6. 远程登录

笔记本： 优秀笔记
创建时间： 2018/12/20 21:03 **更新时间：** 2018/12/21 15:55
作者： 306798658@qq.com

1. 字符型远程客户端工具介绍

Windows
Putty，开源免费，但是功能稍弱：下载地址：https://link.jianshu.com/?t=https%3A%2F%2Fwww.putty.orgl

SecureCRT：付费软件

Xshell（推荐）：界面友好，功能丰富，我们可以使用免费版，下载地址 `https://www.netsarang.com/download/down_form.html?code=622` （说明：`License` **type** 选择**"Home and** `school` **use"**）

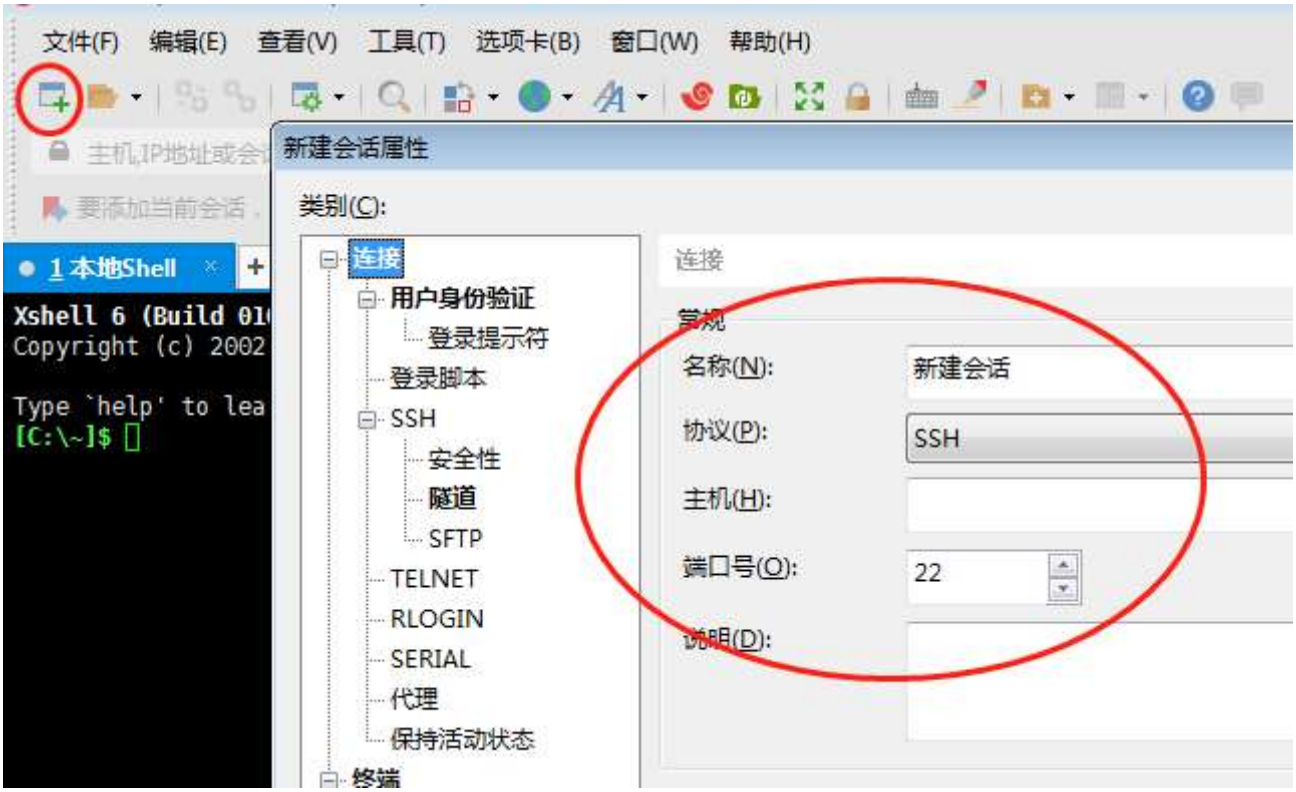
MacOS 或 Linux
MacOS 属于 UNIX-Like，直接通过‘终端’或‘iTerm’即可使用ssh客户端

Linux 可直接用命令行访问

2. Windows 远程访问方法

——仅举例 Xshell 的方法，其他工具大同小异

a. 新建连接



b. 填写基本链接信息如：命称、协议、主机、端口等


新建会话属性
类别(C):
连接
用户身份验证
登录提示符
登录脚本
SSH
安全性
隧道
SFTP
TELNET
RLOGIN
SERIAL
代理
保持活动状态
终端
键盘
VT 模式
高级
外观
窗口
Highlight
高级
跟踪
Bell
日志记录
文件传输
X/YMODEM
ZMODEM
连接
常规
名称(N):
choco-01
协议(P):
SSH
主机(H):
192.168.1.254
端口号(O):
22
说明(D):
重新连接
连接异常关闭时自动重新连接(A)
间隔(V):
0
秒
限制(L):
0
分钟
TCP选项
使用Nagle算法(U)
连接
确定
取消

c. 填写认证信息

4. MacOS 或 Linux 远程访问方法

命令：ssh -p <端口号> <username>@<ip_addr>

如：

```
# ssh -p 5555 root@192.168.1.1
```

注意：
若不加-p 参数，默认访问服务端22端口
若不加 username@，默认以 **当前使用的本地账户** 登录远程服务器

5. 在线用户查看

命令1： w

```
[root@choco-02 ~]# w
11:01:38 up  1:21,  3 users,  load average: 0.00, 0.01,
0.05USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1                      09:40   29:38   0.09s  0.09s -bash
root     pts/0    192.168.1.1      10:31   26:50   0.04s  0.04s -bash
root     pts/1    192.168.1.1      10:52    2.00s  0.05s  0.01s w
```

第一行显示：**当前系统时间、系统持续运行的时间、在线用户数、当前负载**

第二行（后面的一样）显示：**在线用户、所用终端、源IP、登录时刻**等

命令2： who

```
[root@choco-02 ~]# who
root     tty1         2018-05-10 09:40
root     pts/0        2018-05-10 10:31 (192.168.1.1)
root     pts/1        2018-05-10 10:52 (192.168.1.1)
```

相当于w的精简版

用秘钥远程登录

远程登录其他主机时总是要输入密码？ 用秘钥登录可免去输入密码的过程

1. 非对称加密原理

分享一个链接：https://www.zhihu.com/question/33645891，讲解很生动。

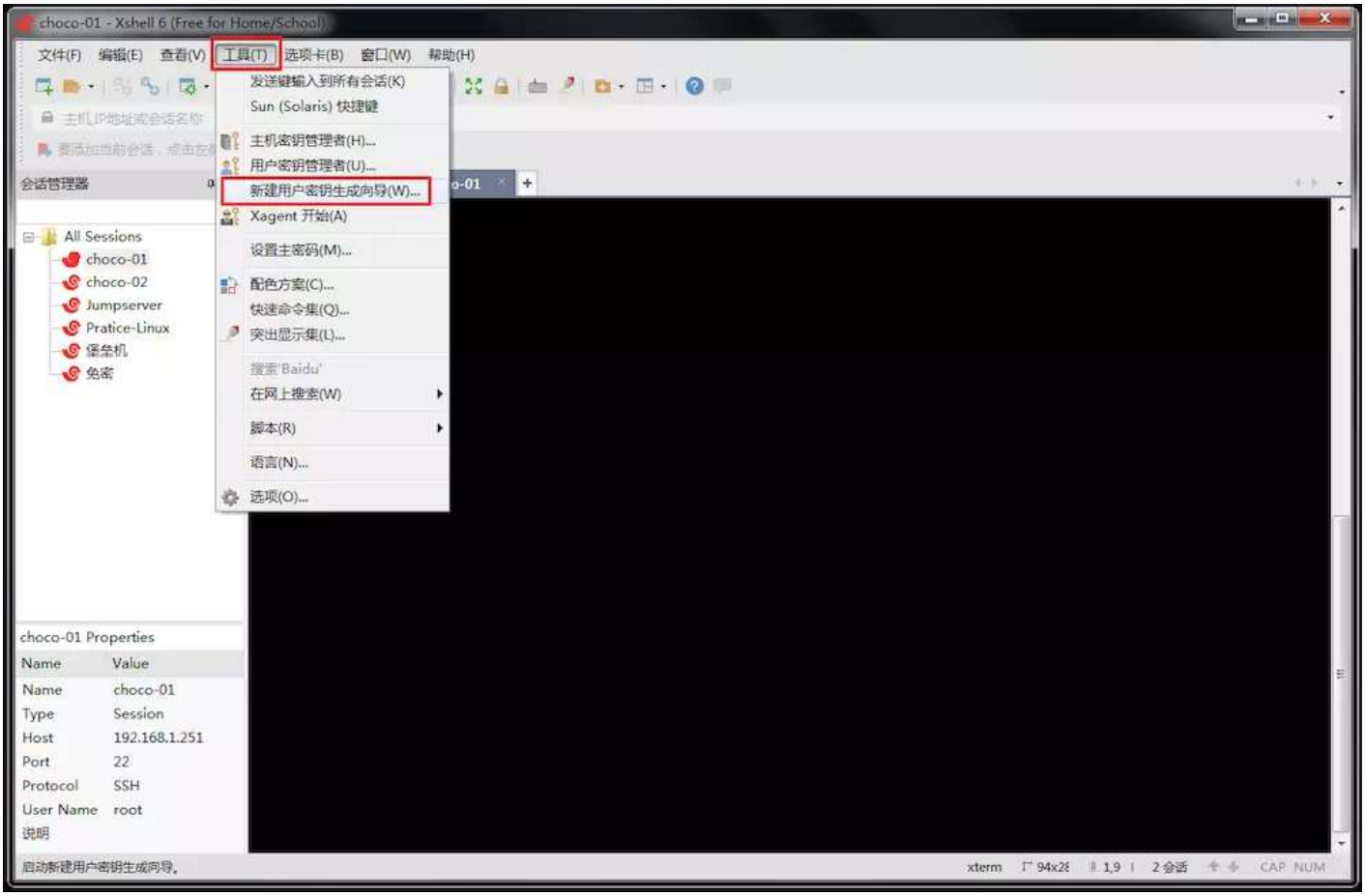
2. 一句话概括秘钥远程登录的配置

Client产生密钥对，将Client的公钥写入Server的 /root/.ssh/authorized_keys 文件中即可

3. Windows操作步骤

——以Xshell为例

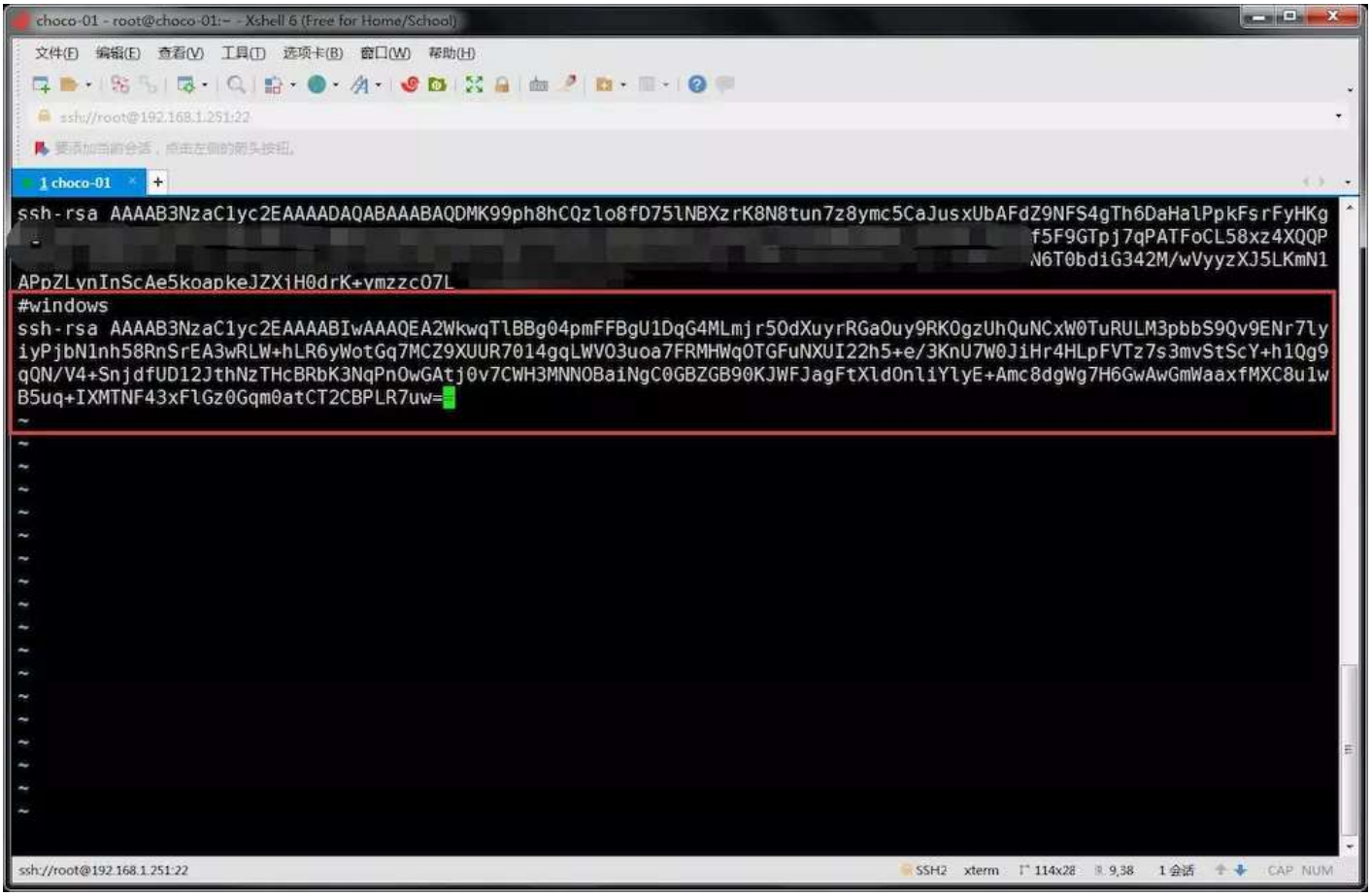
a. 在**工具**菜单中，选择**新建用户秘钥生成向导**



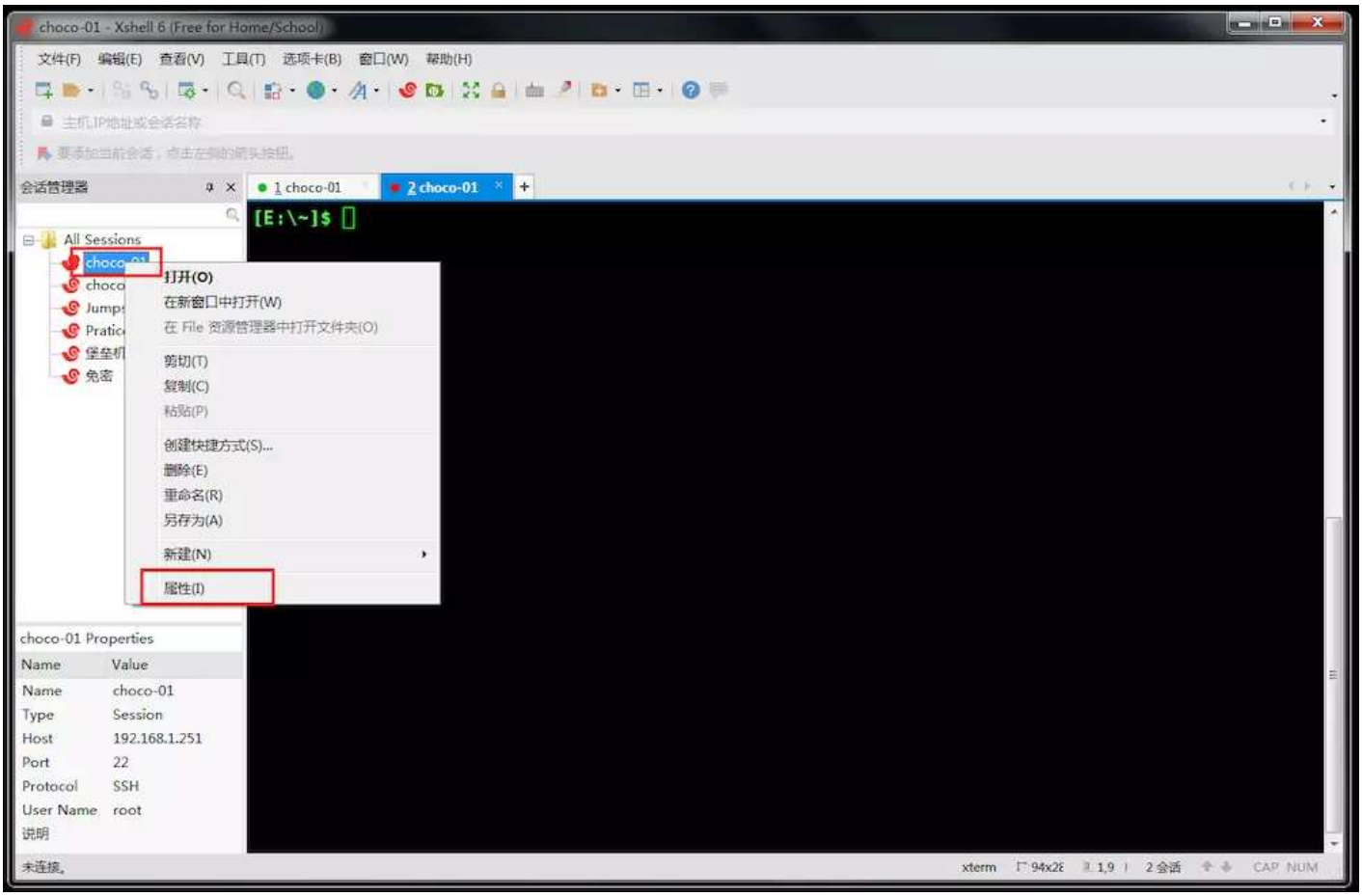
b. 一路下一步后，输入要生成的密钥对的名称，以及对应的密码，并点击下一步

c. 复制所提供的公钥内容

d. 粘贴进Server中 /root/.ssh/authorized_keys文件中，并做好注释


choco-01 - root@choco-01:~ - Xshell 6 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
1 choco-01
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMK99ph8hCQzlo8fD75lNBXzrK8N8tun7z8ymc5CaJusxUbAFdZ9NFS4gTh6DaHalPpkFsrFyHKg
f5F9GTpj7qPATFoCL58xz4XQQP
N6T0bdiG342M/wVyyzXJ5LKmN1
APpZLynInScAe5koapkeJZXjH0drK+ymzzcO7L
#windows
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2WkwqTlBBg04pmFFBgU1DqG4MLmjr5OdXuyrRGaOuy9RKOgzUhQuNCxW0TuRULM3pbbS9Qv9ENr7ly
iyPjbN1nh58RnSrEA3wRLW+hLR6yWotGq7MCZ9XUUR7014gqLWVO3uoa7FRMHWqOTGFuNXUI22h5+e/3KnU7W0JiHr4HLpFVTz7s3mvStScY+h1Qg9
qQN/V4+SnjdfUD12JthNzTHcBRbK3NqPnOwGAtj0v7CWH3MNNOBaiNgC0GBZGB90KJWFJagFtXldOnliYlyE+Amc8dgWg7H6GwAwGmWaaxfMXC8u1w
B5uq+IXMTNF43xFlGz0Gqm0atCT2CBPLR7uw=
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
ssh://root@192.168.1.251:22
SSH2 xterm 114x28 9,38 1 会话
CAP NUM

e. 修改原会话的属性


choco-01 - Xshell 6 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
会话管理器
1 choco-01
2 choco-01
[E:\~]$
All Sessions
choco-01
choco
Jumps
Pratic
堡垒机
免密
打开(O)
在新窗口中打开(W)
在 File 资源管理器中打开文件夹(O)
剪切(T)
复制(C)
粘贴(P)
创建快捷方式(S)...
删除(E)
重命名(R)
另存为(A)
新建(N)
属性(I)
choco-01 Properties
Name Value
Name choco-01
Type Session
Host 192.168.1.251
Port 22
Protocol SSH
User Name root
说明
未连接。
xterm 94x28 1,9 2 会话
CAP NUM

f. 用户身份验证部分，选择Public Key方法，并输入对应的用户，选择秘钥，填入之前设置的密码。此时再次连接会话已是密钥登陆。

4. Linux操作步骤

a. Client上创建密钥对（一路回车即可）

命令：ssh-keygen -t rsa ##其实不加-t rsa也可，默认就是用rsa加密算法的

```
[root@choco-02 ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:SHA256:Ohww3/rX2kOTGcbnwVz9IiGrSMb8saqtK9Fg4lwdeoE root@choco-02
The key's randomart image is:
+---[RSA 2048]----+
|    .            .|
|   E o    . .   o|
|    =oo    + + ..|
|. oo *=.. . = * .|
|oo.o.oooS+ . B o |
| o. ...++   = .  |
|   .  =.   o .   |
|  .  ..o  ..o    |
|   .++. ......   |
+----[SHA256]-----+
```

最终在 /root/.ssh下生成密钥对，id_rsa为私钥，id_rsa.pub为公钥

b. 将公钥内容传递到Server的 /root/.ssh/authorized_keys 文件内（方法较多）

前提：在Server的 /root/ 目录下，有权限为 700 的 .ssh 目录；在 .ssh 目录中有权限为 600 的 authorized_keys 文件。但如果使用下述第二种方式则会自动建立以上目录及文件。

第一种：在Xshell中复制Client的公钥内容，粘贴进Server的authorized_keys中。

第二种：使用ssh-copy-id命令

命令：ssh-copy-id -i <Pub_key_file> <user_name>@<remote_server>

- 在Client上传输公钥至Server

```
[root@choco-02 .ssh]# ssh-copy-id -i id_rsa.pub root@192.168.1.251
/usr/bin/ssh- copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install
the new keys
root@192.168.1.251's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.1.251'"
and check to make sure that only the key(s) you wanted were added
[root@choco-02 .ssh]#
```

- 此时在Server的/root/.ssh/authorized_keys中已存在Client的公钥

```
[root@choco-01 ~]# cat .ssh/authorized_keys
ssh-rsa A.................此处省略.........7L root@choco-02
```

- Client已可以使用密钥登陆Server

```
[root@choco-02 .ssh]# ssh root@192.168.1.251
Last login: Thu May 10 11:44:13 2018 from 192.168.1.1
```

第三种：用scp传输公钥，并用 cat .... >> /root/.ssh/authorized_keys的方式将Client公钥追加至该文件尾部。