链滴

SSH 登录细节

作者：changming

原文链接：https://ld246.com/article/1471061205958

来源网站：链滴

在使用openssh的过程中，整理了知识细节，回过头来发现，基础的原理是非常重要的不要被各种工具的GUI所蒙蔽，比如putty和CRT。以下设定情景是客户端使用的ubuntu，工具使用openssh，服务端是linux服务器。ssh比telnet协议安全，所以对于管理员来说大多数用ssh来登录管理服务器，先来看清楚一次登录过程是怎样的。
1. 客户端发起登录请求
2. 服务器端返回自己的公共密钥给客户
3. 客户端接受后，使用服务器端的公共密钥给密码进行加密，然后再次发送服务器端
4. 服务器端接收到后，在使用自己的私有密钥进行解密，解密成功并且密码正确，客户端即登录成功
客户端登录命令如下：
$ ssh user@host   # user 为服务端的用户名，host为服务端的ip，或者别名
$ passwd:
输入密码，如果正确，即可登录成功。以上为口令登录，但是对于管理员来说，次输入密码是很繁琐的一件事，为了避免每次输入相同的密码，我们来介绍另外一种登录方式，公共钥登录，具体过程如下：

1. 客户端首先将自己的公共密钥发送给服器端存储起来
2. 客户端发起登录请求，服务器端接受到后，发送一段随机的符串给客户端
3. 客户端接受该随机字符串后使用自己的私有密钥进行加密，后发送给服务端
4. 服务端接收后，使用存储的客户端公共密钥进行解密，解成功，客户端即可登录，就无须输入密码

以上过程中，有几个具体作，如下：
1. 如果发送客户端自己的公共密钥给服务器端
$ ssh-copy-id user@host
2. 发成功后，服务器端会将客户端的公共密钥保存在user主目录下的.ssh/下，文件名称为authorized_key中，如果客户端没有公共密钥，使用如下命令生成即可：
$ ssh-keygen
生成后有2个文件，位于~/.ssh/下，id_rsa.pub 为公共密钥 id_rsa 为私有密钥。

另外，在你很久没有登录某台服务器后，有天再次登录后发现无法登录，提示有可能受到 main-in-the-middle attack,需要你联系管理员，这种情是有可能服务器的公共密钥和你本机存储的该服务器上的公共密钥不同，使用信息提示提供的方法删该服务器对应的密钥，然后重新登录服务器即可，删除方法如下：
 ssh-keygen -f "~/.ssh/known_hosts" -R IP
i地址为服务器端地址，know_hosts文件中存储的即是客户端存储的服务器端公共密钥的记录，以上令是删除掉该IP对应的公共密钥的记录。know_hosts文件的位置和客户端公共密钥的位置相同。

以上就是在使用ssh协议登录时候需要了解的底层细节。