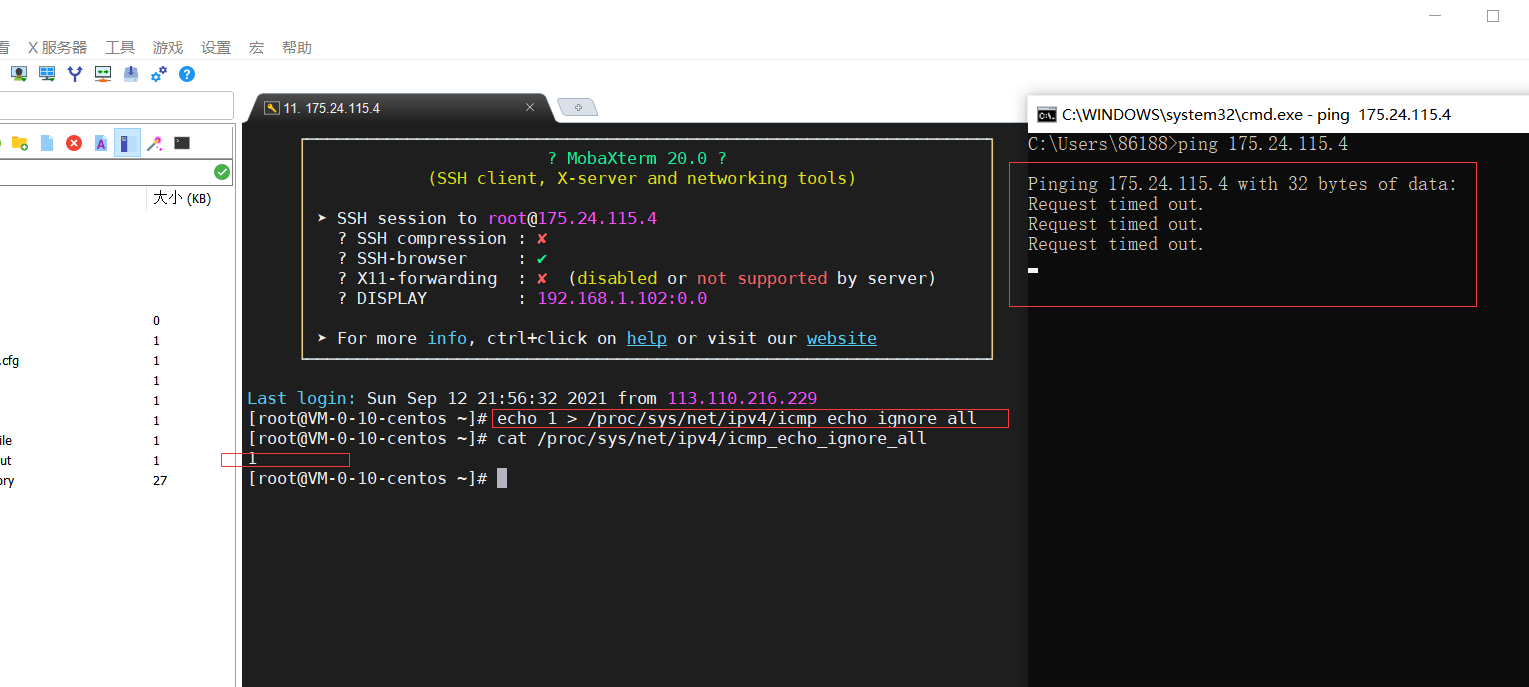
**Linux加固**

**1、禁ping**

[root@VM-0-10-centos ~]# echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

取消禁ping

[root@VM-0-10-centos ~]# echo 0 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all



**2、或iptables禁ping**

**0x01参考：**

https://www.cnblogs.com/ssooking/p/7890192.html

**0x02执行：**

iptables -A INPUT -p icmp -s 0/0 -j DROP

**0x03解释：**

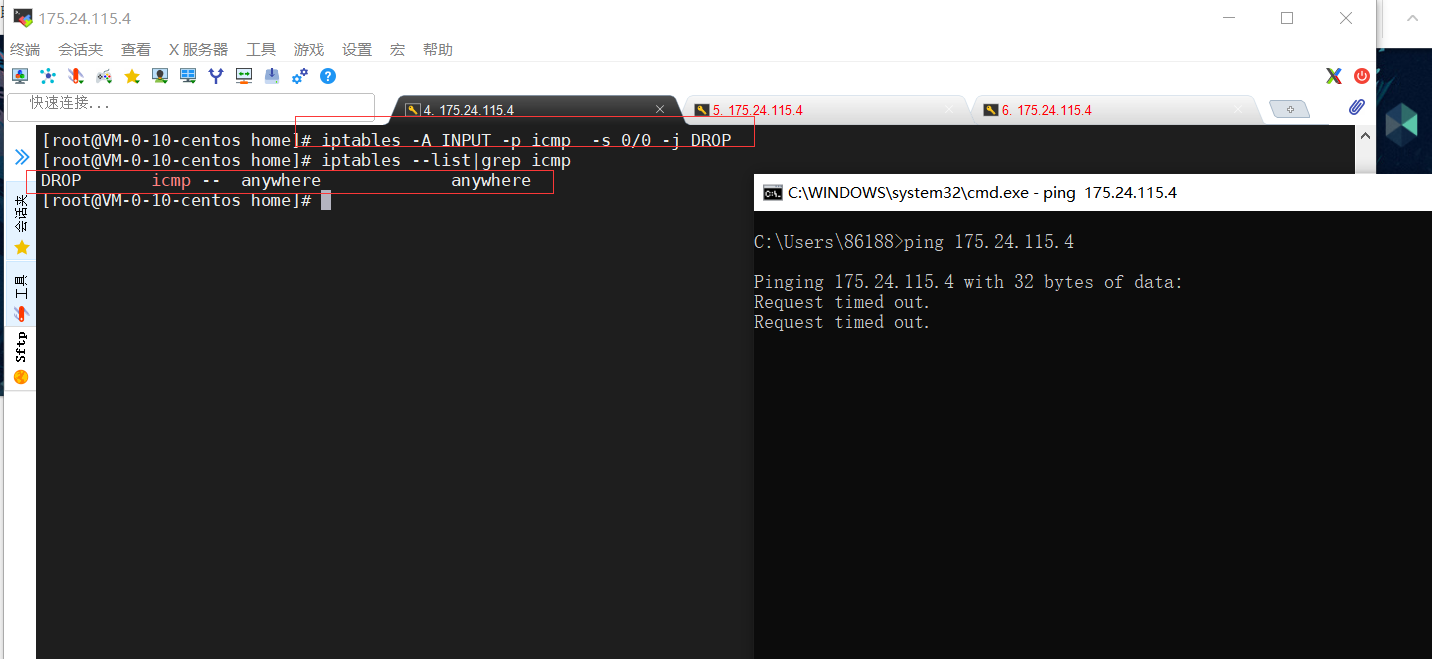
-A 在链的尾部添加一条规则

-p 指定协议类型

-s 指定源ip

-j 处理动作

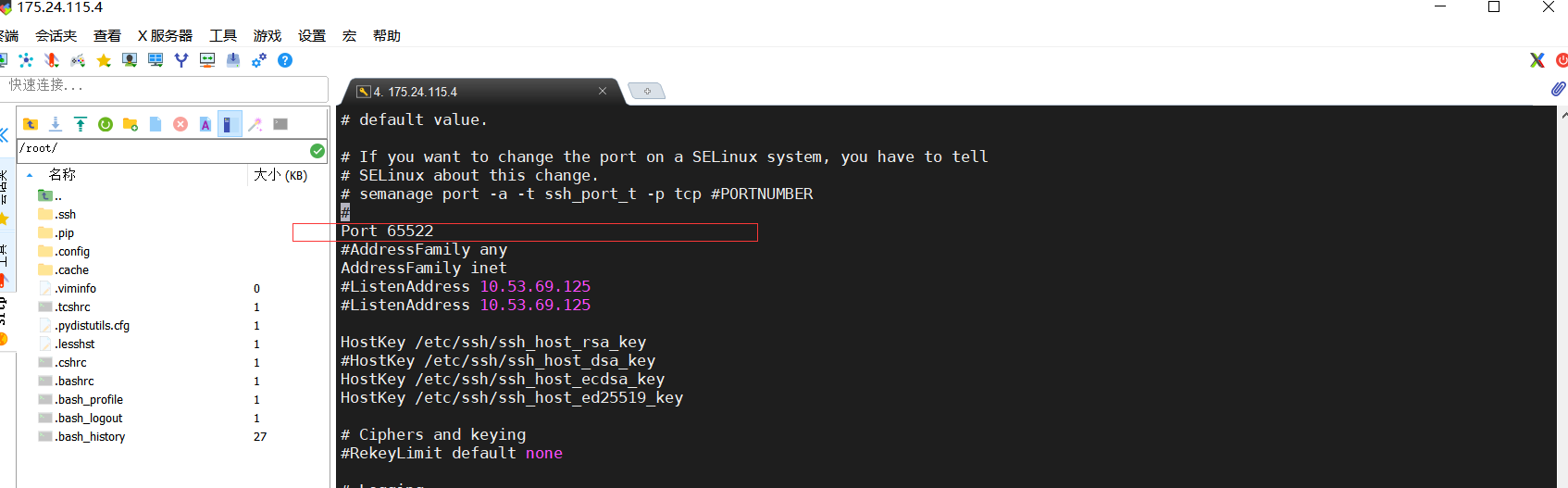
**0x04备注：清空规则:iptables -F**



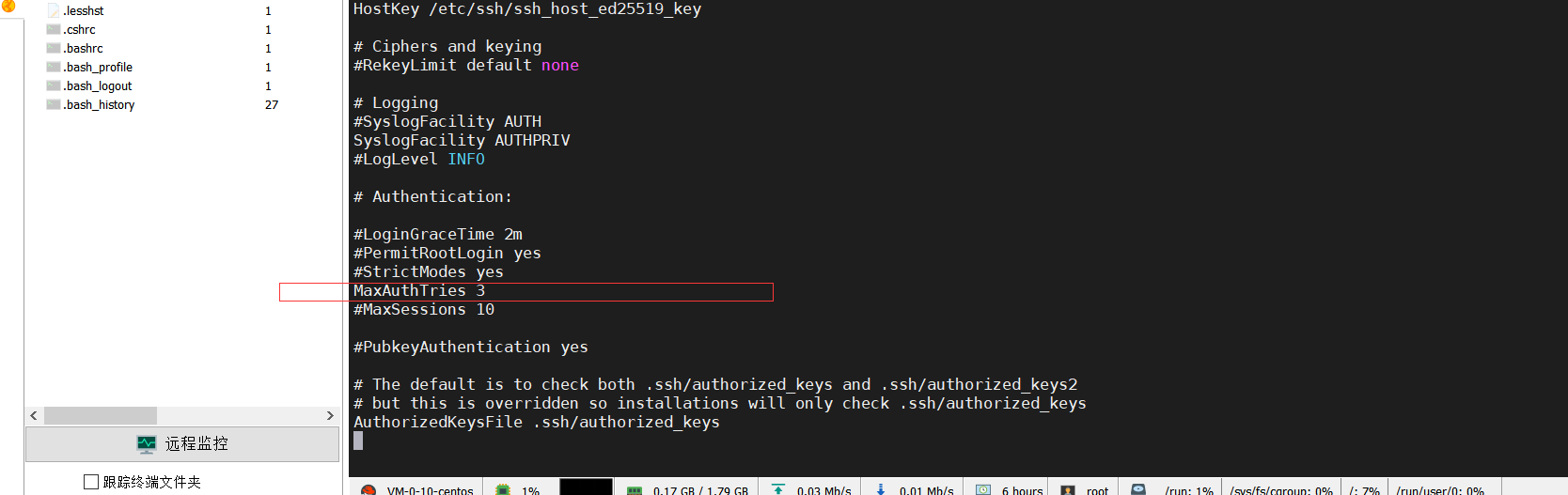
**3、修改sshd\_config配置文件**

[root@VM-0-10-centos root]# vi /etc/ssh/sshd\_config

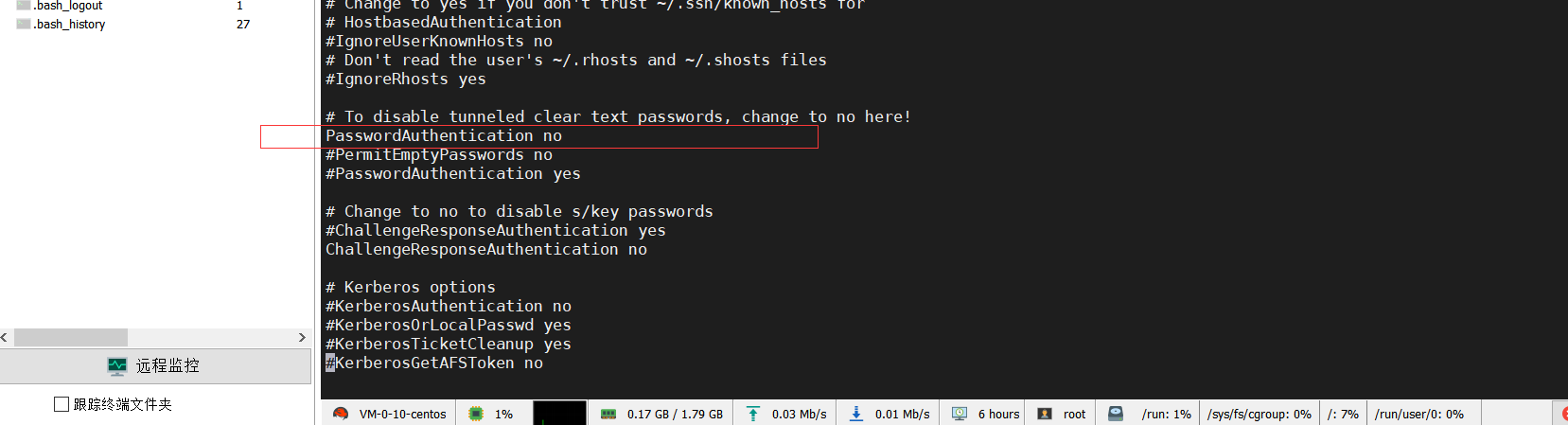
**0x01ssh端口改为：65522**



**0x02修改允许密码错误次数（默认6次），设置 MaxAuthTries 的值为 3**



**0x03不用允许密码登录，设置PasswordAuthentication 的值为 no**



**4、生成密钥,使用密钥登录ssh**

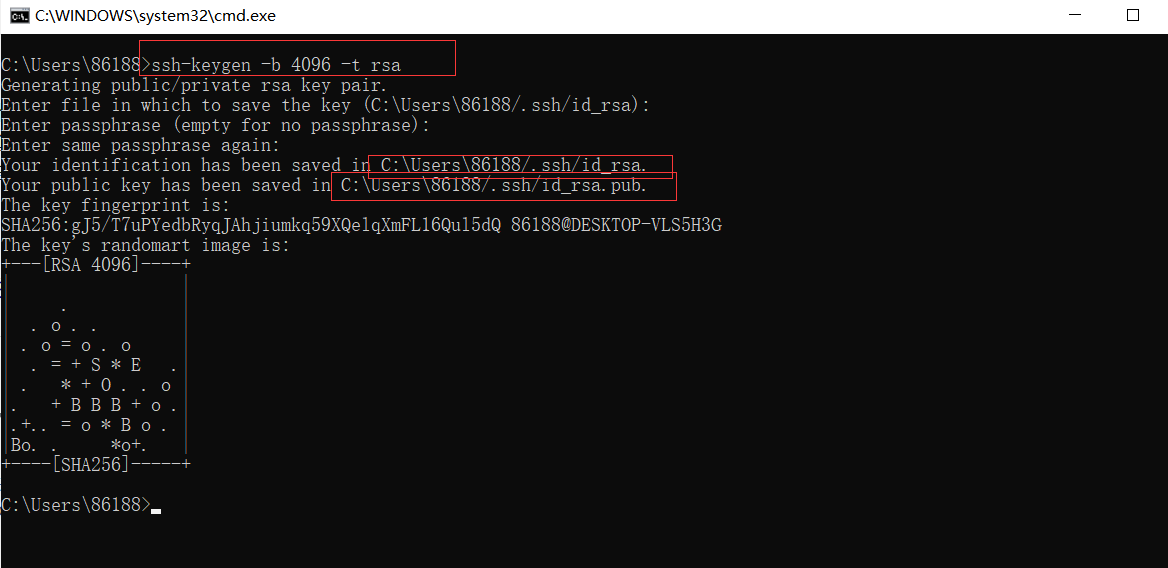
**0x01执行:**

ssh-keygen -b 4096 -t rsa

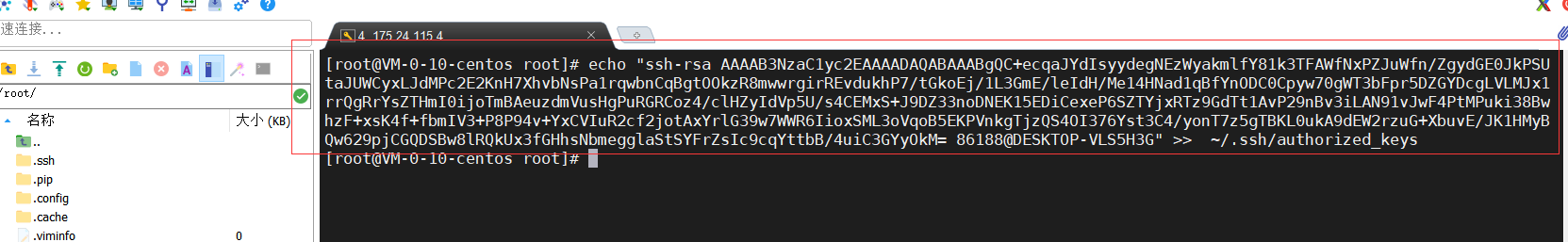
**0x02解释：**

-b：指定密钥长度，通常是2048位，也就1024 \* 2

-t：指定要创建的密钥类型



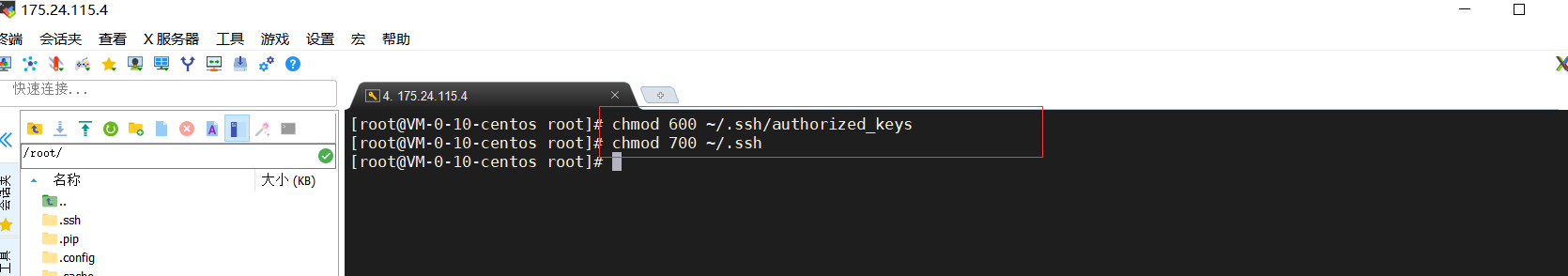
**5、使用秘钥登录，将id\_rsa.pub公钥里的所有内容追加到到 ~/.ssh/authorized\_keys文件里**



**0x01编辑完成后还得修改权限**

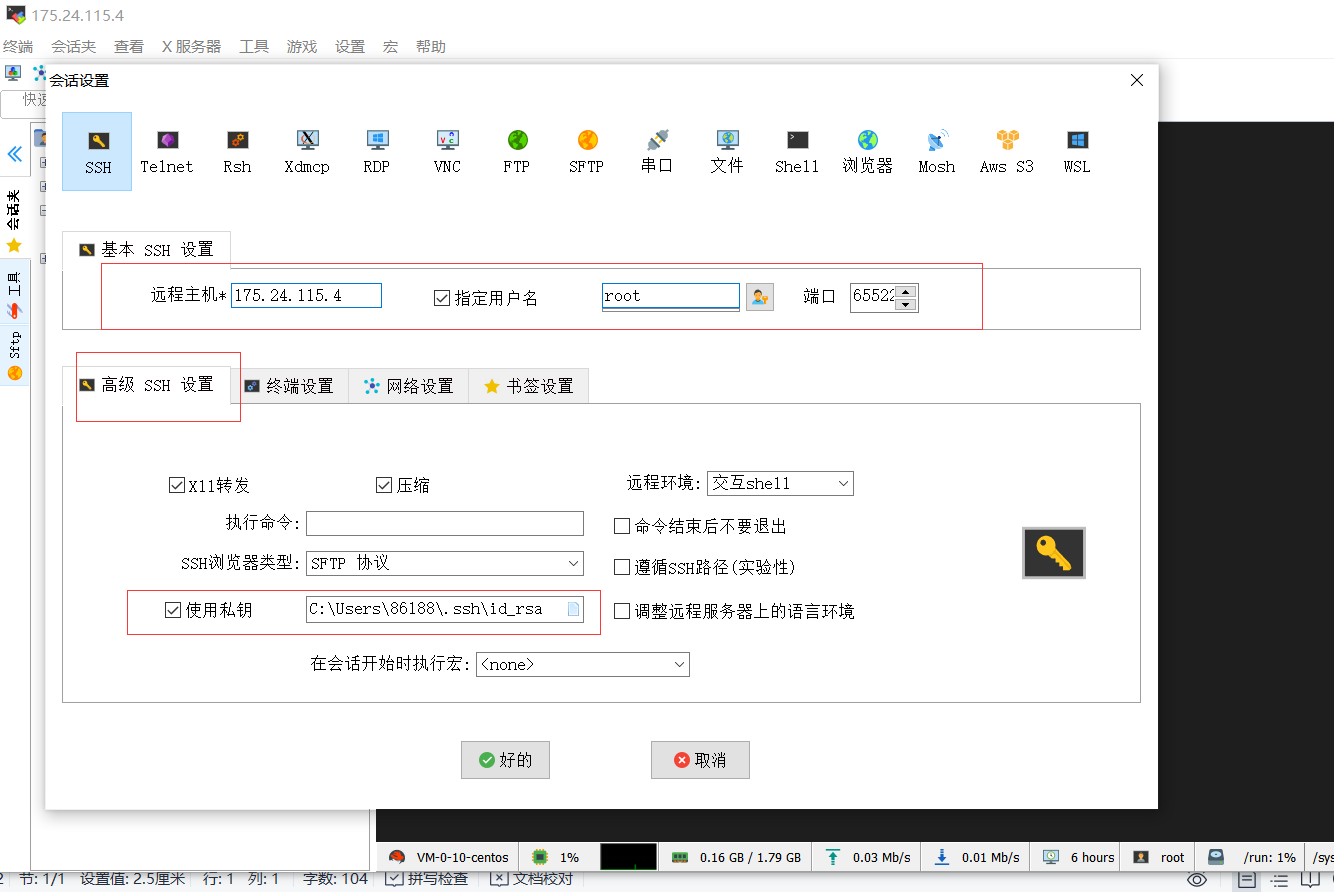
chmod 600 ~/.ssh/authorized\_keys

chmod 700 ~/.ssh

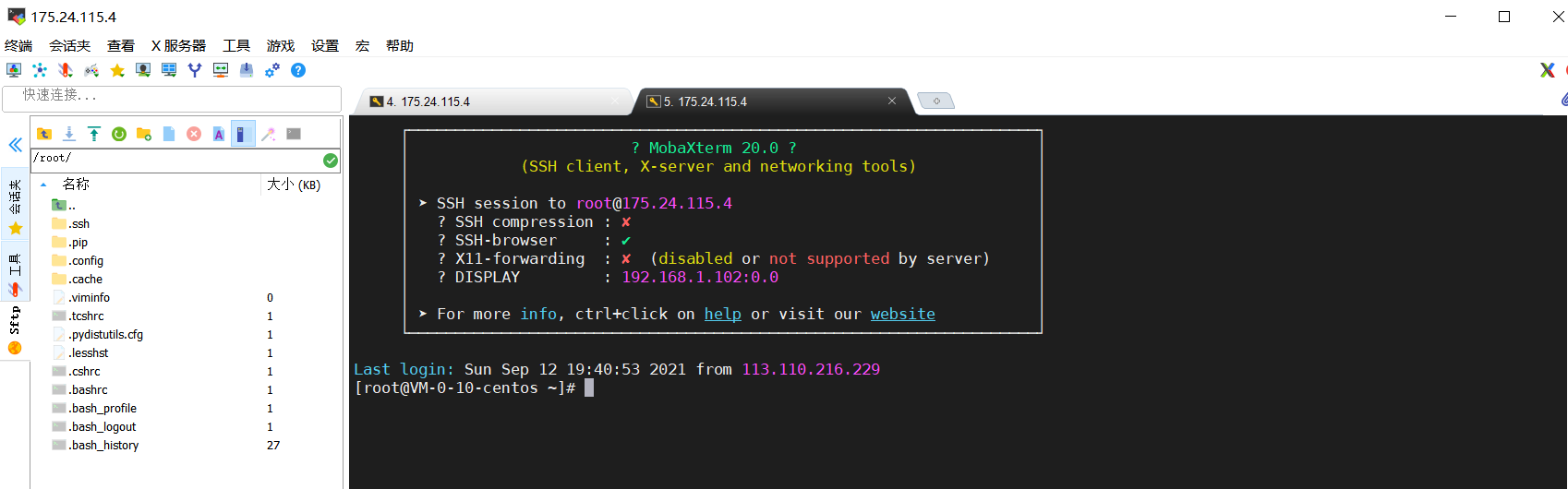


**0x02 Window：Mobaxterm连接，选择对应私钥，用户名root，端口65522，主机：175.24.115.4**

**0x03 Linux：命令行方式连接：ssh -i /root/.ssh/id\_rsa root@目标ip**



**6、连接成功**



**7、编辑/etc/profile，记录所有用户的登录和操作日志**

vi /etc/profile # 打开配置文件

# 修改配置文件,追加以下内容

history

USER=`whoami`

USER\_IP=`who -u am i 2>/dev/null| awk '{print $NF}'|sed -e 's/[()]//g'`

if [ "$USER\_IP" = "" ]; then

USER\_IP=`hostname`

fi

if [ ! -d /var/log/history ]; then

mkdir /var/log/history

chmod 777 /var/log/history

fi

if [ ! -d /var/log/history/${LOGNAME} ]; then

mkdir /var/log/history/${LOGNAME}

chmod 300 /var/log/history/${LOGNAME}

fi

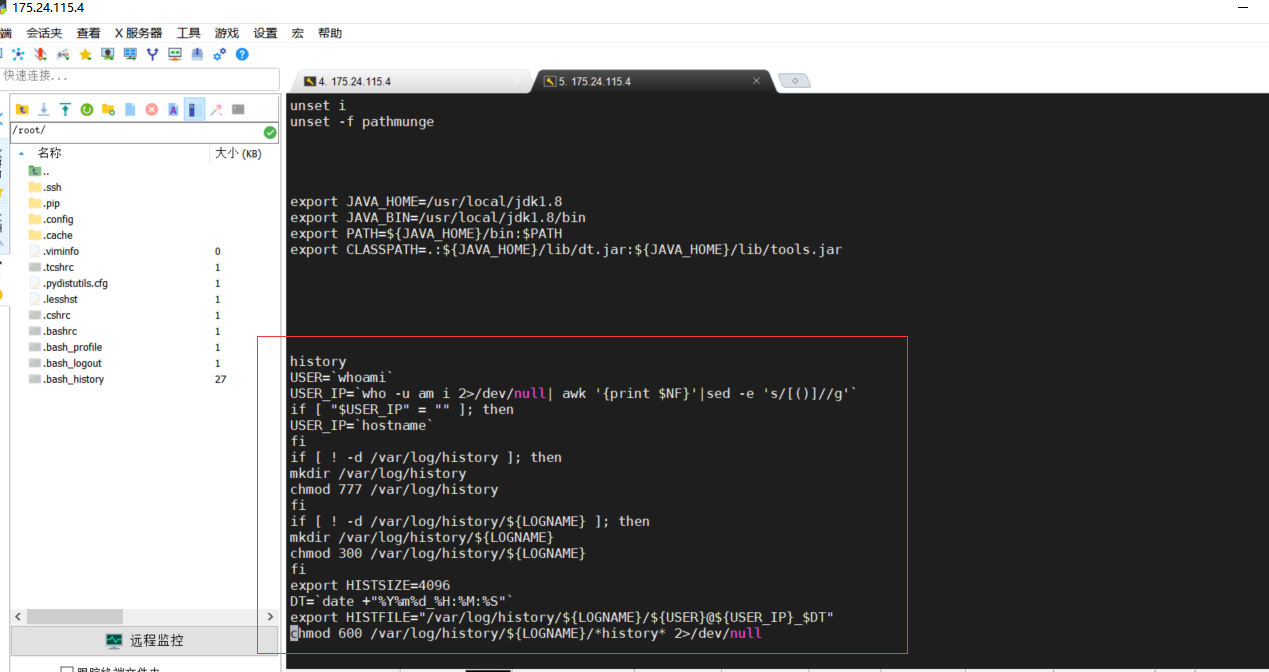
export HISTSIZE=4096

DT=`date +"%Y%m%d\_%H:%M:%S"`

export HISTFILE="/var/log/history/${LOGNAME}/${USER}@${USER\_IP}\_$DT"

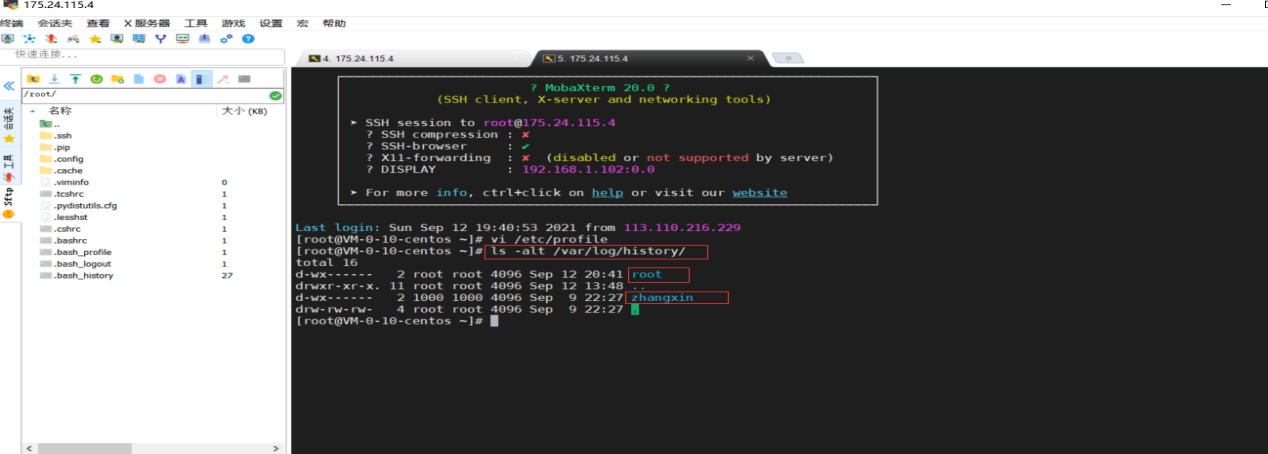
chmod 600 /var/log/history/${LOGNAME}/\*history\* 2>/dev/null

source /etc/profile # 加载配置生效



**8、效果为：在/var/log/history 路径下记录所有用户命令操作日志，可以自定义路径**

**0x01可以看到有root和zhangxin两个用户的文件夹**



**0x02在路径：/var/log/history/root/下可以看到root用的每一次shell登录日志以及里面的操作命令日志记录**

