**实 验 报 告**

**《信息安全技术》实验 三**

**专业 网络工程　　　　　 实验日期\_\_2023\_年\_\_4\_\_月\_25\_\_\_日**

**班级\_\_\_22网工2班\_\_\_\_\_\_ 学号\_\_\_\_\_220708214\_\_\_\_\_\_ 姓名\_\_\_\_石嘉馨\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| 课程名称 | | 信息安全技术 |
| 实验\_ 3 \_名称 | | 操作系统安全 |
| 实验目的与要求 | | 了解Windows账户与密码的安全策略设置，掌握用户和用户组的权限管理、审核，以及日志的启用，并学会使用安全模版来分析配置计算机。 |
| 实验地点  与实验环境 | | 现教505 计算机网络环境 WindowsServer |
| 实验内容  或实验  主要步骤  实验结果 | 账户与口令  （1）删除不再使用的账户，禁用Guest账户。进入“控制面板”→“用户账户和家庭安全”→“用户账户”→“管理其他账户”，如图 1所示。找到未使用的用户，选择“删除账户”，如果确定永久不再使用，那么相应的账户文件也要选择删除；找到“来宾账户”，选择“关闭来宾账户”；更改管理员账户的名称，避免“admin”等简单账户名。    （2）启用账户策略。进入“控制面板”→“管理工具”→“本地安全策略”。  在“账户策略”→“密码策略”中，启用“密码必须符合复杂性要求”和设置“密码长度最小值”提升密码强度；设定“密码最短使用期限”防止短期内入侵者修改密码；设定“密码最长使用期限”提醒用户定期修改密码，防止密码使用时间过长带来的安全问题。 | |
| 实验内容  或实验  主要步骤  实验结果 | 在“账户策略”→“账户锁定策略”中，设置用户连续登录失败多次，则锁定一段时间，如连续登录失败3次，则锁定30分钟。    在“本地策略”→“安全选项”中，启用“交互式登录：不显示最后的用户名”，防止攻击者从本地或Terminal Service的登录界面看到用户名；启用“网络访问：不允许枚举SAM账户和共享的匿名枚举”，防止攻击者通过空连接匿名枚举出本地所有用户名，如图3所示。 | |
|  | （3）用户和用户组权限管理。任意选择一个文件或者文件夹，右键选择“属性”→“安全”，可以查看到组或用户的管理权限，包括修改、读取和执行、列出内容、读取、写入等，如图4所示。    点击“高级”，进入高级安全设置，选择需要更改的用户或组，点击“编辑”，在弹出的权限项目中勾选权限允许或者拒绝。 | |
|  | 审核与日志  1.启用审核。进入“控制面板”→“管理工具”→“本地安全策略”。在“本地策略”→“审核策略”中，选择需要审核的策略，勾选审核的具体操作。例如更改“审核账户管理”，对成功和失败操作都进行审核 | |
|  | 2．查看日志事件。进入“控制面板”→“管理工具”→“事件查看器”，可以看到“Windows日志”、“应用程序和服务日志”等内容，打开“Windows日志”→“安全”即可查看所有安全事件。    安全模板  （1）启用安全模板。打开“运行”，输入“mmc”进入系统控制台，进入“文件”“添加/删除管理单元”，添加“安全模板”和“安全配置和分析”，如图8所示。    （2）新建安全模板。在“安全模板”中选择“新加模板”，填入名称及描述，建立成功后可以看到该模板下的所有策略，按照不同的需求更改不同的策略项目并保存即可，如图9所示。 | |
|  | （3）添加完毕后回到控制台，在“安全配置与分析”项目中，按照提示打开或新建数据库，如图10所示。(此步骤需要系统中存在配置文件才能操作)    （4）成功导入数据库后，选择“立即分析计算机”，并设置日志文件路径，系统开始按照上一步中选定的安全模板，以确定当前系统的安全设置是否符合要求，分析完毕后可在目录中选择查看各安全设置的分析结果。选择“立即配置计算机”，则按照所选择的安全模板的要求对当前系统进行配置。 | |
| 实验总结 | 合理的权限设置和严格的密码策略可以有效防止恶意攻击。同时，审核策略和日志分析为系统安全提供了重要的监控手段。 | |