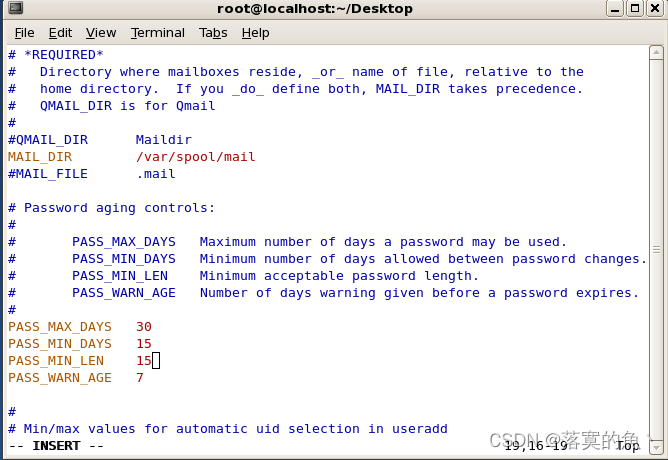
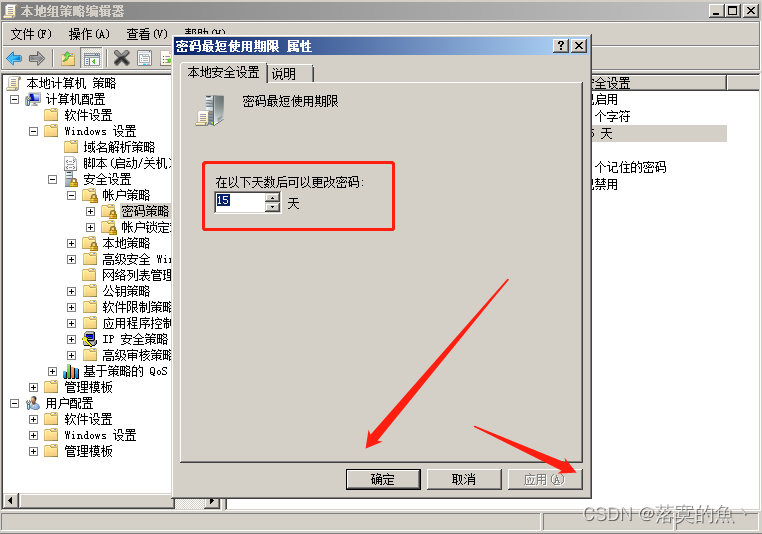
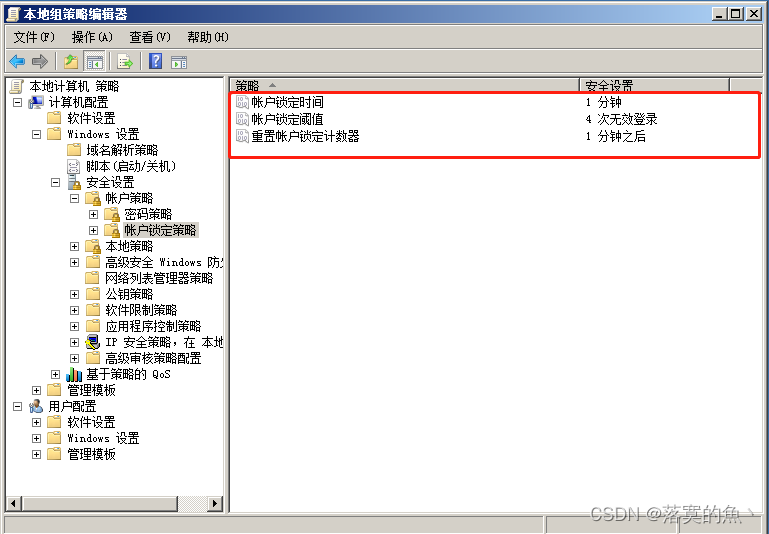
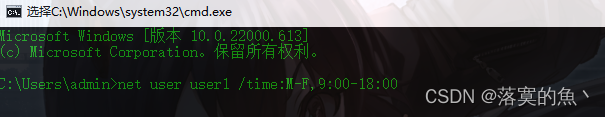
* Windows：管理工具-本地安全策略-帐户策略-密码策略，设置密码长度 15
* Linux：修改/etc/login.defs文件PASS\_MIN\_LEN细分参数 15  
    
  b.一分钟内仅允许4次登录失败，超过4次，登录帐号锁定1分钟。
* windows：计算机配置–windows 设置–安全设置–账户锁定策略  
  账户锁定时间为一分钟 账号锁定阈值 为4次 锁定计算器为1分钟以后  
    
  linux：vim /etc/pam.d/login 添加： **auth required pam\_tally2.so deny=4 unlock\_time=60 even\_deny\_root root\_unlock\_time=240**  
  五次登录失败:**deny =4** 设置登录账号锁定一分钟:**unlock\_time=60**

2.用户安全管理  
a.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；  
  
两种方法：

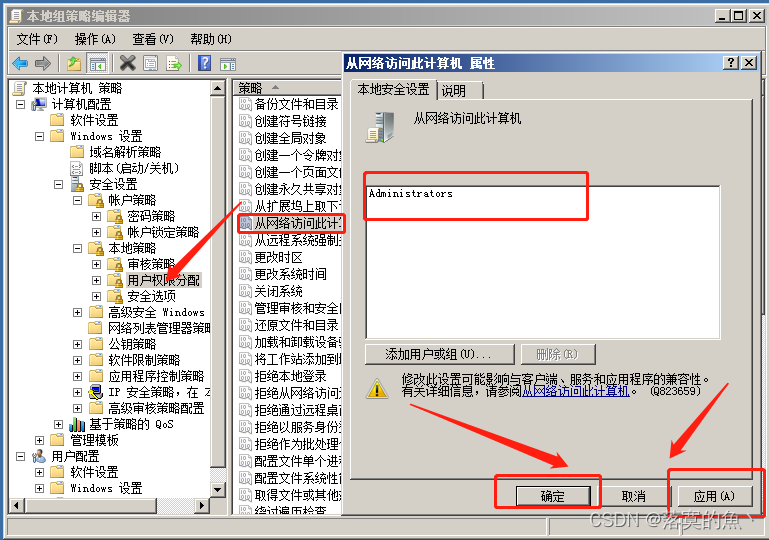
> net user username /time:M-F,09:00-18:00

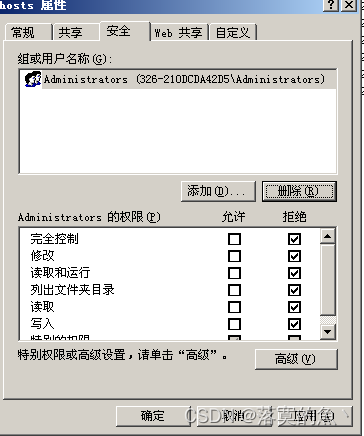
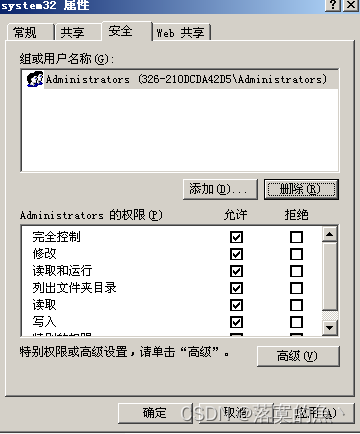
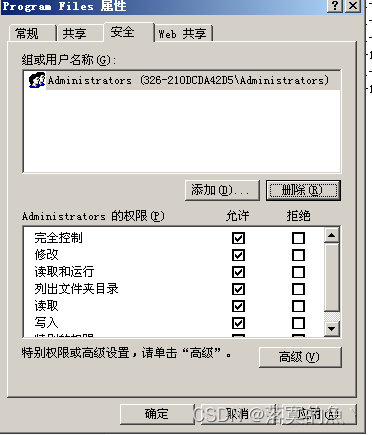
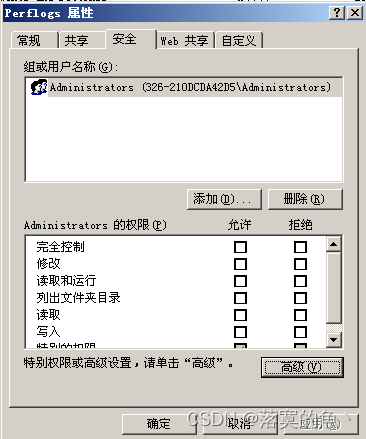
> net user username/time:M-F,9am-18pm

如果你取消账户的时间限制，可以使用如下命令：

> net user user1 /time:all

b.在组策略中只允许管理员账号从网络访问本机；

* 计算机配置-Windows设置-安全设置-本地策略-用户权限分配-从网络访问此计算机  
  

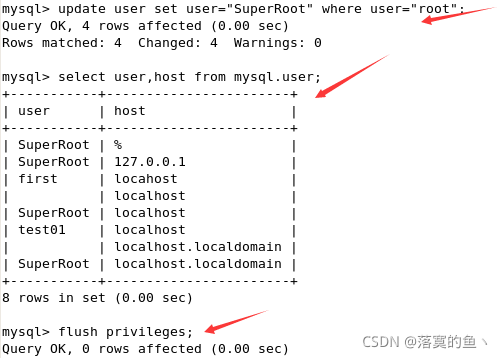
c.设置操作系统中的关键目录（system32、hosts、Program Files、Perflogs）的权限为最优状态，即仅允许管理员用户进行读取及运行。  
  
  
  
  
**A-2任务二 数据库安全策略**  
3.以普通帐户mysql安全运行mysql服务，禁止mysql以管理员帐号权限运行；

vim /etc/my.cnf 在配置中进行设置 [mysqld] 修改user=mysql

4.删除默认数据库(test)；

drop databases test;

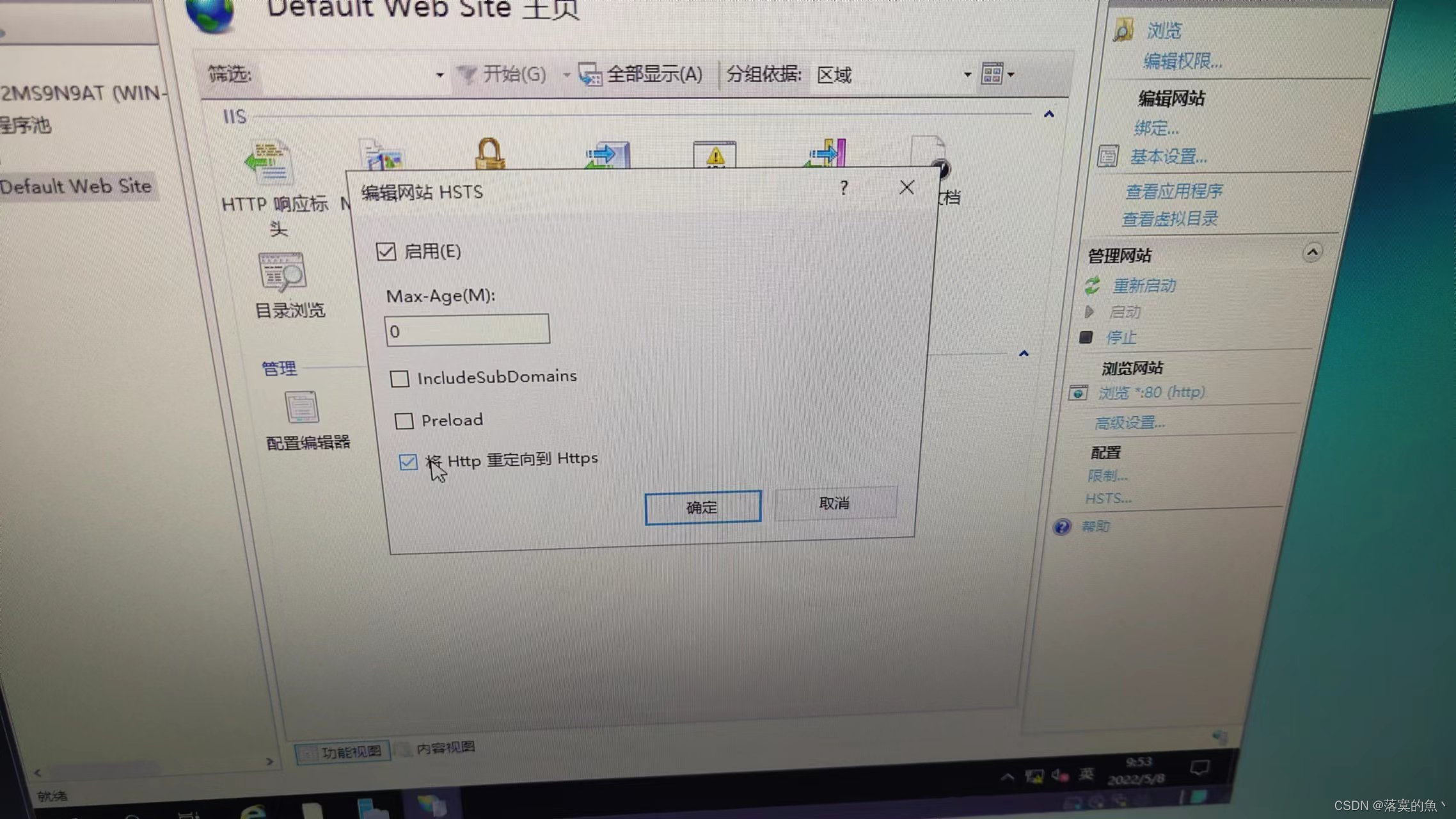
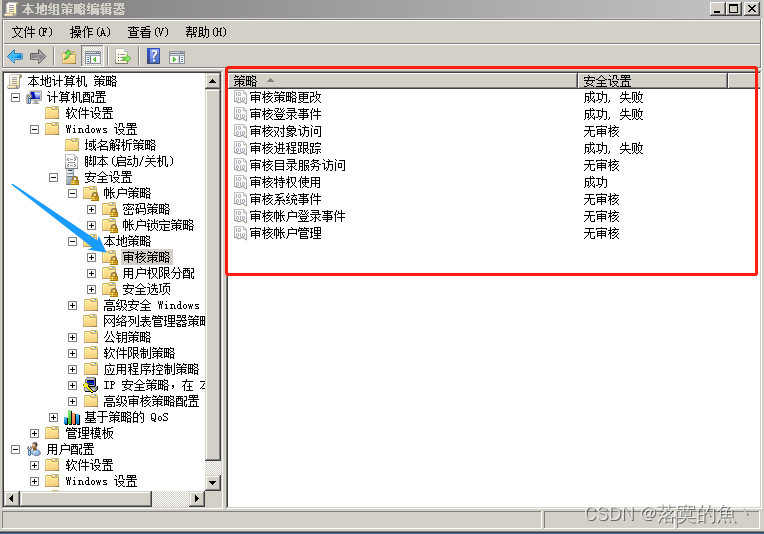
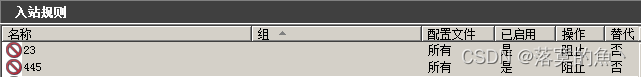
5.改变默认mysql管理员用户为:SuperRoot；

update user set user="SuperRoot" where user="root"；  


flush privileges；

6.使用mysql内置MD5加密函数加密用户user1的密码为(P@ssw0rd1!)。

update mysql.user set password=md5(“P@ssw0rd1!”) where user = ‘user1’；

**A-3任务三 流量完整性**  
7.对Web网站进行HTTP重定向HTTPS设置，仅使用HTTPS协议访问网站（Windows）(注：证书颁发给test.com 并通过https://www.test.com访问Web网站)。  
  
**A-4任务四 事件监控**  
8.将Web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。  
  
**A-5任务五 防火墙策略**  
9.Windows系统禁用445端口；  
在这里插入图片描述  
**（windows都是设置两条的一条 udp一条tcp）**  
10.Windows系统禁用23端口；  
  
11.Linux系统使用iptables禁用23端口；

Iptables -A INPUT -p tcp --dport 23 -j DROP

12.Linux系统使用iptables禁止别人ping通。

iptables -A INPUT -p icmp -j DROP

**A-6任务六 IP协议安全配置**  
13.指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为5；

windows+R打开运行，输入“regedit”打开注册表编辑器—>根据推荐值配置windows  
service的注册表键值路径HKEY\_ LOCALMACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters  
新建DWORD值，根据站点规则配置。 没有的话新建一个

  
14.指定处于SYN\_RCVD状态的TCP连接数的阈值为500；  
  
15.指定处于至少已发送一次重传的SYN\_RVCD状态中的TCP连接数的阈值为400。  
  
**总结：**