https://www.cnblogs.com/yyds/p/6992125.html

cnblogs.com/toulanboy/p/8706741.html

偷懒人首页联系管理

ssh 免密码登录 与 密钥公钥原理讲解

前言#

由于最近频繁需要登录几个服务器，每次登录都需要输入密码，故相对麻烦。

由于个人服务器用于实验，故对安全性要求不是很高，故想实现ssh免密登录。

通过阅读ssh 公钥私钥认证操作及原理以及ssh公钥登陆。成功实现了自己的需求。

下面来说下讲解公钥密钥的工作原理以及ssh免密登录的实现步骤。

公钥密钥原理概述#

在课程计算机基础中，我记得是学过公钥密钥的，公钥和密钥是同时生成的。

公钥用于加密，私钥用于解密。

公钥是很多人可以持有，而密钥只能自己持有。

在ssh中，只需公钥放在服务器A上，那么你就可以通过私钥登录服务器A。

当你连接已放置你公钥服务器A时，服务器A和客户端之间大概存在以下认证流程。

（以下认证流程来自博客：ssh 公钥私钥认证操作及原理）

为了说明方便，以下将使用这些符号。

Ac 客户端公钥

Bc 客户端密钥

As 服务器公钥

Bs 服务器密钥

认证过程分为两个步骤。在认证之前，客户端需要通过某种方法将公钥 Ac 登录到服务器上。

会话密钥(session key)生成

客户端请求连接服务器，服务器将 As 发送给客户端。

服务器生成会话ID(session id)，设为 p，发送给客户端。

客户端生成会话密钥(session key)，设为 q，并计算 r = p xor q。

客户端将 r 用 As 进行加密，结果发送给服务器。

服务器用 Bs 进行解密，获得 r。

服务器进行 r xor p 的运算，获得 q。

至此服务器和客户端都知道了会话密钥q，以后的传输都将被 q 加密。

认证

服务器生成随机数 x，并用 Ac 加密后生成结果 S(x)，发送给客户端

客户端使用 Bc 解密 S(x) 得到 x

客户端计算 q + x 的 md5 值 n(q+x)，q为上一步得到的会话密钥

服务器计算 q + x 的 md5 值 m(q+x)

客户端将 n(q+x) 发送给服务器

服务器比较 m(q+x) 和 n(q+x)，两者相同则认证成功

#

ssh免密登录实验步骤#

（实验环境：Ubuntu 17）

1. 若还没安装ssh服务的同学，请先安装。#

1

sudo apt-get install ssh

本文博客地址：http://www.cnblogs.com/toulanboy/#

2. 进入家目录下的.ssh文件夹#

（若没有该目录，请创建。）

1

cd ~/.ssh

#

3. 生成密钥对#

（中途会让你输入密钥对的密码，由于我们想免密，故按回车跳过即可。）

（假如设置了，后面通过私钥连接服务器时，则需要输入密钥对的密码。）

1

ssh-keygen -t rsa

4. 将客户端.ssh目录下的id\_rsa.pub复制到服务器A的家目录下#

（下面指令的115.115.115.115是服务器IP，lgq是你想登录服务器的用户名）

1

scp id\_rsa.pub lgq@115.115.115.115:~/

5. 在服务器A上，将客户端的id\_rsa.pub追加到服务器的ssh的认证列表中#

1

cat ~/id\_rsa.pub >> ~/.ssh/authorized\_keys

#

6. 客户端后面直接可以通过私钥免密登录了。#

1

ssh lgq@115.115.115.115

至此完毕。希望对你有帮助。

参考：ssh 公钥私钥认证操作及原理以及ssh公钥登陆。

作者：toulanboy

出处：https://www.cnblogs.com/toulanboy/p/8706741.html

版权：本作品采用「署名-非商业性使用-相同方式共享 4.0 国际」许可协议进行许可。

希望对你有用，么么哒~