**基于IPSec的远程桌面连接**

概述：在企业里，网络管理员管理服务器的方法之一就是在自己的机器上，以远程桌面的形式登录到服务器上，为了完成实验，设计如下拓扑：



**1、一般的实现方法**

1）在DC上启用远程桌面（右击桌面上的“我的电脑”---属性，选择“远程”，在下面的远程桌面下，打勾）

注意：启用远程桌面后，服务器端就会开启3389端口进行侦听，客户端能够连接上，还要解决以下问题：

a,该用户是管理员或加入到Remote Desktop Users组，并且密码非空

b,如果服务器端有防火墙，要放行3389端口

说明：对于以上2点，需要提示若是域环境下，服务器是DC,若连接用户是属于普通用户，仅将其加入Remote Desktop Users组还是不够的，需再修改默认域控制器策略（假设demo是我的测试账户）



设置完成后通过gpupdate /force使组策略立即生效。

顺便查看一下服务器侦听情况：



2）客户端使用mstsc /v:172.16.10.1可以完成连接，要求输入相应的用户名和密码，验证通过登录成功



以上是一般的连接方式

**2、实现安全的远程桌面连接**

 通过前面的实例我们已经实现了远程桌面的连接，可以用来管理服务器了，各位试想，他人只要用相应的扫描端口的软件就能知道你的机器开启了那些端口，这样一来，也就知道了你的机器开启的远程桌面功能，再使用相应的方法获取你的管理员的密码，也就可以对你的机器进行远程桌面的连接了，怎么可以实现安全的连接呢？

基于以上想法：我们从以下3点出发：

a,将3389端口改掉，如6689

b,对通信过程加密

c,对远程桌面连接及客户机进行身份验证

对于后2者，使用IPSEC来实现

a)改端口

简单操作步骤：打开"开始→运行"，输入"regedit"，打开注册表，进入以下路径：[HKEY\_LOCAL\_MACHINE\SYSTEM\ CurrentControlSet\Control\Terminal Server\ Wds\rdpwd\Tds\tcp]，看见PortNamber值了吗？其默认值是3389（改为十进制显示），修改成所希望的端口，例6689。

 再打开[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp]，将PortNumber的值（默认是3389）修改成端口6689

关闭注册表编辑器后重启计算机，即可生效。
通过如下命令再次查看：



会发现在6689侦听，此时我们用客户机验证一下，先使用默认端口3389（mstsc /v:172.16.10.1）



改用6689端口：





连接成功！

b)对通信过程进行加密

c)对用户进行身份验证

使用IPSec时各位需要注意，多数情况下我们需要在两边都要做，在我们这个案例中，要求两边所选择的加密方式和身份验证要一致。具体操作如下所示：

1、服务器端配置IPSec

开始菜单---运行---mmc，然后添加“IP安全策略管理”控制台组件(连接本地计算机)



然后创建IP安全策略



向导，下一步，命名ip策略



不激活默认规则



选编辑属性，完成

在这里我们看到**任何一条规则包含三要素：筛选器、筛选器操作、身份验证方法。**

首先新建IP筛选器，并不使用向导，并编辑属性



接着指定协议



确定，选定改筛选器，切换到“筛选器操作”标签，点“添加”-新建筛选器操作



确定，点“常规”标签，命名“协商”



确定，选中“协商”筛选器操作，切换到“身份验证方法”



这里有三种验证方法：
**Kerberos(需要AD支持）**
**证书（需要CA）**
**预共享密钥。**
我们这里是域环境，所以我们可以选择Kerberos这种方式，如果你不是域环境，可以选择下面两种，至于证书，你需要在企业里搭建CA，预共享密钥比较简单，取个密钥就可以了

完成后，需要指派该策略，使其生效！



此时，可以现在客户端上测试连接，发现连接失败。



2、**客户端配置IPSec:**其实操作如法炮制，**注意要和服务器选择的加密和身份验证方法一样**。**最后也把它启用**，就OK了，需要注意的地方



ok，终于做完了，在客户端利用命令mstsc /v:n1:6689连接一下，OK，成功！



3、普通远程连接和安全连接的区别

这里使用windows server 2003 自带的网络监视器来抓包分析：

这幅图其实就是普通的连接，协议显示的是TCP，并用端口及内容看得很清楚！



下面是利用IPSec之后的连接，各位可以看到，协议显示的是ESP（加密的），内容等都看不到了



总结：这就是基于域的安全远程桌面连接。