**2021年技能大赛“网络安全”（中职组）**

**A模块电子答题卡**

**组号：**

一、项目和任务描述：

假定你是某企业的网络安全工程师，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。

二、服务器环境说明

服务器WindowsServer

用户名:administrator密码：123456

服务器：LinuxServer

用户名：root，密码：123456

数据库用户名：root，密码：123456

请对服务器WindowsServer按要求进行相应的设置，提高服务器的安全性。

三、说明：

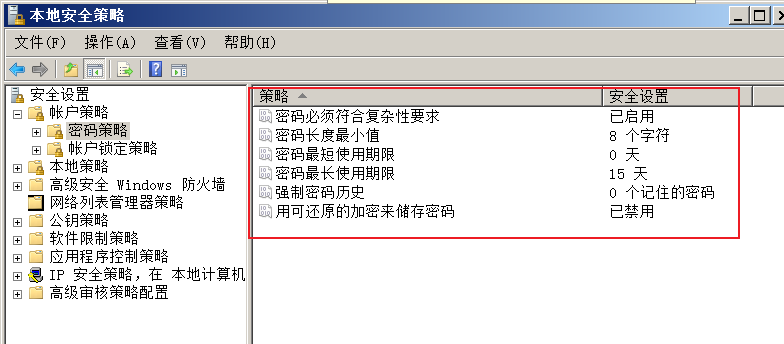
1.所有截图要求截图界面、字体清晰，并粘贴于相应题目要求的位置；

2.文件名命名及保存：网络安全模块A-XX（XX为工位号），PDF格式保存；

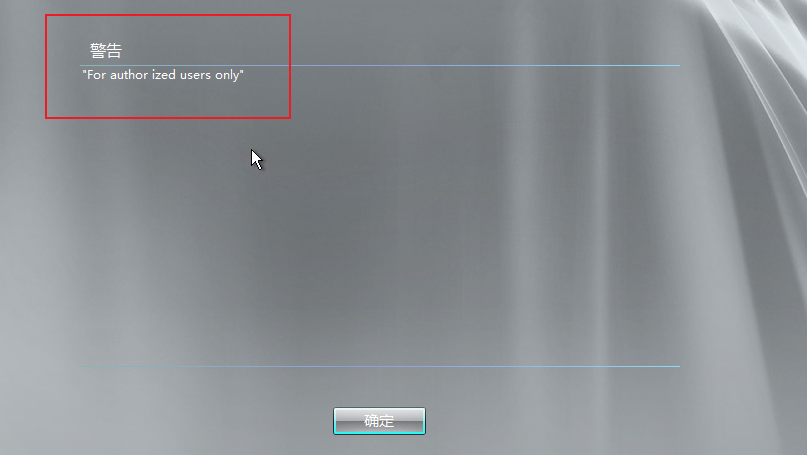
3.文件保存到U盘提交。

### A-1：Windows操作系统安全配置

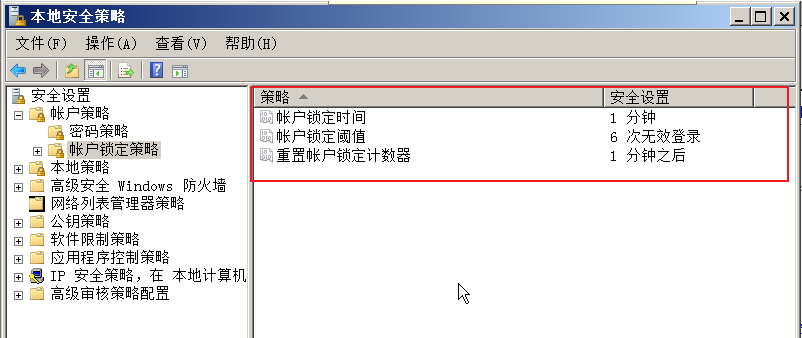
1.设置密码策略必须同时满足大小写字母、数字、特殊字符，最小密码长度不少于8个字符，密码最长使用期限为15天。将服务器上密码策略配置信息截图;



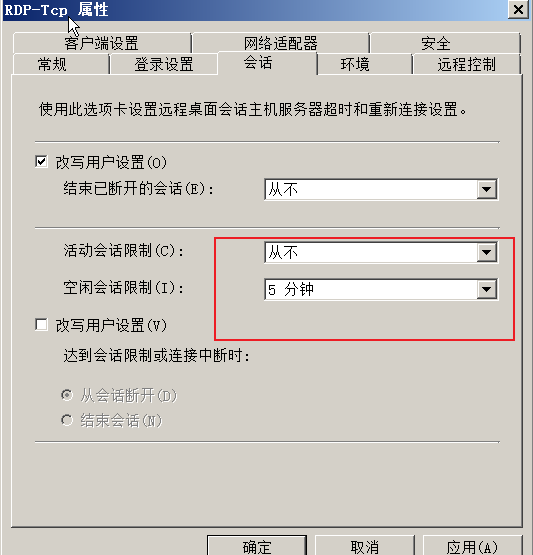
2.在用户登录系统时，应该有“For authorized users only”提示信息，将登录系统时系统弹出警告信息窗口截图;



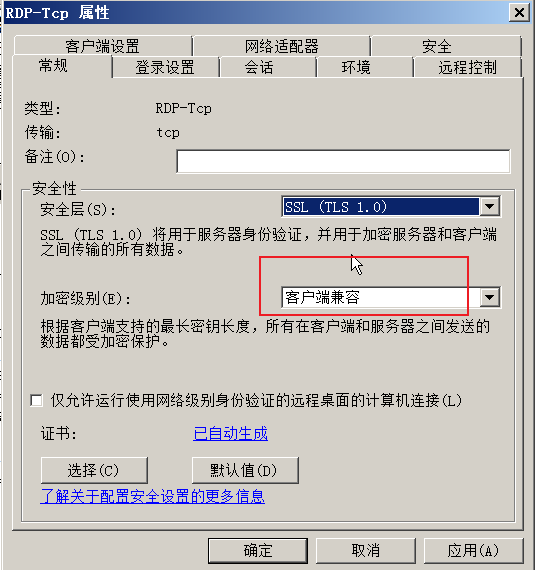
3.一分钟内仅允许5次登录失败的尝试，超过5次，登录帐号锁定1分钟,将账号锁定策略配置信息截图；



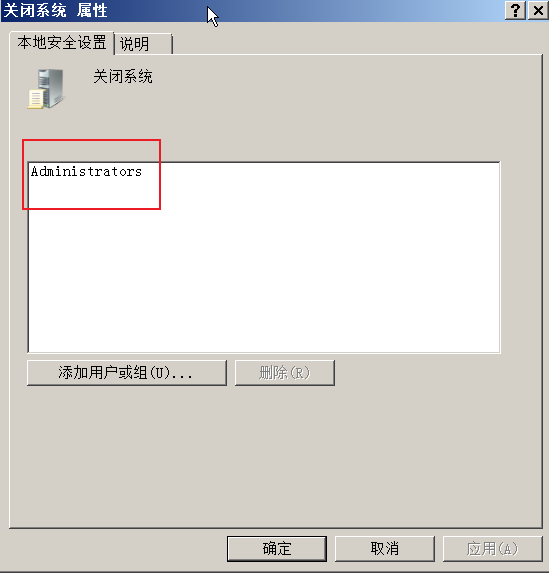
1. 设置远程桌面用户非活动会话连接超时应小于等于5分钟，将RDP-Tcp属性对应的配置界面截图；



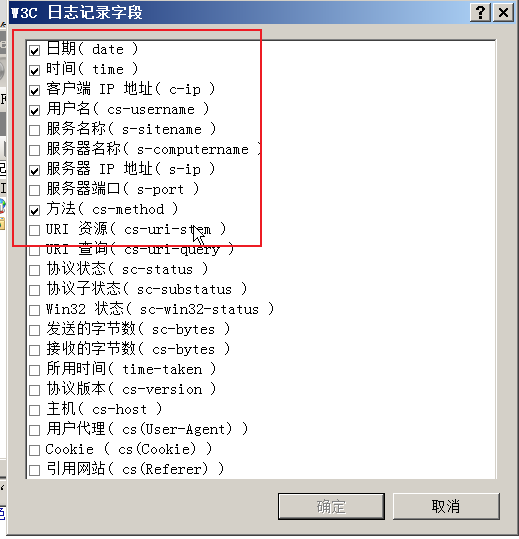
5.通过SSL（TLS 1.0）加密服务器的远程桌面服务，将RDP-Tcp属性对应的配置界面截图；



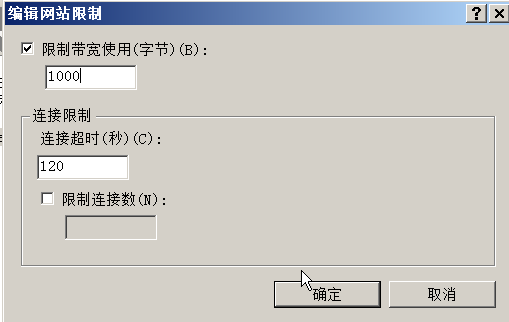
6.仅允许超级管理员账号关闭系统，将关闭系统属性的配置界面截图；



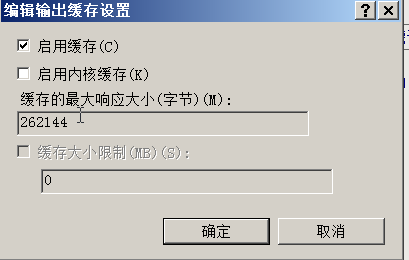
7.开启IIS的日志审计记录，日志文件保存格式为W3C,只记录日期、时间、客户端IP地址、用户名、服务器端口、方法，将W3C日志记录字段的配置界面截图；



8.设置网站的最大并发连接数为1000，网站连接超时为60s，将编辑网站限制的配置界面截图；



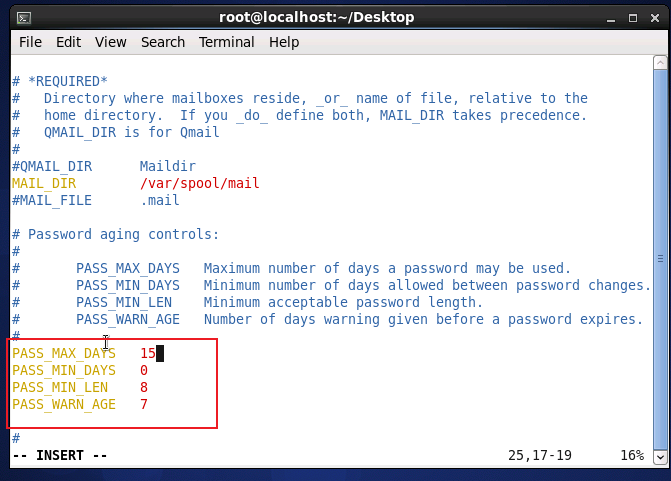
1. 禁用IIS内核缓存，避免对方利用ms15\_034漏洞进行DOS攻击，出现蓝屏的现象，将编辑输出缓存设置的配置界面截图；



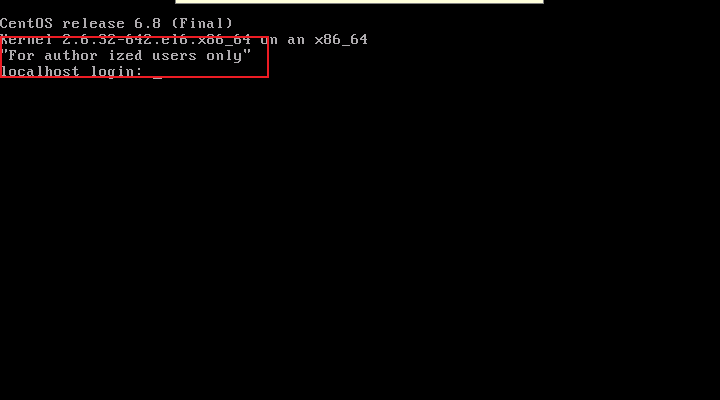
1. 设置user1用户只能在上班时间（周一至周五的9:00~18:00）可以登录。将user1的登录时间配置界面截图。

A-2：Linux操作系统安全配置

1.设置最小密码长度不少于8个字符，密码最长使用期限为15天。将/etc/login.defs配置文件中对应的部分截图;

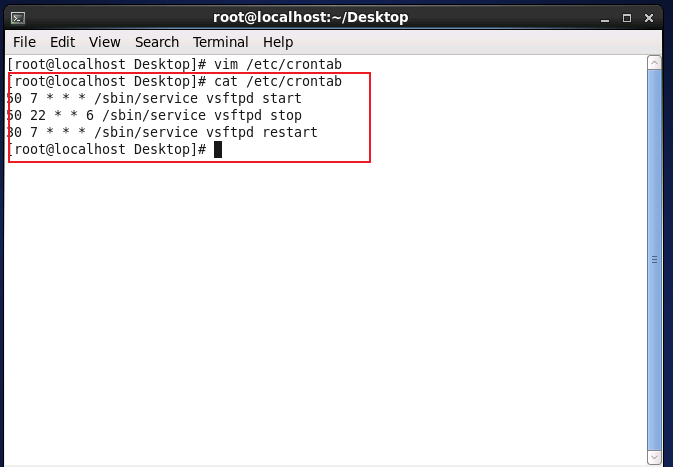


2.设置在用户登录系统时，会有“For authorized users only”提示信息，将登录系统时系统弹出提示信息界面截图;

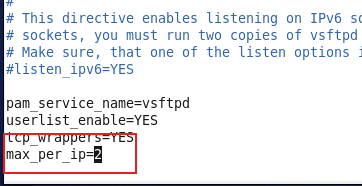


3.设置root用户的计划任务。每天早上7:50自动开启vsftpd服务，22点50时关闭；每周六的7:30时，重新启动vsftpd服务。使用crontab –l 查看计划任务，将回显结果截图；

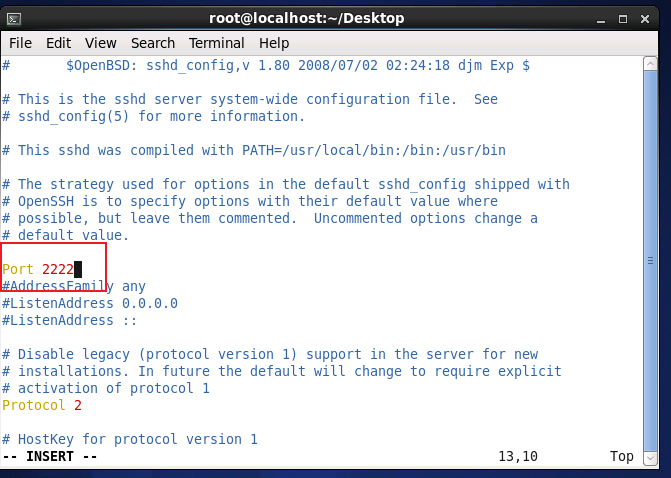
4.禁止匿名用户登录vsftpd服务，将/etc/vsftpd/vsftpd.conf配置文件中对应的部分截图；

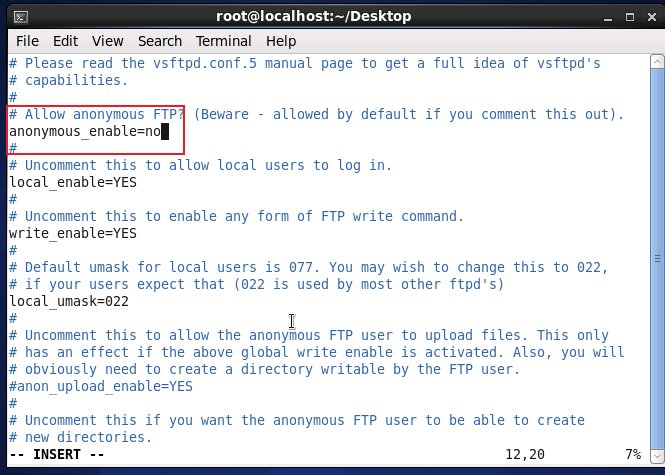


5.限制客户端连接vsftpd服务时，同一个IP最多只能打开两个连接，将/etc/vsftpd/vsftpd.conf配置文件中对应的部分截图；

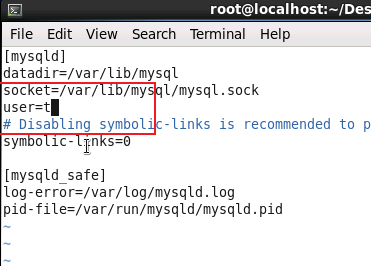


6.将SSH服务的端口号修改为2222 ,使用命令netstat -anltp | grep sshd查看SSH服务端口信息，将回显结果截图；

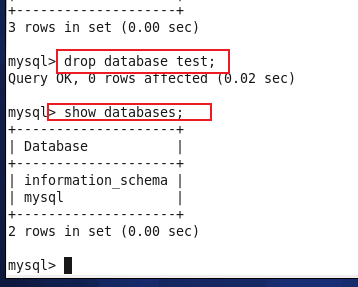


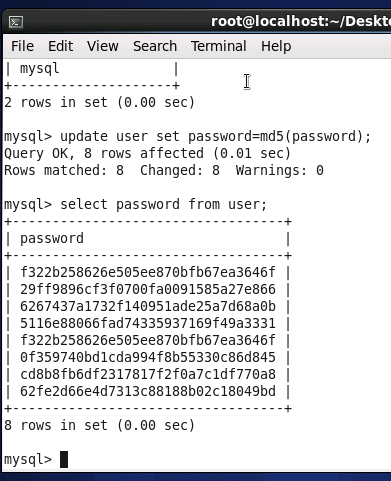
7.禁止root用户通过SSH远程登录，将/etc/ssh/sshd\_config 配置文件中对应的部分截图；

8.禁止mysql服务以管理员权限的账号运行，将/etc/my.cnf配置文件中对应的部分截图；



9.删除默认数据库test, 然后使用show databases;命令查看当前的数据库信息，将回显结果截图；



10.将数据库用户user1的密码使用MD5加密，然后在数据库中使用select password from user where user=’user1’;命令查看user1的密码，将回显结果截图。