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： | 翟健宏 |
| 学生姓名： | 郭茁宁 |
| 组 号： | A48 |
| 实验日期： | 2020.5.18 |
| 实验地点： |  |
| 实验成绩： |  |

实验报告撰写要求

实验操作是教学过程中理论联系实际的重要环节，而实验报告的撰写又是知识系统化的吸收和升华过程，因此，实验报告应该体现完整性、规范性、正确性、有效性。现将实验报告撰写的有关内容说明如下：

1、 实验报告模板为电子版。

2、 下载统一的实验报告模板，学生自行完成撰写和打印。报告的首页包含本次实验的一般信息：

*  组 号：例如：2-5 表示第二班第5组。
*  实验日期：例如：05-10-06 表示本次实验日期。(年-月-日)……
*  实验编号：例如：No.1 表示第一个实验。
*  实验时间：例如：2学时 表示本次实验所用的时间。

实验报告正文部分，从六个方面（目的、内容、步骤等）反映本次实验的要点、要求以及完成过程等情况。模板已为实验报告正文设定统一格式，学生只需在相应项内填充即可。续页不再需要包含首页中的实验一般信息。

3、 实验报告正文部分具体要求如下：

一、实验目的

本次实验所涉及并要求掌握的知识点。

二、实验环境

实验所使用的设备名称及规格，网络管理工具简介、版本等。

三、实验内容与实验要求

实验内容、原理分析及具体实验要求。

四、实验过程与分析

根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。

详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。

五、实验结果总结

对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

六、附录

一、实验目的

*本次实验所涉及并要求掌握的知识点。*

1）掌握利用 Kerberos 网络认证协议搭建方法；

2）掌握 WindowsServer2003 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

*实验所使用的设备名称及规格，网络管理工具简介、版本等。*

域服务器：WindowsServer2003

客户机：WindowsXP

所用到的工具 WindowsServer 2003 ResourceKitTools

三、实验内容与实验要求

*实验内容、原理分析及具体实验要求。*

1）Kerberos 协议在 Windows 中的集成 WindowsServer2003 中的ActiveDirectory 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：KerberosV5、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。 ActiveDirectory 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。ActiveDirectory 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 KerberosV5。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，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

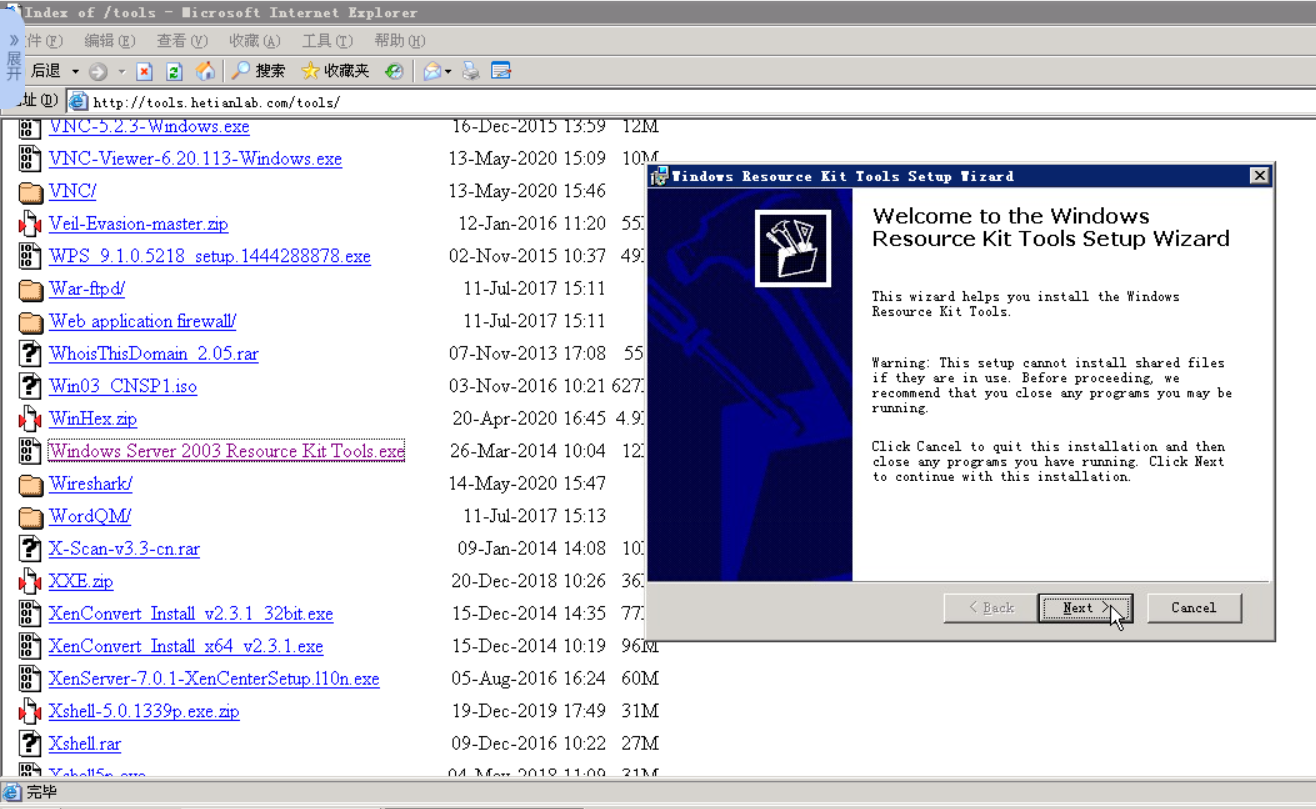
按实验指导书完成相应操作，撰写实验报告

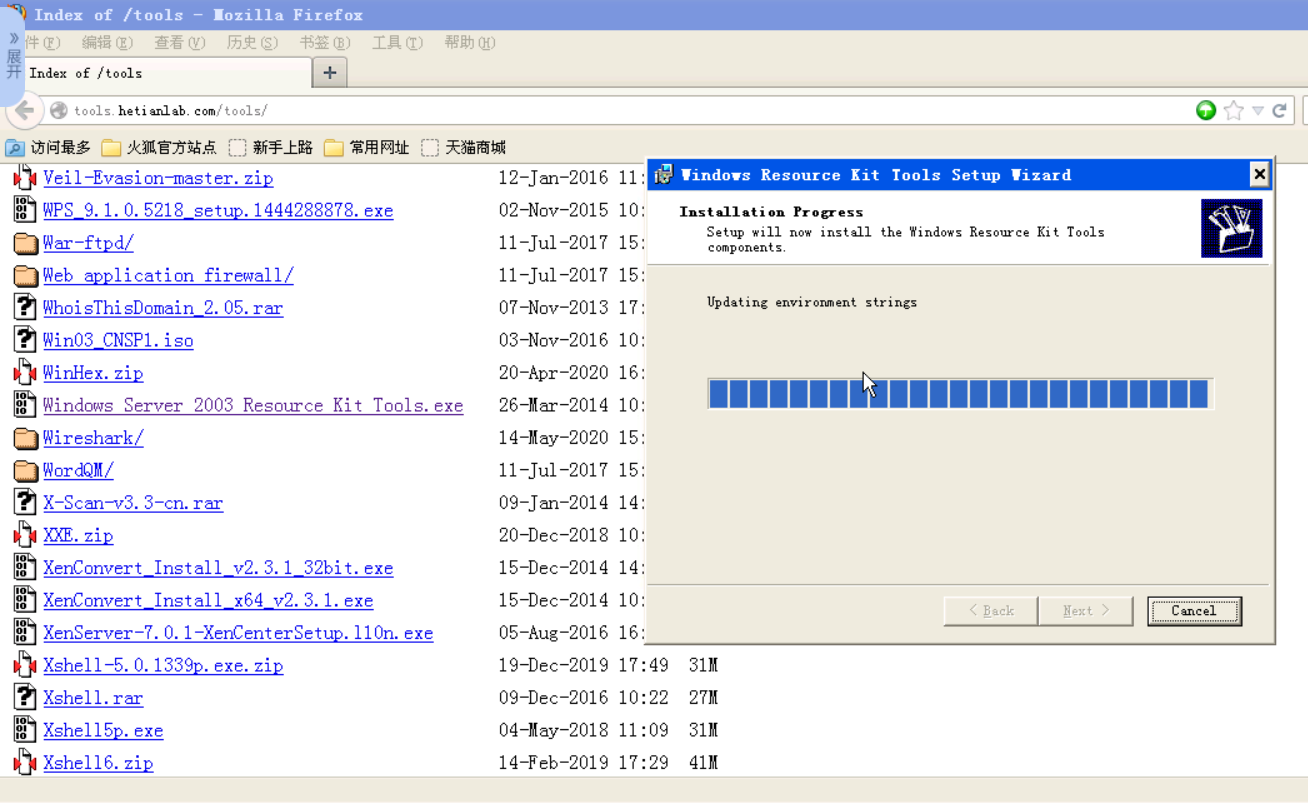
四、实验过程与分析

*根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。*

*详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。*

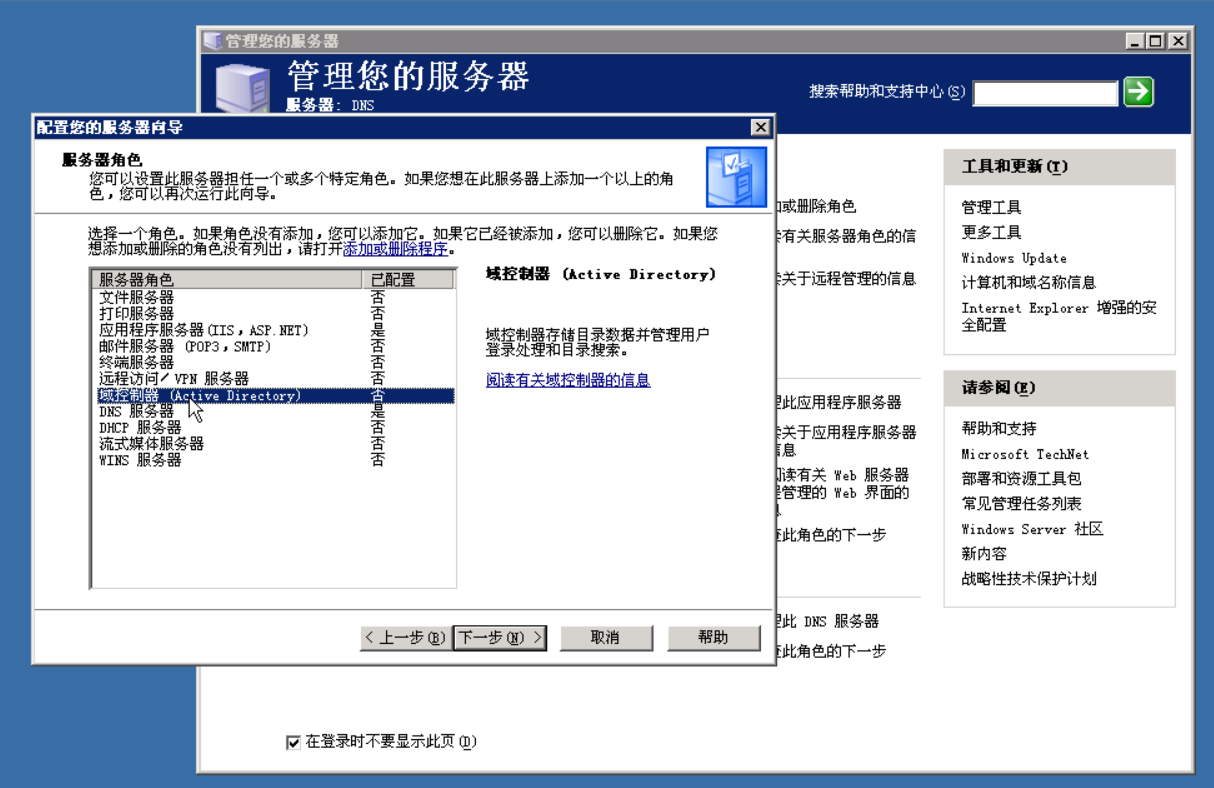
访问<http://tools.hetianlab.com/tools>，找到Windows Server 2003 Resource Kit Tools，在两台机器上都安装好 Windows Server 2003 Resource Kit Tools 下载好安装文件之后，安装，一直点“Next”就可以。





在Windows2003实验机上安装域控服务器：

切换到 Windows2003 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”

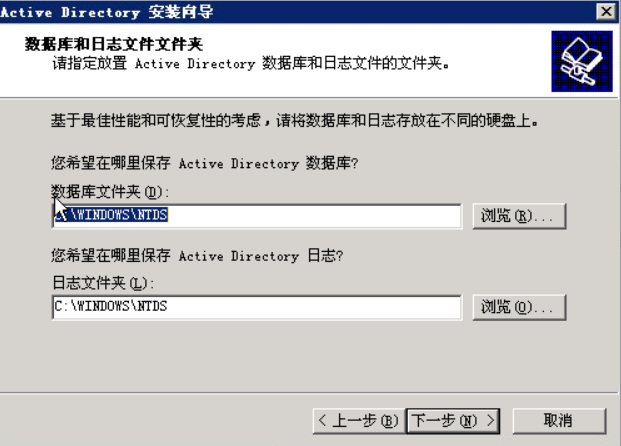


点击“下一步”，选择“域控制器（ActiveDirectory）”，然后点“下一步”

然后点“下一步”，在弹出的“ActiveDirectory 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”，选择“在新林中的域”之后点“下一步”，在“新域的 DNS 全名”输入框中输入域名称。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，并不是卡住了。

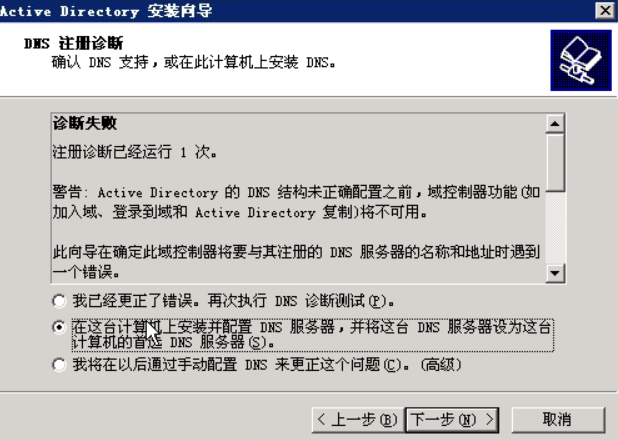


在“域 NetBIOS 名”这里保持默认不做修改，点“下一步”，在设置“数据库和日志文件夹”界面设置好数据库和日志存放文件夹，可以 保持默认，也可以自定义其他文件夹，然后点“下一步”

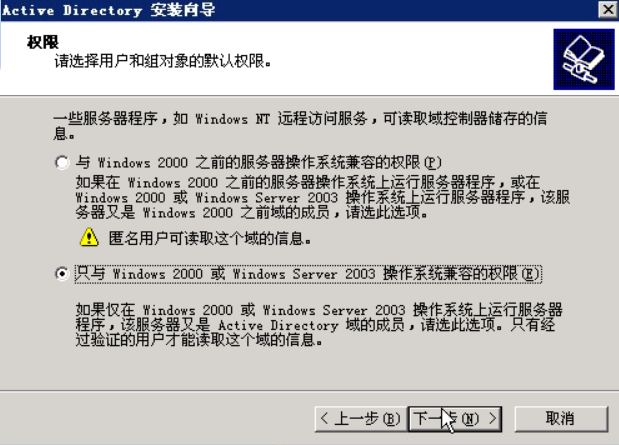


设置“共享的系统卷 ”，可以保持默认，也可以自定义，设置好之后点“下一步”

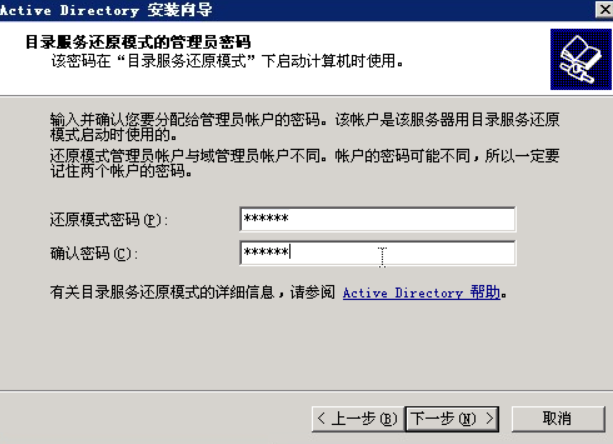
在“DNS 注册诊断”设置处选择“在这台计算机上安装并配置 DNS 服务 器....”，然后点“下一步”



在“权限”设置里面选择“只与 Windows2000 或 WindowServer2003 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”



在“摘要”界面确定设置无误之后，点“下一步”，如果要修改设置，可以 点“上一步”返回修改。



系统开始安装“ActiveDirectory”服务，等待完成



选择“立即重启计算机



然后等待重启完成，重启完成之后，会提示“此服务器现在是域控制器”，点“完成”，至此域 控制器安装完成



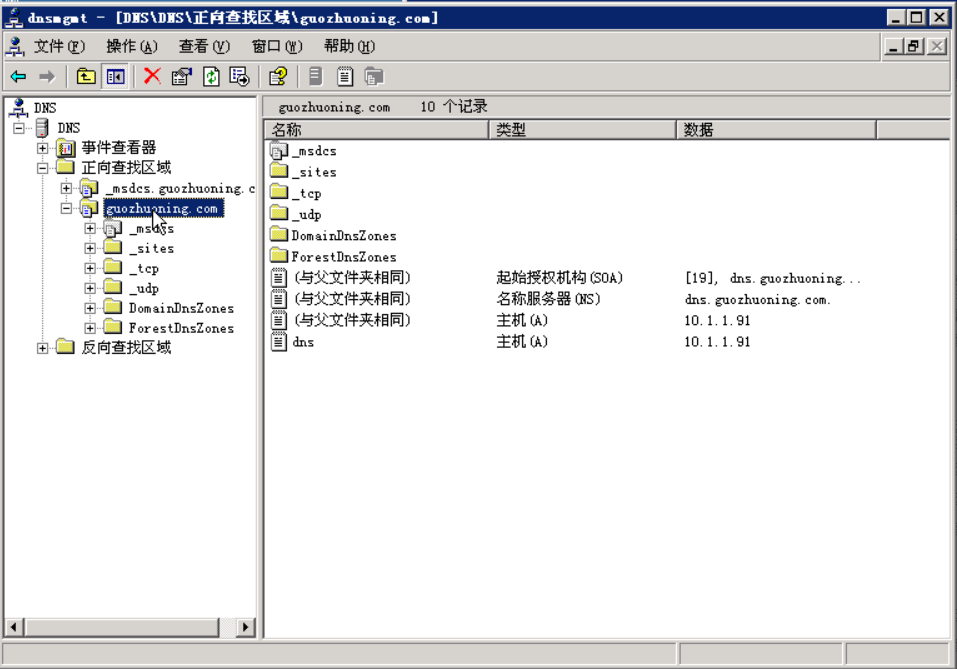
重启后，连接实验机。

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”

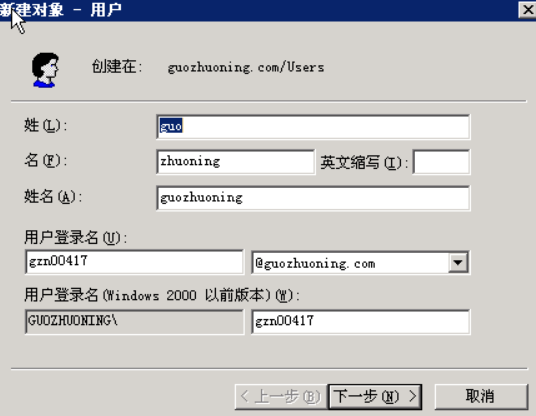
检查正向查找区域的域名配置是否正常



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 ActiveDirectory 中的用户和计算机”

在弹出的“ActiveDirectory 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”

填写必要的账号信息，然后点“下一步”



设置符合要求的密码，然后点“下一步”

设置好密码之后，点“下一步”，然后点“完成”，即可完成域用户的创建



实验步骤三

5、将 WindowsXP 加入域环境

切换到 Windowsxp 实验机进行配置

设置 Windows xp 电脑的首选 DNS 服务器为 Windows 2003 的 ip 地址。

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”

进入“网络标识向导”设置中，点“下一步”

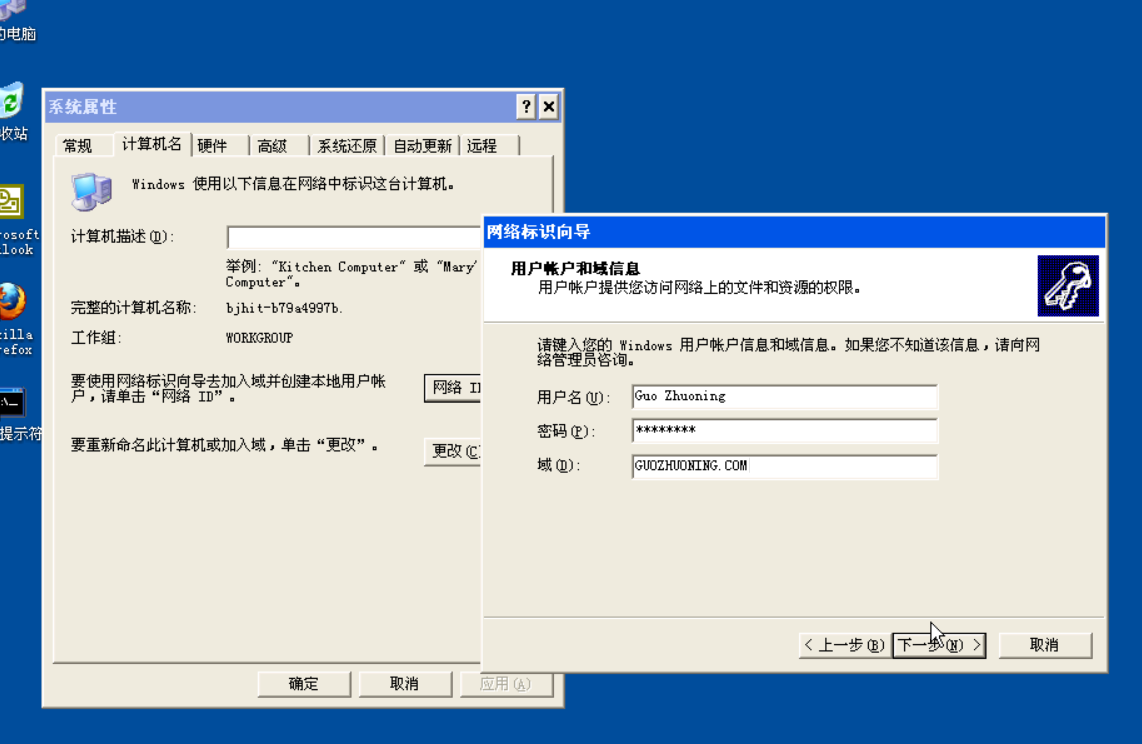
选择“公司使用带域的网络”，然后点“下一步”

输入域账号和密码以及域名，然后点“下一步”

输入计算机名和域信息，然后点“下一步”

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。

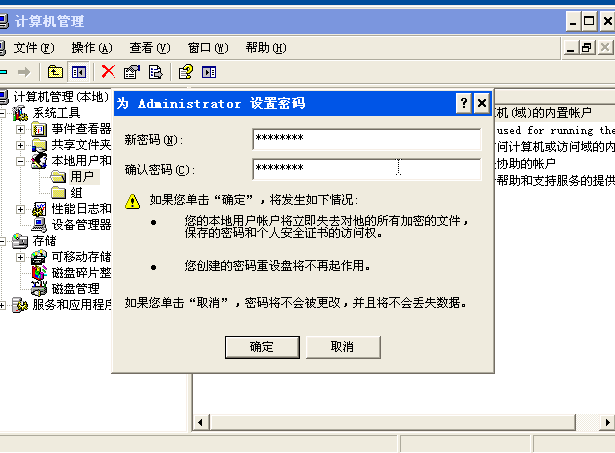
加入域向导完成，点“完成”



提示需要重启计算机，点“确定”

提示需要重启计算机，点“确定”

先不要点确定，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”



然后设置一个密码即可

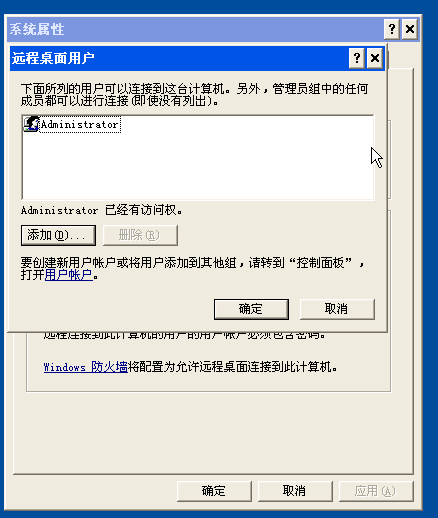
然后回到“系统属性”设置那里，点“确定”，然后在弹出的是否重启计算 机询问框点“是”

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（默认只有管理员权限才有连接远程桌面的权限，普通用户没办法连接到远程 桌面） 右键“我的电脑”-->“属性”-->"远程"--"选择远程用户"

点“添加”



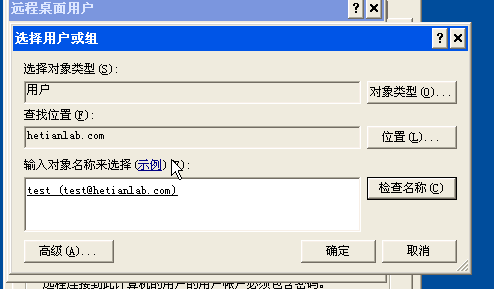
点击“位置”

根据提示输入域账号信息，然后点确定



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”



一直点确定即可

这样，远程桌面权限就添加好了

6、登录到域环境

在 Windowsxp 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

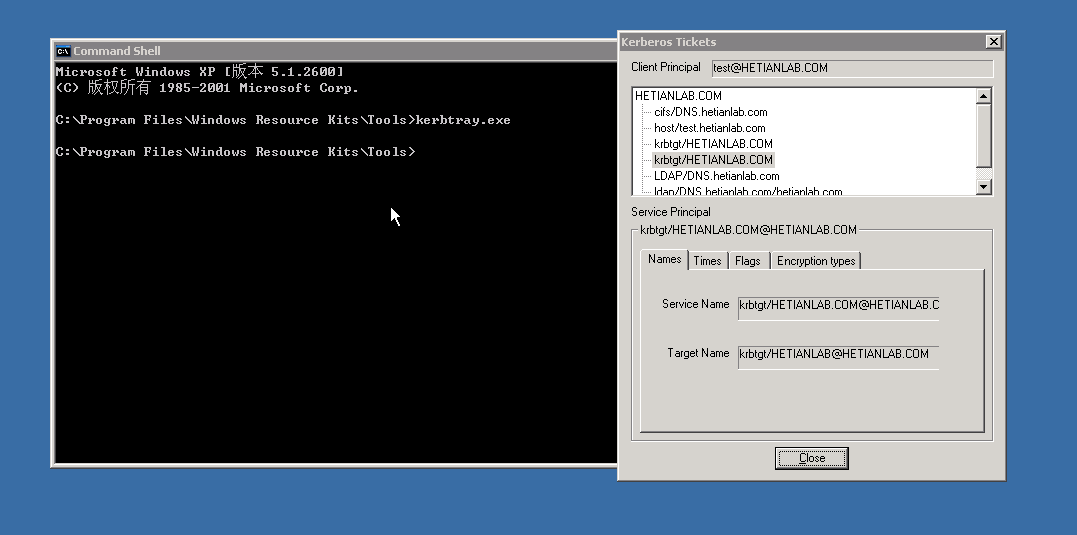
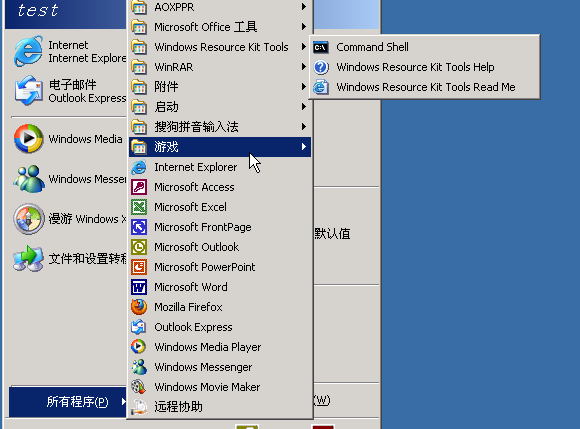
然后输入相关的域账号信息和选择登录到相应的域，然后点确定即可登录成

功

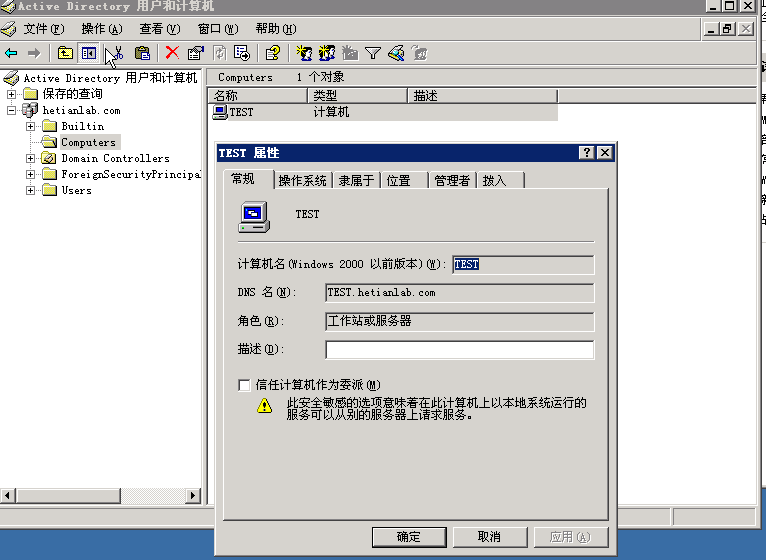


7、查看票据

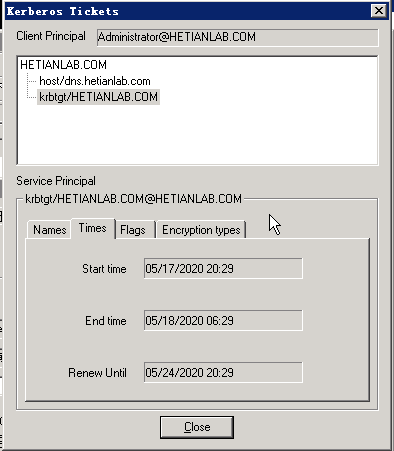
依 次 点 击 “ 开 始 ” --> “ 所 有 程 序 ” -->"Windows Resource Kit Tools"-->"CommandShell"，然后输入“kerbtray.exe”回车，在桌面右下角的任务 栏就会出现一个绿色小票的图标，双击就能看到票据。



在 Windows2003，也就是域控制服务器上，的“ActiveDirectory 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。



使用“WindowsResourceKitTools”查看票据信息



故障和问题分析、解决方法：

问题1：在虚拟机连不上网，找不到报告中提到的exe文件

分析、解决方法：因为虚拟机本身是连不上外网的，该文件要我们自己搜索，经过同学提醒，输入域名地址成功找到文件，并安装成功。

问题2：设置密码由于复杂性要求没有通过

分析、解决方法：我按照了要求步骤，将策略设置禁用，但是依然没有通过，因为我没有返回上一步。返回上一步再重新点击即可顺利通过。

问题3：做到一半突然卡死了

分析、解决方法：没有解决掉，不知道出了什么问题，即使点击了刷新也是没反应，只好重新开始。

五、实验结果总结

*对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。*

1. 写出实验完成过程。

见上文

1. 更改Kerberos策略，如何能兼顾安全性和票据的有效期？

采用改进的防密码猜测字典攻击和报文重放攻击的Kerberos单点登录协议。使用动态密钥作为client和AS之间的共享密钥。动态密钥每次认证时都不相同。考虑到安全性，动态密钥由一个本地的离线key，上一次的加密密钥kd和一个由client和AS在上一次认证过程中协商的随机数rmd通过单向函数运算得到。

3）分析Kerberos认证协议的局限性。

1.失败于单点：它需要中心服务器的持续响应。当Kerberos服务宕机时，没有人可以连接到服务器。这个缺陷可以通过使用复合Kerberos服务器和缺陷认证机制弥补。

2.Kerberos要求参与通信的主机的时钟同步。票据具有一定有效期，因此，如果主机的时钟与Kerberos服务器的时钟不同步，认证会失败。默认设置要求时钟的时间相差不超过10分钟。在实践中，通常用网络时间协议后台程序来保持主机时钟同步。

3.管理协议并没有标准化，在服务器实现工具中有一些差别。

4.因为所有用户使用的密钥都存储于中心服务器中，危及服务器的安全的行为将危及所有用户的密钥。

5.一个危险客户机将危及用户密码。