

本实验要求实验者具备如下的相关知识。

1) Kerberos协议在Windows中的集成

Windows Server 2003 中的Active Directory 支持许多安全的Internet 标准协议和身份验证机制，用于在登陆时证明身份，包括：Kerberos V5、X.509 v3 证书、智能卡、PKI、SSL、LDAP等。Kerberos认证协议支持双向验证，用于在客户端/服务器环境中提供身份验证。

客户端需要向其访问的资源服务器进行身份验证，服务器也需要向客户端证明自己的身份。

Active Directory在安装完成后，域控制器的域名即派生为Kerberos的域名。域控制器可以提供Kerberos中密钥分发中心KDC服务。Active Directory中存储着用户的身份信息，包括用户名和一个由密码生成的密钥。同时也储存着域中的每一个服务器也将机子的账号名称和密钥。当用户登陆域时，提供有效的用户名和密码，接着，域控制器发给用户一个票据。

票据可用于在网络上请求域内其他网络资源。

2) Kerberos协议原理

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：

$C \rightarrow AS: ID_C, ID_{TGS}, Nonce_1$
 $AS \rightarrow C: \{K_{C,TGS}, Nonce_1\}K_C, \{T_{C,TGS}\}K_{TGS}$

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：

$C \rightarrow TGS: \{A_C\}K_{C,TGS}, \{T_{C,TGS}\}K_{TGS}$
 $TGS \rightarrow C: \{K_{C,S}, \{T_{C,S}\}K_S\}K_{C,TGS}$

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：

$C \rightarrow S: \{A_C\}K_{C,S}, \{T_{C,S}, Nonce_2\}K_S$
 $S \rightarrow C: \{Nonce_2\}K_{C,S}$

其中，ID_x表示X的实体名，Nonce表示随机数，T_{c,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，T_{c,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，A_c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。

辅助工具

（一）Kerbray

1. 简介

Kerbray 是一个 GUI 实用工具，是Windows Server 2003 资源工具包的一部分，可用于查看和清除计算机上的Kerberos票证缓存。

2. 工具使用详解

(1)启动 Kerbray

依次单击“开始”、“所有程序”，“Windows Resource Kit Tools”“Command Shell”，输入 Kerbray；双击任务栏中的“Kerbray”图标，以显示“Kerbray”对话框。可以看到“列出票证”和“清除票证”两个选项。

(2)针对“列出票证”对话框的操作

Kerbray 对话框有四个选项：

客户端主体：列出了与该帐户关联的 Kerberos 客户端主体的名称。

域和票证：列出了自登录后一直使用的服务的域和票证。从此部分中选择一项可显示该项在对话框的其他部分中的属性。

服务主体：列出了“域和票证”列表中所选票证的服务主体。

属性：详细说明了“域和票证”列表中所选票证的属性。“属性”部分分为四个选项卡：“名称”、“时间”、“标志”和“加密类型”。

“名称”选项卡包含票证所属主体的详细信息。

“时间”选项卡包含有关票证剩余生存期的详细信息，包括可续订的生存期。

“标志”选项卡包含票证所具有的属性的详细信息。

“加密类型”选项卡详细说明了票证中所用的加密方法。

(3)针对“清除票证”对话框的操作

选择“清除票证”选项将销毁所有缓存的票证。这将阻止对 Kerberos 资源进行身份验证。

如果选择了此选项，而后又要重新获得票证，需要先注销，然后再进行登录。此时将发行新的票证。

(二) klist

Klist是 Kerbray的命令行版本。它能够显示票证和授权票证的票证，也能清除所有票证的缓存。Klist显示的信息不如通过 Kerbray获得的信息详细。Klist有三个开关：tickets、tgt和 purge。下面介绍操作和用法。

(1)使用 Klist 查看缓存的票证，如下操作：

依次单击“开始”、“所有程序”，“Windows Resource Kit Tools”“Command Shell”，输入以下命令： klist tickets。此命令显示了自登录后已经经过身份验证的服务的最新缓存票证。

(2)使用Klist 查看缓存的授权票证的票证，如下操作：

依次单击“开始”、“所有程序”，“Windows Resource Kit Tools”“Command Shell”，输入以下命令： klist tgt。此命令显示初始Kerberos TGT 的属性。

(3)使用Klist 清除缓存的票证，如下操作：

依次单击“开始”、“所有程序”，“Windows Resource Kit Tools”“Command Shell”，输入以下命令： klist purge。

以上工具可点击

<http://tools.heetian.com/tools/Windows Server 2003 Resource Kit Tools.exe>下载。

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；

实验环境

域服务器Windows Server 2003， 客户机Windows XP

所用到的工具

- Windows Server 2003 Resource Kit Tools

实验步骤一

Windows Server 2003上面

添加域控制器

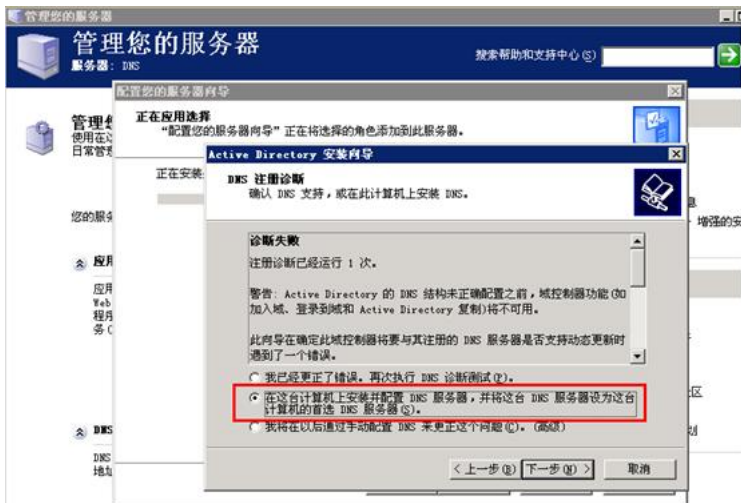
“开始”菜单----“控制面板”----“管理工具”----“管理您的服务器”



选择“域控制器”



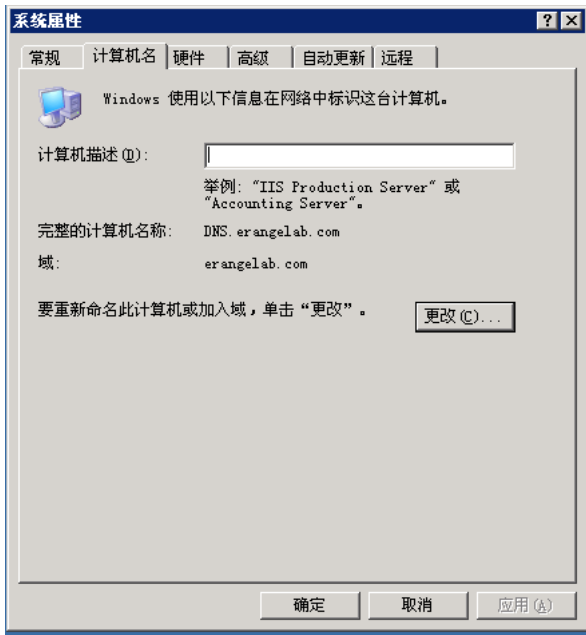
名称自定义





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。



任务一

Kerberos解决的问题是： 【单选题】 20分

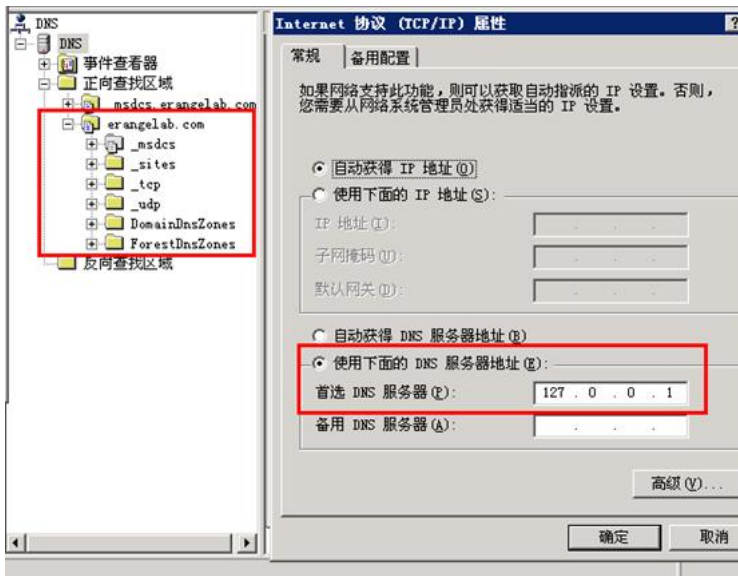
- ☐ 【A】 客户机与服务器的认证问题；
- ☐ 【B】 建立隧道进行安全传输的问题；
- ☐ 【C】 对数据进行加密，保证数据传输安全的问题；
- ☐ 【D】 对内网的安全防护；

提交

实验步骤二

查看DNS服务器

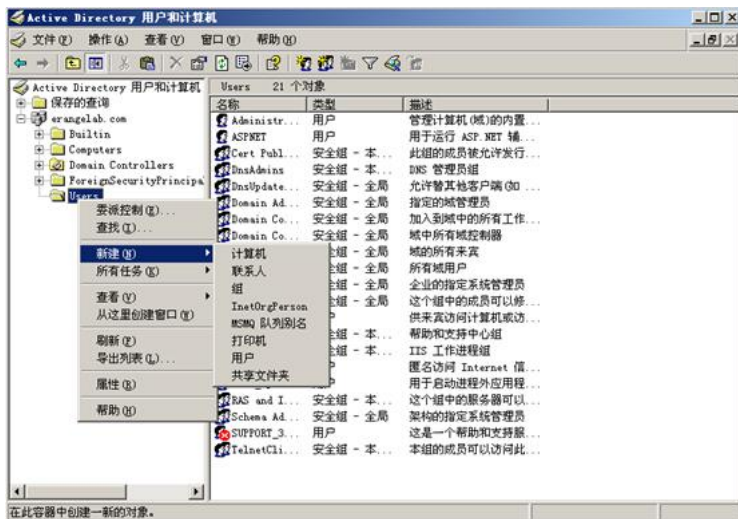
“开始”——“管理工具”——“DNS”此时能看到DNS，本地连接已经自动将DNS设定为本机了

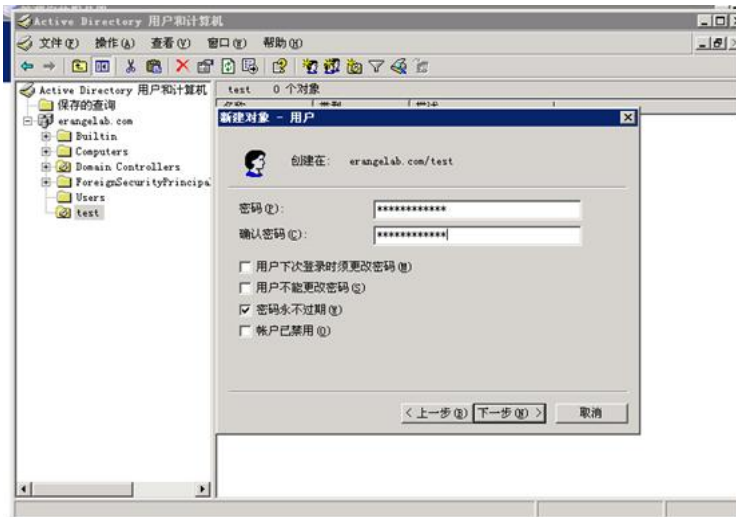
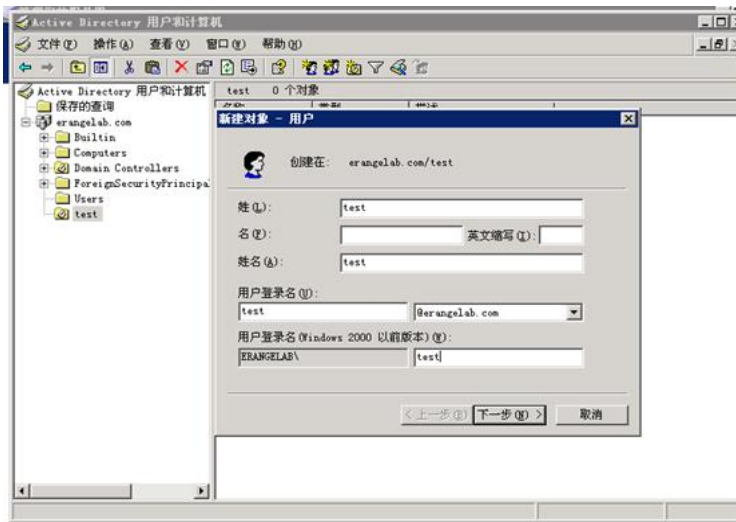


创建测试用户



新建用户





此处的密码一定要复杂

密码必须符合复杂性要求

描述

该安全设置确定密码是否符合复杂性要求。

如启用该策略，则密码必须符合以下最低要求：

- 不包含全部或部分的用户帐户名
- 长度至少为六个字符
- 包含来自以下四个类别中的三个的字符：
 - 英文大写字母（从 A 到 Z）
 - 英文小写字母（从 a 到 z）
 - 10 个基本数字（从 0 到 9）
 - 非字母字符（例如，!、\$、#、%）

更改或创建密码时，会强制执行复杂性要求。

要创建自定义筛选器，请参阅位于 [Microsoft 网站](#) 上的 Microsoft 平台软件开发工具包和 TechNet。

默认值：

- 在域控制器上已启用。
- 在独立服务器上已禁用。

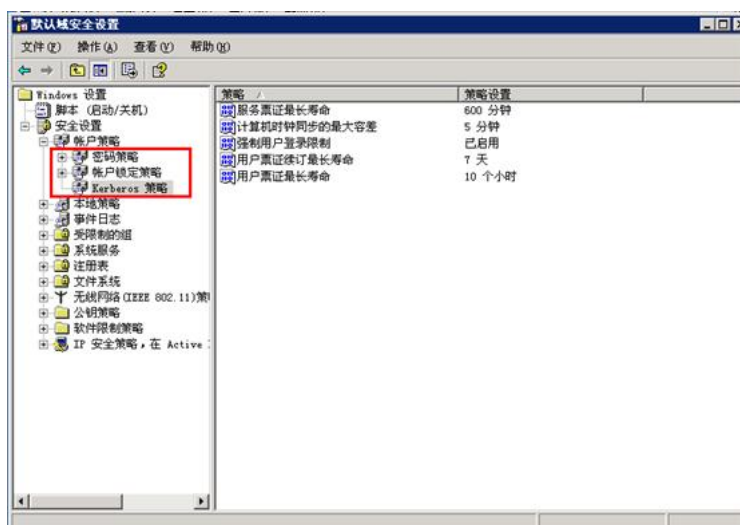
注意

- 默认情况下，成员计算机的配置与其域控制器的配置相同。

域安全策略



可以设定Kerberos策略



任务二

在本实验中，客户机为：【单选题】 20分

- ☐ 【A】 dns.erangelab.com
- ☐ 【B】 erangelab.com
- ☒ 【C】 test.erangelab.com
- ☐ 【D】 cifs/DNS.erangelab.com

提交

实验步骤三

Windows XP 上面

1、加入域

系统属性

?

×

常规

计算机名


硬件

高级

系统还原

自动更新

远程



Windows 使用以下信息在网络中标识这台计算机。

计算机描述 (D):

举例: "Kitchen Computer" 或 "Mary's Computer"。

完整的计算机名称:

heetian-test.dns.heetian.com

域:

dns.heetian.com

要使用网络标识向导去加入域并创建本地用户帐户, 请单击“网络 ID”。

网络 ID (N)

要重新命名此计算机或加入域, 单击“更改”。

更改 (C)...

确定


取消

应用 (A)

网络标识向导

用户帐户和域信息

用户帐户提供您访问网络上的文件和资源的权限。



请键入您的 Windows 用户帐户信息和域信息。如果您不知道该信息, 请向网络管理员咨询。

用户名 (U):

test

密码 (P):

域 (D):

ERANGELAB.COM

< 上一步 (B)


下一步 (N) >

取消

网络标识向导

计算机域

您的计算机必须属于某个域。



在 ERANGELAB.COM 域中, Windows 找不到您计算机的帐户。

请输入您计算机的名称及计算机域。(计算机域有可能不同于您登录的用户帐户域)。

计算机名 (C):

TEST

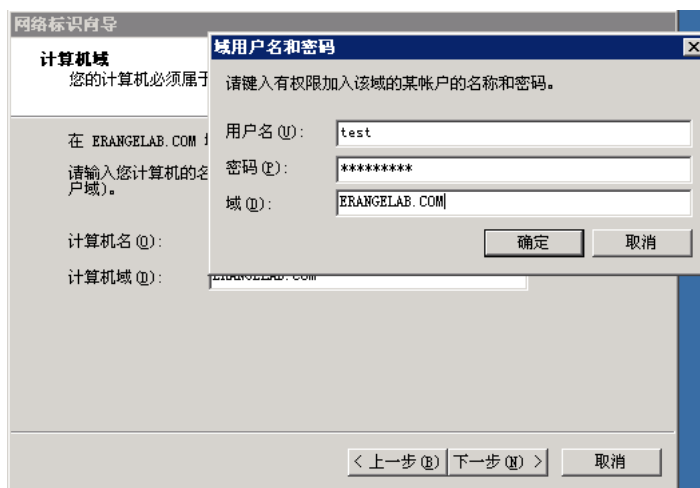
计算机域 (D):

ERANGELAB.COM

< 上一步 (B)

下一步 (N) >

取消



(提示：本机DNS地址需为域服务器的IP)

重启系统，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：

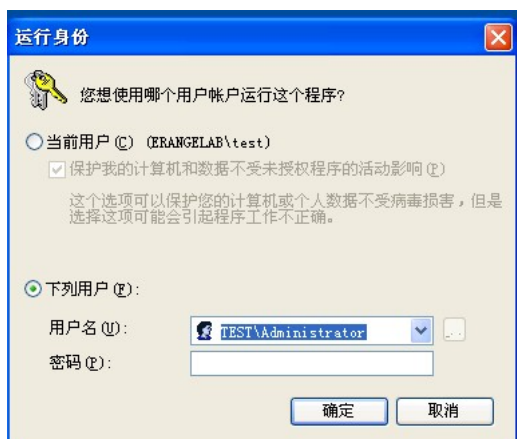


确定后注销用test登录到erangelab

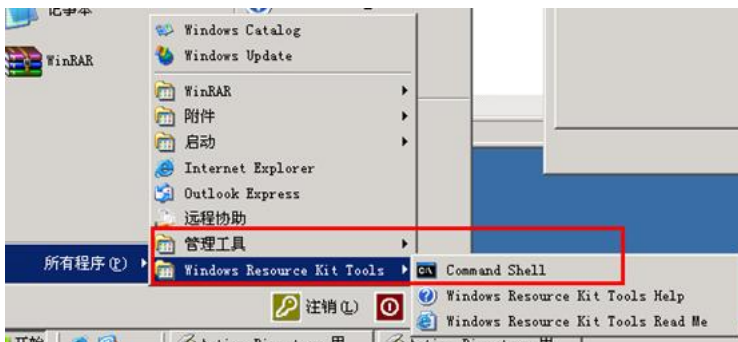


2、查看票据

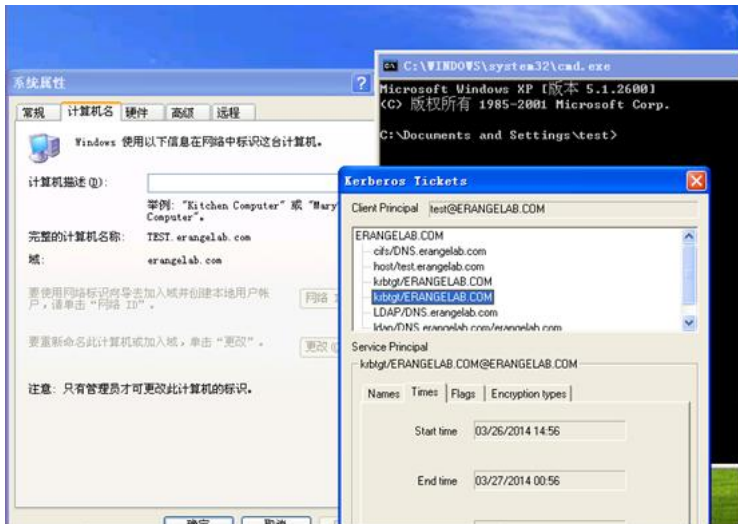
找到安装好的Windows Server 2003 Resource Kit Tools工具，然后右击运行方式



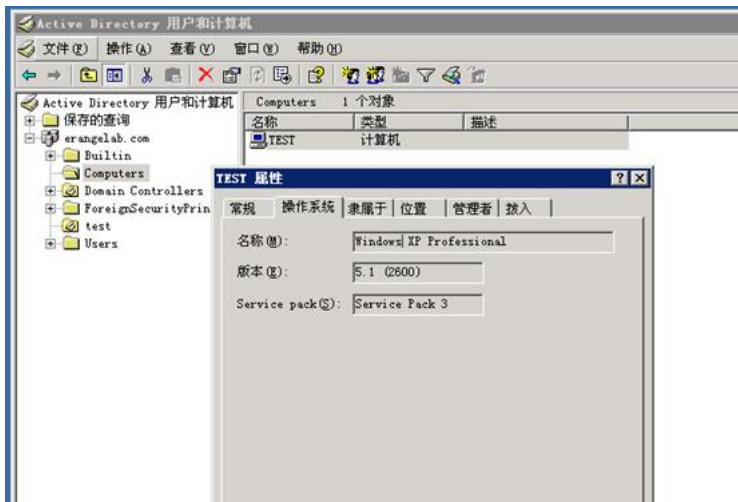
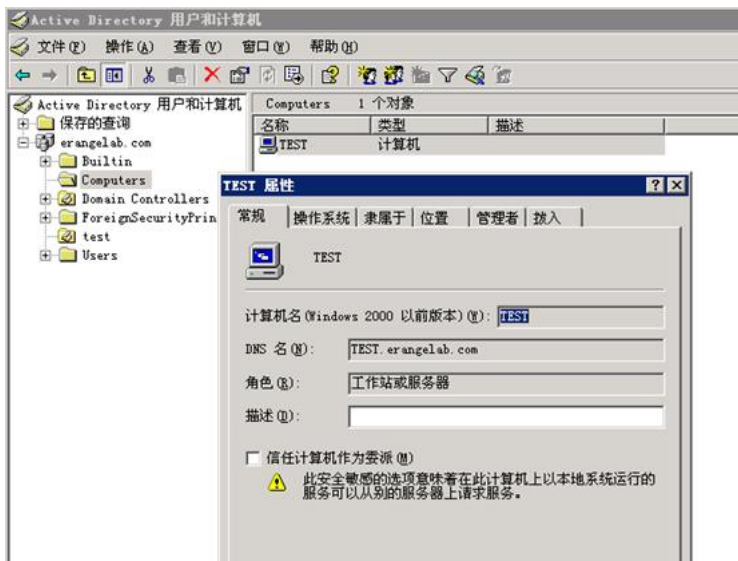
确定后从开始菜单打开



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。



3、Windows Server 2003上也能看到注册了的票据和计算机



Kerberos Tickets

Client PrincipalAdministrator@ERANGELAB.COM

ERANGELAB.COM

cifs/DNS.erangelab.com

host/dns.erangelab.com

krbtgt/ERANGELAB.COM

krbtgt/ERANGELAB.COM

ldap/DNS.erangelab.com/erangelab.com

Service Principalhost/dns.erangelab.com@ERANGELAB.COM

NamesTimesFlagsEncryption types

Start time03/26/2014 13:44

End time03/26/2014 23:44

Renew Until04/02/2014 13:44

Close