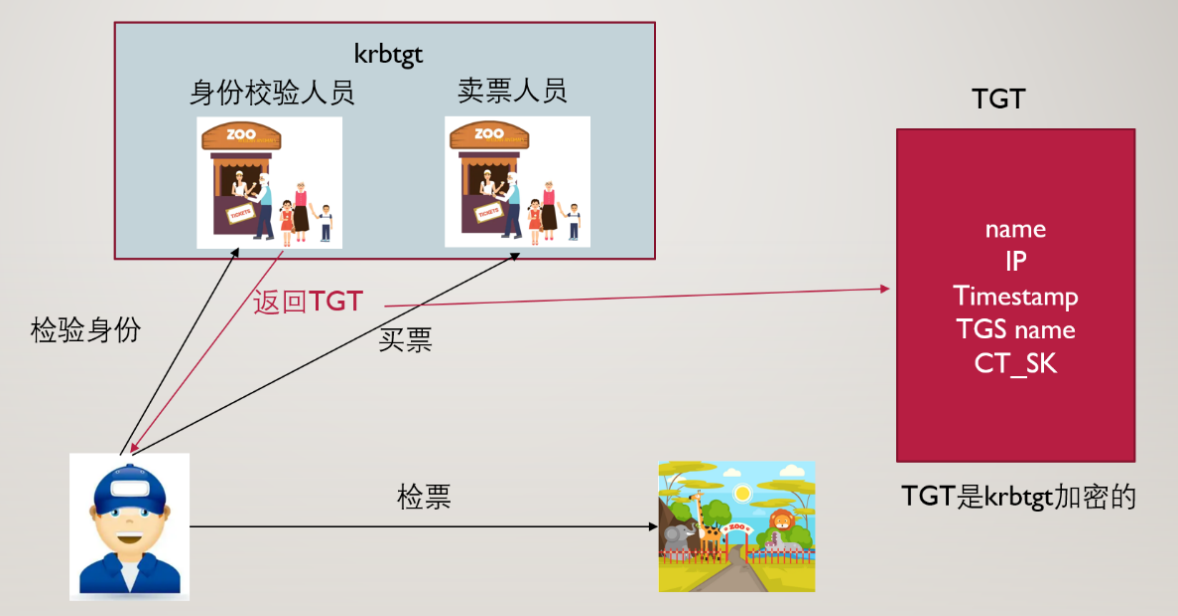
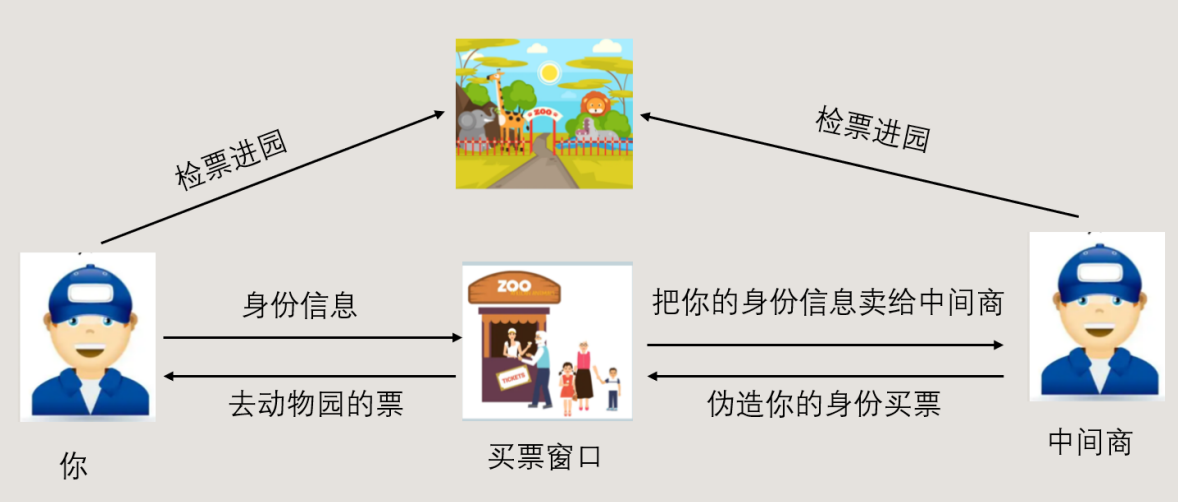
域内委派攻击概述

委派是什么

我们先看一下kerberos协议



我们要去买票，但是自己又不想去，我们就可以委托中间商，给我们买票，这个就是委派



域委派是指将域内用户的权限委派给服务账户，使得服务账号能够以用户的权限在域内展开活动。

委派是域中的一种安全设置，可以允许某个机器上的服务代表某个用户去执行某个操作，主要分为三种：

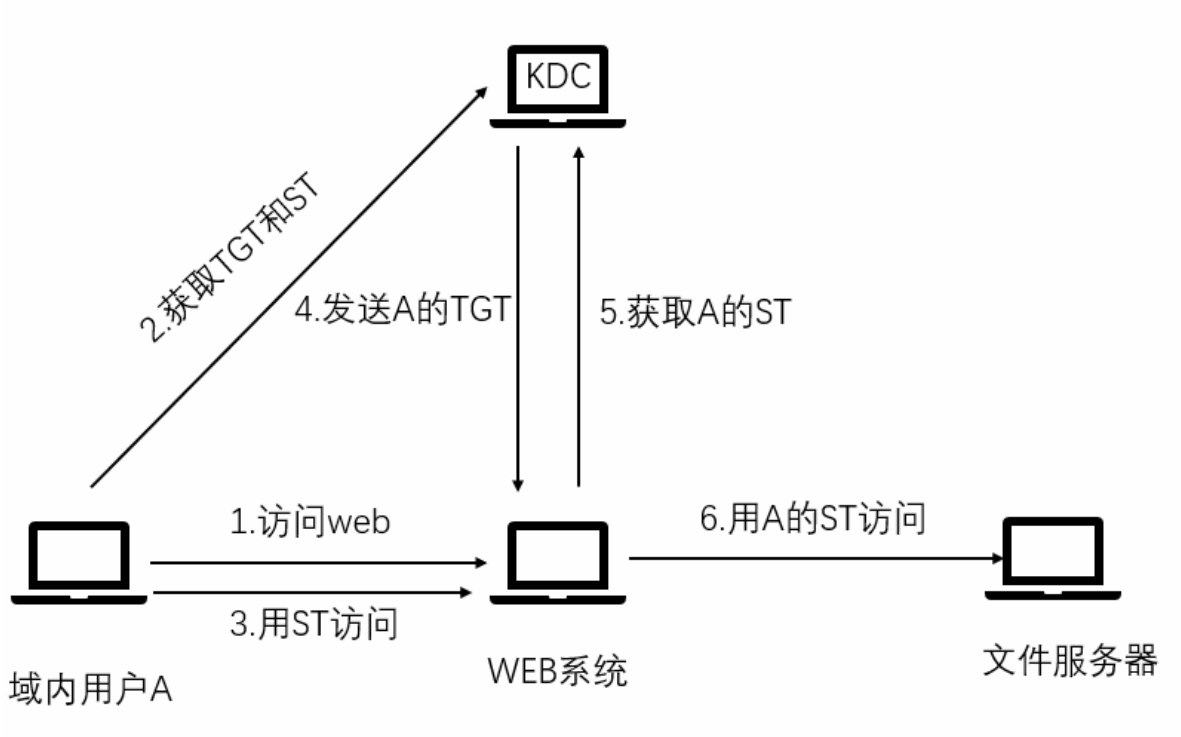
1、非约束性委派

2、约束性委派

3、基于资源的约束性委派

委派攻击的工作场景

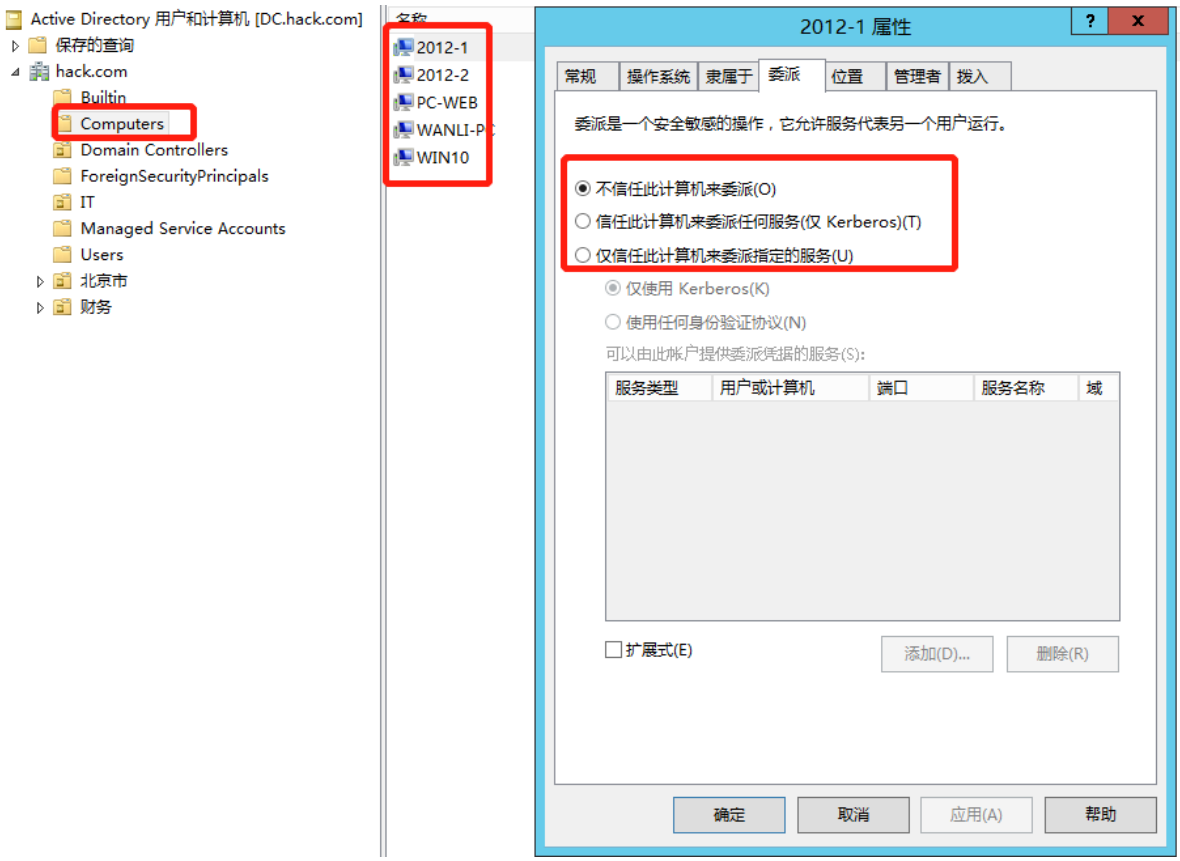
一个域内用户访问WEB服务，但是一些资源在文件服务上，这个时候就需要委派gongj



怎么设置委派

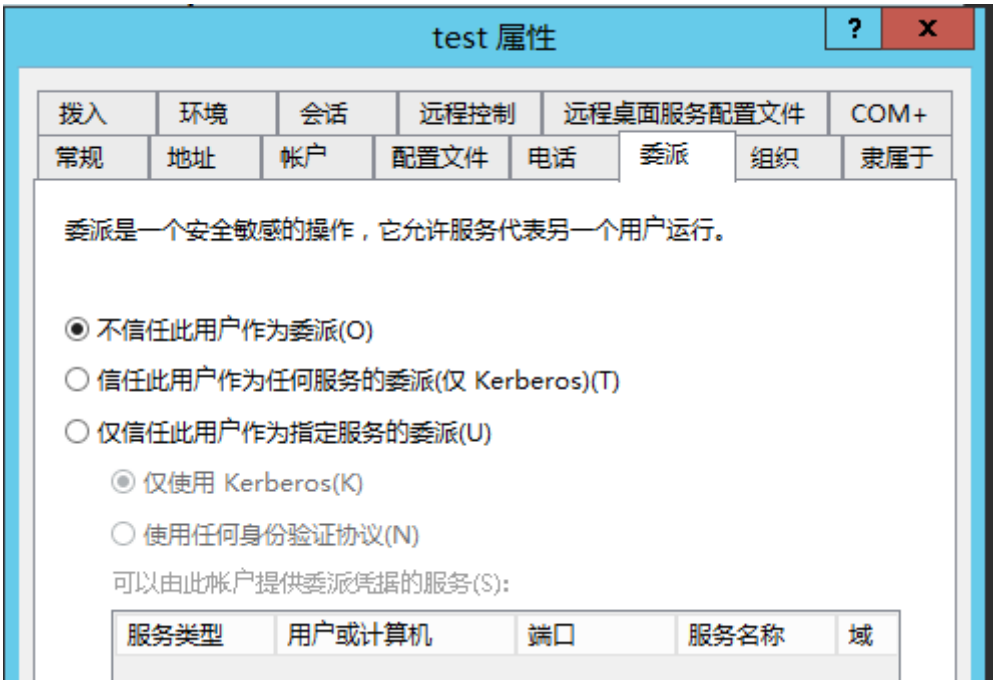
在域内只有主机账号和服务账号才有委派属性

主机账号：活动目录中的computers组内的计算机，也被称为机器账号。

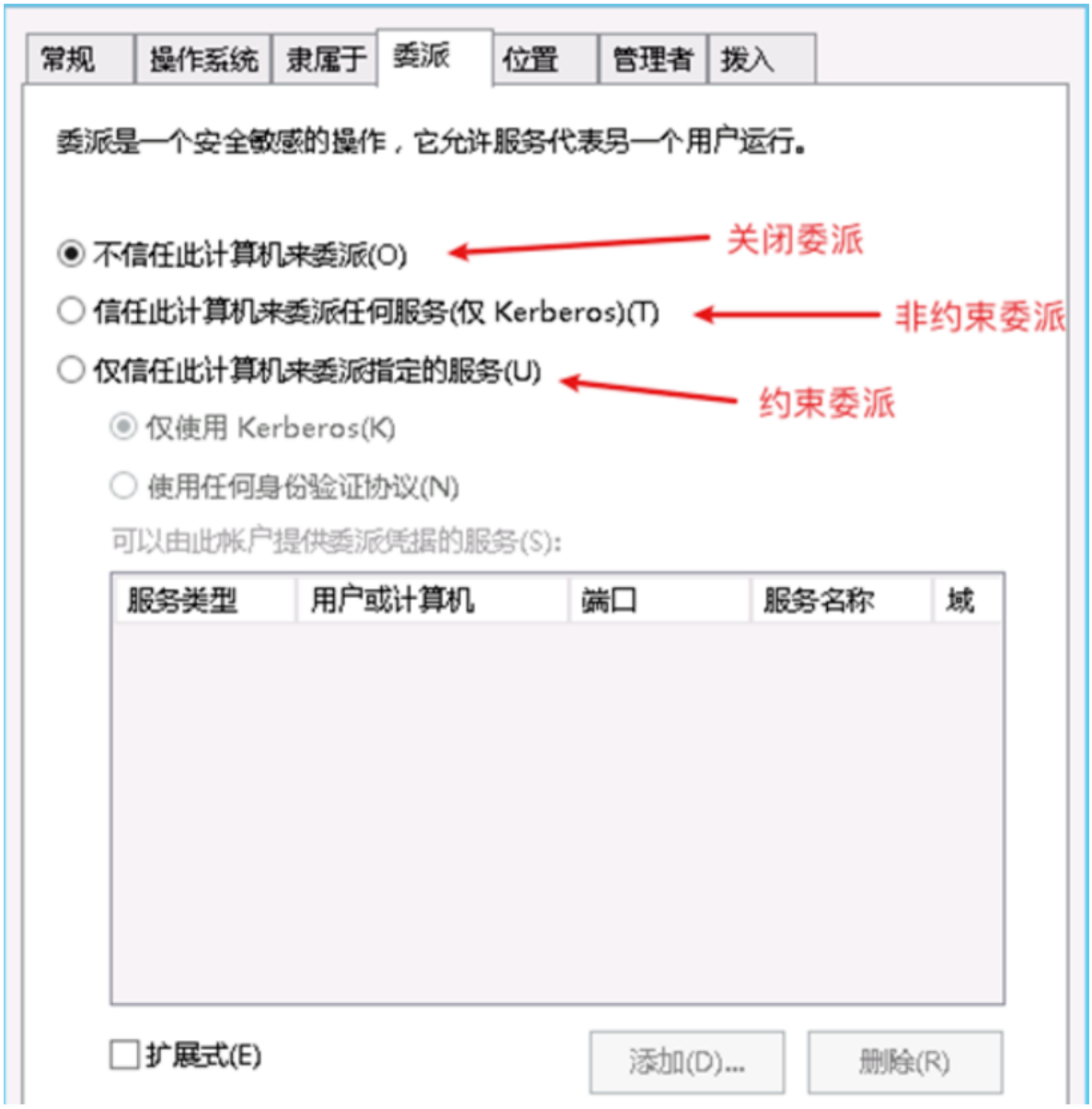


服务账号：域内用户的一种类型，是服务器运行服务时所用的账号，将服务运行起来加入域内，比如：SQLServer,MYSQL等；域用户通过注册SPN也能成为服务账号。

```
net user test123 Admin@123 /add /domain 创建一个普通用户
setspn -U -A priv/test test123  注册为服务账号
```



开启委派如图


常规
操作系统
隶属于
委派
位置
管理者
拨入
委派是一个安全敏感的操作，它允许服务代表另一个用户运行。
不信任此计算机来委派(O)
关闭委派
信任此计算机来委派任何服务(仅 Kerberos)(T)
非约束委派
仅信任此计算机来委派指定的服务(U)
约束委派
仅使用 Kerberos(K)
使用任何身份验证协议(N)
可以由此帐户提供委派凭据的服务(S):
服务类型
用户或计算机
端口
服务名称
域
扩展式(E)
添加(D)...
删除(R)