

哈尔滨工业大学

信息安全概论课程实验报告

实验一

## 学院：计算机学院

## 班级：11403202

## 学号：1140320206

## 姓名：霍峻杰

1. 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；

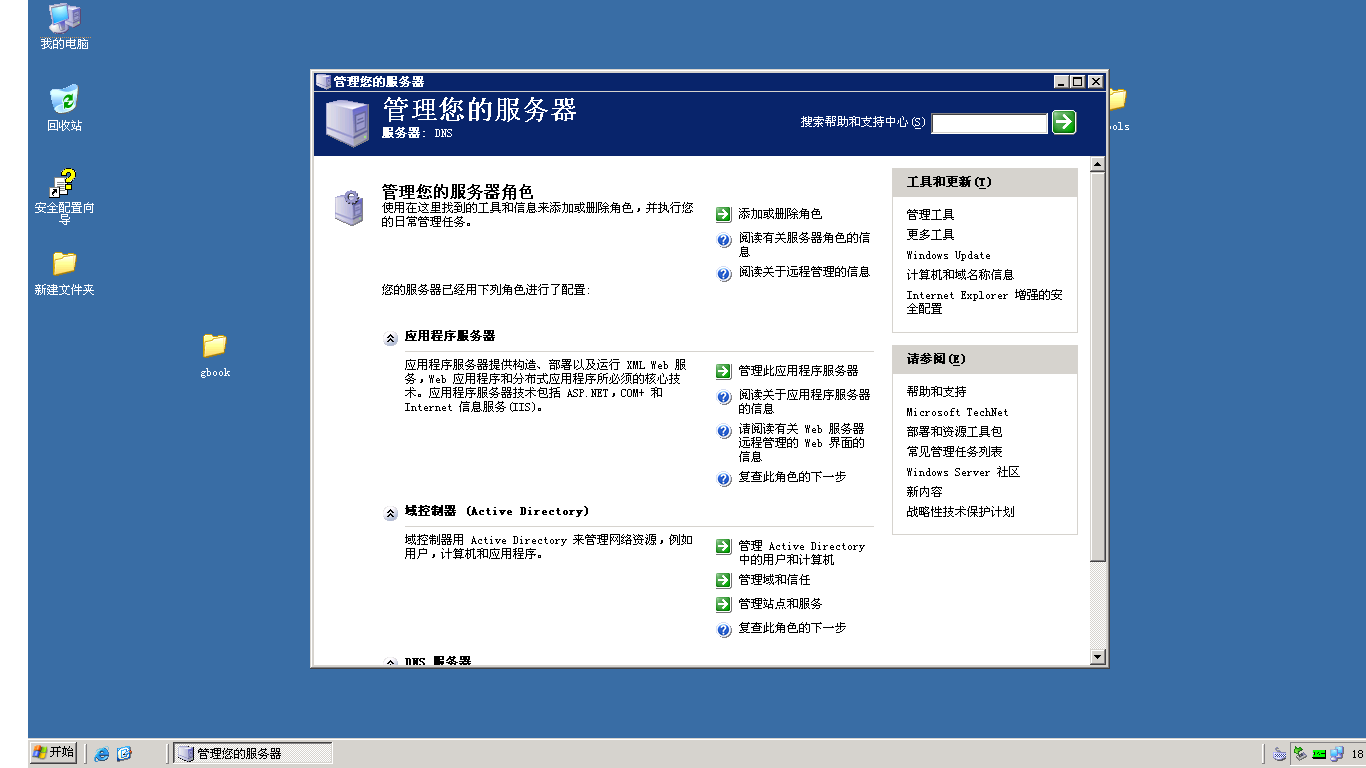
1. 实验内容及实现

**实验1**

Windows Server 2003上面

添加域控制器

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



      选择“域控制器”



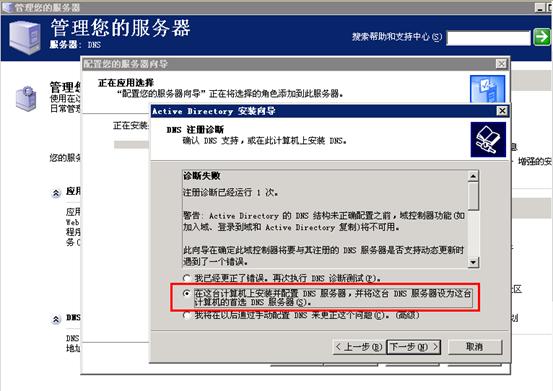
(由于做的时候没截图，这些图都是后来截的，安装完Active Directory提示重新安装，就直接拿了网上的图，实际操作也是按照这个一步一步来的，后面可以看到我新创建的域是成功的)。





      名称自定义



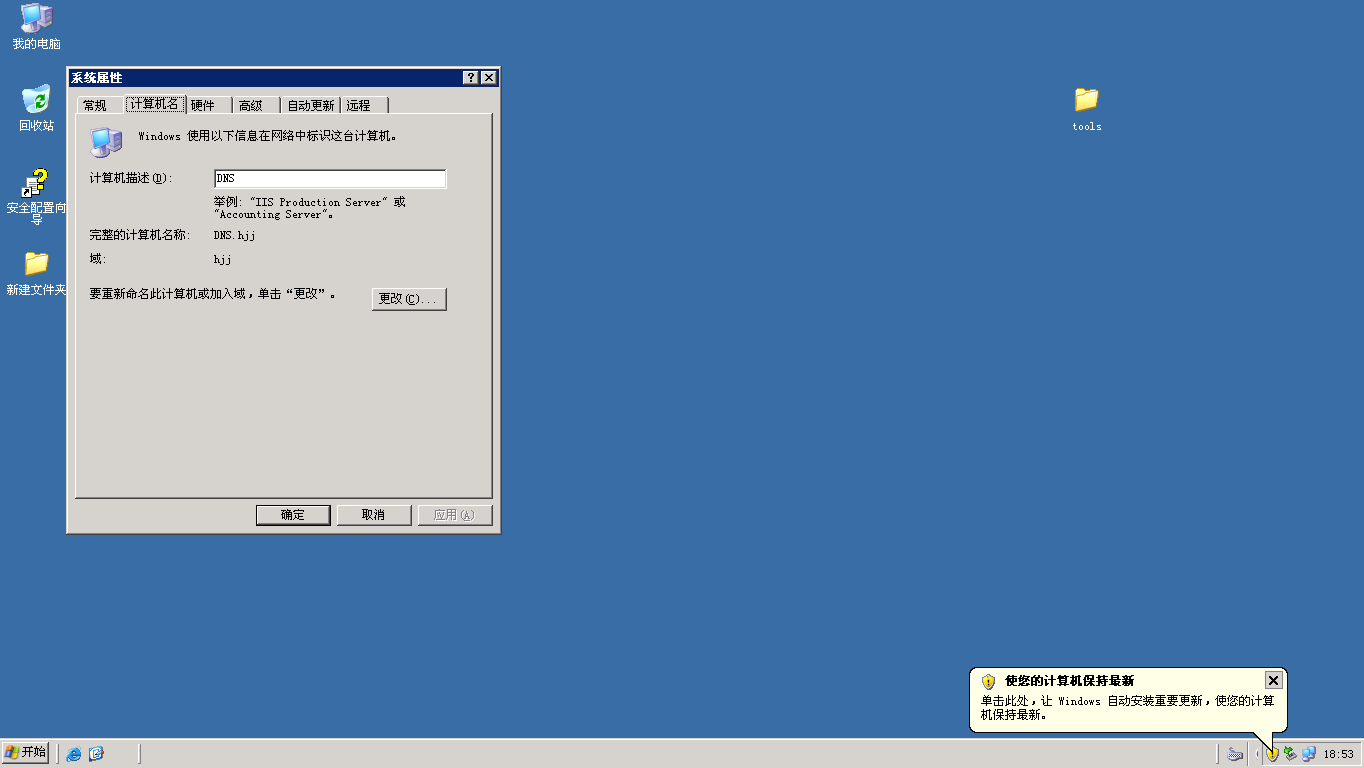






     还原模式密码默认设置为：123456；

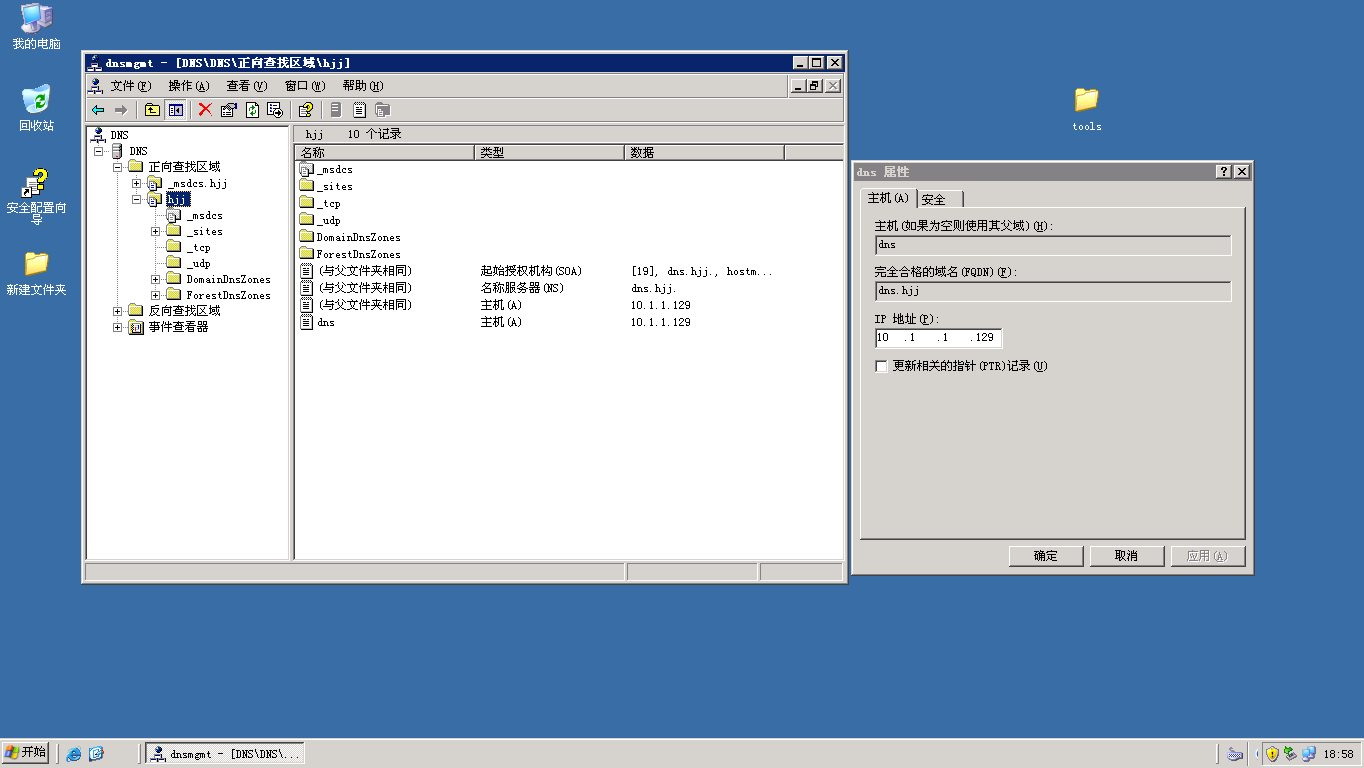
     下一步至完成后重启系统，耐心等待几分钟。（这里可以看见我的域创建成功，名字是hjj[我的缩写]）。



**实验2**

查看DNS服务器

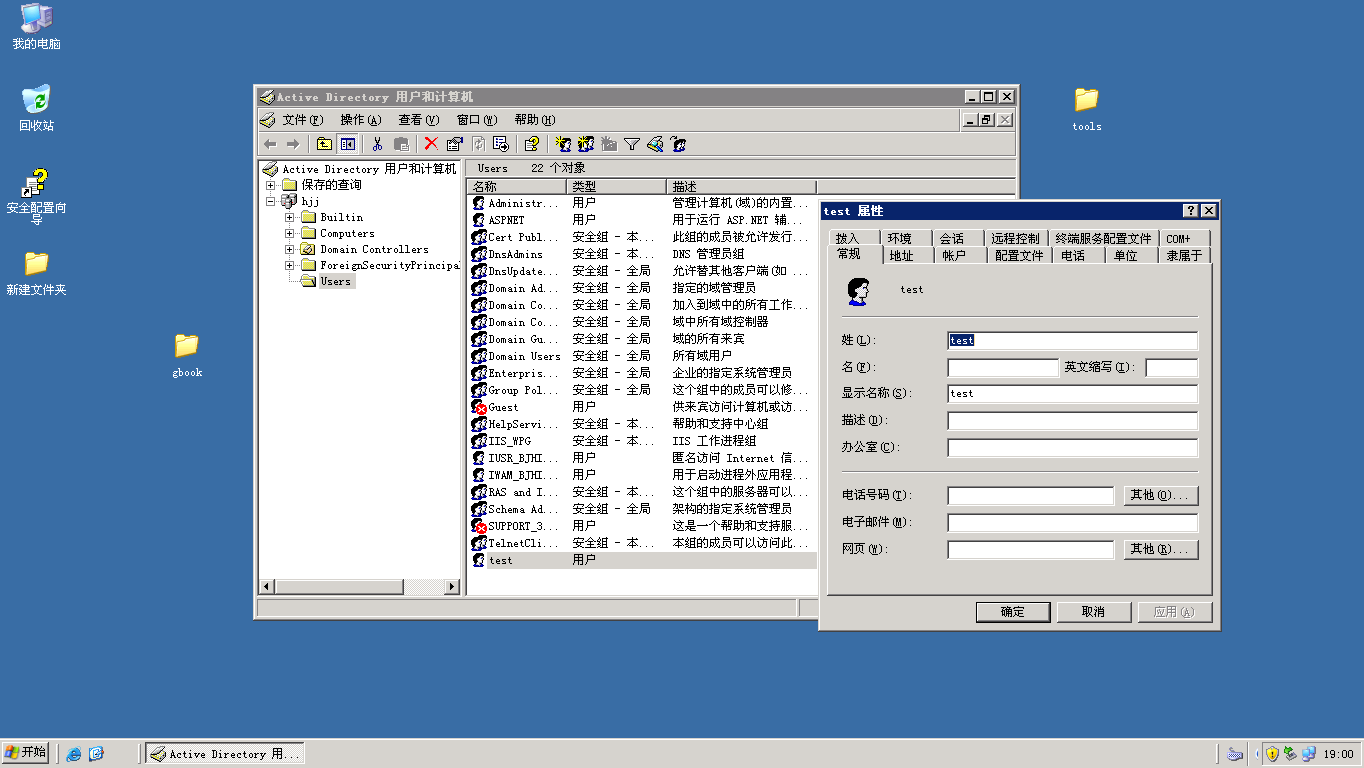
      “开始”——“管理工具”——“DNS”此时能看到DNS，本地连接已经自动将DNS设定为本机了



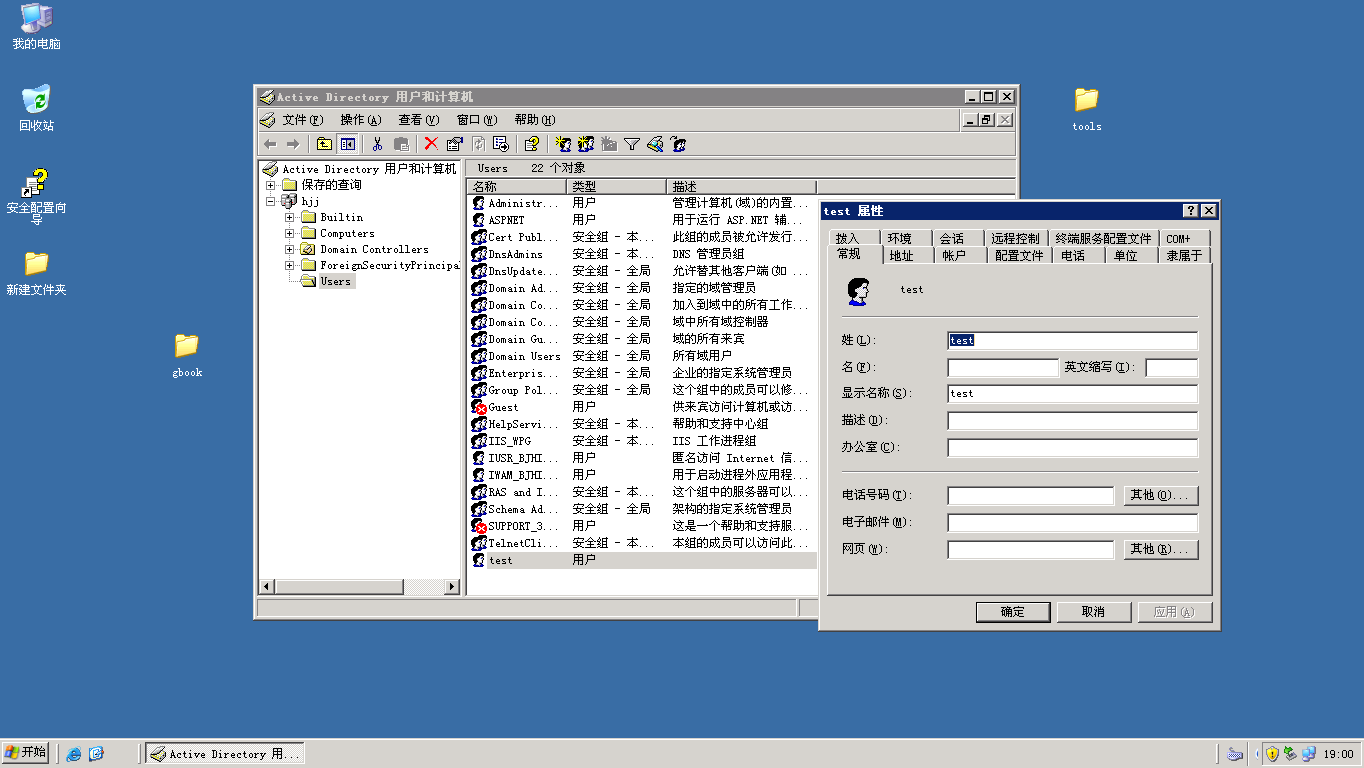
      创建测试用户



      新建用户

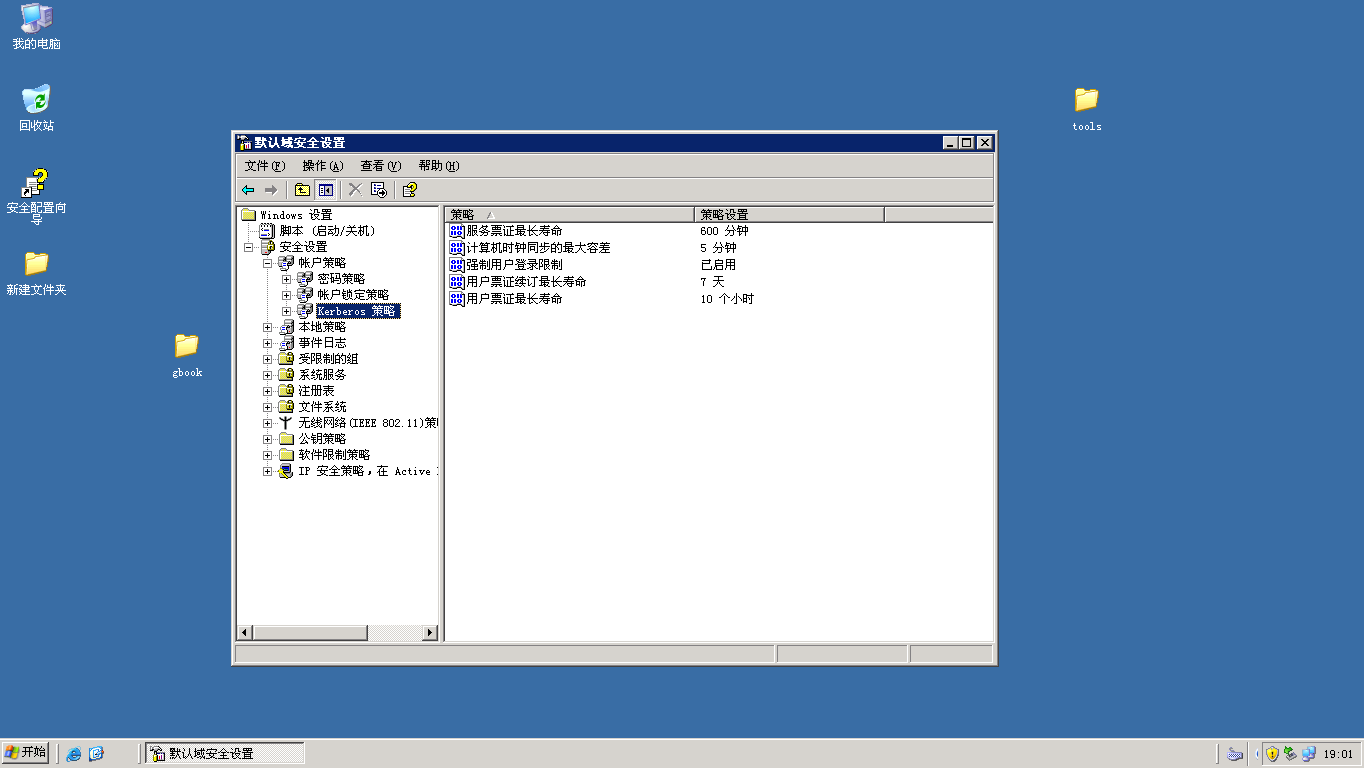


       此处的密码一定要复杂



      域安全策略

      可以设定Kerberos策略

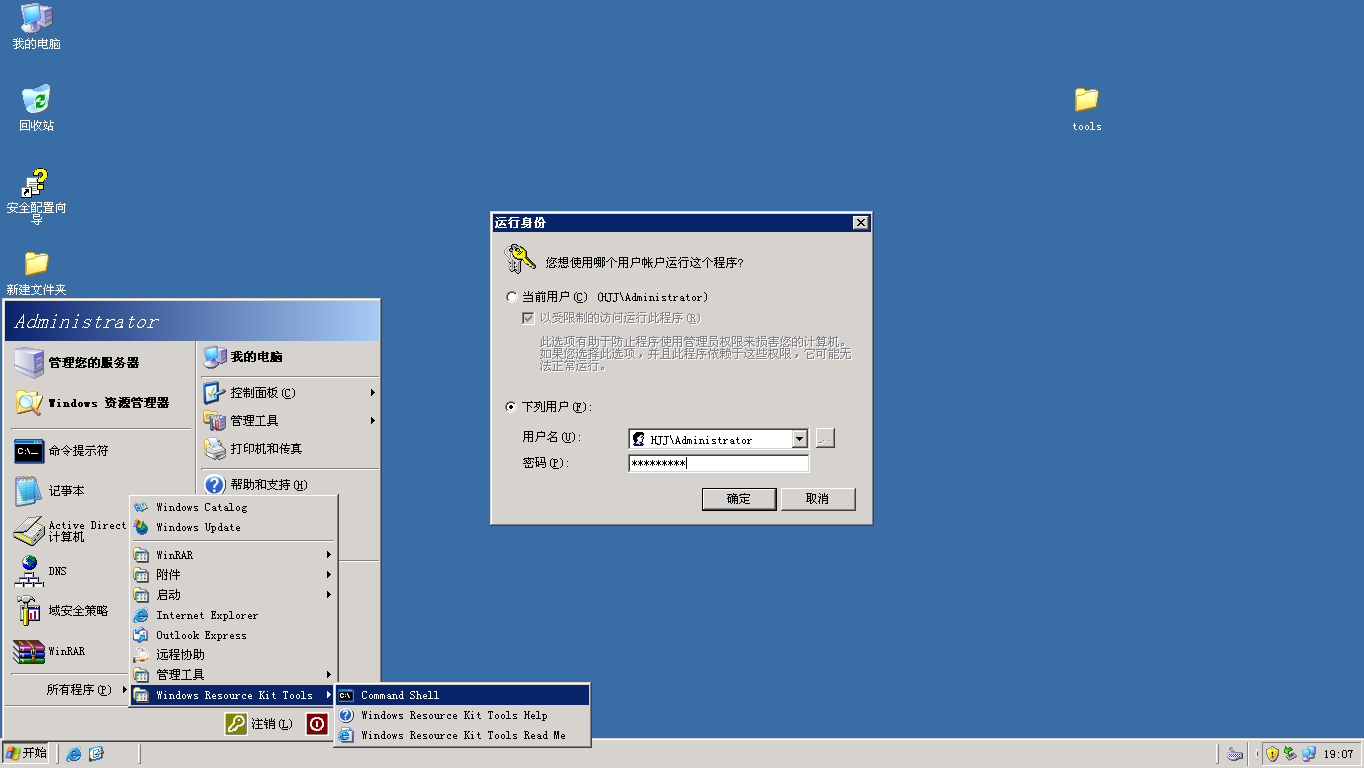


**实验3**

Windows 03 上面

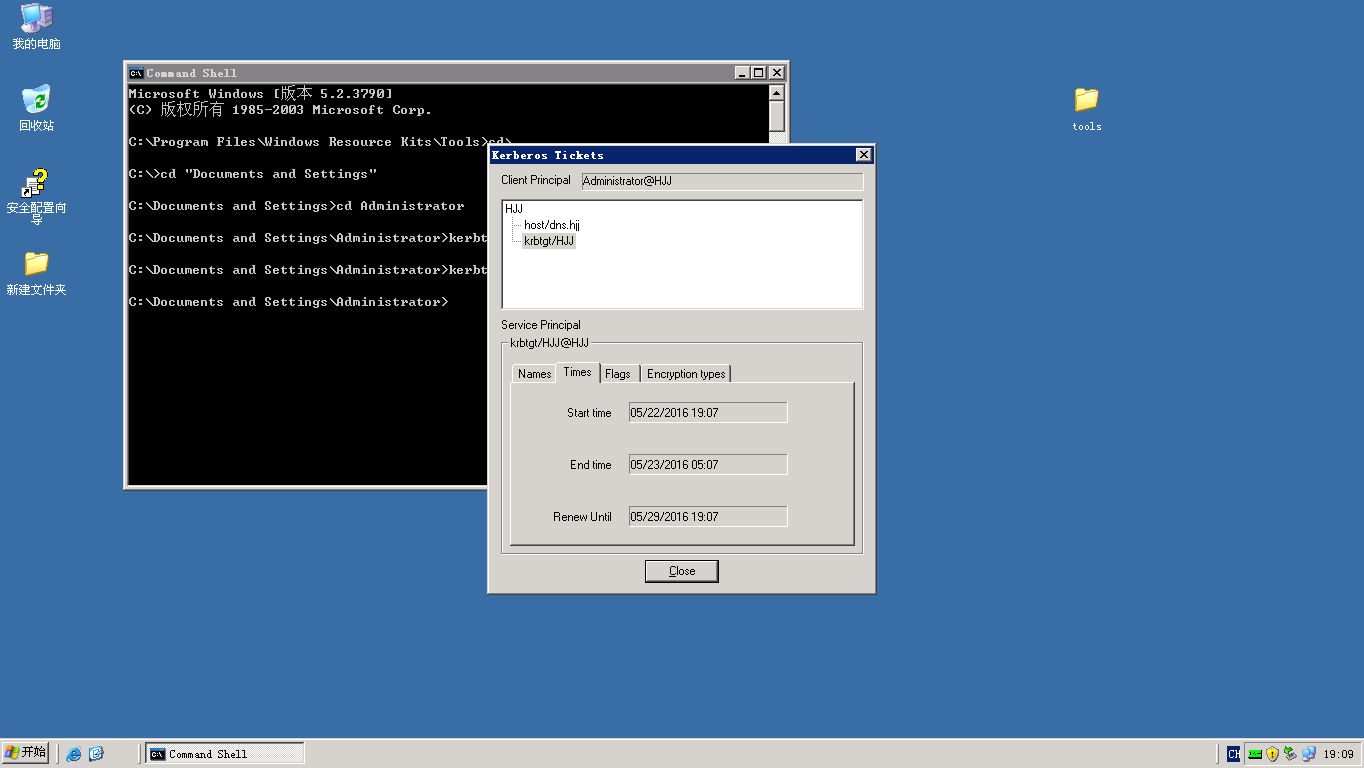
1、查看票据

      找到安装好的Windows Server 2003 Resource Kit Tools工具，然后右击运行方式



      确定后从开始菜单打开

      输入kerbtray.exe，然后右下角托盘有个绿色小票的标志，双击就能查看票据。



     实验总结

通过这次的实验，我首先学会了如何用命令行打开远程控制桌面，并进行了第一次的远程桌面操作，感觉很好玩。同时，还在其中学会了如何将本机的文件同步到远程控制端。实验一，我学会了通过安装Active Directory产生新的Kerberos域名，成功的创建了一个DNS名为hjj的新域，通过这个实验，我成功接触了Kerberos，并在建立的过程中简单地回顾和更深刻的理解了kerberos协议。实验二，我学会了查看DNS，并发现已经连到了本机。光创建了域还不够，还需要测试用户的建立，其中注意，设置用户密码是要复杂，数字，小写大写字母等多种字符的组合。除此之外，还可以找到并设定kerberos安全策略。实验三，目的是查看和清除kerberos票证缓存。这里需要借助一个工具—kerbtray，修改运行身份为自己的运行身份。打开命令行，输入kerbtray.exe，打开kerbtray，观察到票据，有名字，开始时间，终止时间，标志等基本信息。

这次试验让我获得了许多知识，并自己动手操作，对一些东西，如kerberos认证，有了更加深刻的理解。