哈尔滨工业大学

计算机科学与技术学院

《信息安全概论》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 信息安全概论 |
| 实验名称： | Kerberos网络认证协议搭建与分析 |
| 指导教师： | 韩琦 |
| 学生姓名： | 马玉坤 |
| 组 号： | 3-19 |
| 实验日期： | 2018年3月20日-2018年3月21日 |
| 实验地点： | 哈尔滨工业大学 |
| 实验成绩： |  |

一、实验目的

1. 掌握利用 Kerberos网络认证协议搭建方法；
2. 掌握Windows Server 2003系统的域和DNS服务器的搭建；
3. 掌握Kerberos 认证原理；

二、实验环境

1. 域服务器Windows Server 2003
2. 客户机Windows XP

在实验中需要用到的工具：

* Windows Server 2003 Resource Kit Tools

三、实验内容与实验要求

实验原理

Kerberos协议最初是麻省理工学院（MIT）为其Athena项目开发的。目前广泛应用的版本是其第五版本Kerberos V5。Kerberos协议的参与实体包括需要验证身份的通信双方，以及通信双方都信任的第三方密钥分配中心（KDC）。KDC包括：一个认证服务器 （AS），一个或多个票据分配服务器（TGS）、一个数据库。协议过程中，发起认证服务的通信方称为客户方，客户方需要访问的对象称为服务器方。客户方与 服务器方通过KDC可以相互验证对方身份，同时建立起用于以后秘密通信的共享密钥。

Kerberos协议可以分为三个阶段，共六个步骤。

**第一阶段**：认证服务交换，客户方向认证服务器请求与TGS通信所需要的票据及会话密钥，如下面消息过程：

http://219.217.226.44:8080/manageUI/img/postImg/0c929f08-a045-4c83-98e8-7fc226c25cef.png

**第二阶段**：票据授权服务交换，客户方向TGS请求与服务方通信所需要的票据及会话密钥，如下面消息过程：

http://219.217.226.44:8080/manageUI/img/postImg/f2aecfd7-431d-4748-93c7-6323ff3735ee.png

**第三阶段**：客户方/服务方的双向认证，客户方在向服务方证实自己身份的同时，证实服务方的身份，如下面消息过程：

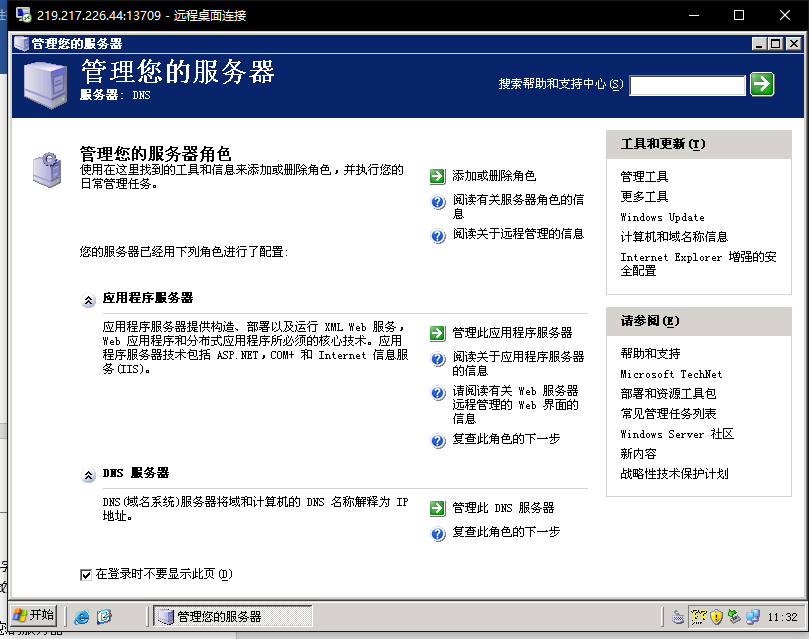
http://219.217.226.44:8080/manageUI/img/postImg/5bec9463-7e71-468c-917e-b20d714e7d25.png

其中，IDx 表示 X 的实体名，Nonce 表示随机数，Tc,tgs, 表示 AS 分配给客户方 C 用于访问TGS 的票据，其中包括客户方实体名、网络地址、TGS 名、时间标记、时限、会话密钥等，Tc,s表示 TGS 分配给客户方 C 用于访问服务方 S 的票据，其中包括客户方实体名、网络地址、服务方实体名、时间标记、时限、会话密钥等，Ac表示客户方对服务方的认证单，其中包括客户方实体名、网络地址、以及时间标记。

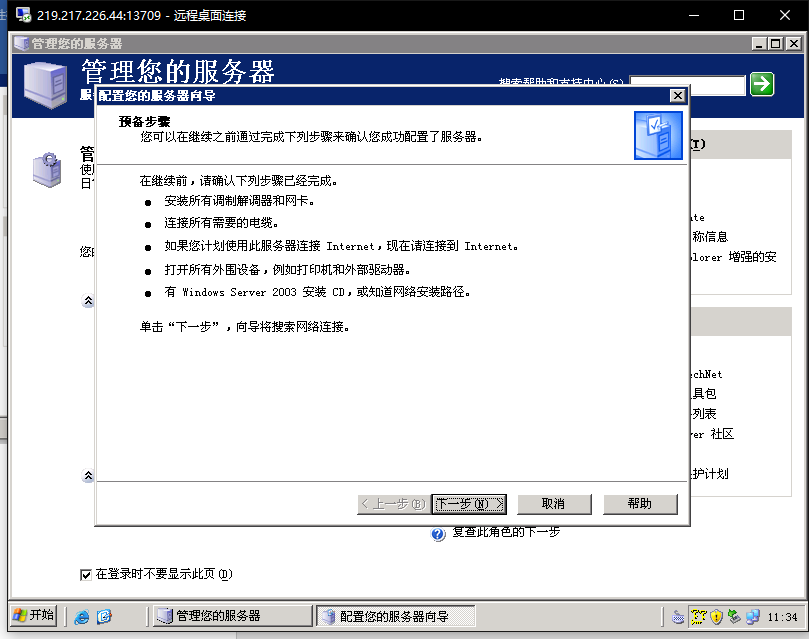
四、实验过程与分析

实验步骤1

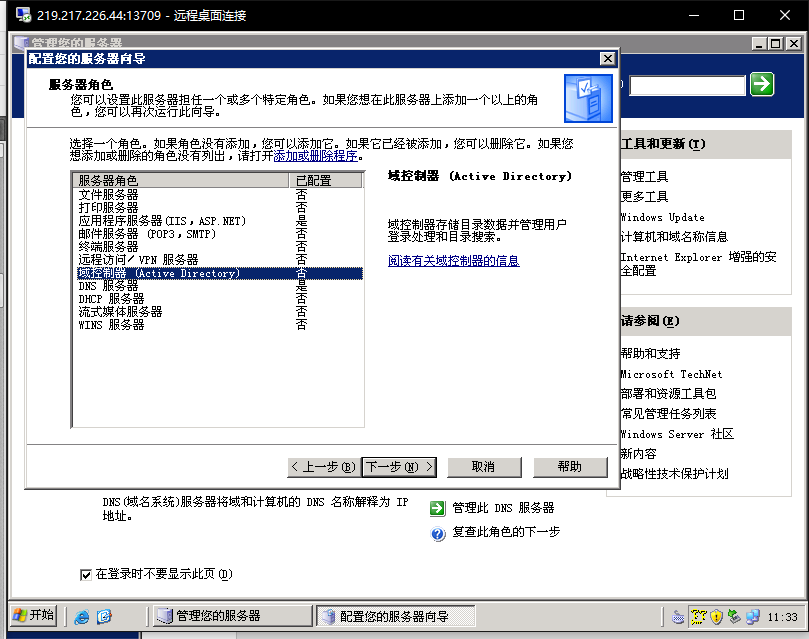
1. 打开“开始”菜单----“控制面板”----“管理工具”----“管理您的服务器”



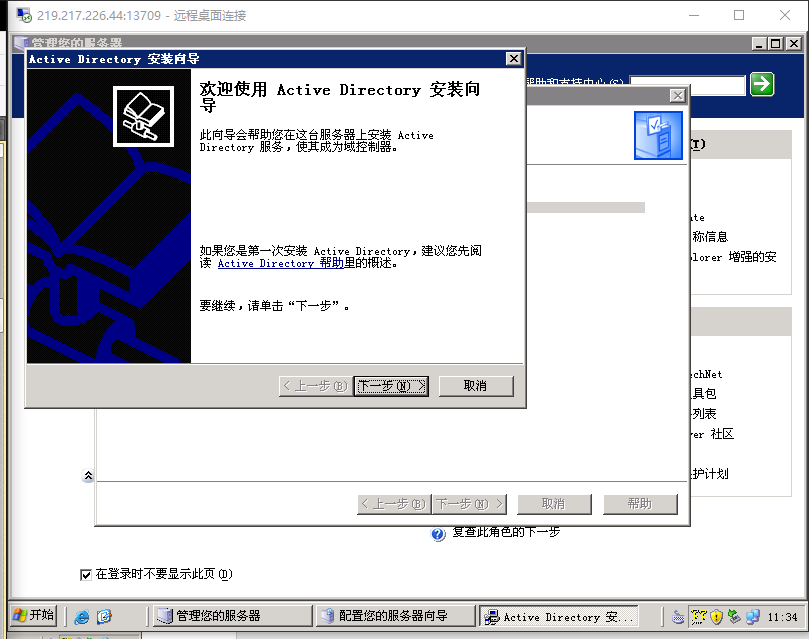
1. 打开“添加或删除角色”

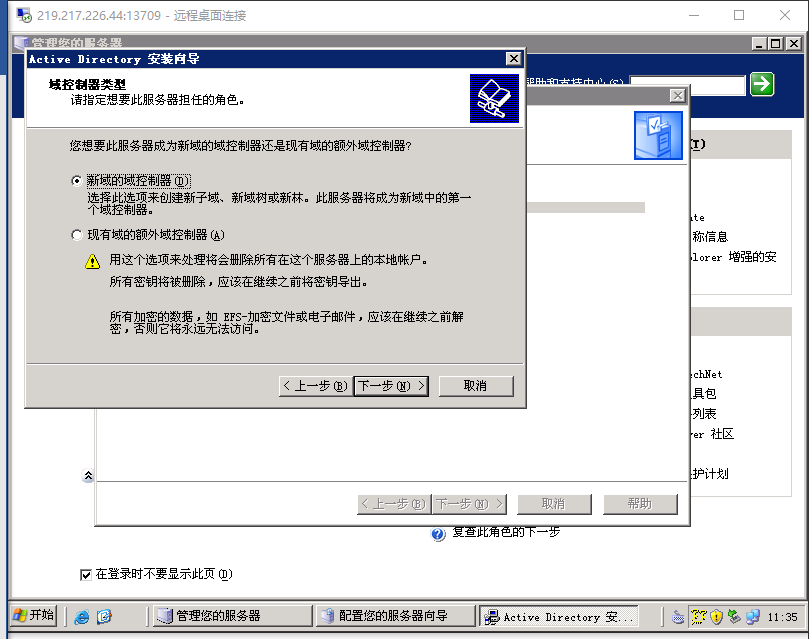


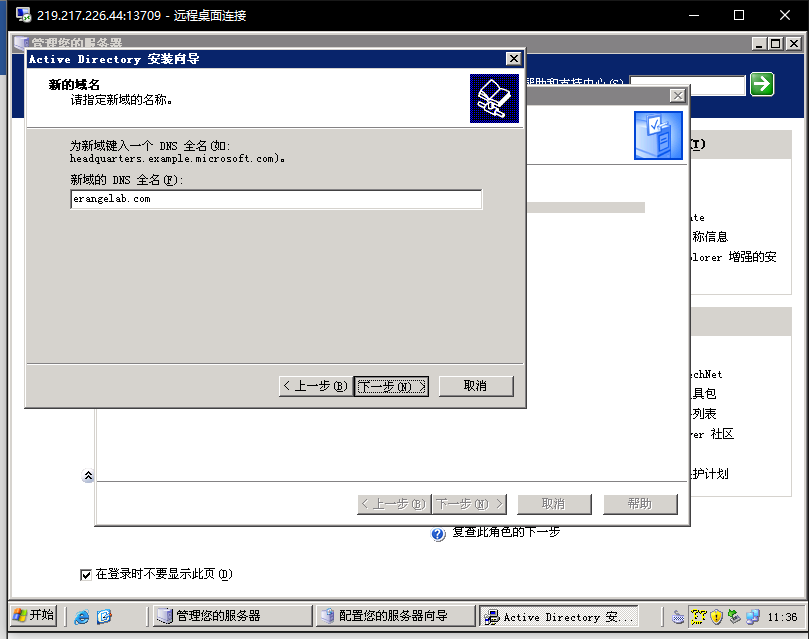
1. 选择域控制器

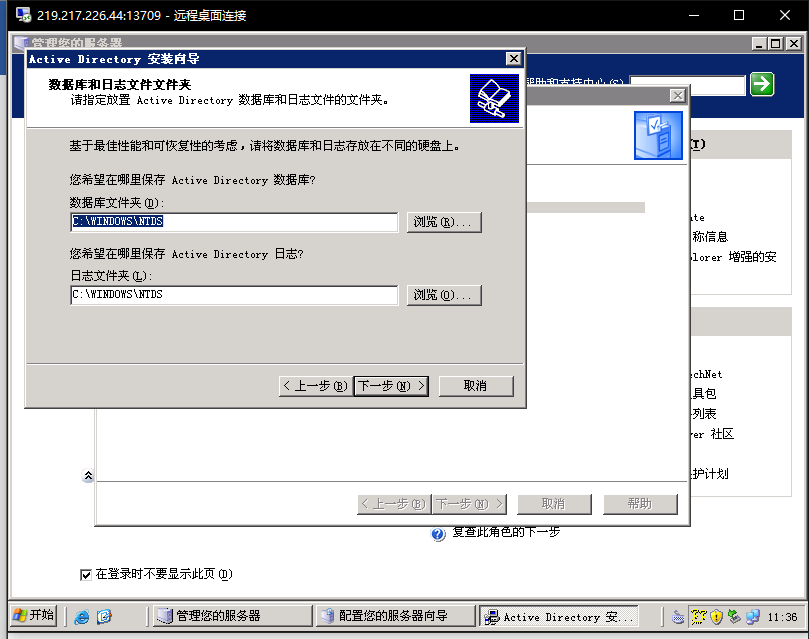


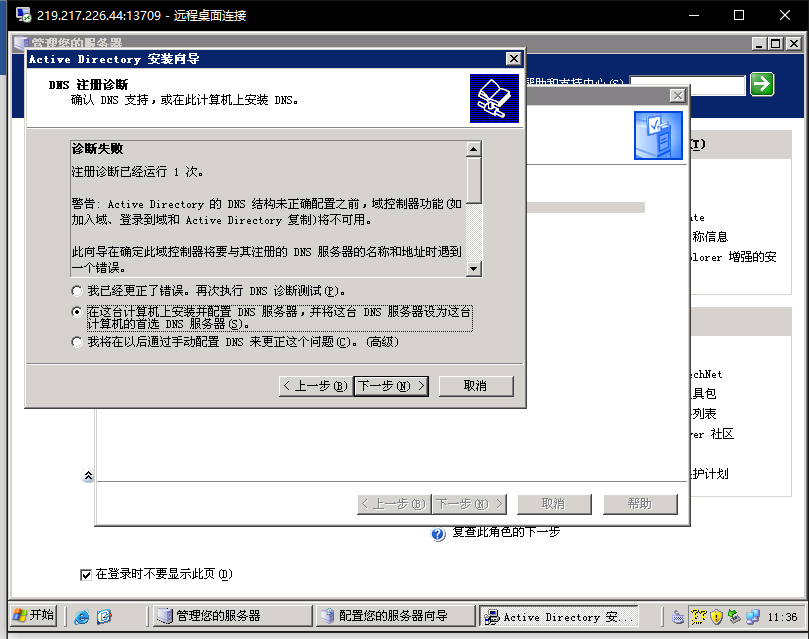
1. 打开安装向导

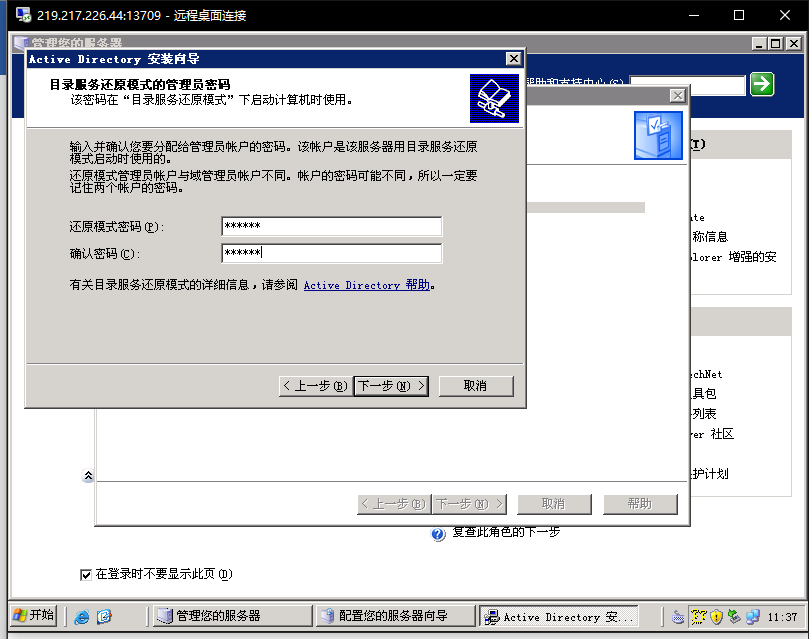


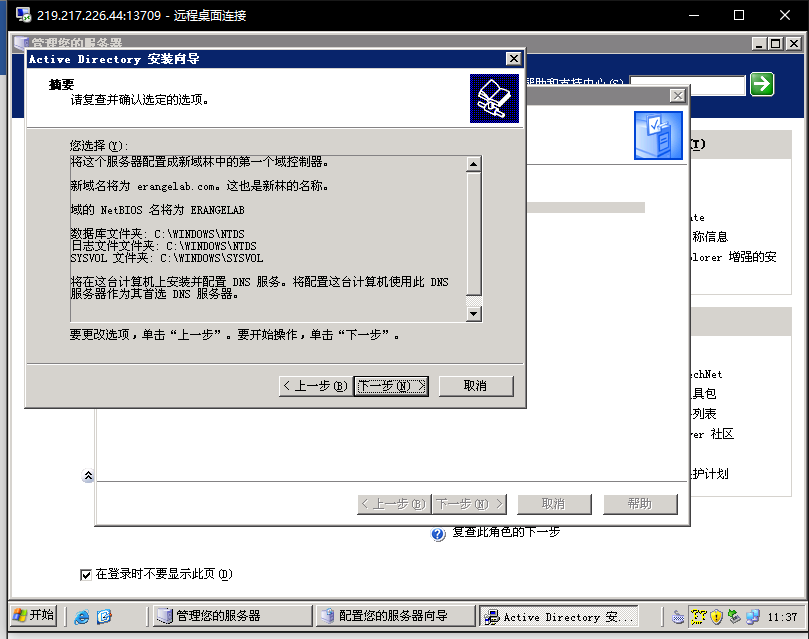


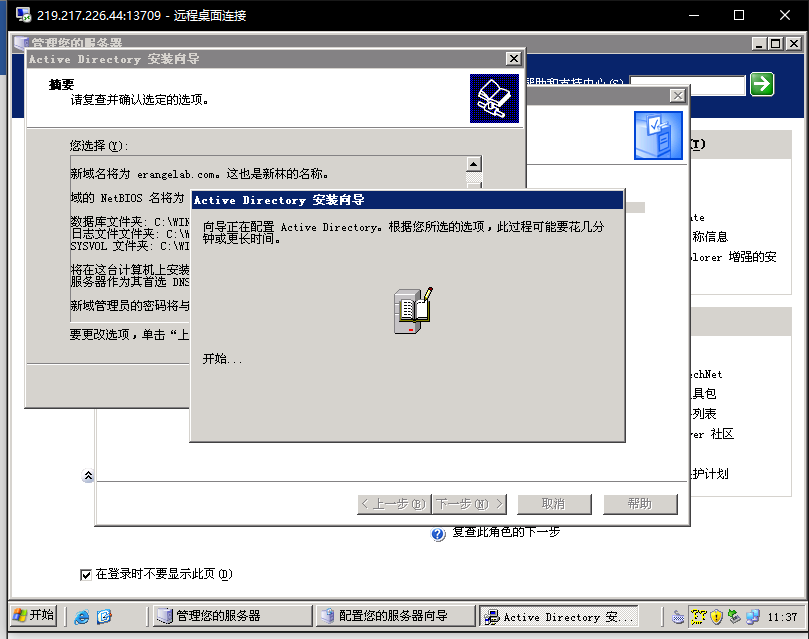


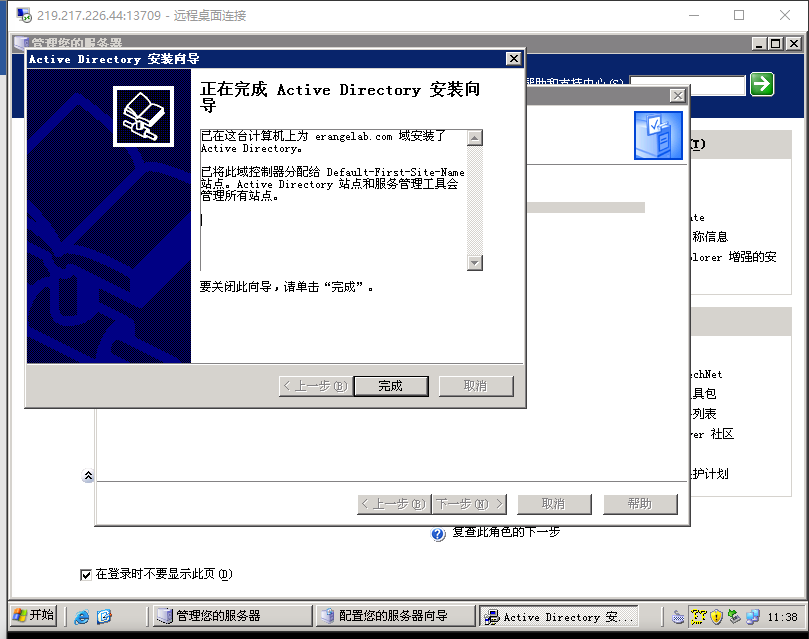






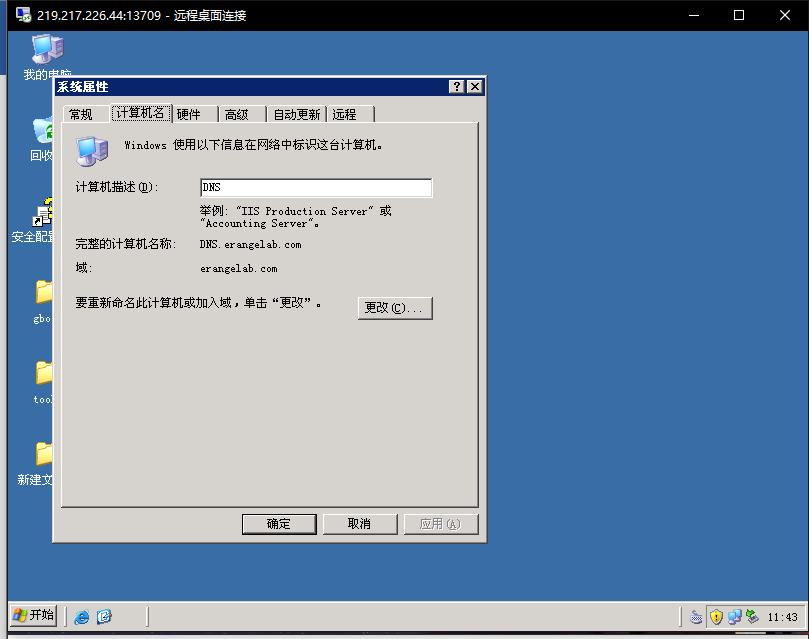




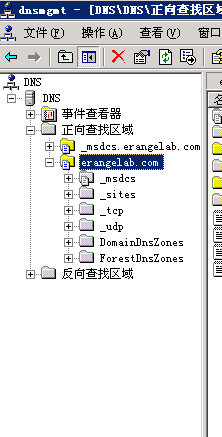




1. 重启远程服务器之后，可以看到完整的计算机名称与域发生了改变

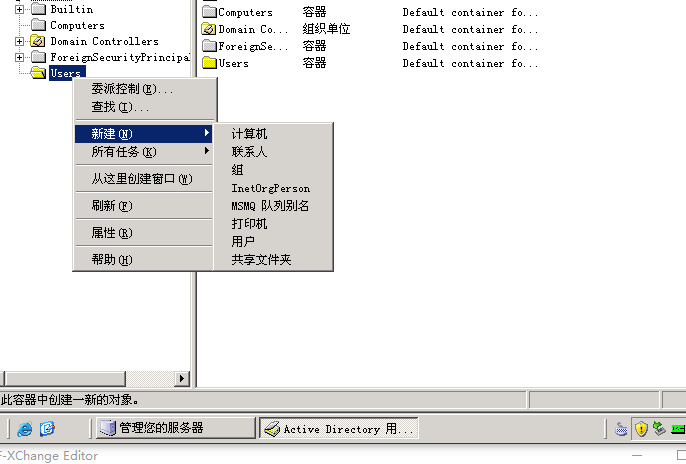


1. 打开“开始”——“管理工具”——“DNS”此时能看到DNS，本地连接已经自动将DNS设定为本机了



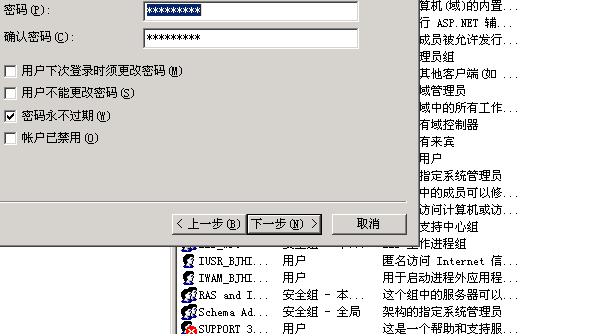
实验步骤2

1. 创建测试用户

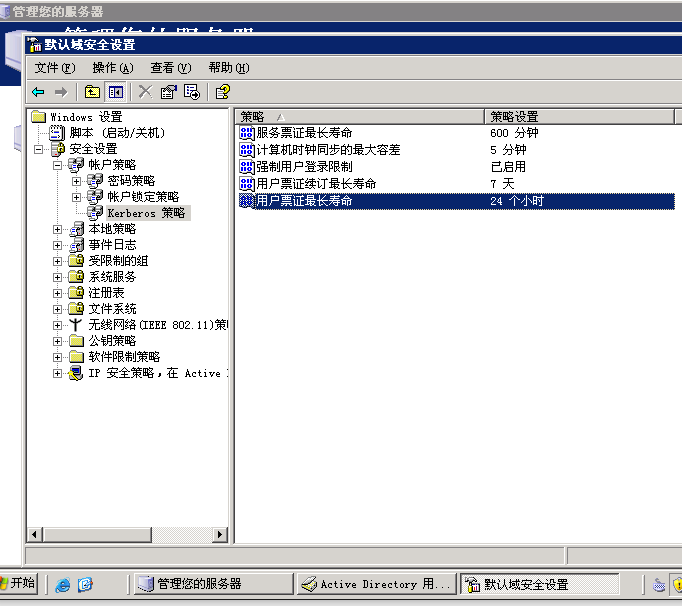




1. 设置用户密码，并选中“密码永不过期”

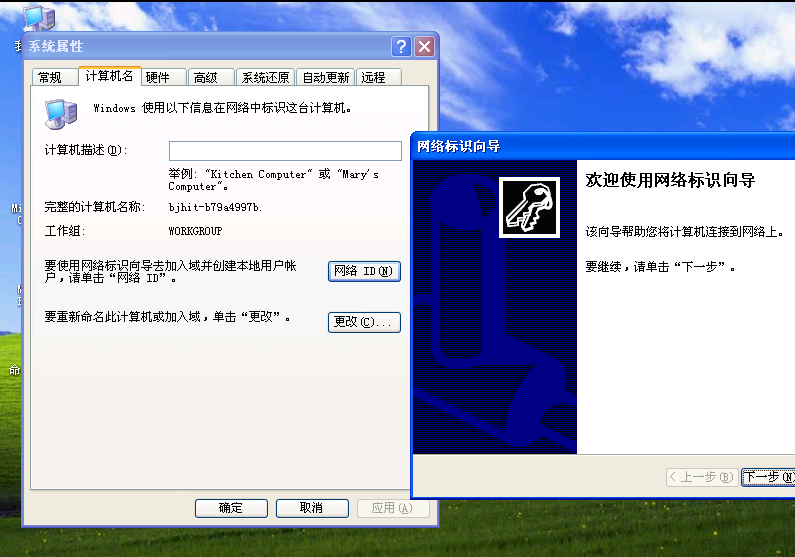


1. 打开“域安全策略”窗口，可以设定Kerberos策略（用户票证最长寿命设为24小时）

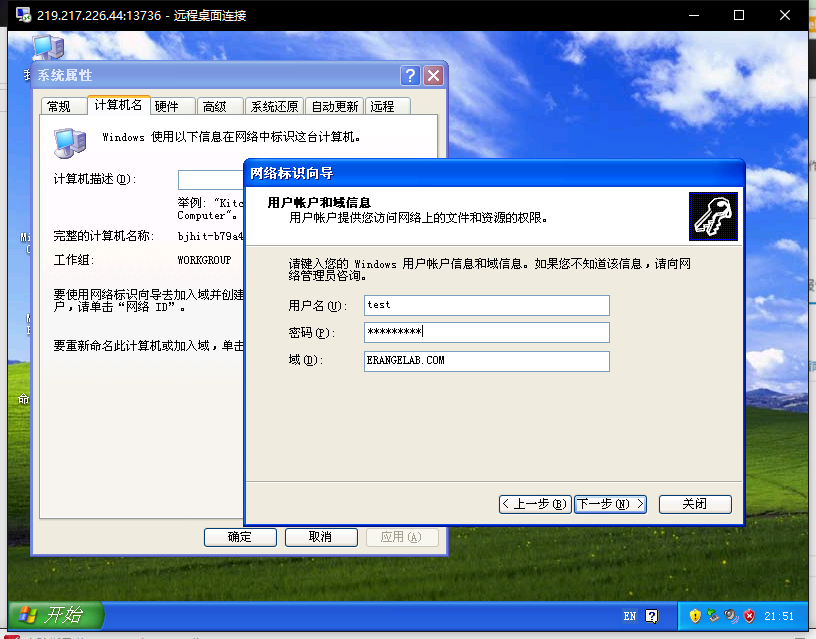


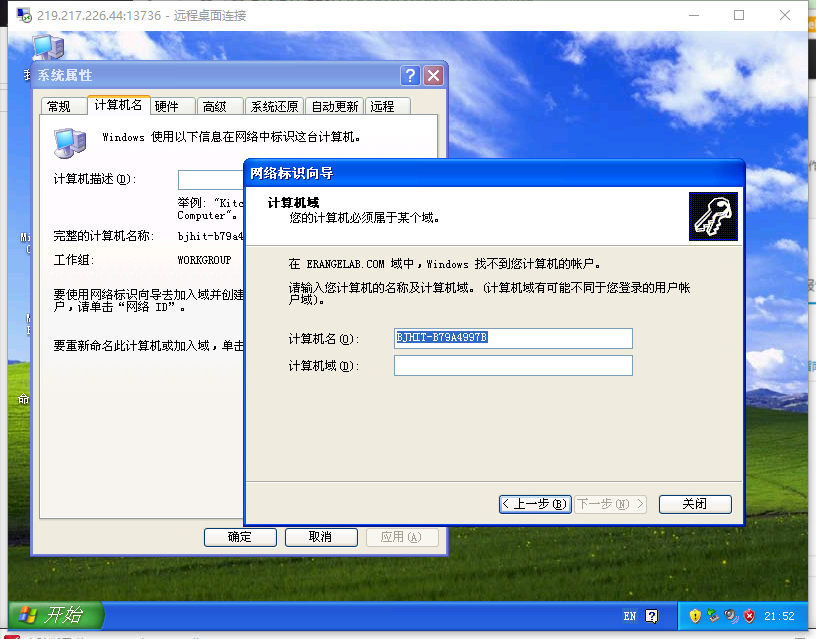
实验步骤3

1. 打开Windows Xp虚拟机，加入域

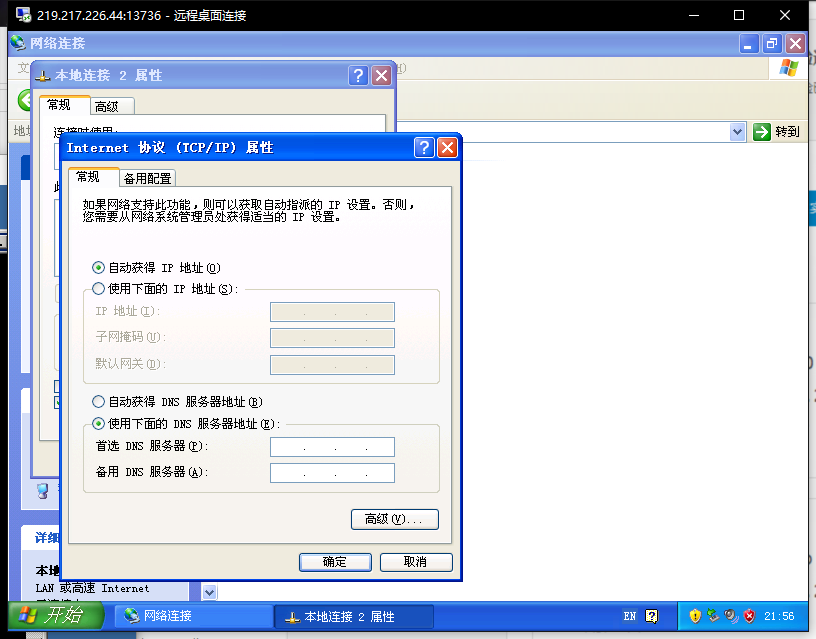


1. 输入用户名、密码和域，会发现无法找到计算机账户

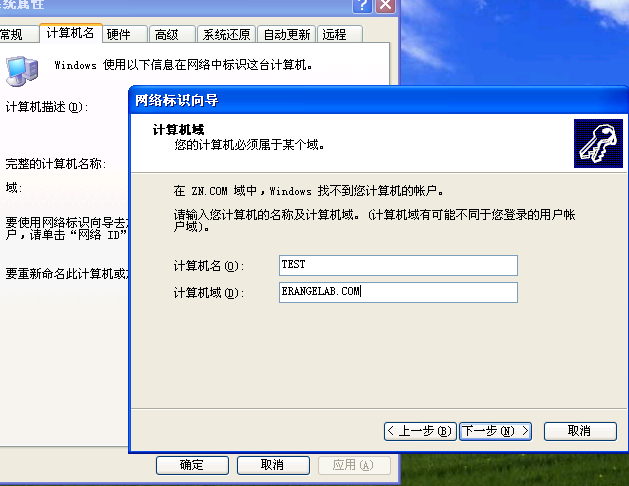


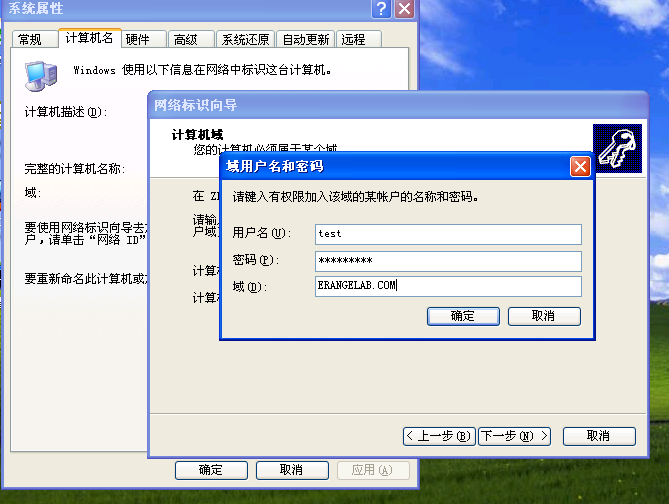


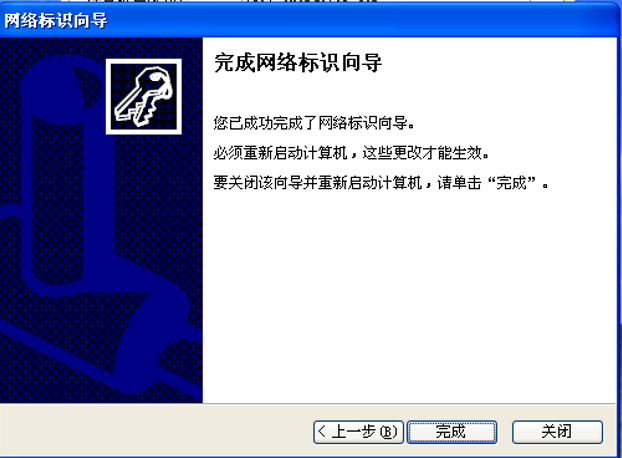
1. 这个时候，我们把xp远程机器上的dns服务器设成win server远程机器的ip



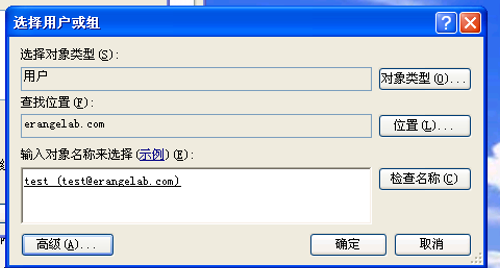
1. 然后重试第2步，输入计算机名和计算机域







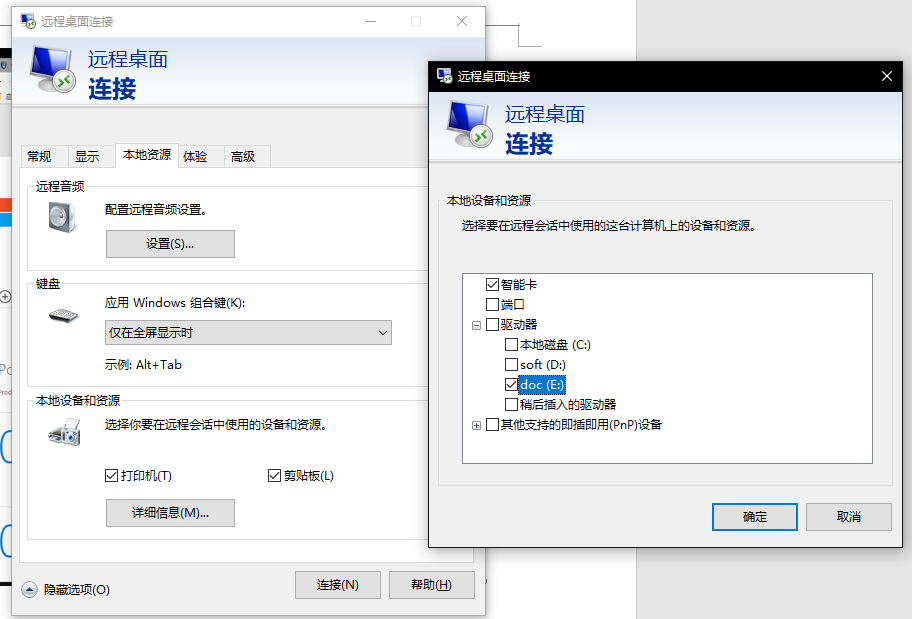
1. 重启远程xp机器，由于权限问题，此处先用管理员帐户登录，进入系统后右击‘我的电脑’----‘属性’----‘远程’----‘选择远程用户’----‘位置’，添加test如下图



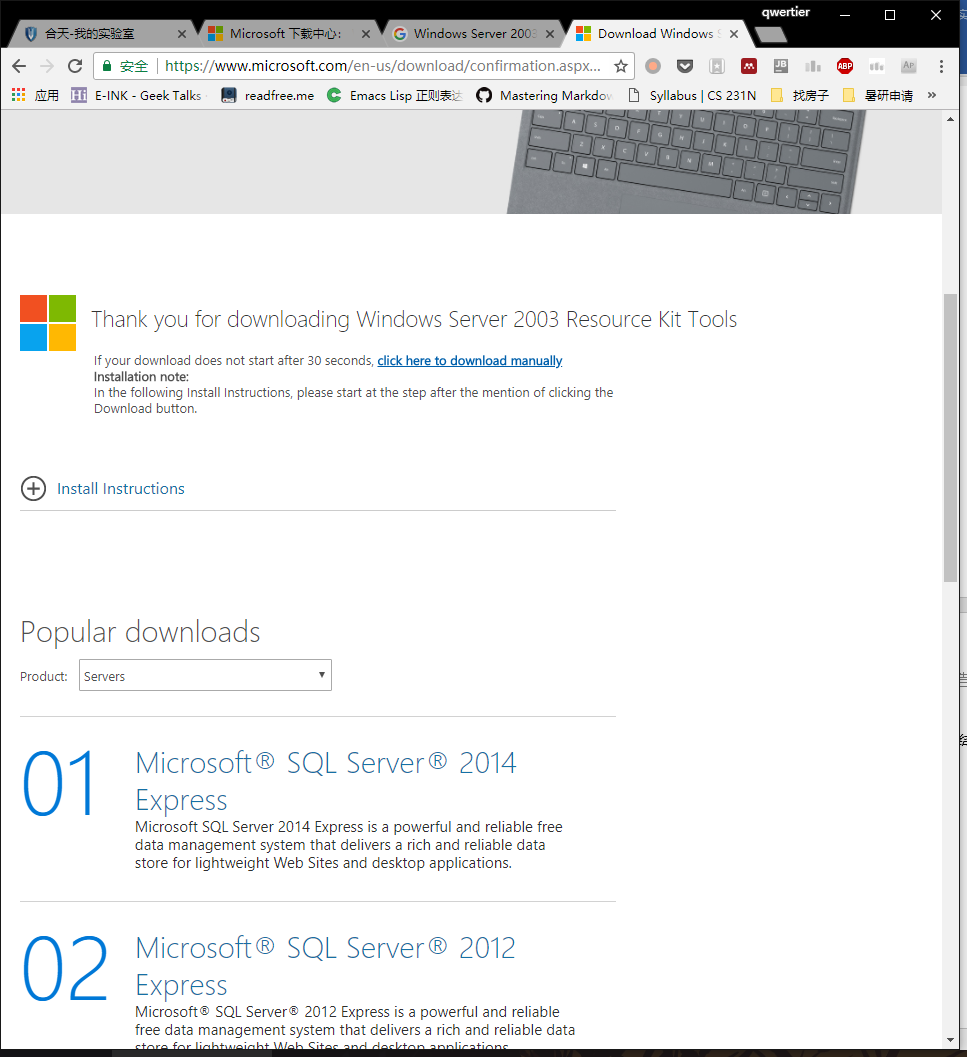
1. 重新启动xp机器，使用test用户登录



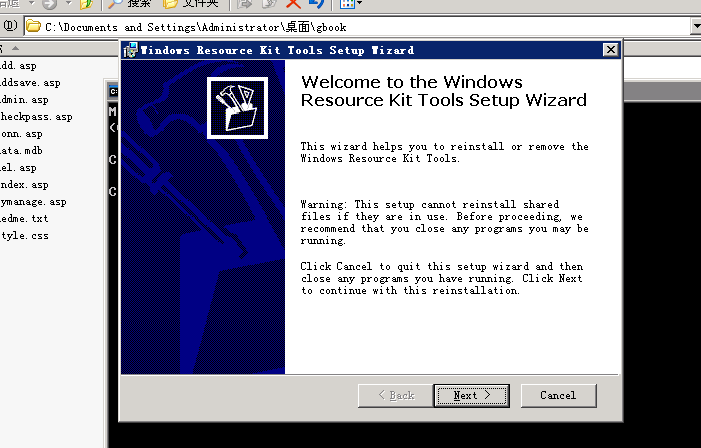
1. 由于需要安装“Windows Server 2003 Resource Kit Tools”，而远程服务器无法访问互联网，因此需要将本地磁盘挂载到远程服务器上



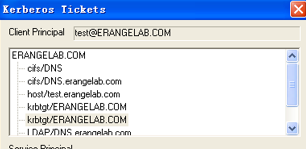
1. 在本地Windows官网上下载该工具



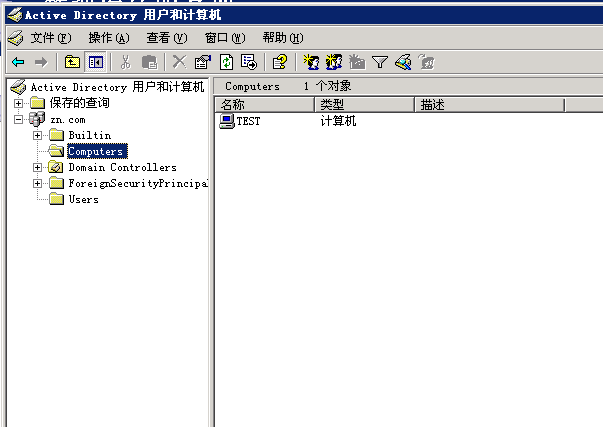
1. 安装该工具



1. 安装成功之后打开“开始”->“所有程序”->“Windows Resource Kit Tools”->“Command Shell”，输入kerbtray.exe回车,点击右下角绿色图标，可以看到票据



1. 此时在服务器上也可以看到注册了的票据和计算机



五、实验结果总结

心得体会

在本次实验中，我掌握了利用 Kerberos网络认证协议搭建方法、Windows Server 2003系统的域和DNS服务器的搭建以及Kerberos 认证原理。该实验令我对Kerberos系统有了更深刻的理解。实验的过程我认为还是有需要一定的耐心、细心和投入。在整个实验的过程中，我锻炼了动手能力，对排查计算机问题也更加耐心。

改进意见

1. 希望实验所用的机器可以更加鲁棒
2. 老师和助教配置远程机器很辛苦，但其实本实验也可以使用本地的虚拟机(Virtual Machine)来做，如果在一开始就告知或有相应的简单的指导就更好了。