哈尔滨工业大学计算机学院

《网络攻击与防御》

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： | xxx |
| 学生姓名： | cycleke |
| 组 号： |  |
| 实验日期： |  |
| 实验地点： |  |
| 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

域服务器：Windows Server 2003

客户机：Windows XP

所用到的工具： Windows Server 2003 Resource Kit Tools

三、实验内容与实验要求

本实验主要介绍了Windows Server 2003系统的域和DNS服务器的搭建，通过本实验的学习学会Kerberos网络认证协议搭建方式。

**基本原理**

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：



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：



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：



其中，*ID*x 表示 X 的实体名，*N*once 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。

**实验内容**

此次实验中，我们需要首先再两台机器上都安装Windows Server 2003 Resource Kit Tools。之后使用Windows Server 2003搭建系统的域控服务器和DNS服务器，创建域用户。最后将Windows XP加入域环境并登录，查看自己的票据。

四、实验过程与分析

**实验步骤一**

1、下载安装Windows Server 2003 Resource Kit Tools

在http://tools.hetianlab.com/tools/Windows Server2003 Resource Kit下载Windows Server 2003 Resource Kit Tools并安装到两台实验机上。

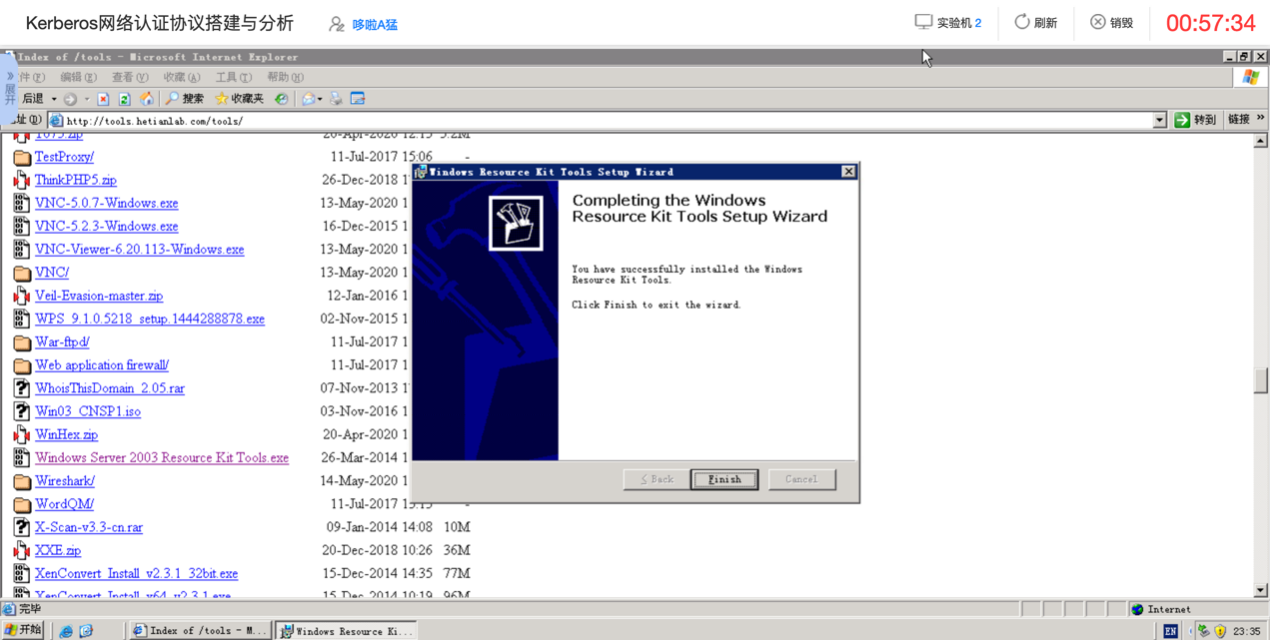


图 1在Windows Server 2003安装Windows Server 2003 Resource Kit Tools

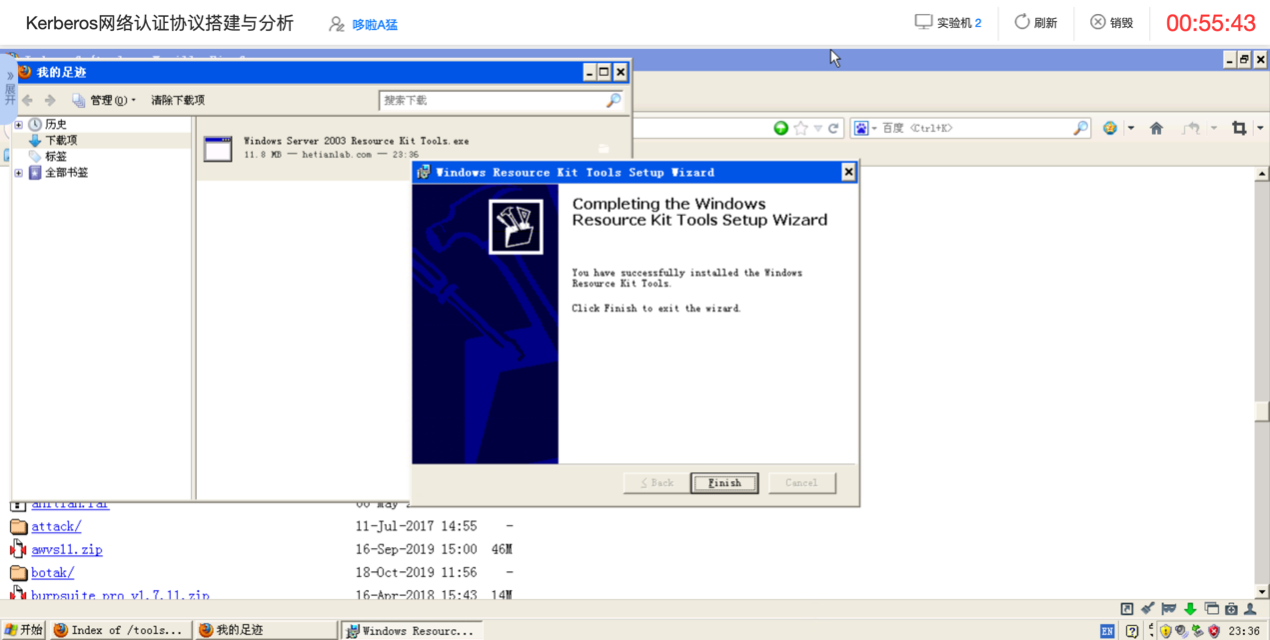


图 2在WindowsXP安装Windows Server 2003 Resource Kit Tools

2、安装域控服务器

切换到Windows Server 2003之后，依次点击“开始”——>“控制面板”——>“管理工具”——>“管理您的服务器”，然后点击“添加或删除角色”，点击“下一步”，选择“域控制器（Active Directory）”，然后点“下一步”。

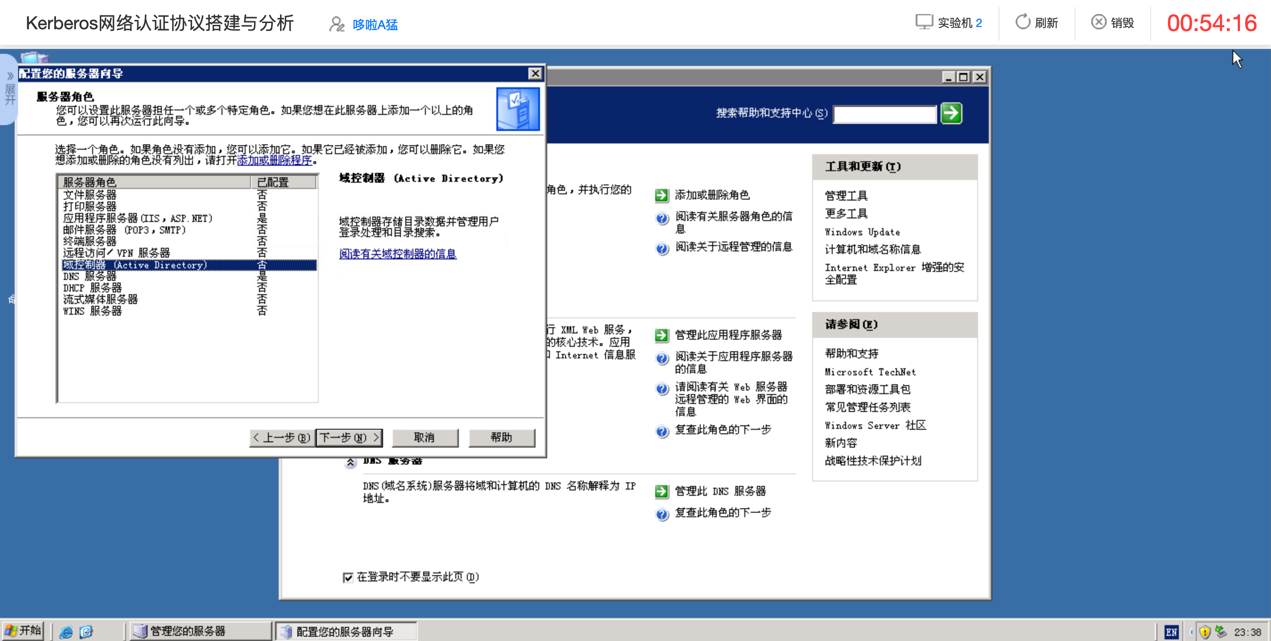


图 3添加域控服务器

在弹出的“Active Directory 安装向导”界面点“下一步” 然后选择“新域的域控制器”，然后点“下一步” 。在“新域的DNS全名”输入框中输入你想要定义的域名称（我使用的是hitlab.com）。设置好之后点“下一步”，这一步会检测是否有冲突而需要一会儿。



图 4设置新的DSN全名

之后一路默认，在“DNS注册诊断”设置处选择“在这台计算机上安装并配置DNS服务器....”，然后点“下一步”。



图 5在“DNS注册诊断”设置处选择“在这台计算机上安装并配置DNS服务器....”

在“权限”设置里面选择“只与Windows 2000或Window Server 2003 操作系统兼容的权限”，然后点“下一步”， 设置“还原模式管理密码”，然后点“下一步”。设置“还原模式管理密码”，然后点“下一步”， 在“摘要”界面确定设置无误之后，点“下一步”，之后系统会开始安装“Active Directory”服务

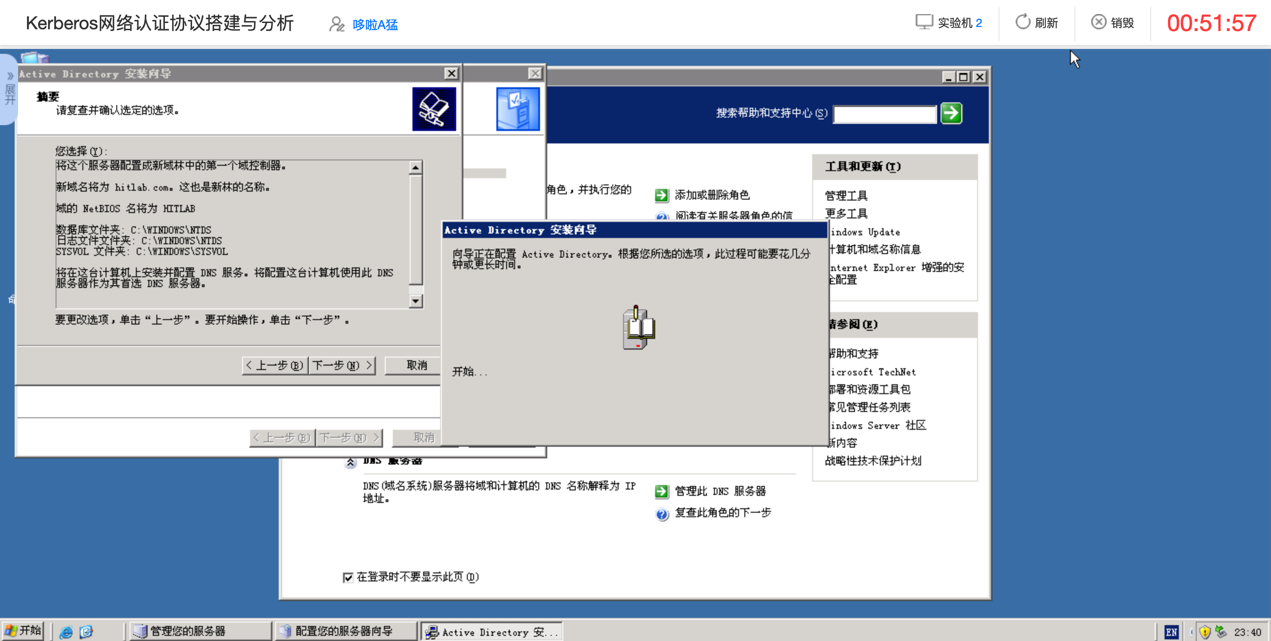


图 6系统开始安装“Active Directory”服务



图 7Active Directory安装完成

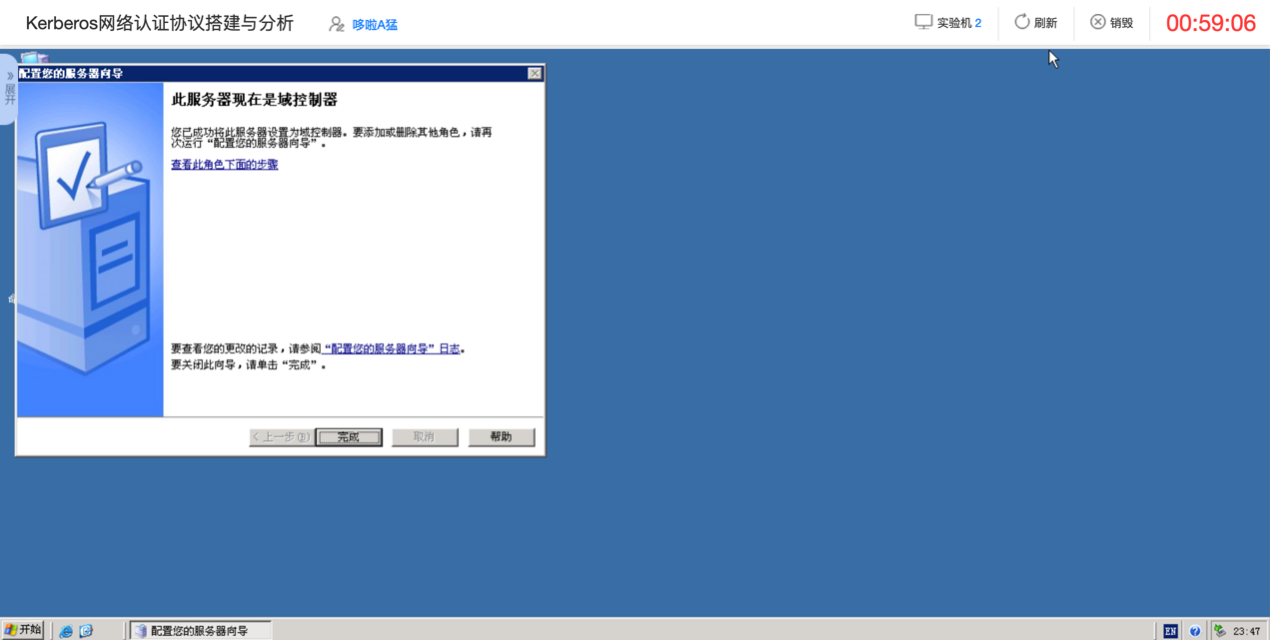


图 8域控制器安装完成

**实验步骤二**

3、查看和配置DNS服务器

在“管理您的服务器”菜单中，选择并点击“管理此DNS服务器”，之后检查正向查找区域的域名配置是否正常。



图 9检查正向查找区域的域名配置是否正常

4、创建域用户

在“管理您的服务器”中的“域控制器”选项中，点击“管理Active Directory中的用户和计算机”。 在弹出的“Active Directory 用户和计算机”中，依次选择需要配置的域名--->“User”，右击“User”选择“新建”--->“用户”。在对话框中填写必要的账号信息，然后点“下一步”。

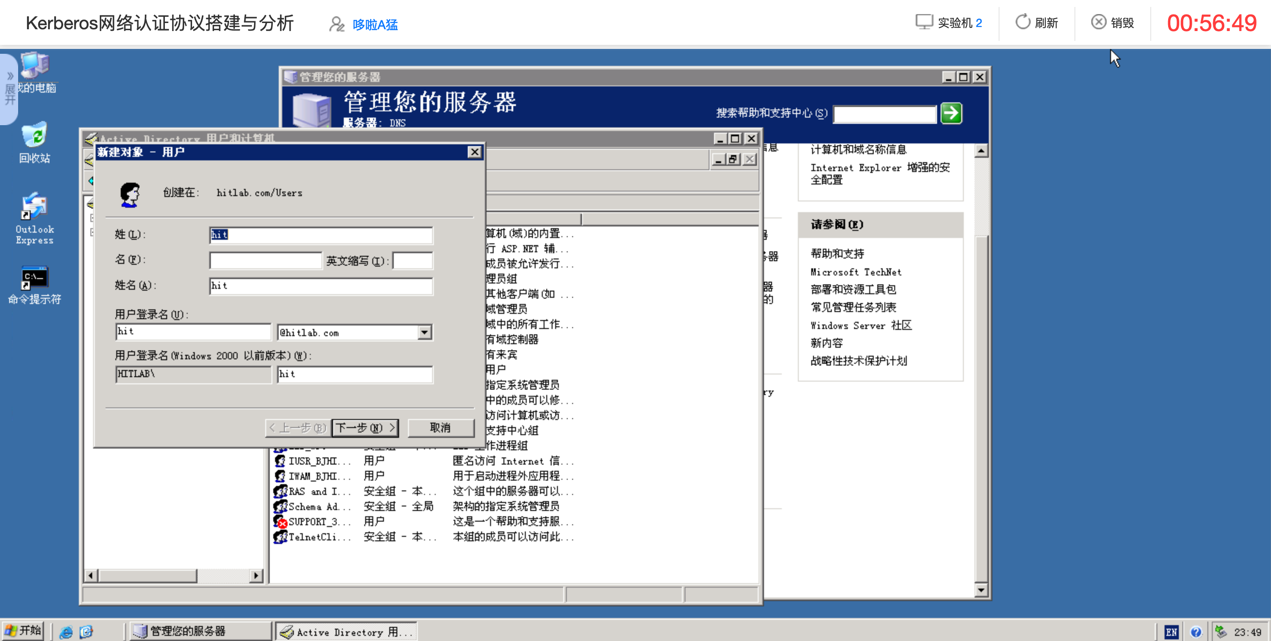


图 10填写必要的账号信息

之后设置符合要求的密码，设置密码永不过期，然后点“下一步”。

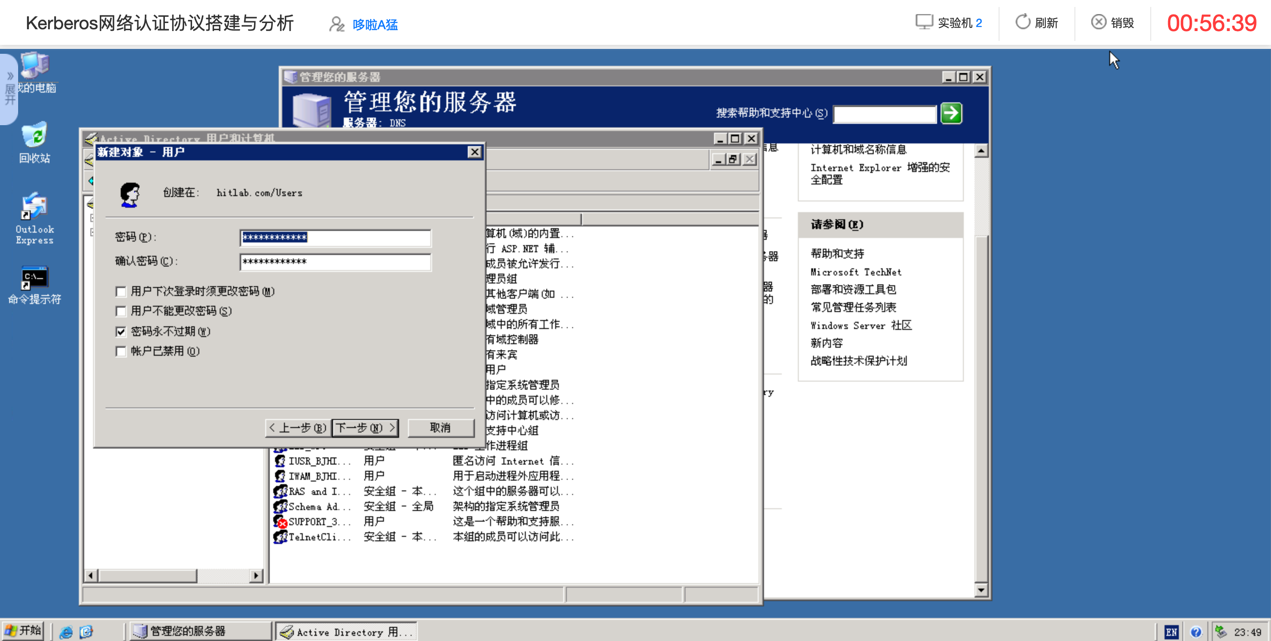


图 11设置用户密码

**实验步骤三**

5、将Windows XP加入域环境

切换到WindowsXP实验机进行配置，设置WindowsXP电脑的首选DNS服务器为Windows Server 2003的IP地址。

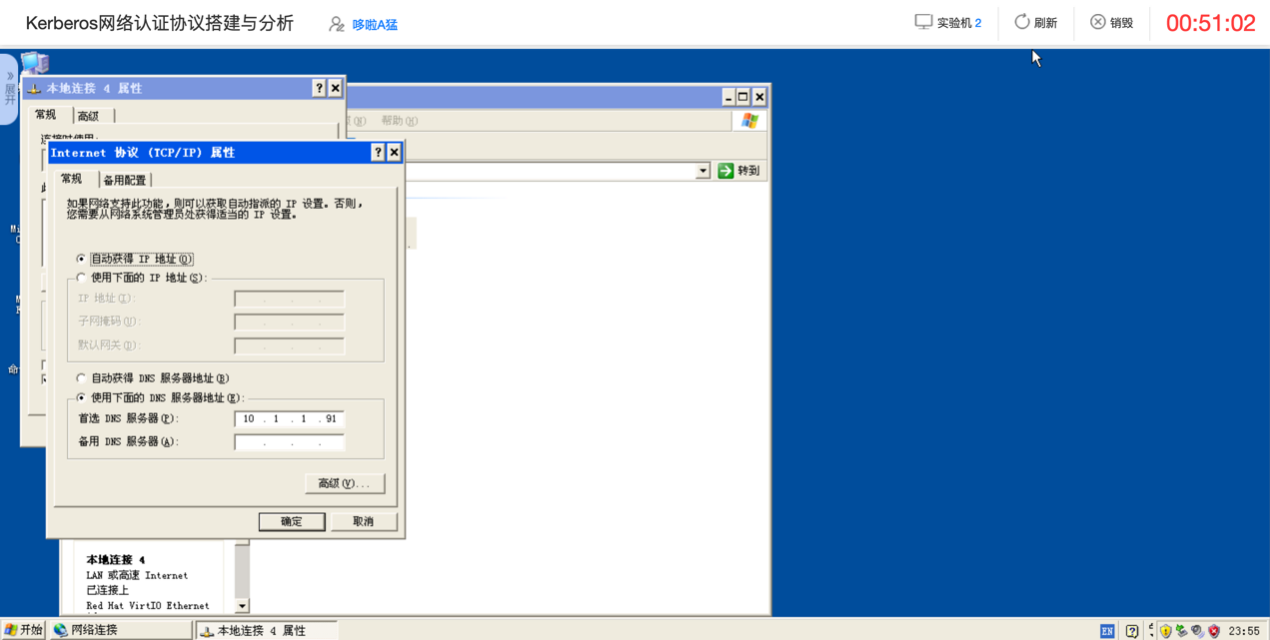


图 12设置WindowsXP的首选DNS服务器

右击“我的电脑”图标，选择“属性”，打开系统属性配置界面，切换到“计算机名”选项卡，点击“网络ID”。 连续点击“下一步”，选择“公司使用带域的网络”，然后点击两次“下一步”。 输入域账号和密码以及域名，然后点“下一步”。

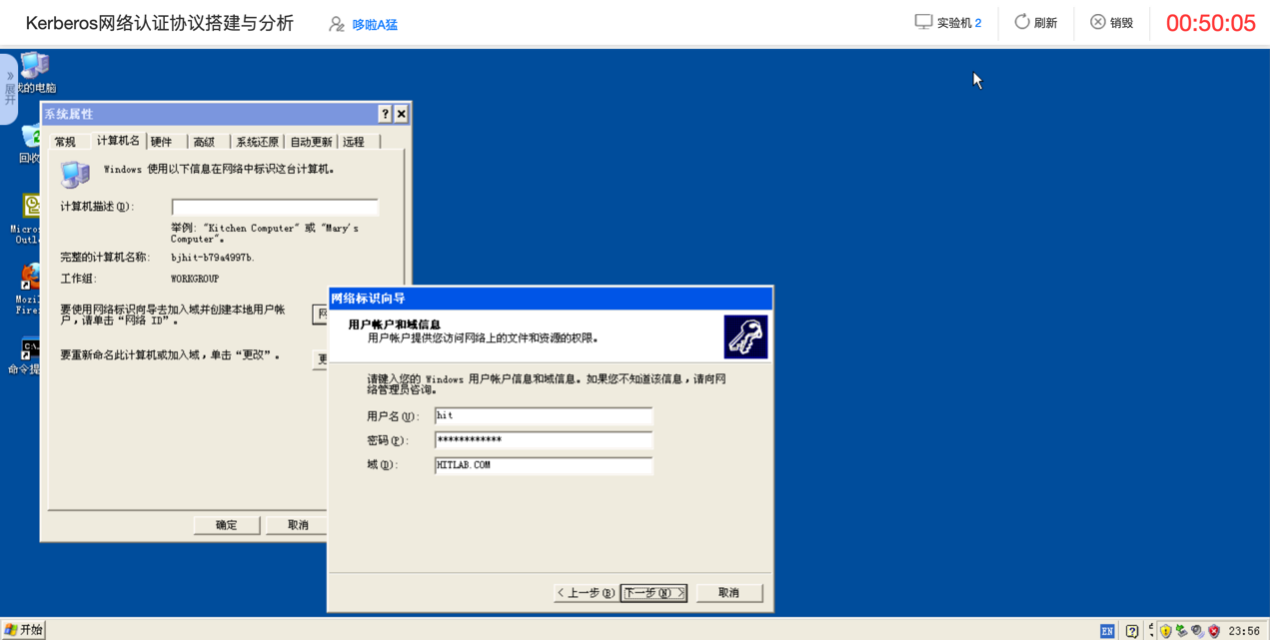


图 13输入域账号和密码以及域名

输入计算机名和域信息，然后点“下一步”。

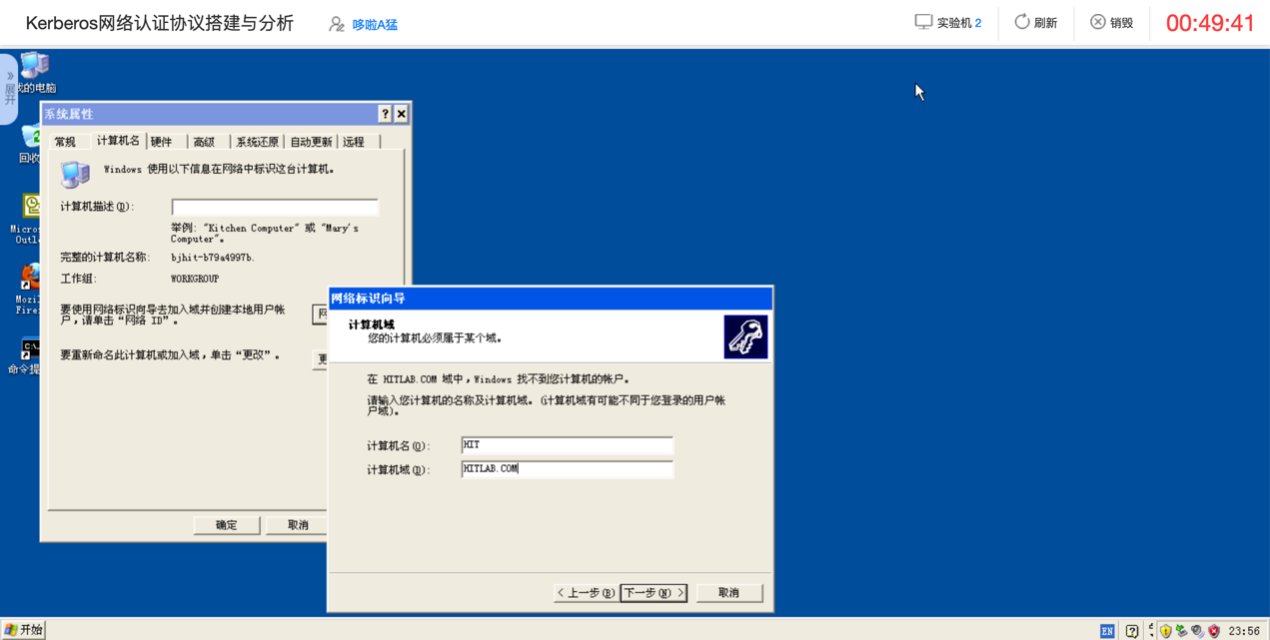


图 14输入计算机名和域信息

根据提示，输入域账号信息和域名信息，点“确定”，然后等一会儿。

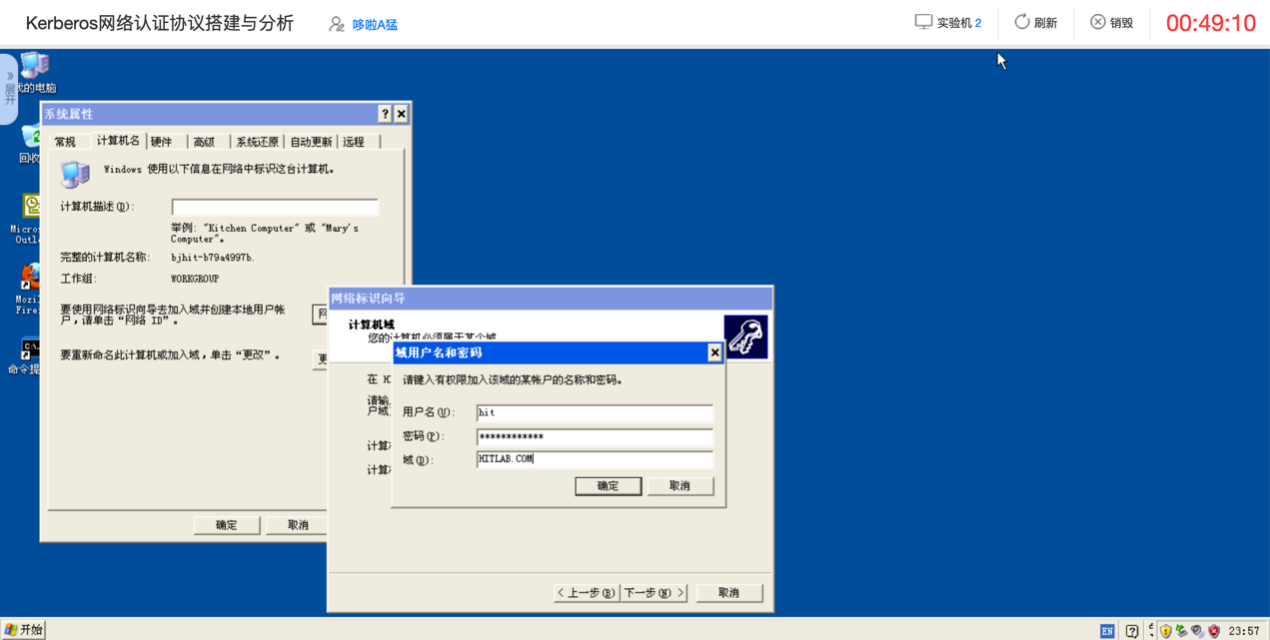


图 15输入域账号信息和域名信息

系统提示需要重启计算机，点“确定”，但是不要立即重启，而是转到用户管理，更改一下管理员密码。右键-“我的电脑”---选择“管理”，在“系统工具”中找到“本地用户和组”-->“用户”，右键点击“Administrator”--->“设置密码”。 点击“继续”，然后设置一个密码即可。

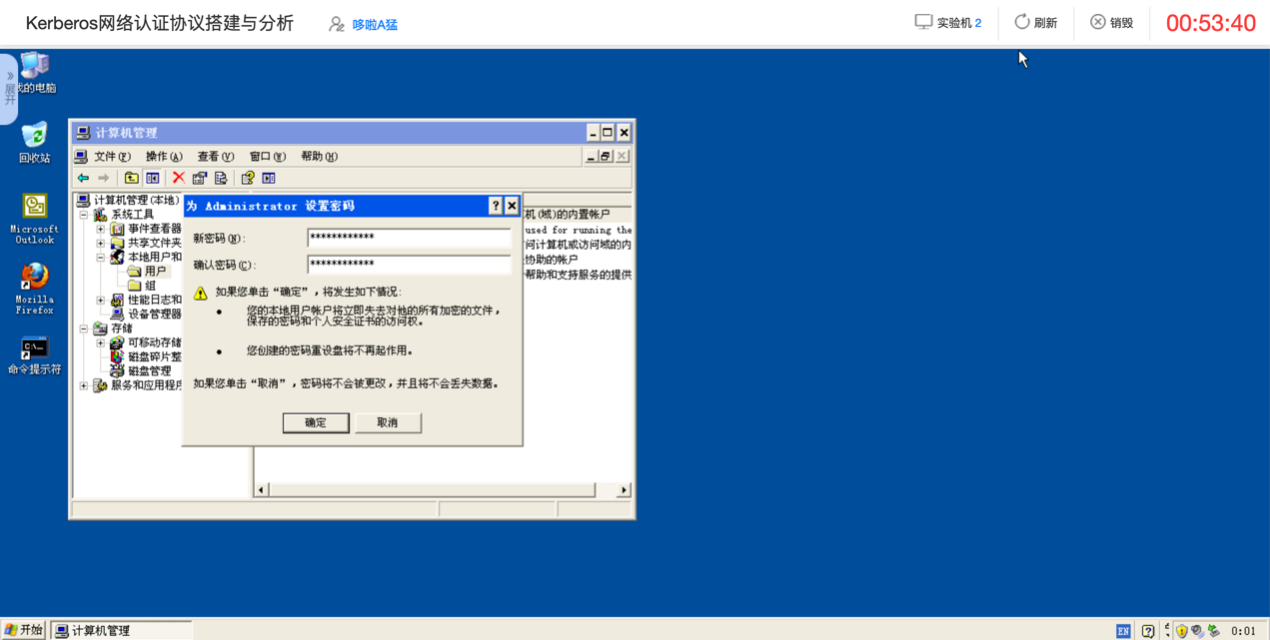


图 16为Administrator设置密码

之后重启系统。等待重启完成，需要1-2分钟，然后点击右上角的“实验机”里面的“xp”机器重新连接即可。之后手动输入我们设置的管理员密码进行登录，登录到选择“本机”。 登录之后，弹出的新硬件向导之类的，直接点取消即可。

为了能切换到我们的域账号，我们需要先给它添加一个能登录远程桌面的权限。右键“我的电脑”-->“属性”-->"远程"--"选择远程用户"。点“添加”， 点击“位置”， 根据提示输入域账号信息，然后点确定。

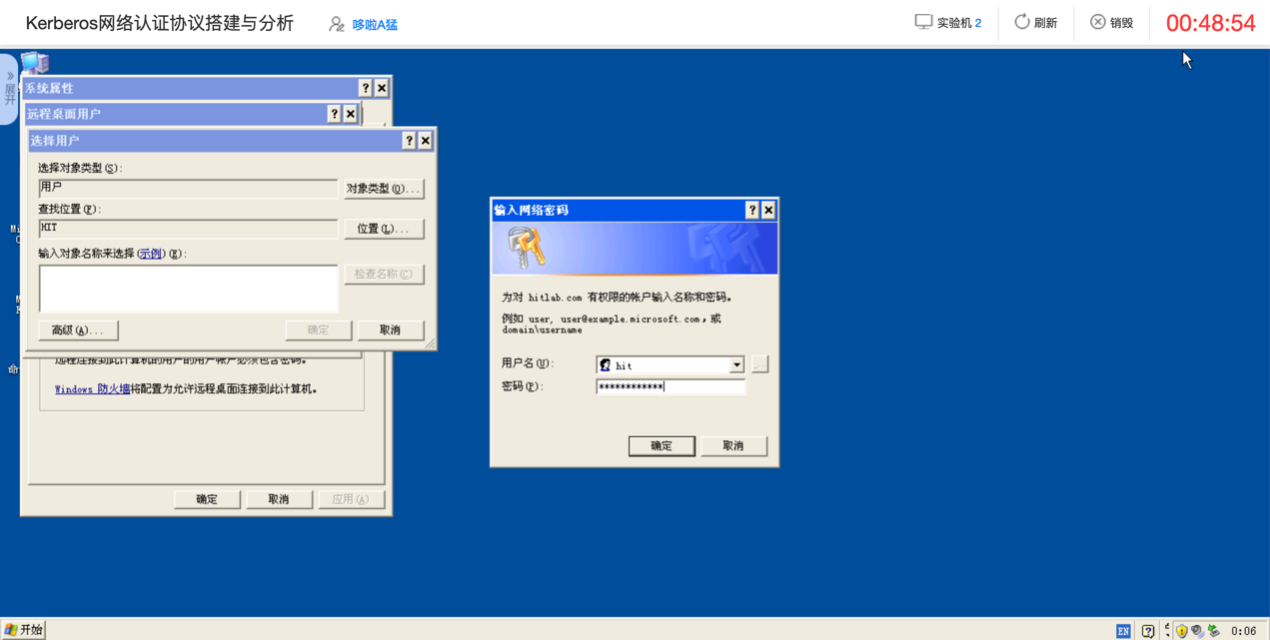


图 17根据提示输入域账号信息

然后在位置选择中，选择需要所属的域，之后点“确定”。 在“输入对象名称来选择”下方的输入框中输入域账号的名称，然后点右边的“检查名称”。 如果账号无误的话，就可以成功找到，然后点确定，之后一路确定即可。

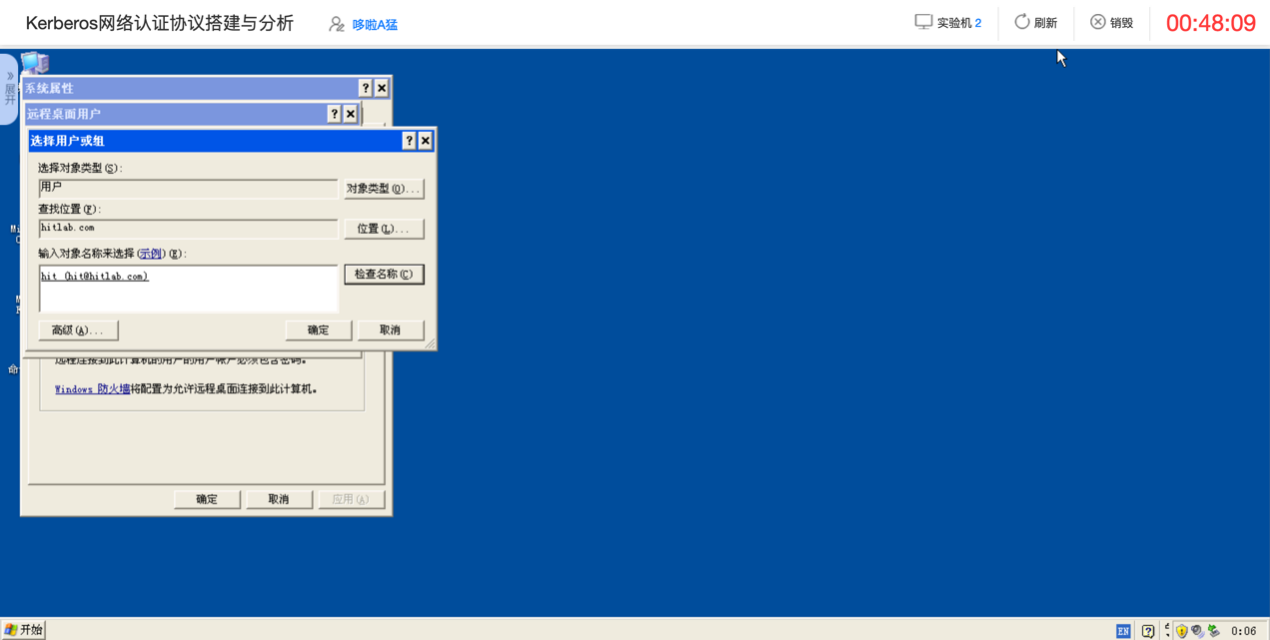


图 18输入域账号的名称

6、登录到域环境

在Windows xp 上点击“开始”-->"注销"，确认注销。然后点击右上角的实验机重新连接一下，然后输入相关的域账号信息和选择登录到相应的域，然后点确定即可登录成功。

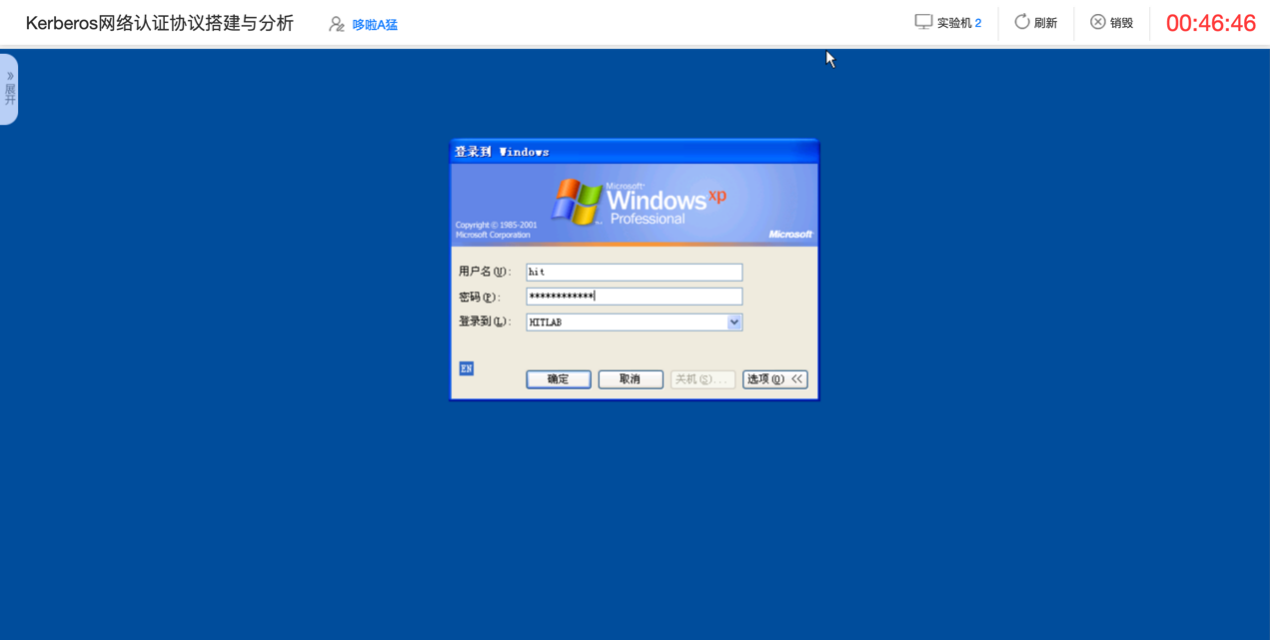


图 19重新登录WindowsXP

7、查看票据

依次点击“开始”-->“所有程序”-->"Windows Resource Kit Tools"-->"CommandShell"，然后输入“kerbtray.exe”回车，在桌面右下角的任务栏就会出现一个绿色小票的图标，双击就能看到票据。

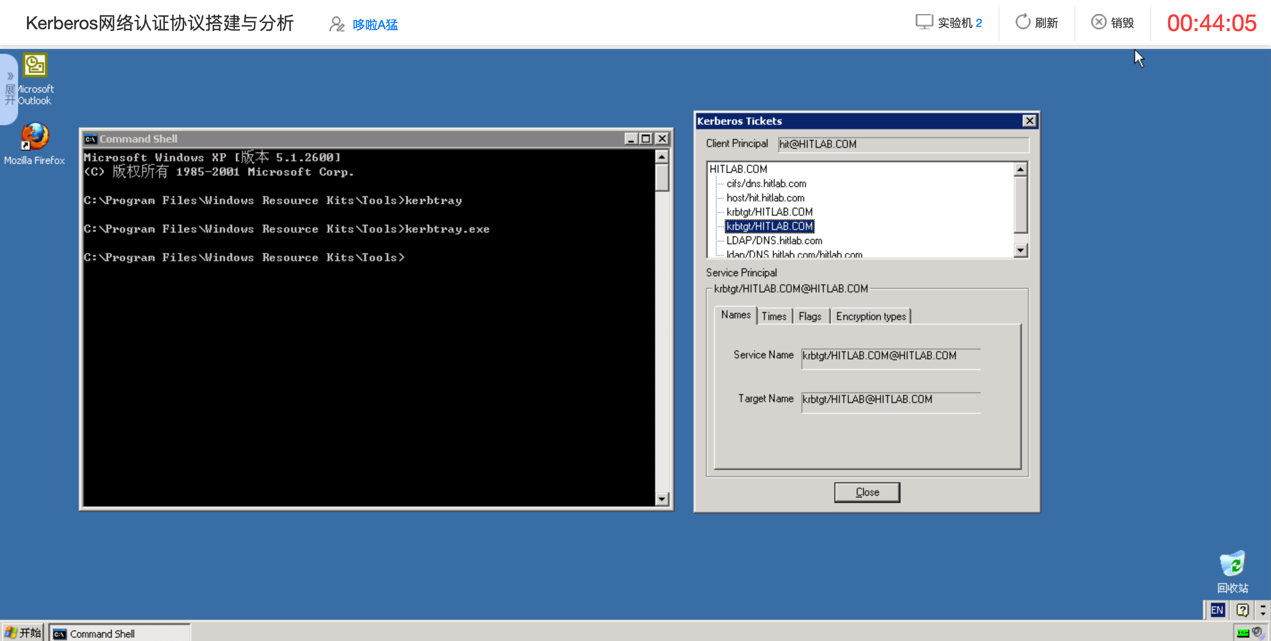


图 20在WindowsXP查看票据

在Windows Server 2003，也就是域控制服务器上，的“Active Directory 用户和计算机”中找到对应的域计算机，右键选择“属性”，也可以查看注册了的票据和计算机。

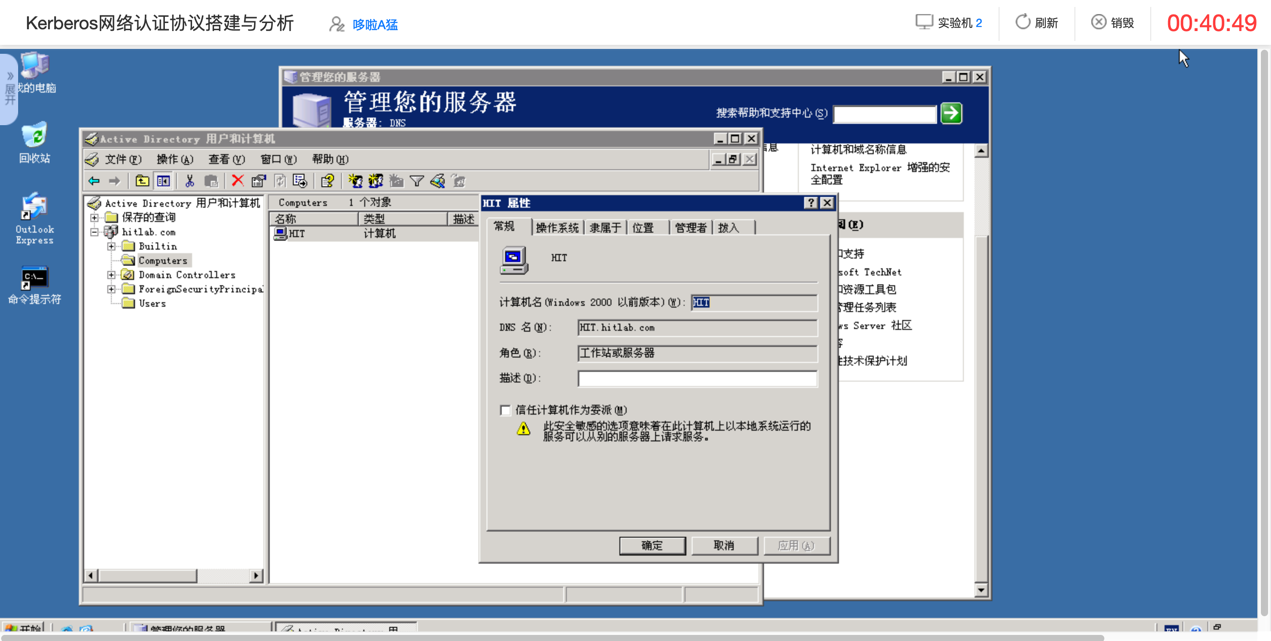


图 21查看HIT用户属性

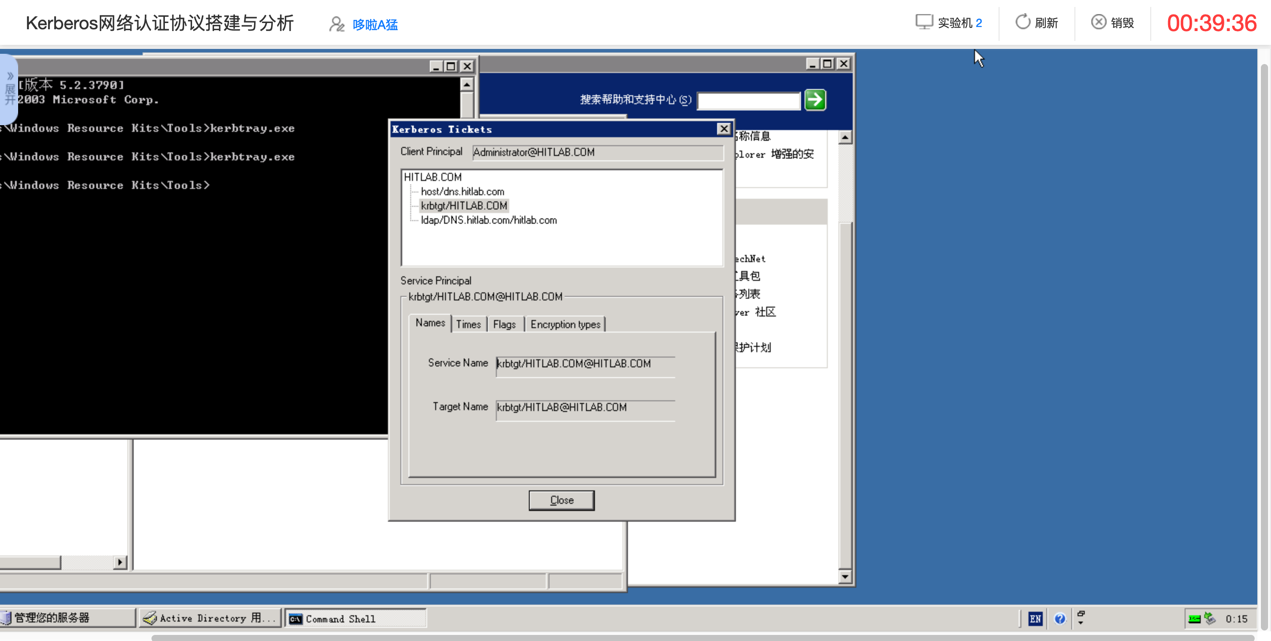


图 22查看票据名称

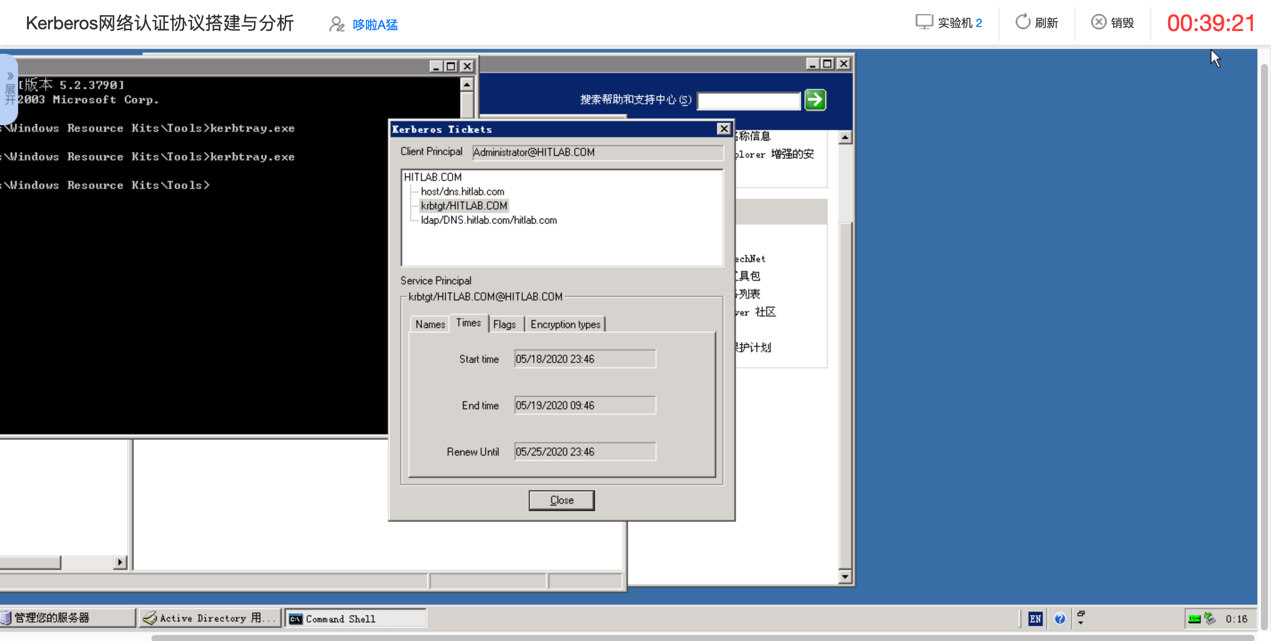


图 23查看票据有效期

五、实验结果总结

**实验结果分析**

在实现Windows Server 2003系统的域和DNS服务器的搭建后，我们可以利用Kerberos协议原理让Windows Server 2003实验机与Windows XP实验机实现认证。利用Kerbtray工具，我们可以在查看实验中获得的票据的相关属性，如服务器/客户端的名称、使用时限，如此次实验中获得的票据服务器的名称为krbtgt/HITLAB.com@HITLAB.com，有效时间为10小时。

**思考题目**

1. 更改Kerberos策略，如何能兼顾安全性和票据的有效期？

Kerberos策略用于域用户账户，用于确定与Kerberos相关的设置，例如票证的有效期限和强制执行。但Kerberos策略只能应用于域中的计算机中。要设置Kerberos策略，可在“默认域安全设置”窗口中，依次选择“Windows设置”→“安全设置”→“账户策略”→“Kerberos 策略”选项。它包含：强制执行用户登录限制、服务票证最长寿命、用户票证最长寿命、用户票证续订最长寿命和计算机时钟同步的最大容差。

“用户票证最长使用期限”策略设置确定可以使用用户的票证授予票证的最长时间 (以小时为单位)。当用户的票证授予票证过期时, 必须请求新帐户, 或者必须续订现有帐户。如果将“用户票证最长使用寿命”的值配置得过高, 用户可能无法在其登录时间之外访问网络资源。此外, 已禁用帐户的用户可能会继续访问具有在帐户禁用之前颁发的有效用户票证的网络服务。如果将此值配置得太低, 则对 KDC 的票证请求可能会影响 KDC 的性能, 并提供 DoS 攻击的机会。

“用户票证续订最长寿命”策略设置确定可以续订用户票证授权票证的时间段 (以天为单位)。如果用户票证续订设置的最长寿命值过高, 用户可以续订非常旧的用户票证。

安全性和票据的有限期是一定程度上存在矛盾的。为了兼顾安全性和票据的有效期，我们可以适当调整“用户票证最长寿命”和“用户票证续订设置的最长寿命”，如将“用户票证设置的最长寿命”设置为10小时，将“用户票证续订最长寿命”设置配置为“7 天”。

1. 分析Kerberos认证协议的局限性。

Kerberos协议本身并不能完全解决网络安全性问题，它是建立在一些假定之上的，只有在满足这些假定的环境中它才能正常运行。

（1）不能对拒绝服务(Denial of Service)攻击进行防护。Kerberos不能解决拒绝服务攻击，在该协议的很多环节中，攻击者都可以阻断正常的认证步骤。这类攻击只能由管理员和用户来检测和解决。

（2）主体必须保证他们的私钥的安全。如果一个入侵者通过某种方法窃取了主体的私钥，他就能冒充身份。

（3）Kerberos无法应付口令猜测攻击。如果一个用户选择了弱口令，那么攻击者就有可能成功地用口令字典破解掉，继而获得那些由源自于用户口令加密的所有消息。

（4）网络上每个主机的时钟必须是松散同步的。这种同步可以减少应用服务器进行重放攻击检测时所记录的数据。松散程度可以以一个服务器为准进行配置。时钟同步协议必须保证自身的安全，才能保证时钟在网上同步。

（5）主体的标识不能频繁地循环使用。由于访问控制的典型模式是使用访问控制列表(ACLs)来对主体进行授权。如果一个旧的ACL还保存着已被删除主体的入口，那么攻击者可以重新使用这些被删除的用户标识，就会获得旧ACL中所说明的访问权限。

**体会与心得**

通过此次实验，我了解了Windows Server 2003系统的域和DNS服务器的搭建，学会了Kerberos网络认证协议搭建方式。之前对于Kerberos协议的理解仍在纸面上，但是实验后我对于协议有了更深的理解，实践让我的认识更加深刻。

不过实验的指导书和视频存在一定的差异，希望以后可以让指导书和视频更加统一。