SSH服务的基础知识

主讲教师：虞菊花

任务引入

QQ功能：远程桌面

Linux操作系统：**SSH**！

远程服务有益于：

- 远程服务器运维
- 远程办公

SSH的基本概念

SSH ： Secure Shell

- 一种安全通信协议，对传输的数据进行加密，实现安全的远程登录和网络服务。
- 基于非对称加密，即公开秘钥加密技术，保证数据不被破坏、泄露和篡改。
- 使用多种加密认证方式，解决身份认证问题，防止网络嗅探和IP欺骗。

SSH的基本概念

SSH协议版本：

- **SSH1** ： 与SSH2不兼容

  免费，采用DES、3DES、Blowfish和RC4等对称加密算法，对称加密算法的密钥是通过非对称加密算法（RSA）来完成交换，且使用循环冗余校验码（CRC）。

- **SSH2** ： 收费，避免了RSA的专利问题，并修补了CRC的缺陷，完善了对称加密算法。

- **openssh** ： 免费，同时支持SSH1及SSH2标准，现**广泛应用于Linux操作系统**中。

默认情况下，CentOS7已经安装openssh软件包。

SSH的基本概念

对称加密：客户端、服务器使用**同一个密钥**对数据加解密

如何安全保存密钥？？

非对称加密： 客户端、服务器都有**公钥**和**私钥**

- 公钥是可以被**公开**的，私钥必须被**安全存放**
- 客户端使用**服务器**的**公钥加密**数据，加密后的数据传输到服务器，**服务器**必须用自己的**私钥**才能**解密**
- 服务器使用**客户端**的**公钥加密**数据，加密后的数据传输到客户端，**客户端**必须用自己的**私钥**才能**解密**

SSH会话建立过程

0：服务器SSH服务正常，双方已建立TCP连接

客户端

1：客户端向服务器发送SSH连接请求

2：服务器发送自己的公钥给客户端

3：客户端校验和确认服务器公钥，
同时生成客户端自己的公钥和私钥，
并将客户端的公钥发送给服务器。

服务器

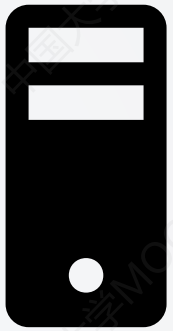
4：服务器校验和确认客户端公钥

客户端和服务器都拥有对方的公钥和自己的私钥，非对称加密信道建立，开始通信！

SSH会话建立过程

客户端

服务器



1. 服务器使用客户端公钥对传输数据进行加密，发送给客户端

客户端←服务器

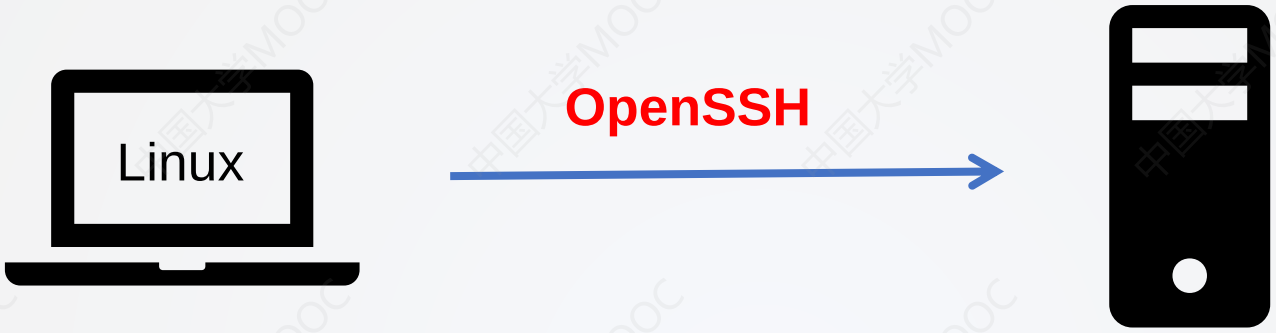
2. 客户端收到数据后，使用服务器的私钥解密后获得数据

客户端→服务器

1. 客户端使用服务器公钥对传输数据进行加密，发送给服务器

2. 服务器收到数据后，使用客户端的私钥解密后获得数据

SSH服务



- **ssh**：SSH客户端程序　　用于**登录远程主机**并在远程主机上执行命令
- **scp**：**远程文件复制**　　用于客户端与服务器之间安全地复制文件
- sftp：文件传输　　与FTP功能相似的文件传输程序
- ssh-keygen：管理密钥　　用于生成、管理和转换SSH认证密钥

SSH服务

使用SSH服务前确认：

- **sshd服务是否安装**
  - yum **install** openssh-server：安装ssh服务端
  - yum **install** openssh-clients：安装ssh客户端
- **sshd服务是否开启**
  - systemctl **start** sshd：开启sshd服务
  - systemctl **enable** sshd ： 使sshd服务开机自启动

感谢您的观看！