**西安电子科技大学**

**信息安全实验课程 实验报告**

**实验名称 SSL配置实验**

经济与管理学院 2106011 班

成 绩

姓名 赵红玉 学号 21069100225

同作者

实验日期 2023 年 12 月 20 日

|  |
| --- |
| 指导教师评语：  指导教师：  年月日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

## 一、实验目的：

**1、熟悉CA证书的申请与审批流程**

**2、理解SSL协议的工作原理**

**3、掌握Web服务器上的证书申请与SSL配置**

## 二、实验所用仪器（或实验环境）

**1、VMware虚拟机**

**2、windows server 2003操作系统**

## 三、实验要求

**1、配置IIS服务器，发布一个web站点，使得用户能够用ip地址访问该站点**

**2、为Web站点申请服务器证书**

**3、CA服务器审批证书**

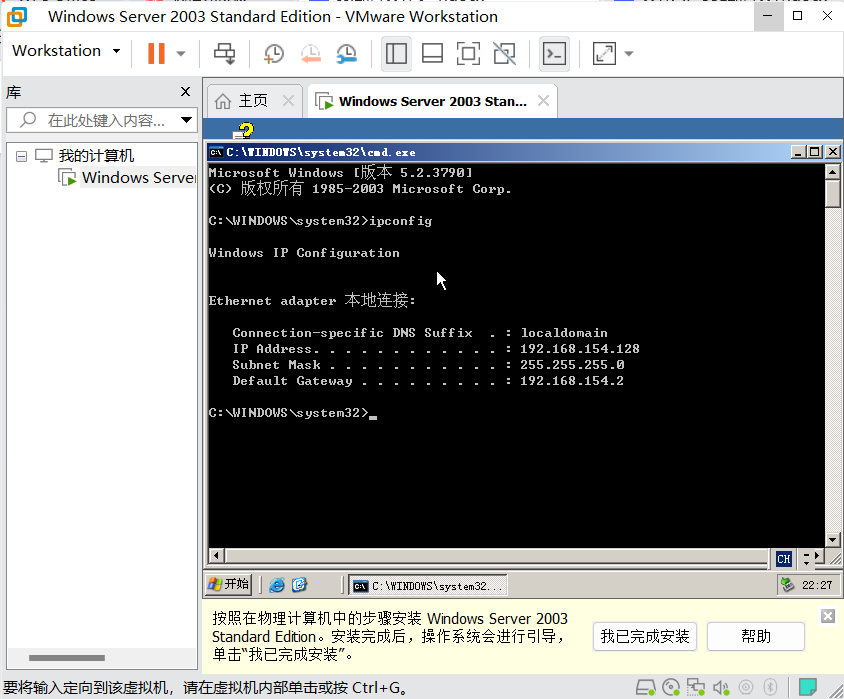
**4、Web站点下载安装证书并配置SSL安全访问**

**5、用户通过https协议访问web站点**

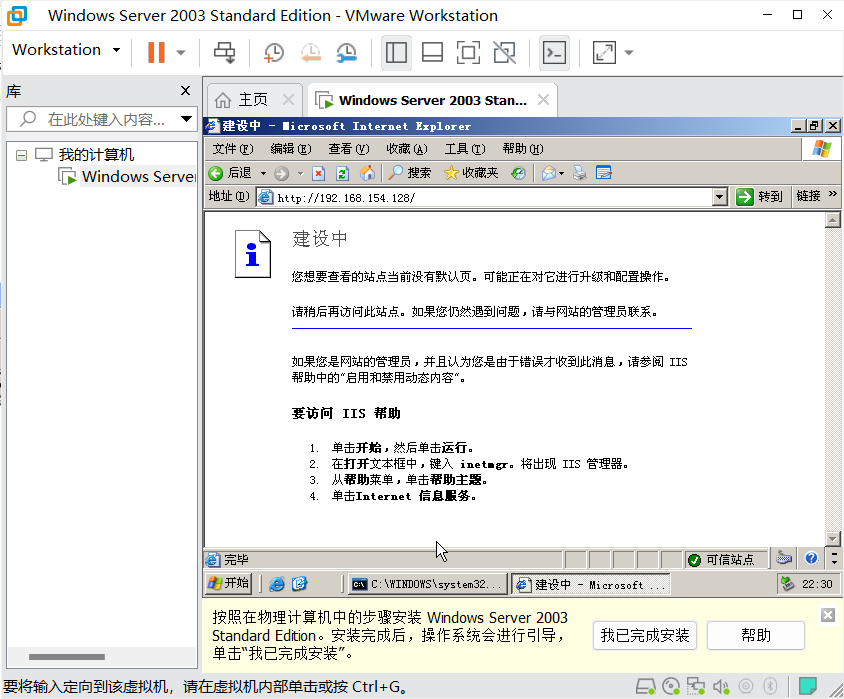
## 四、实验步骤及实验数据记录

### 1、配置IIS服务器，发布一个web站点，使得用户能够用ip地址访问该站点

**在虚拟机的cmd窗口里，用ipconfig命令，查看虚拟机的ip地址。**

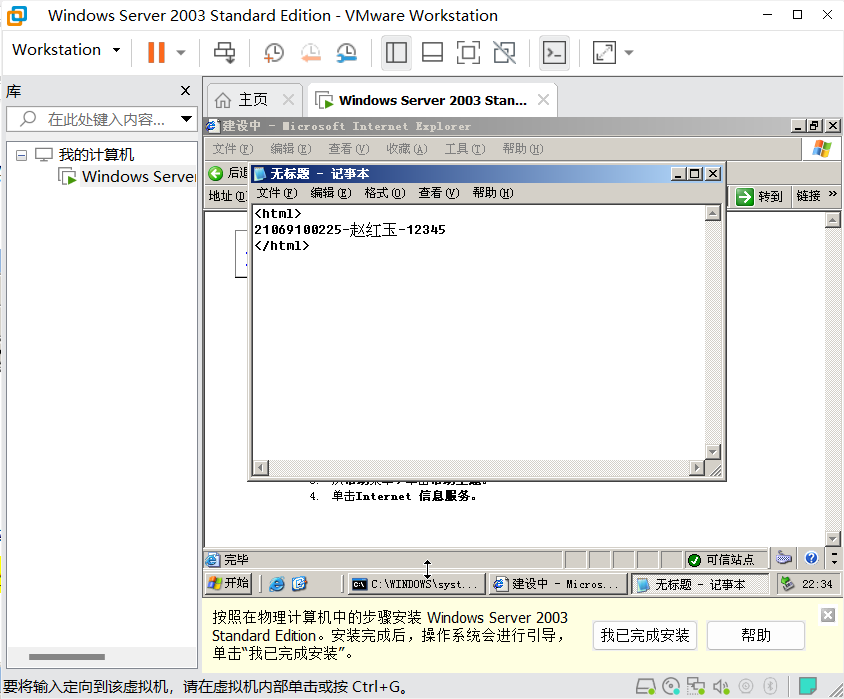


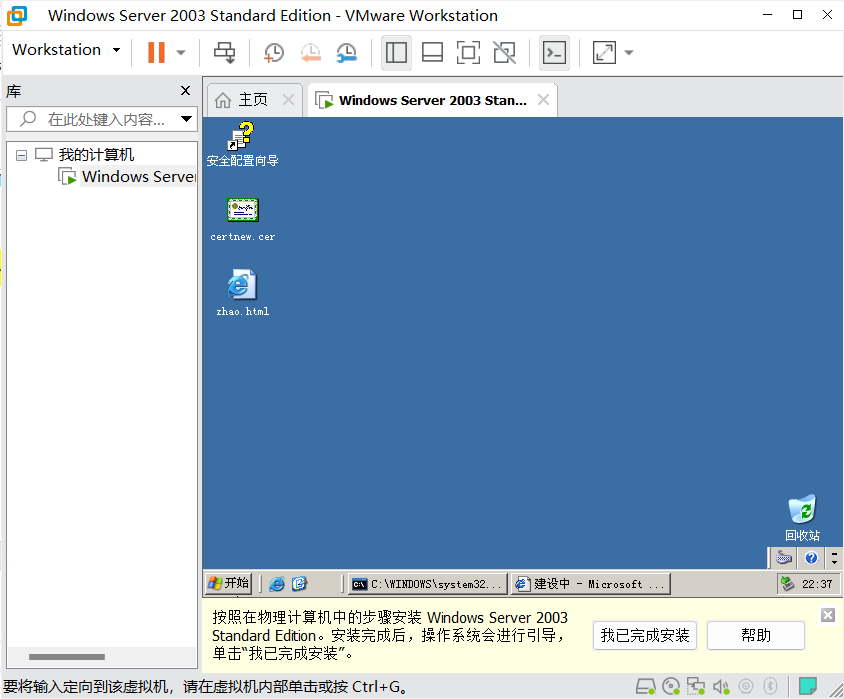
**ie浏览器里，输入虚拟机的ip地址。**



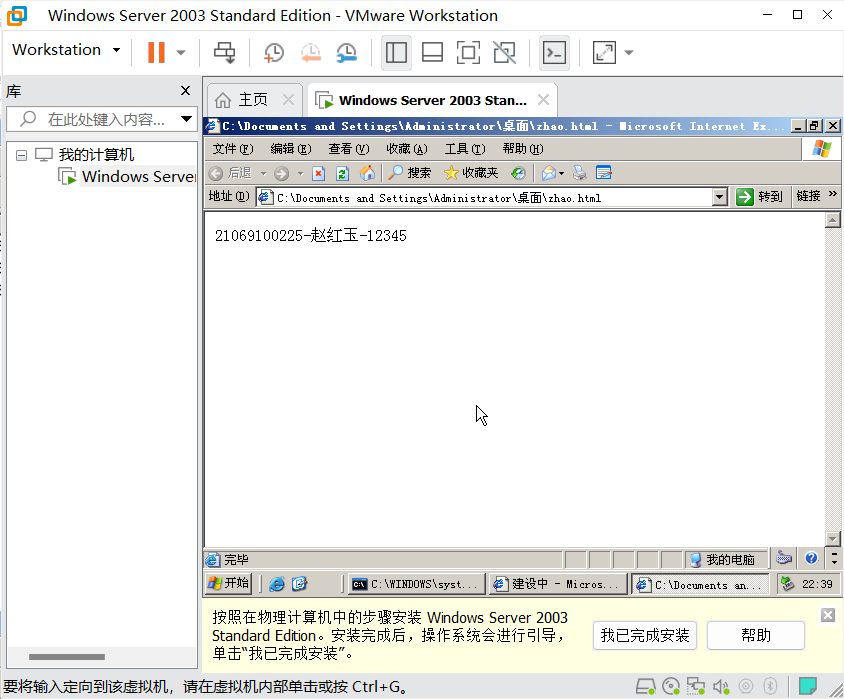
**建设站点。**

**打开一个txt，写html，写上了学号和姓名，保存成html文件。**

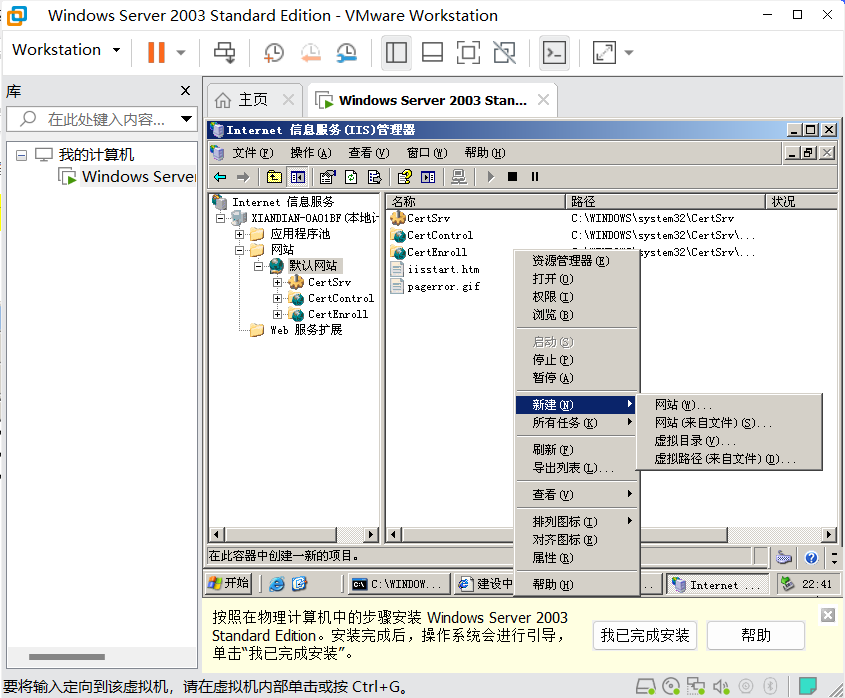


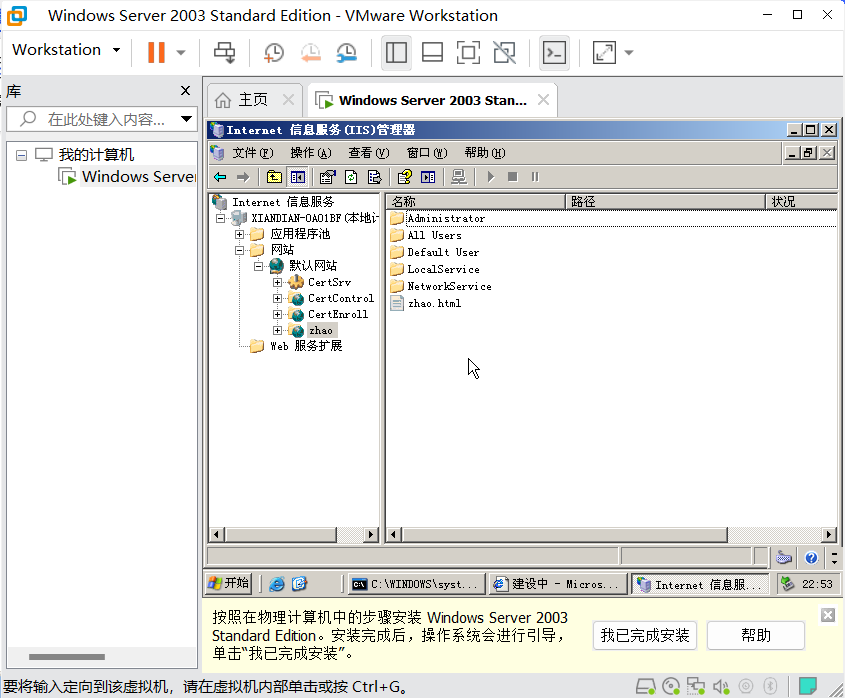


**最简易的web站点，静态页面，发布出去，可以用ip地址访问页面。**

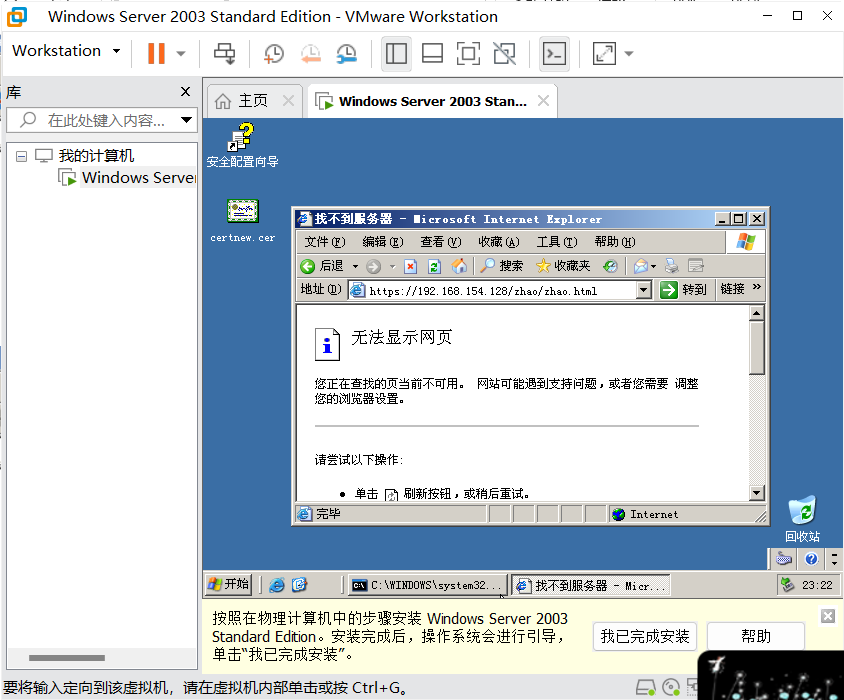


**配置IIS，选择“默认网站”，鼠标右键，“新建”——“虚拟目录”，用向导配置一下。指定放了web页面的文件夹。**

****

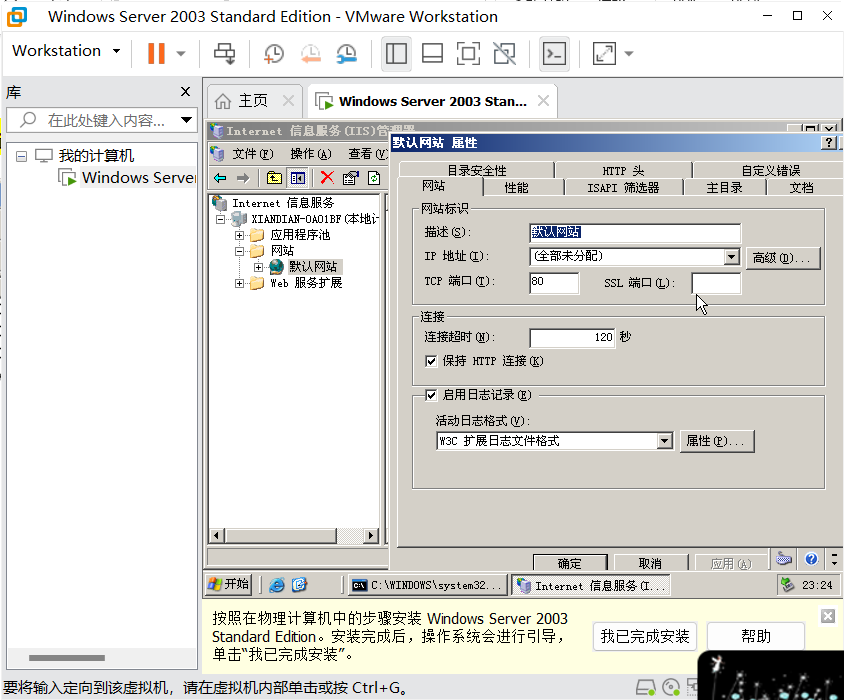
****

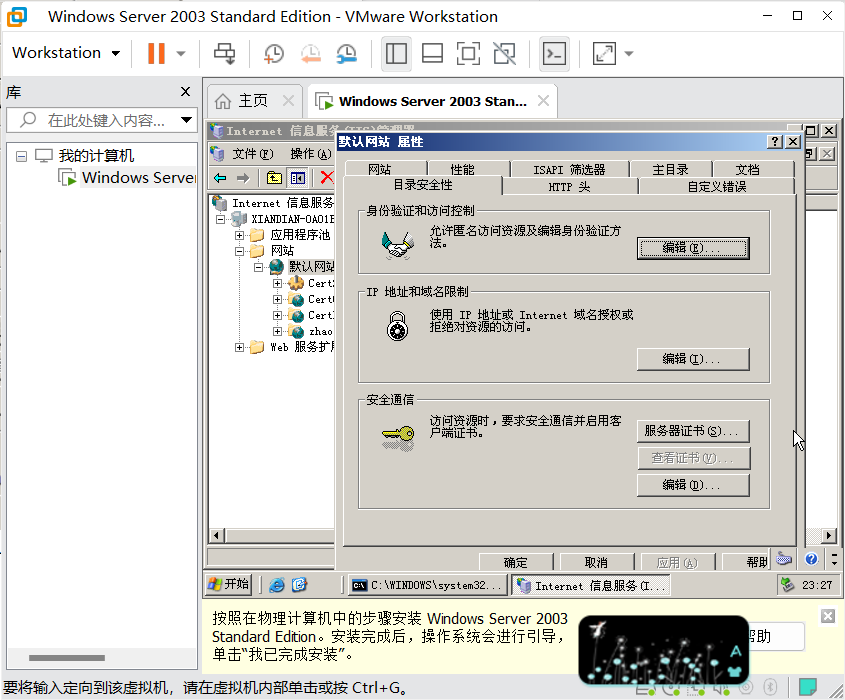
**尝试用https协议，发现不行。**



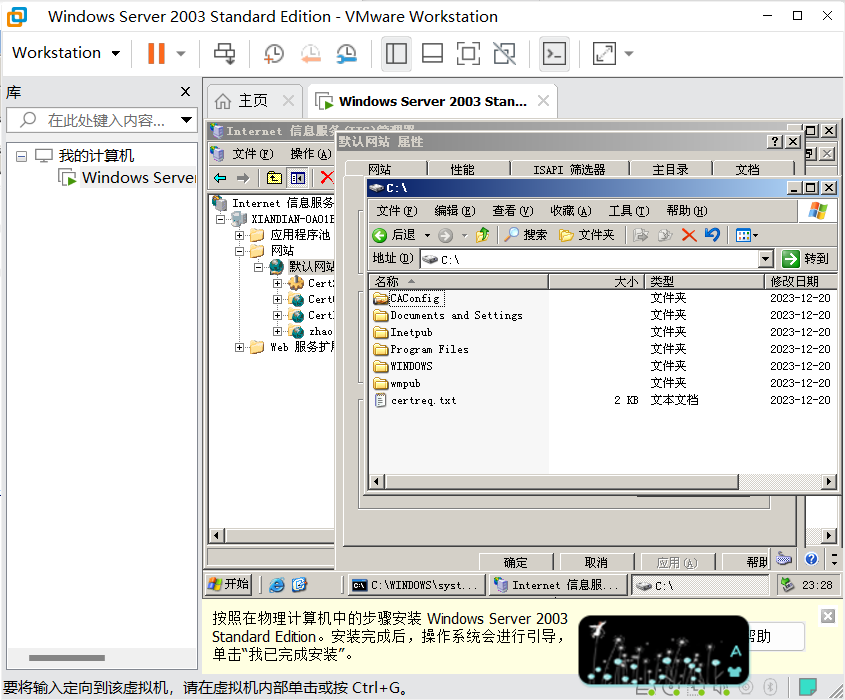
### 为Web站点申请服务器证书

**选中默认站点，右键“属性”——“目录安全性”——“证书服务器”，跟着向导下一步。**



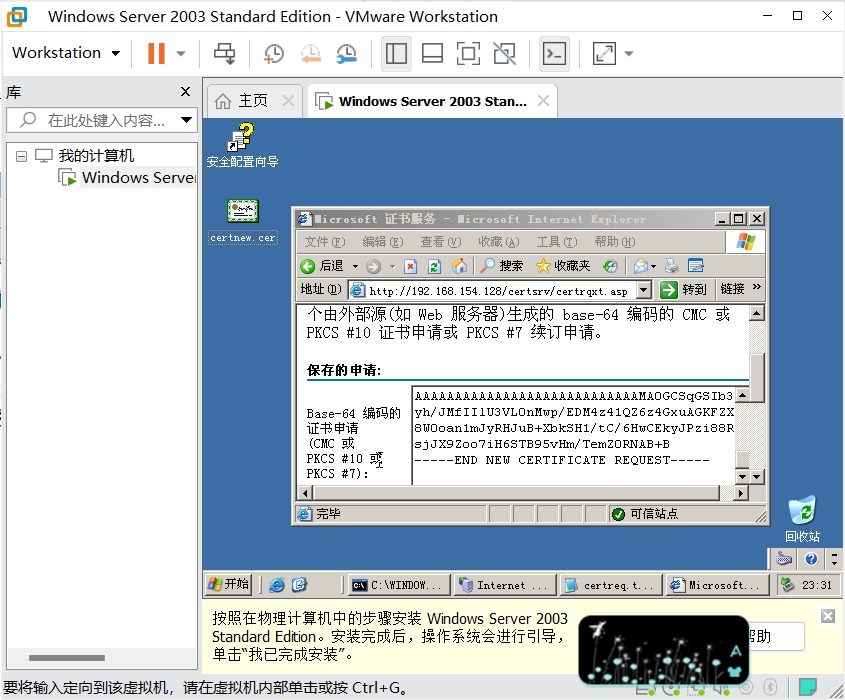


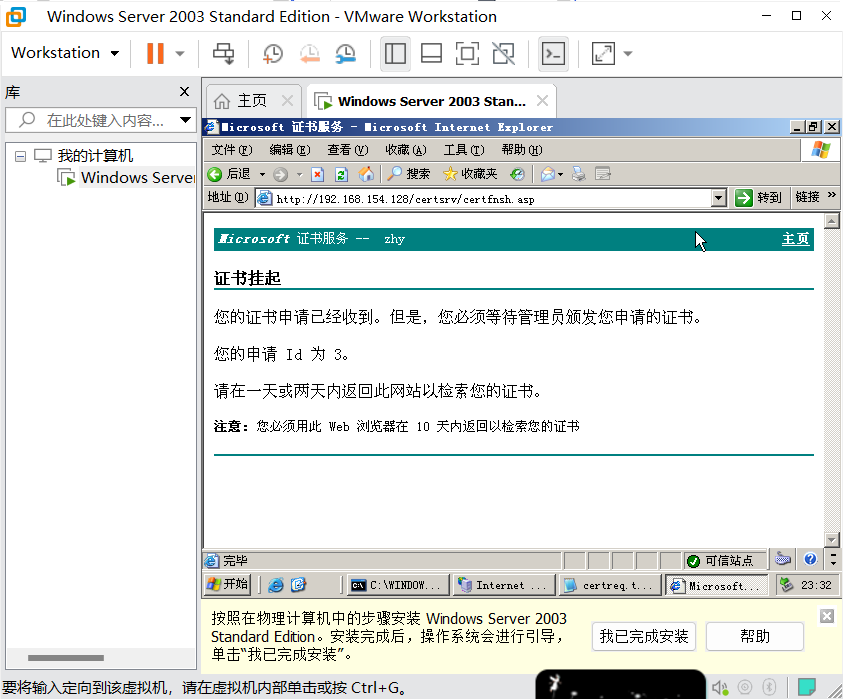
**生成一个证书的txt文件，自动放C盘。**

****

**把txt里的内容全部复制下来**

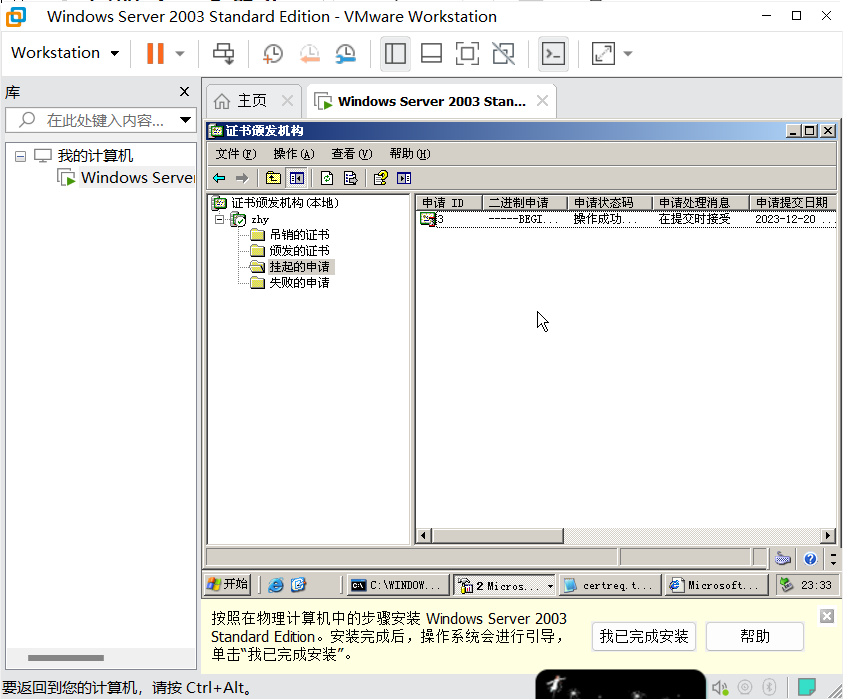
**然后去到证书申请页面，申请一个高级证书，用base64编码申请，然后把txt里的内容全贴进去。“提交”**

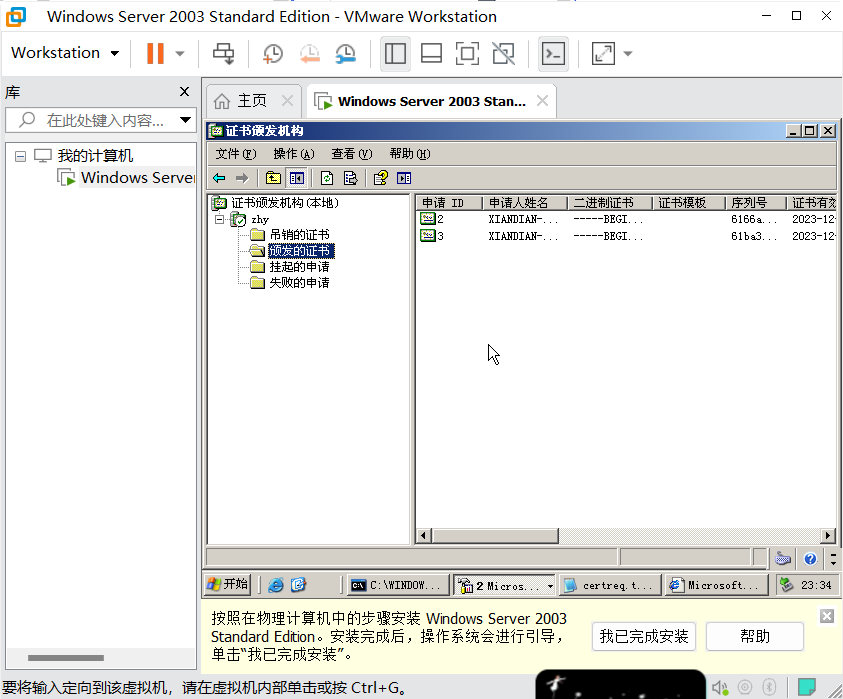
****

****

### CA服务器审批证书

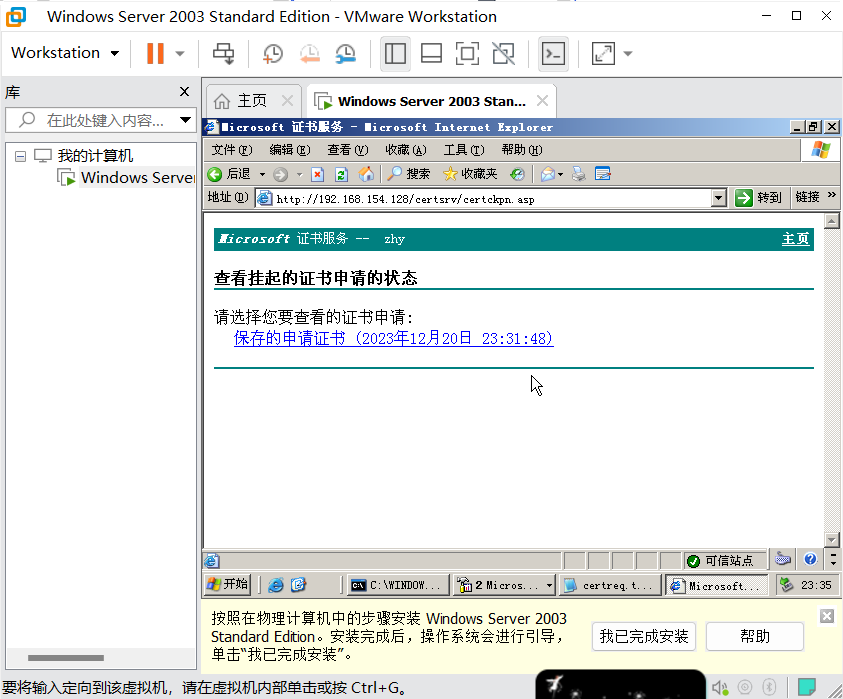
**充当CA证书服务器审批证书。**



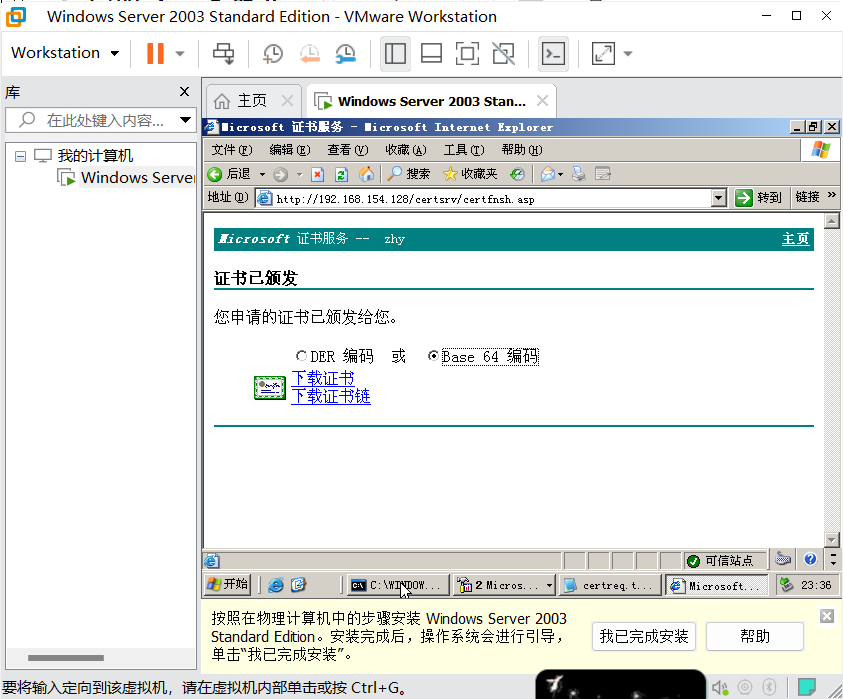


### Web站点下载安装证书并配置SSL安全访问

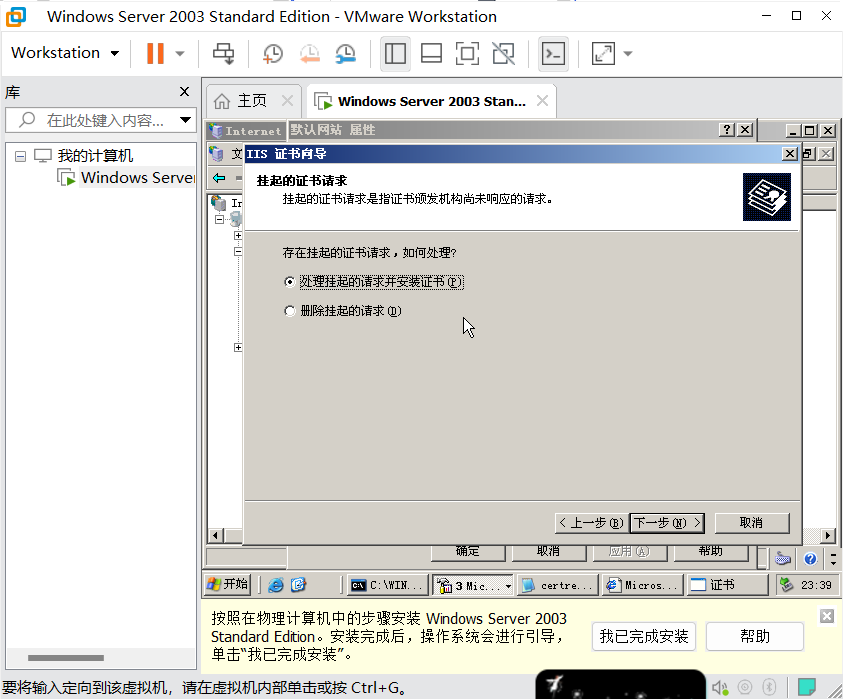
**当证书申请者，看证书的审批结果。**

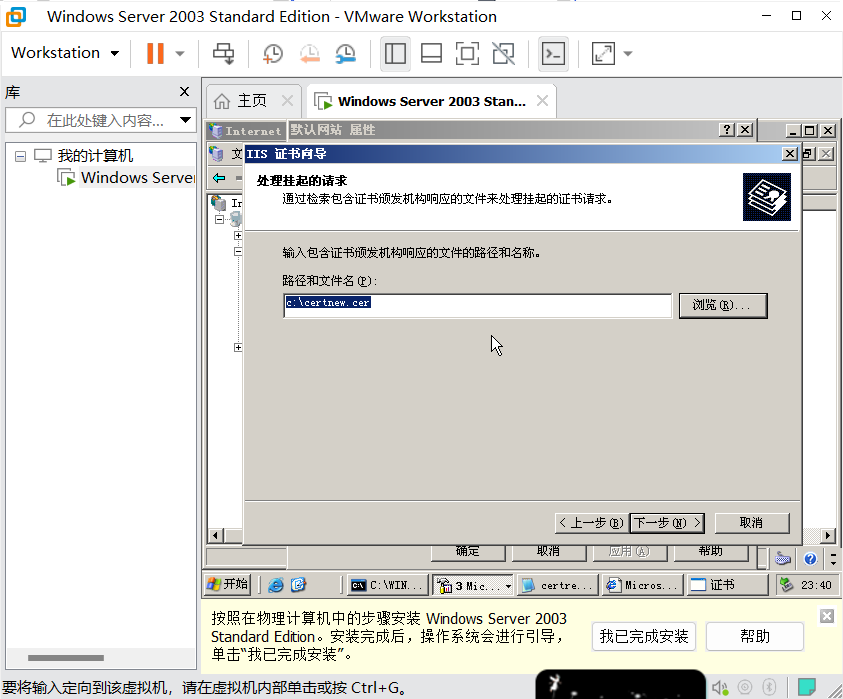
****

**用base64的格式下载证书。**

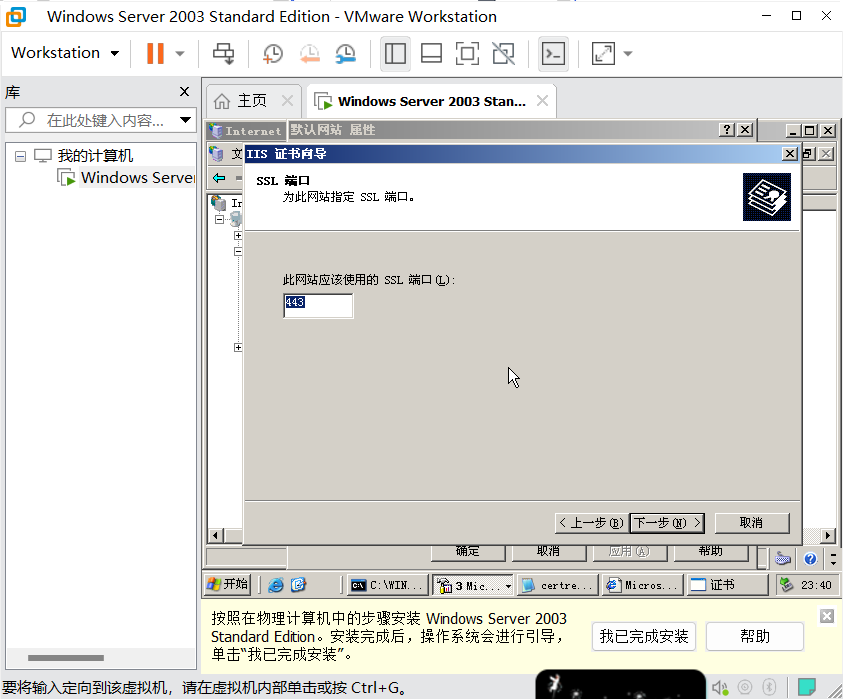
****

**回到iis配置的页面，点“服务器证书”，跟着向导。**

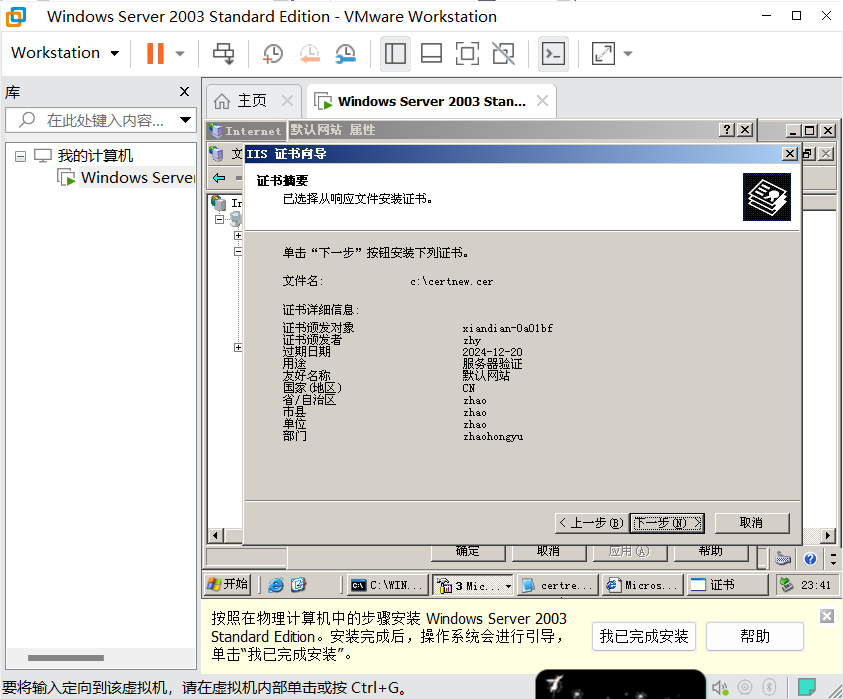
****



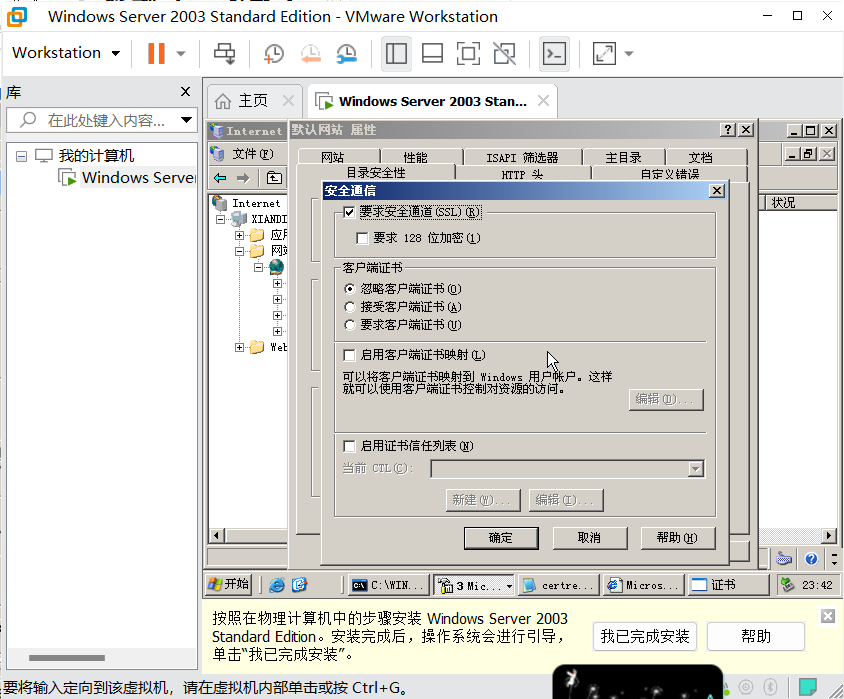
**选择刚才下载好的证书。**



**默认端口443，查看证书摘要。**



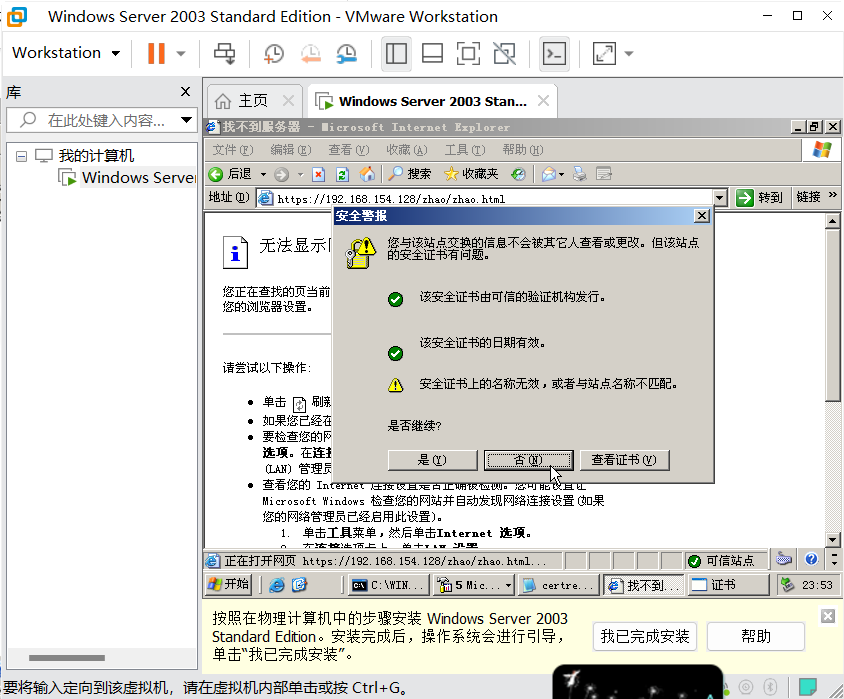
**安装完成后，还是回到“目录安全性”，在“安全通信”选择“编辑”，选中“要求安全通道”。**



### 5、用户通过https协议访问web站点

**配好了ssl，发现，http的方式访问站点已经不能访问了。必须用https**





**用https访问。**



## 实验结果分析及实验总结与体会

### 实验结果分析：

**1. 熟悉CA证书的申请与审批流程：通过实验，已经熟悉了CA证书的申请与审批流程。学会了在Windows Server 2003操作系统上配置IIS服务器，并为Web站点申请服务器证书。还了解了证书申请的相关信息和步骤，以及如何提交证书申请给CA服务器进行审批。**

**2. 理解SSL协议的工作原理：在实验中，已经对SSL协议的工作原理有了深入理解。学会了如何为Web服务器配置SSL证书，以实现加密通信和安全访问。了解SSL协议如何使用公钥加密、数字签名和握手协议来确保通信的机密性和完整性。**

**3. 掌握Web服务器上的证书申请与SSL配置：通过实验，已经掌握了在Web服务器上进行证书申请与SSL配置的技能。了解了如何为Web站点申请服务器证书，并将证书与Web服务器配置进行关联。熟悉如何在IIS服务器上启用SSL协议、配置加密算法和证书绑定，以确保安全的HTTPS访问。**

### 实验总结与体会：

**通过完成上述实验，获得了对CA证书申请与审批流程的熟悉和理解。学会了在VMware虚拟机中搭建Windows Server 2003操作系统，并配置IIS服务器来发布Web站点。还掌握了为Web站点申请服务器证书、CA服务器审批证书以及将证书配置到Web服务器上实现SSL安全访问的技能。**

**在实验过程中，不仅学习了理论知识，还获得了实际操作的经验。了解了Web服务器上证书申请的流程和相关信息，以及如何使用CA服务器进行证书的审批。还学会了在IIS服务器上配置SSL协议，实现加密通信和安全访问。**

**通过实验，还遇到了一些挑战和问题，例如证书申请和审批的时间周期、证书配置过程中的错误和调试等。这些问题可以帮助进一步加深对CA证书和SSL协议的理解，并为未来的实际应用提供宝贵的经验。**

**总之，完成这个实验让对CA证书的申请与审批流程以及SSL协议的工作原理有了更深入的理解。还获得了在Windows Server 2003操作系统上配置IIS服务器和SSL证书的实际技能。这些知识和技能对于保护网站的安全性和用户隐私具有重要的意义。**