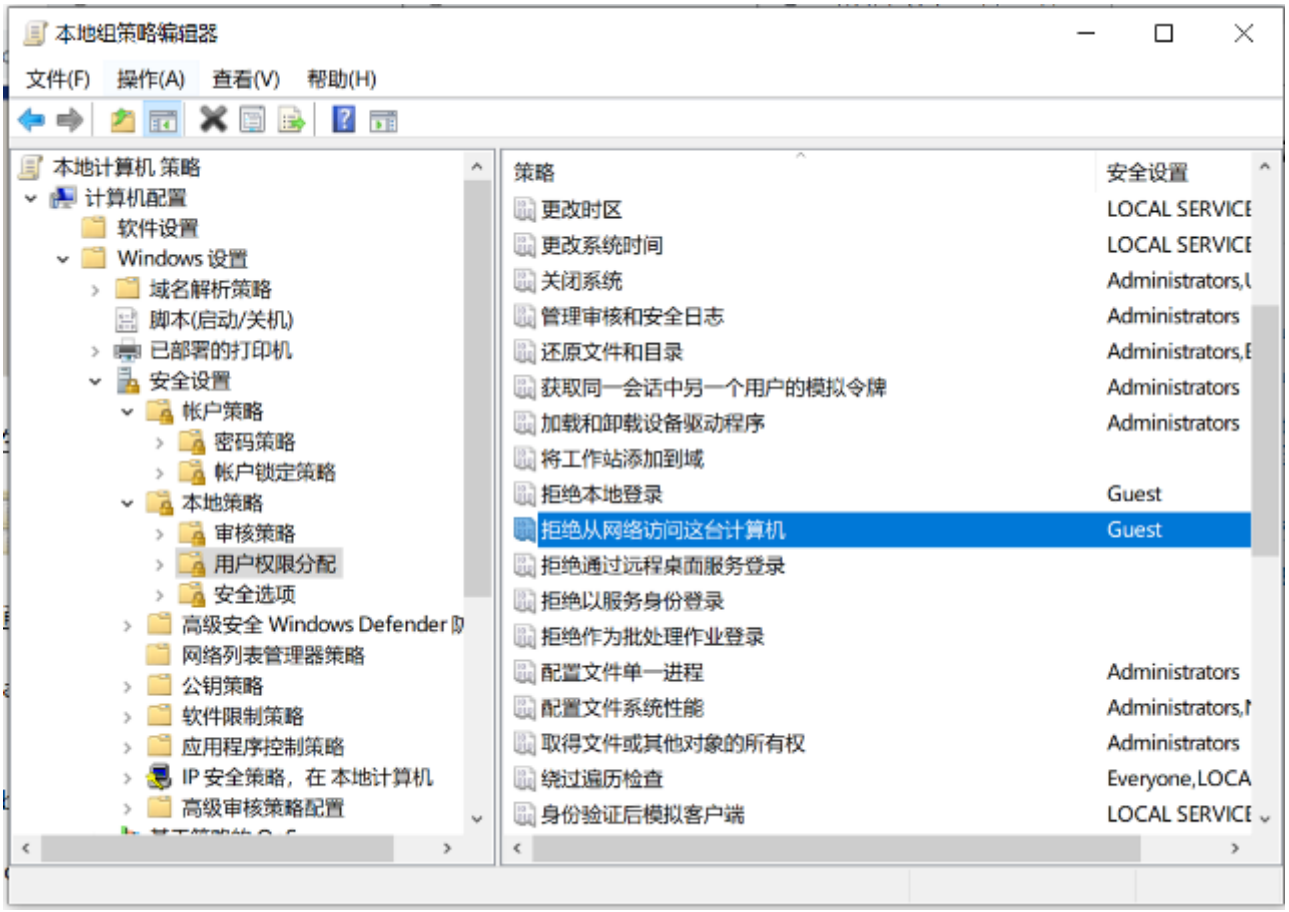
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` .

2.查看键“LocalAccountTokenFilterPolicy”的设置，如果没有则右键点击“新建”，新建类型为“DWORD值",数据值为“0”。

3.启动组策略管理控制台（运行命令 `gpedit.msc` ）；

4.在控制台树中，打开“计算机配置”——"Windows设置"——“安全设置”；

5.继续打开“本地策略”——“用户权限分配”



6.查看当前有哪些用户被禁止从网络访问本台计算机。将结果截图记录于实验报告中。

> windows建议：拒绝所有本地管理员帐户的网络登录。

五.拒绝所有本地管理员帐户的网络登录

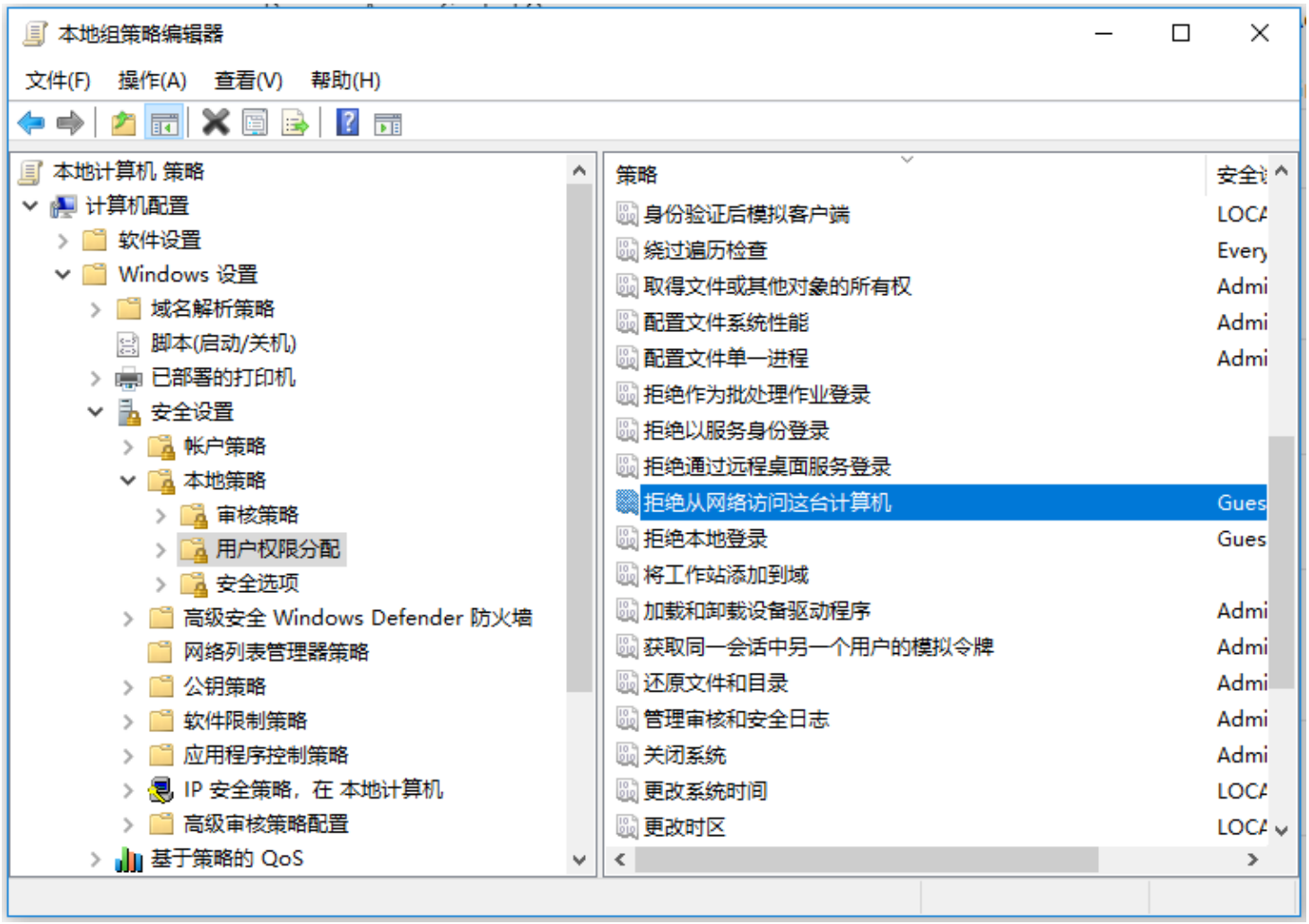
1.运行 `gpedit.msc` ，打开本地组策略编辑器。

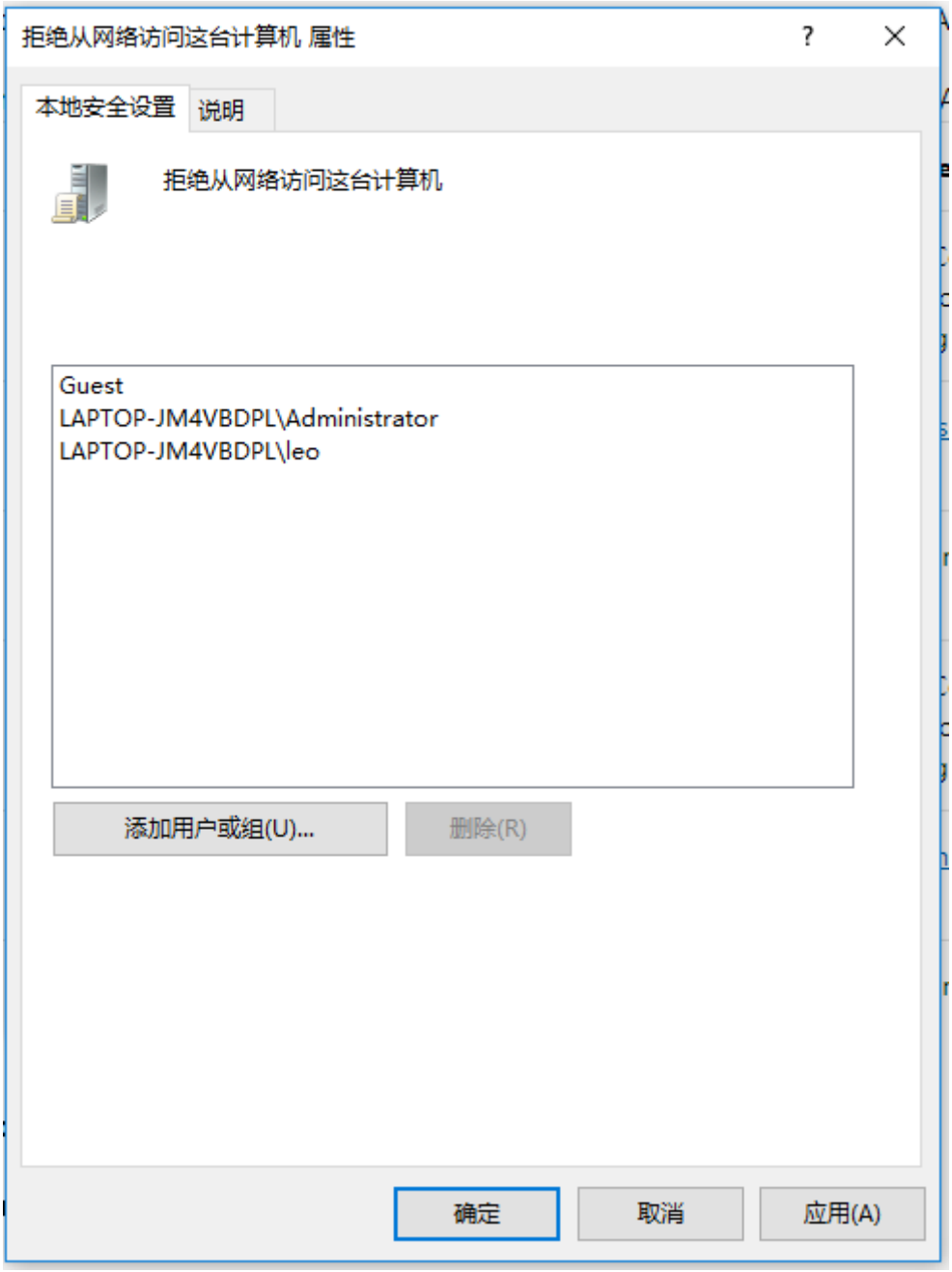
2.找到“本地计算机 策略”-“计算机配置”-“Windows 设置”-“安全设置”。

3.在“安全设置”中，打开“本地策略”-“用户权限分配”。

4.找到“拒绝从网络访问这台计算机”这一策略。

5.双击打开后，点“添加用户或组”，然后找到所有管理员用户，之后确定。


本地组策略编辑器
文件(F)
操作(A)
查看(V)
帮助(H)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析策略
脚本(启动/关机)
已部署的打印机
安全设置
帐户策略
本地策略
审核策略
用户权限分配
安全选项
高级安全 Windows Defender 防火墙
网络列表管理器策略
公钥策略
软件限制策略
应用程序控制策略
IP 安全策略，在 本地计算机
高级审核策略配置
基于策略的 QoS
策略
安全
身份验证后模拟客户端
绕过遍历检查
取得文件或其他对象的所有权
配置文件系统性能
配置文件单一进程
拒绝作为批处理作业登录
拒绝以服务身份登录
拒绝通过远程桌面服务登录
拒绝从网络访问这台计算机
拒绝本地登录
将工作站添加到域
加载和卸载设备驱动程序
获取同一会话中另一个用户的模拟令牌
还原文件和目录
管理审核和安全日志
关闭系统
更改系统时间
更改时区



> windows server 安全建议：拒绝所有本地管理员帐户的网络登录。

六.更改账户登录和密码策略

1.启动组策略管理控制台（运行命令 `gpedit.msc`)。

2.在控制台树中，打开“计算机配置”——"Windows设置"——“安全设置”。

3.继续打开“本地策略”——“账户锁定策略”

4.修改其中“账户锁定阈值”为5次。

5.更改系统建议的“账户锁定时间”为30分钟。

6.更改“充值账户锁定计数器”为30分钟后。

7.修改“密码策略”中的密码长度最小值为8个字符。

8.修改“密码最长使用期限”为30天。

9.开启“密码必须符合复杂性要求”。

以上题目的答案请以实验报告形式提交到高校邦。