Kerberos简介

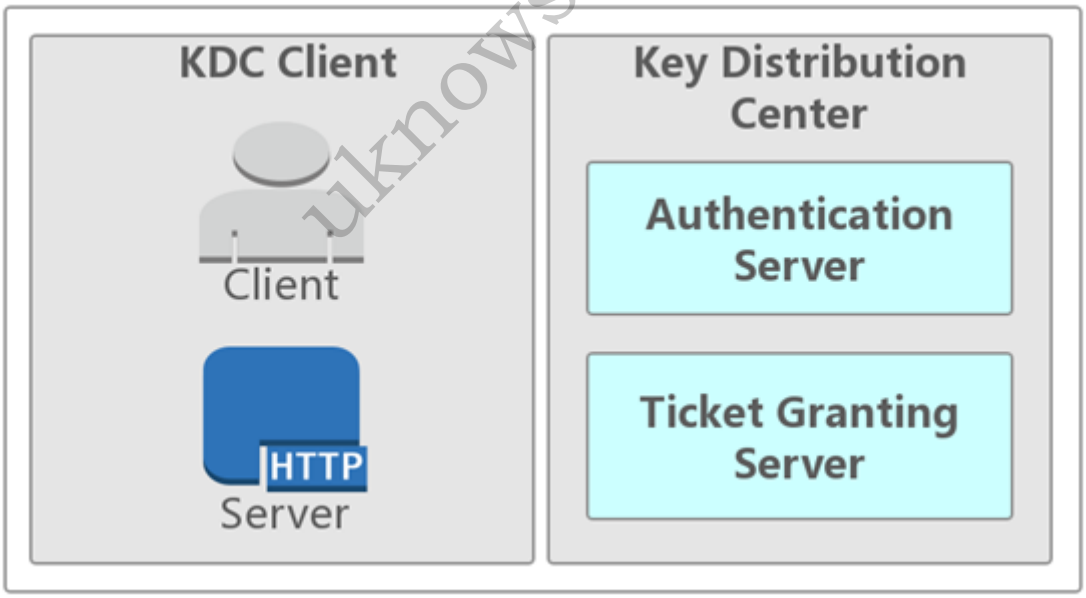
在Kerberos认证中，最主要的问题是如何证明“你是你”的问题，如当一个Client去访问Server服务器上的某服务时，Server如何判断Client是否有权限来访问自己主机上的服务，同时保证在这个过程中的通讯内容即使被拦截或篡改也不影响通讯的安全性，这正是Kerberos解决的问题。在域渗透过程中Kerberos协议的攻防也是很重要的存在。

Kerberos协议框架

在Kerberos协议中主要是有三个角色的存在：

- 访问服务的Client
- 提供服务的Server
- KDC（Key Distribution Center）密钥分发中心

  其中KDC服务默认会安装在一个域的域控中，而Client和Server为域内的用户或者是服务，如HTTP服务，SQL服务。在Kerberos中Client是否有权限访问Server端的服务由KDC发放的票据来决定。

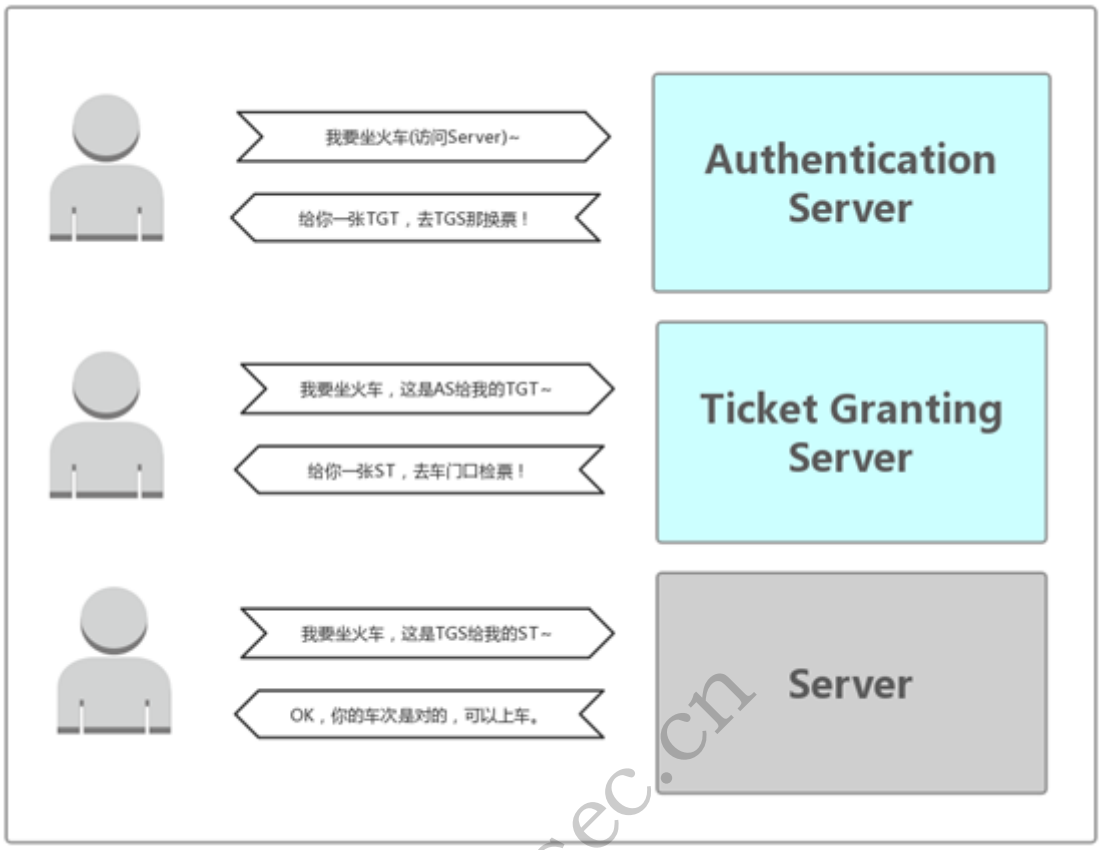


如果把Kerberos中的票据类比为一张火车票，那么Client端就是乘客，Server端就是火车，而KDC就是就是车站的认证系统。如果Client端的票据是合法的（由你本人身份证购买并由你本人持有）同时有访问Server端服务的权限（车票对应车次正确）那么你才能上车。当然和火车票不一样的是Kerberos中有存在两张票，而火车票从头到尾只有一张。

由上图中可以看到KDC又分为两个部分：

Authentication Server： AS的作用就是验证Client端的身份（确定你是身份证上的本人），验证通过就会给一张TGT（Ticket Granting Ticket）票给Client。

Ticket Granting Server： TGS的作用是通过AS发送给Client的票（TGT）换取访问Server端的票（上车的票ST）。ST（ServiceTicket）也有资料称为TGS Ticket，为了和TGS区分，在这里就用ST来说明。



KDC服务框架中包含一个KRBTGT账户，它是在创建域时系统自动创建的一个账号，可以暂时理解为他就是一个无法登陆的账号。

```
选定 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net user

\\OWA2010SP3 的用户帐户

-------------------------------------------------------------------------------
0day                     Administrator            alan
antivirus                backup                   boss
dev                      ftpuser                  Guest
hr                       itadmin                  jack
jerry                    klion                    klionsec
krbtgt                   lowser                   mary
RedTeamBox               Redteamer                secretary
SM_32dfa537f3d34e8db     SM_a53ca95cbbc2400a8     SM_b9293dd4eb974c39a
SM_cabbcb1fa25c4786a     sqladmin                 sqlsvr
tadmin                   test                     webadmin
websvr
命令成功完成。
```

Kerberos认证

流程当Client想要访问Server上的某个服务时，需要先向AS证明自己的身份，然后通过AS发放的TGT向Server发起认证请求，这个过程分为三块：

The Authentication Service Exchange：Client与AS的交互

The Ticket-Granting Service (TGS) Exchange：Client与TGS的交互

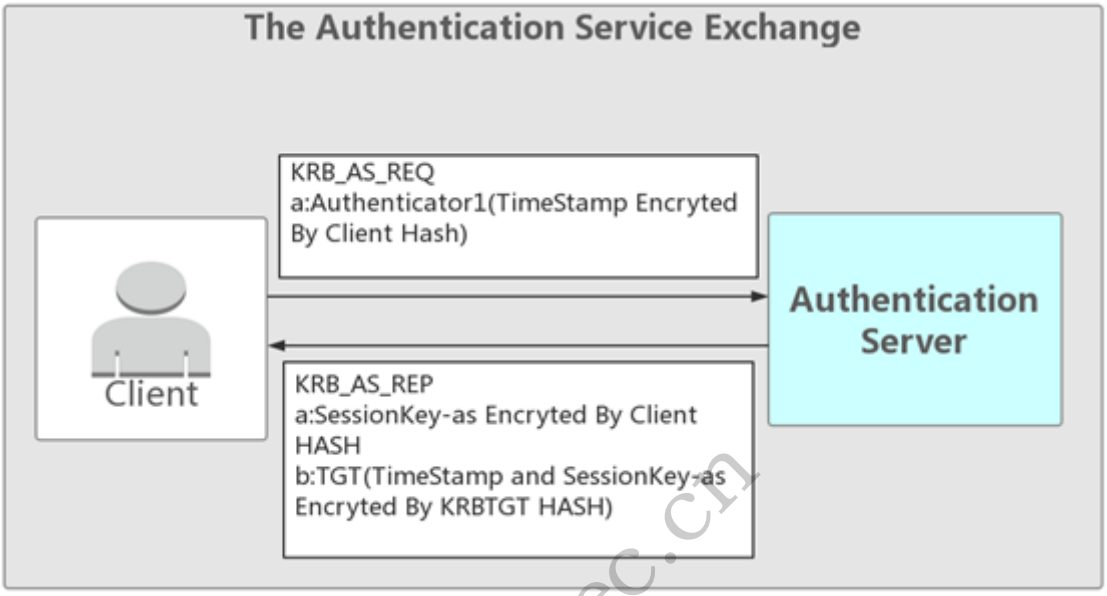
The Client/Server Authentication Exchange：Client与Server的交互

(1)TheAuthentication Service Exchange

KRB_AS_REQ

Client->AS：发送 Authenticator1(Client 密码加密 TimeStamp)

第一步 Client 先向 KDC 的 AS 发送 Authenticator1，内容为通过 Client 密码 Hash 加密的时间戳、ClientID、网络地址、加密类型等内容。



KRB_AS_REP

AS-> Client：发送 Client 密码加密的 sessionkey-as 和票据 TGT(KRBTGT HASH 加密的 sessionkey-as 和 TimeStamp)

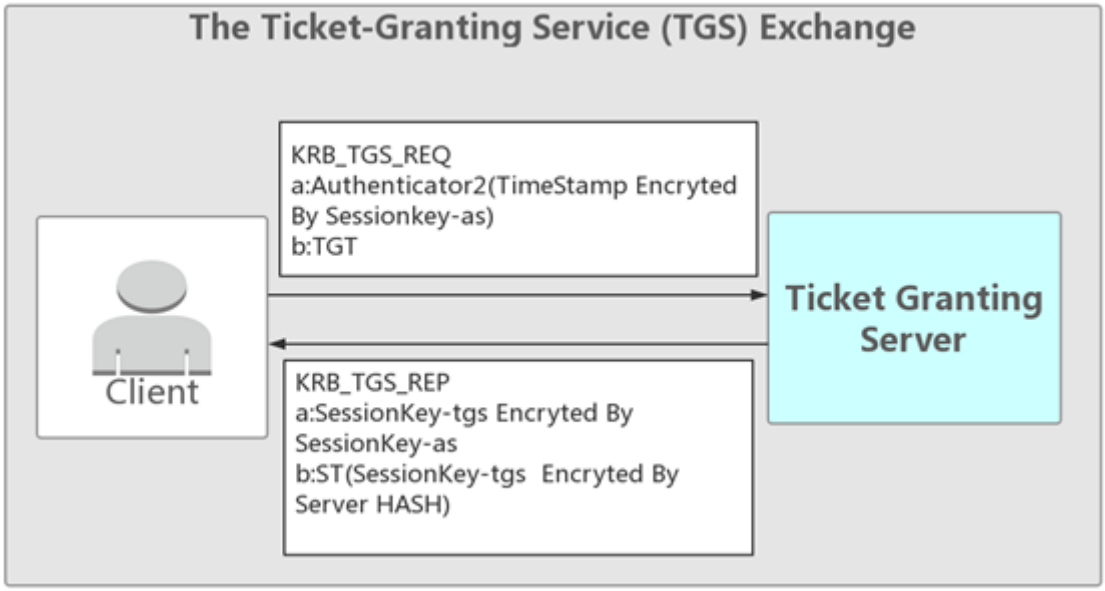
在 KDC 中存储了域中所有用户的密码 HASH，当 AS 接收到 Client 的请求之后会根据 KDC 中存储的密码来解密，解密成功并且验证信息。验证成功后返回给 Client 由 Client 密码 HASH 加密的 sessionkey-as 和 TGT（由 KRBTGT HASH 加密的 sessionkey-as 和 TimeStamp 等信息）。

(2)TheTicket-Granting Service (TGS) Exchange

KRB_TGS_REQ

Client ->TGS 发送 Authenticator2 (sessionkey-as 加密 TimeStamp) 和票据 TGT(KRBTGT HASH 加密的 sessionkey-as 和 TimeStamp)

Client 接收到了加密后的 Sessionkey-as 和 TGT 之后，用自身密码解密得到 Sessionkey-as，TGT 是由 KDC 密码加密，Client 无法解密。这时 Client 再用 Sessionkey-as 加密 TimeStamp 和 TGT 一起发送给 KDC 中的 TGS（TicketGranting Server）票据授权服务器换取能够访问 Server 的票据。



KRB_TGS_REP

TGS-> Client 发送 密文 1(sessionkey-as 加密 sessionkey-tgs) 和 票据 ST(Server 密码 HASH 加密 sessionkey-tgs)

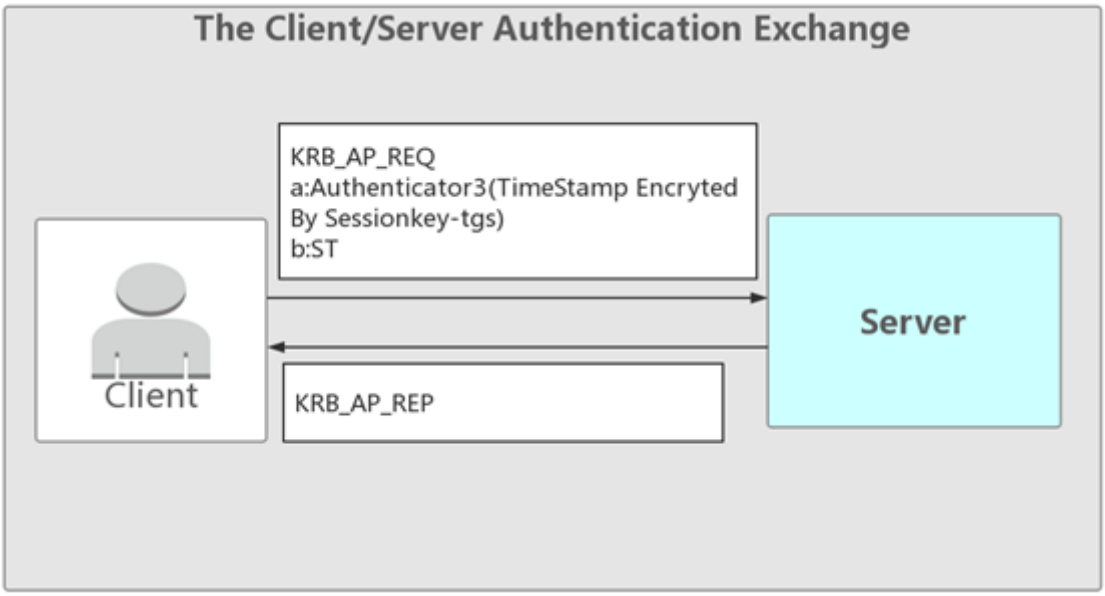
TGS 收到 Client 发送过来的 TGT 和 Sessionkey-as 加密的 TimeStamp 之后，首先会检查自身是否存在 Client 所请求的服务。如果服务存在，则用 KRBTGT 密码解密 TGT。一般情况下 TGS 会检查 TGT 中的时间戳查看 TGT 是否过期，且原始地址是否和 TGT 中保存的地址相同。验证成功之后将用 sessionkey-as 加密的 sessionkey-tgs 和 Server 密码 HASH 加密的 Sessionkey-tgs 发送给 Client。

(3)TheClient/Server Authentication Exchange

KRB_AP_REQ

Client ->Server 发送 Authenticator3(sessionkey-tgs 加密 TimeStamp) 和票据 ST(Server 密码 HASH 加密 sessionkey-tgs)

Client 收到 sessionkey-as 加密的 sessionkey-tgs 和 Server 密码 HASH 加密的 sessionkey-tgs 之后用 sessionkey-as 解密得到 sessionkey-tgs，然后把 sessionkey-tgs 加密的 TimeStamp 和 ST 一起发送给 Server。



KRB_AP_REP

Server-> Client

server 通过自己的密码解密 ST，得到 sessionkey-tgs, 再用 sessionkey-tgs 解密 Authenticator3 得到 TimeStamp，验证正确返回验证成功。