

**Kerberos**

**整理编写者：于康**

1. **Kerberos 简介：**

**Internet上的很多协议本身并不提供安全属性。怀有恶意的hackers用”sniff”等工具嗅探口令是非常普遍的事，因此在网络上不经加密就传送口令是很不安全的。许多网站使用防火墙来解决安全问题，但是，防火墙都是假定攻击都来自外部，但事实常常不是这样，许多攻击事件都是内部人员所为，而且防火墙还有一个缺点就是会对正常的用户使用Internet一定限制。**

**由MIT开发的Kerberos协议就是针对这样的网络安全问题的。Kerberos协议使用了强密码，以使client能通过一个不安全的Internet连接向server证明他的身份。在client和server用Kerberos证明了各自的身份后，还可以对数据加密从而保证数据的保密性和完整性。Kerberos是一个分布式的认证服务，它允许一个进程(或客户)代表一个主体(或用户)向验证者证明他的身份，而不需要通过网络发送那些有可能会被攻击者用来假冒主体身份的数据。Kerberos还提供了可选的client和server之间数据通信的完整性和保密性。**

1. **Kerberos基本概念：**

* **Principal（安全个体）**

**被认证的个体， 有一个名字(name)和口令(password)**

* **KDC(Key distribution center)**

**是一个网络服务，提供ticket和临时的会话密钥**

* **Ticket**

**一个记录，客户可以用它来向服务器证明自己的身份，其中包括客户的标识、会 话密钥、时间戳，以及其他一些信息。**

* **Authenticator**

**一个记录，其中包含一些最近产生的信息，产生这些信息需要用到客户和服务器 之间共享的会话密钥。**

* **Credentials**

**一个ticket加上一个秘密的会话密钥**

1. **Kerberos应用环境假设：**
2. **Kerberos协议的基本应用环境为，在一个分布式的client/server体系机构中采用一个或多个Kerberos服务器提供一个鉴别服务。Client想请求应用服务器server上的资源，首先client向Kerberos认证服务器请求一张身份证明，然后到将身份证明交给server进行验证，server在验证通过后，即为client分配请求的资源。**
3. **Kerberos协议本身并不是无限安全的，而且也不能自动提供安全，它建立在一些假定之上的，只有在满足这些假定的环境中它才能正常运行。**
4. **不存在拒绝服务器(Denial of server)攻击。Kerberos不能解决拒绝服务器(Denial of server)攻击，在该协议的很多环节中，攻击者都可以阻断正常的认证步骤。这类攻击只能由管理员和用户来检测和解决。**
5. **主体必须保证他们私钥的安全。如果一个入侵者通过某种方式窃取了主体的私钥，他就能冒充身份。**
6. **Kerberos无法应付口令猜测(Password guessing)攻击。如果一个用户选择了弱口令，那么攻击就有可能成功的用口令字典破解，继而获得那些源自于用户口令加密(由用户口令形成的加密链)的所有消息。**
7. **网络上每个主机的时钟必须是松散同步的(loosely synchronized)。这种同步可以减少应用服务器进行重放攻击检测时所有记录的数据。松散程度可以以一个服务器为准进行配置。时钟同步协议必须保证自身的安全，才能保证时钟在网上同步。**
8. **主体的标识不能频繁循环使用。由于访问控制的典型模式是使用访问控制列表(ACL)来对主体进行授权。如果一个旧的ACL还保存着已被删除主体的入口，那么攻击者可以重新使用这些被删除的用户标识，就会获得旧ACL中所说明的访问权限。**
9. **Kerberos的优缺点：**

**优点：**

1. **Kerberos将认证从不安全的工作站移到了集中的认证服务器上，为开放网络中的 两个主体提供身份认证， 并通过会话密钥对通信进行加密。**
2. **对于大型的系统可以采用层次化的区域 (realm) 进行管理。**
3. **Kerbero:系统对用户的口令进行处理之后作为用户的私钥， 从而避免了用户的口 令在网络上显示传输， 使得窃听者难以在网络上取得相应的口令信息。**
4. **Kerberos对用户是透明性的， 用户在使用过程中， 仅在登录时要求输入命令， 与平常的操作完全一样。**

**缺点：**

1. **AS 在传输用户与 TGS 间的会话密钥时是以用户密钥加密的， 而用户密钥是由用户口令生成的， 因此可能受到口令猜测的攻击。**
2. **Kerberos使用了时间戮， 因此存在时间同步问题。**
3. **要将 Kerberos 用于某一应用系统， 则该系统的客户端和服务器端软件都要作一定的修改。**
4. **随用户数增加，密钥管理较复杂。 Kerberos 拥有每个用户口令的散列值，AS与TGS 负责用户间通信密钥的分配。当n个用户想同时通信时，需要n\*( n-l)/2个密钥。**

**以上只是简单介绍**