1．Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

认证过程具体如下：客户机向认证服务器（AS）发送请求，要求得到某服务器的证书，然后 AS 的响应包含这些用客户端密钥加密的证书。证书的构成为： 1) 服务器 “ticket” ； 2) 一个临时加密密钥（又称为会话密钥 “session key”） 。客户机将 ticket （包括用服务器密钥加密的客户机身份和一份会话密钥的拷贝）传送到服务器上。会话密钥可以（现已经由客户机和服务器共享）用来认证客户机或认证服务器，也可用来为通信双方以后的通讯提供加密服务，或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。

上述认证交换过程需要只读方式访问 Kerberos 数据库。但有时，数据库中的记录必须进行修改，如添加新的规则或改变规则密钥时。修改过程通过客户机和第三方 Kerberos 服务器（Kerberos 管理器 KADM）间的协议完成。有关管理协议在此不作介绍。另外也有一种协议用于维护多份 Kerberos 数据库的拷贝，这可以认为是执行过程中的细节问题，并且会不断改变以适应各种不同数据库技术。

Kerberos又指麻省理工学院为这个协议开发的一套计算机网络安全系统。系统设计上采用客户端/服务器结构与DES加密技术，并且能够进行相互认证，即客户端和服务器端均可对对方进行身份认证。可以用于防止窃听、防止replay攻击、保护数据完整性等场合，是一种应用对称密钥体制进行密钥管理的系统。Kerberos的扩展产品也使用公开密钥加密方法进行认证。

简要大概地说一下Kerberos是如何工作的：

1、假设你要在一台电脑上访问另一个服务器（你可以发送telnet或类似的登录请求）。你知道服务器要接受你的请求必须要有一张Kerberos的“入场券”。

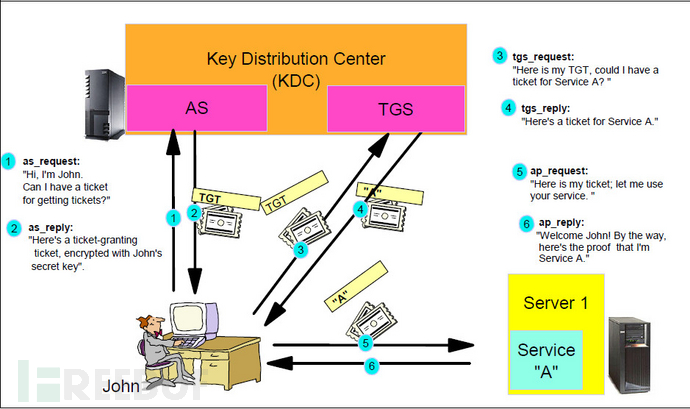
2、要得到这张入场券，你首先要向验证服务器（AS）请求验证。验证服务器会创建基于你的密码（从你的用户名而来）的一个“会话密钥”（就是一个加密密钥），并产生一个代表请求的服务的随机值。这个会话密钥就是“允许入场的入场券”。

3、然后，你把这张允许入场的入场券发到授权服务器（TGS）。TGS物理上可以和验证服务器是同一个服务器，只不过它现在执行的是另一个服务。TGS返回一张可以发送给请求服务的服务器的票据。

4、服务器或者拒绝这张票据，或者接受这张票据并执行服务。

5、因为你从TGS收到的这张票据是打上时间戳的，所以它允许你在某个特定时期内（一般是八小时）不用再验证就可以使用同一张票来发出附加的请求。使这张票拥有一个有限的有效期使其以后不太可能被其他人使用。

实际的过程要比刚才描述的复杂得多。用户过程也会根据具体执行有一些改变。



**通过对Kerberos的分析发现以下几点问题：**

1、密钥来源于用户密码；

2、密钥存储在内存中；

3、使用RC4加密算法的密钥没有进行加盐处理，NTLM哈希值即为RC4密钥；

4、KDC（密钥分配中心）使用的密钥来源于krbtgt用户密码，尽管该账户已被禁用，并且从未被使用；

5、krbtgt用户密码很少更改（只有当域功能级别改变时才有可能会更改），且更改后的旧密码仍然可用；

6、TGT票据使用krbtgt密钥进行加密，PAC数据使用krbtgt密钥进行进行签名，并且系统很少会验证PAC数据；

7、Kerberos在用户登录20分钟后才会验证用户账户

基于以上原因，攻击者可借助krbtgt密码绕过身份验证系统，获取管理员访问权限，进而执行一系列管理员操作（如创建用户，下载文件等），还可以根据密码为用户创建响应的密钥。

krbtgt帐号：

我想请教一下 krbtgt这个帐号主要是做什么的呢？如果删除会有什么影响？删除后如何恢复呢？

回答：我对您所提出的问题的理解是：

1.什么是Krbtgt账号？

2.Krbtgt账号的作用是什么？

3.Krbtgt账号是否可以被删除或重建？

关于您所提出的这些问题：

问：什么是Krbtgt账号？

答：Krbtgt账号是在新建一台域控制器时，由系统自动创建的，用于Kerberos验证的服务账号，同时，系统会随机分配一个密码给到Krbtgt账号。

问：Krbtgt账号的作用是什么？

答：我们知道，在Kerberos的验证过程中，有一个很重要的环节，就是生成Secret Key。而系统正是通过krbtgt账号的密码来生成Secret Key。您看到的文章来自活动目录seo http://adirectory.blog.com/category/active-directory/

问：Krbtgt账号是否可以被删除或重建？

答：由于这是系统服务账号，所以不能被删除，当您试图去删除的时候，系统会提示无法删除。

关于更详细的信息，您可以参考以下微软技术文档：

Authentication for Administrative Authority

http://technet.microsoft.com/en-us/library/cc750037.aspx

由于krbtgt账号是kerberos的服务账号，所以默认是无法删除的。在开始解决您所遇到的问题前，请您按下列步骤确认下该账号是否存在：

第一步：打开Active Directory Users and Computers

第二步：选择您的域名，例如lab.contoso.com，按右键选择“find”

第三步：输入krbtgt后点击“find now”

如果您能找到该账号，请同时确认该账号是否在Users OU里，由于系统服务账号如果被移动到别的OU的话，会对系统服务造成影响。