一、搭建堡垒机（堡垒机，就是跳板机，从公网跳到私网的）

1、具备堡垒机的条件，该设备需具有公网IP和私网（其他服务器的IP）；

2、堡垒机安全设置（iptables端口限制、除开自己用的端口外，其他全封了）；

3、用户、命令权限限制（jailit）;

http://blog.chinaunix.net/uid-28310119-id-3503318.html

4、客户机器日志审计（不能在跳板机上做，需要到各个客户机上去做）

http://www.68idc.cn/help/server/linux/2014042190951.html

二、安装jailkit实现chroot

下载安装包

wget https://olivier.sessink.nl/jailkit/jailkit-2.19.tar.bz2

tar jxvf jailkit-2.19.tar.bz2 //解压

3、安装

./configure

make && make install

4、创建虚拟用户的根目录

mkdir /home/jail

5、配置jailkit,就是开放一些常用服务和命令给虚拟用户

jk\_init -v -j /home/jail/ basicshell

jk\_init -v -j /home/jail/ editors

jk\_init -v -j /home/jail/ ssh

jk\_init -v -j /home/jail/ netutils

6、mkdir /home/jail/usr/sbin

7、cp /usr/sbin/jk\_lsh /home/jail/usr/sbin/jk\_lsh

8、创建系统用户,创建多个用户，重复执行8、9、10三步

useradd zhangsan

passwd zhangsan

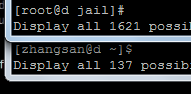
9、创建虚拟用户

jk\_jailuser -m -j /home/jail/ zhangsan

10、vim /home/jail/etc/passwd //将、/usr/sbin/jk\_lsh 改为/bin/bash



11、登录创建的虚拟用户，发现能用的目录很少的，root有1621个，而虚拟只有137个。



三、日志审计

1、指定设备ssh到客户机，需要在客户机上设置ssh规则，编辑 vim /etc/hosts.allow ，

添加如下内容：

sshd: 192.168.1.24 //只允许指定IP登录到该设备

vim /etc/hosts.deny

添加如下内容：

sshd: ALL //除开allow里面的IP，其他IP都禁止登录该设备。

2、在所有的客户机上，及需要登录到跳板机的设备上，执行下面的操作

[root@b ~]# mkdir /usr/local/records

[root@b ~]# chmod 777 /usr/local/records/

[root@b ~]# chmod +t /usr/local/records/ // t权限是防止被删除的。

3、vi /etc/profile //添加

if [ ! -d /usr/local/records/${LOGNAME} ]

then

mkdir -p /usr/local/records/${LOGNAME}

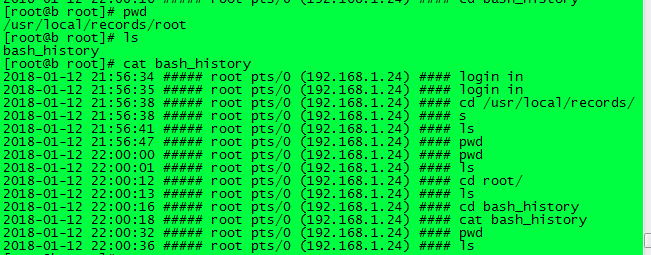
chmod 300 /usr/local/records/${LOGNAME}

fi

export HISTORY\_FILE="/usr/local/records/${LOGNAME}/bash\_history"

export PROMPT\_COMMAND='{ date "+%Y-%m-%d %T ##### $(who am i |awk "{print \$1\" \"\$2\" \"\$5}") #### $(history 1 | { read x cmd; echo "$cmd"; })"; } >>$HISTORY\_FILE'

4、重新登录会在 /usr/local/records下发现有root目录，里面会记录登录该设备的用户操作记录。



四、jumpserver（在centos7上去做）

http://blog.51cto.com/qiangsh/1882193 //别人做的

**Ⅰ、安装jumpserver（0.3.3）**

下载安装包，放在一个空间大的目录里面

wget https://github.com/jumpserver/jumpserver/archive/0.3.3.zip

unzip 0.3.3.zip

自动安装

[root@bogon install]# cd

[root@bogon ~]# cd /mnt/jumpserver-0.3.3/

[root@bogon jumpserver-0.3.3]# cd install/

[root@bogon install]# python install.py

备注：如果安装的时候，系统没有安装mysql，请根据提示安装mysql

请输入您服务器的IP地址，用户浏览器可以访问 [192.168.1.33]:

是否安装新的MySQL服务器? (y/n) [y]: y

请输入数据库服务器IP [127.0.0.1]: //:这里回车就可以了

请输入数据库服务器端口 [3306]:

请输入数据库服务器用户 [jumpserver]:

请输入数据库服务器密码: //回车，默认密码是5Lov@wife

请输入使用的数据库 [jumpserver]:

连接数据库成功

请输入SMTP地址: smtp.163.com //163邮箱服务器

请输入SMTP端口 [25]:

请输入账户: googleqicq@163.com //我的邮箱和密码

请输入密码: 911911@qq

完成后，邮箱会收到邮件：内容“Mail test passed!”

vim .conf //这里面有配置的文件。

**Ⅱ、登录jumpserver**

ip:8000来登录

192.168.1.33:8000

用户名：admin

密码：5Lov@wife

**Ⅲ、创建管理用户**

在搭建好的jumpserver上，在承担菜单里面找到“设置”选项

1、在默认管理用户里面设置一个用户名，我设置的是“jz”

2、密码我选择了跳过

3、默认ssh端口：填入“22”

4、默认密钥是在jumpserver服务器上自动生成的私钥

[root@bogon ~]# mkdir /root/.ssh

[root@bogon ~]# chmod 700 !$

chmod 700 /root/.ssh

cd /root/.ssh

[root@bogon ~]# ssh-keygen -f jz //生成公钥和私钥

jz jz.pub //前面的是私钥，填入第4步。

5、在客户端上创建，“jz”帐号，不用密码

6、在客户端上 ： su - jz

7、在jz用户里面 创建 mkdir .ssh

vim .ssh/authorized\_keys //把生成的公钥，及 jz.pub的内容copy进去

8、chmod 700 .ssh

chmod 400 .ssh/authorized\_keys

9、在jumpserver服务端上，以jz登录到客户端上去。

ssh -i jz jz@192.168.1.28 //28是客户端的IP，正常无需密码自动登录。

Ⅳ、**创建普通用户**

1、创建用户组

2、创建用户

3、填写正确的email

4、收到的邮件内容

Hi, zhangsan

您的用户名： zhangsan

您的权限： 普通用户

您的web登录密码： zOinJ17uXL7QsZAb

您的ssh密钥文件密码： Tm\_RJ2zvAXJjVNuq

密钥下载地址： http://192.168.1.33/juser/key/down/?uuid=f217757e2b104d42894bf6216f903c0e

说明： 请登陆跳板机后台下载密钥, 然后使用密钥登陆跳板机！

**Ⅴ、添加机器 （在登录的jumpserver web上）**

1、添加资产组

2、添加资产

3、visudo //在客户机上执行，



4、如果正常，查看资产，点击更新，会出现设备信息。

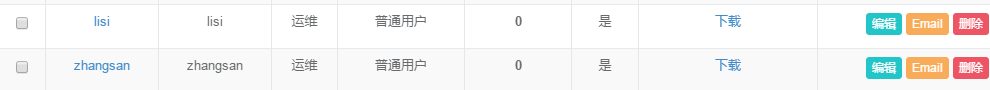


5、如果要添加多个资产情况

a、在要添加的设备上，请参照，**Ⅲ的**5、6、7、8、9步和V的第3步即可。

**Ⅵ添加系统用户并授权（在登录的jumpserver web上）**

1、在授权管理里面选择系统用户，选择添加系统用户（就是用户里面添加的用户）



2、自定义用户密码。

3、用户密钥，在jumpserver服务器上用下面的命令生成（这个地方填写私钥）

ssh-keygen -f zhangsan

4、将生成的私钥也就是 zhangsan里面的内容复制到用户密钥里面去，保存的时候会报错，这是软件bug，不影响。

5、选择系统用户，选择推送，选择资产及你要把这个用户推送到哪个客户几上去，就是说你要在哪个客户机上自动创建该用户。

推送报错

Aborting, target uses selinux but python bindings (libselinux-python) aren't installed!

解决办法：

在客户机上：yum install libselinux-python -y

并且要关闭selinux

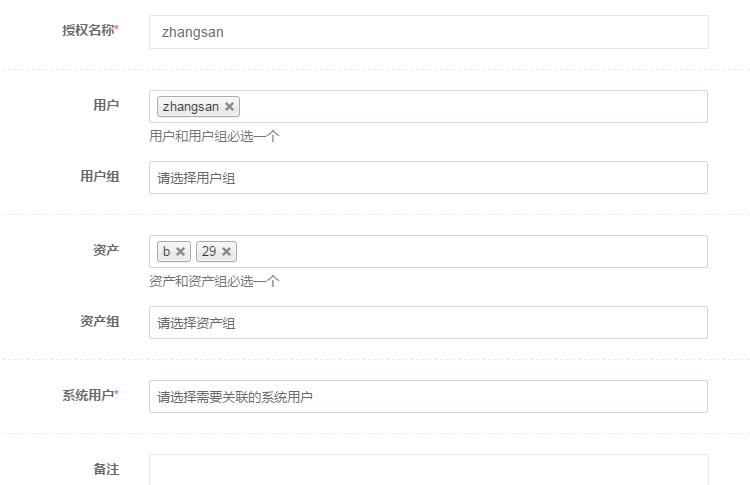
6、如果正常，会显示推送成功，并且客户机上也会有该用户



**Ⅶ、添加授权规则**

1、选择授权规则

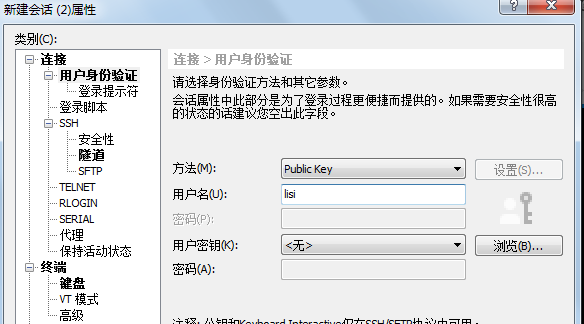
2、添加授权

3、

规则就是让jumpserver里面的用户及web里面“查看用户里面的用户”去对应web里面的系统用户。

**Ⅷ、客户端登录jumpserver**

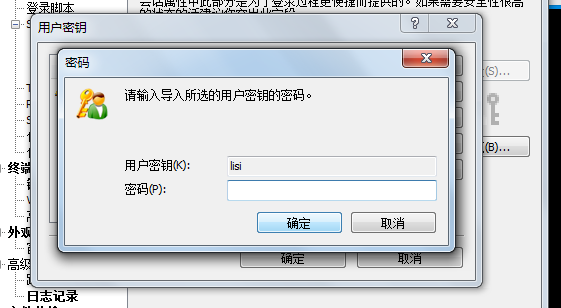
用xshell



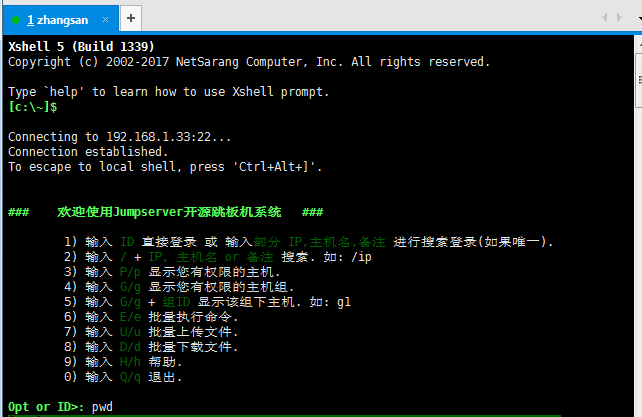
2、导入下载的密钥



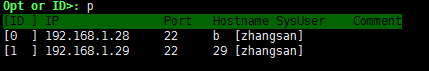
3、密码为邮件里的“您的ssh密钥文件密码”，点击连接即可



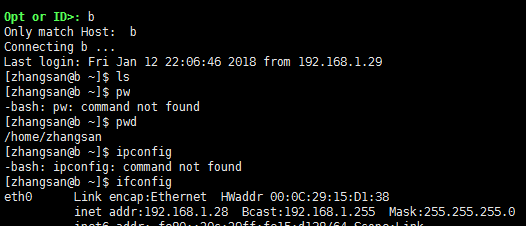
4、正常界面



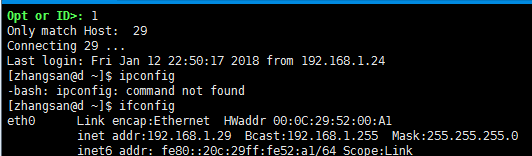
输入"p" //查看有权限的客户机及能通过该跳板机登录到哪些客户机。



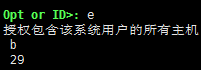
输入Hostname "b"，直接就进到该客户机里面去了



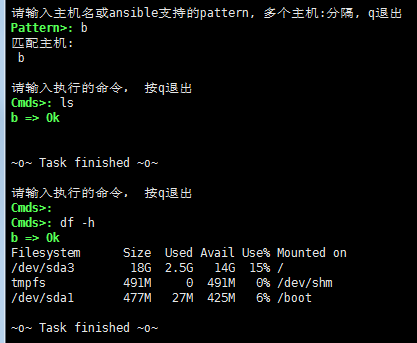
输入"ID" 输入1，直接进到另外一台客户机



输入“e”



针对单独的设备执行命令



多台设备执行

