西南科技大学

网络攻击与防御
实验报告

实验题目：操作系统加固

学生姓名：

学生学号：

一、 实验作业题目

1. 本地安全策略
2. 账户安全
3. 服务安全

二、 实验思路

本地安全策略

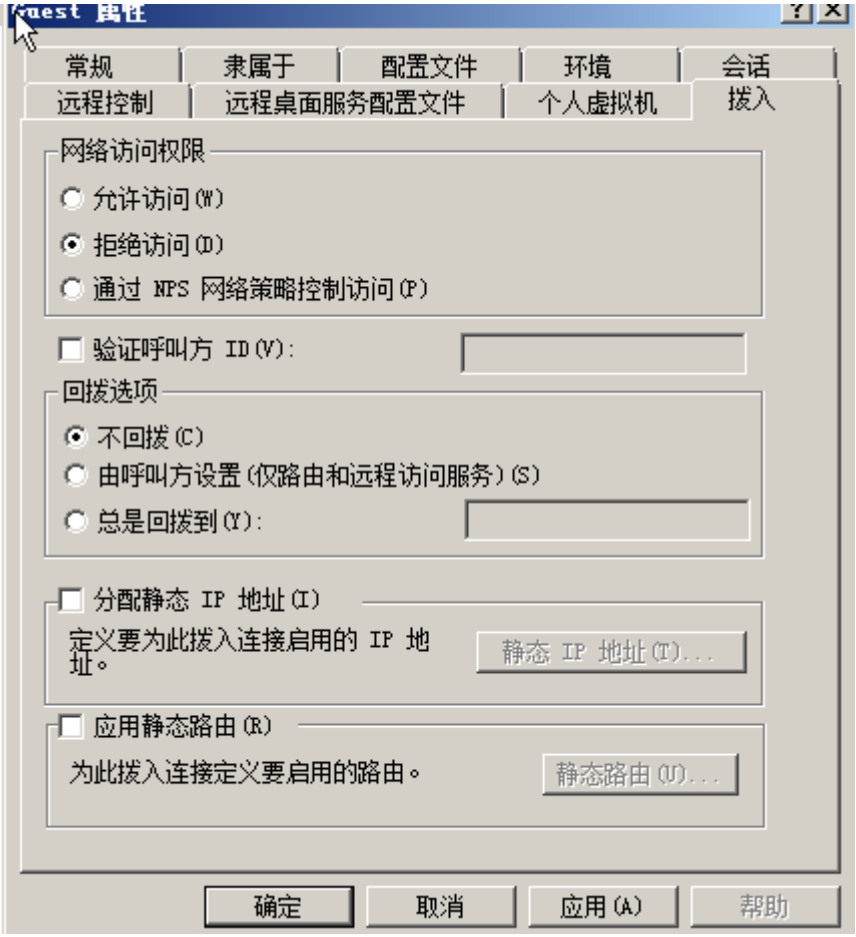
查看本地策略“从网络访问此计算机”，将 Adiministrators 和 Everyone 移除。

更改“拒绝从网络访问此计算机”和“拒绝通过远程桌面服务登

录”，加入 Everyone 防止攻击。

账户安全

将 Guest 用户网络访问权限设置为“拒绝访问”



服务安全

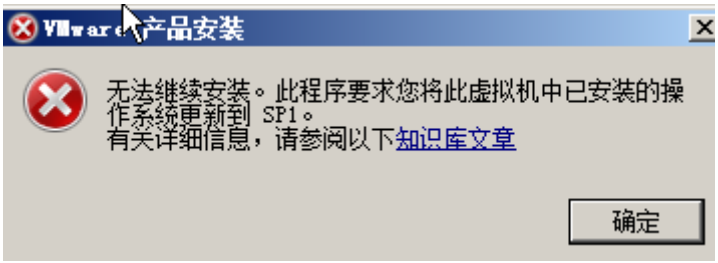
禁用 Computer Browser

禁用 Remote Registry

手动启动 Distributed Transaction Coordinator

三、 实验分析及总结（写自己在实践过程中遇到的问题及解决方法；本次实验体会、收获）

问题：安装系统后，无法安装 vmtools



解决办法：镜像比较老，更换镜像重新安装就可以安装成功。

思考 1：服务器版与专业版在安全设置方面需考虑哪些不同？

服务版通常面向企业网络环境，需严格限制外部网络对服务器的访问，配置防火墙规则时要精细划分不同网段的访问权限。涉及大量用户和用户组，需根据业务角色严格分配权限，定期审查用户权限，防止权限滥用。需制定完备的备份策略且要定期测试恢复流程，确保数据在遭受攻击或丢失时能快速恢复。需部署专业监控工具，实时监测服务器性能、网络流量、用户操作等。对关键操作进行审计记录，便于追溯问题和排查安全事件。

专业版需遵循行业法规要求，需关注软件兼容性带来的安全风

险。及时更新补丁，对新发现的漏洞要迅速评估和修复，同时测试补丁对业务系统的影响。需要更高级别的身份认证方式，如双因素认证、生物识别认证等。采用更严格的安全隔离措施。

思考 2：你所了解的 IIS 服务有哪些安全隐患，应该如何进行安全加固？

安全隐患：代码执行漏洞、文件上传漏洞、弱密码与默认配置、SSL/TLS 配置缺陷等。

安全加固：定期对应用程序代码进行安全审计，检查输入验证、输出编码等环节，防止注入漏洞；采用安全的编码规范，避免使用存在安全风险的函数和方法；严格限制文件上传类型，只允许上传必要的文件格式，并对上传文件进行重命名和存储路径隔离，防止恶意脚本执行；强制要求管理员设置强密码，定期更换密码；修改 IIS 默认配置；定期审查用户账户，删除无用账户；使用最新且安全的 SSL/TLS 协议版本，配置安全的加密算法套件；定期检查证书有效期，及时更新证书；安全补丁更新。

体会及收获：

在本地安全策略设置中，调整“从网络访问此计算机”等策略，账户安全方面，设置 Guest 用户网络访问权限为“拒绝访问”，降低潜在风险。服务安全操作里，禁用不必要服务、手动启动关键服务，增强了系统安全性。