SSH复习外加建立安全隧道Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_SSH_E5_A4_8D_E4_B9_A0_E5_c103_644672.htm SSH复习外加建立安全隧道 SSH Secure SHell protocol telent是一种明文传输，人所共知，所以不建议使用，因为可以被窃听到你传输的资料，即使是不重要，你也不想陌生人知道你的东西把。所以有ssh的出现，ssh是加密传输的，加密方法目前在 SSH 使用上，主要是利用 RSA/DSA/Diffie-Hellman 等制喔！具体什么就各自去查了～了解就好。 每次 SSH daemon (sshd)，就生一支 768-bit 的公(或 server key)存放在 Server 中；若有 client 端的 ssh 需求送，那 Server 就一支公 client，此 client 也比一下支公的正性。比的方法利用 /etc/ssh/ssh_known_hosts 或 ~/.ssh/known_hosts 案容。 在 Client 接受 768-bit 的 server key 之後，Client 自己也生一支 256-bit 的私(host key)，且以加密的方式 server key host key 整合成一完整的 Key pair，且 Key pair 也送 server ；之後，Server Client 在次的中，就以一 1024-bit 的 Key pair 行料的！ 这个是大致的整个连线步骤，从鸟哥那cp过来的，懒得打字了，大概明白怎么进行传输的就OK，另外注意一下目前ssh已经加入了diffie－hellman机制来进行每次传输的资料的源检查时候正确，更进一步的加强了安全。 vi /etc/ssh/sshd.config port ssh 的端口 protocol ssh的协议,最好用2,最新版安全 hostkey /etc/ssh/ssh_host_rsa_key rsa算法密钥 hostkey /etc/ssh/ssh_host_dsa_key dsa 算法密钥 syslogfacility AUTHPRIV 当有人ssh等入系统是,ssh会记录到/var/log/secure下 permitrootlogin no 把root紧闭进入,安全起见

pubkeyAUTHENTICATION yes 是否允许用public key AUTHORIZEkeysFILE .ssh/authorized_keys 这个东西很重要就是要是否要登录密码进行登录ssh, printMotd no 列印出/etc/motd 这个文件的内容,安全起见 no printlastlog yes 显示上次等入的信息 Keepalive yes 通过传送一个keepalive给client 来保持双方连线正常,避免任何一方挂掉而导致另一方的僵死 Maxstartups 10 排队进入ssh的数量 Subsystem sftp /usr/libexec/openssh/sftp-server 关于sftp的设定大概就这样 ssh 帐号@ip或者主机名 -p ssh端口默认是22 第一次登录会有一系列的设定之类,确认好就好了,然后输入密码正确就连接上去 但是经过第一次登录后,你的~目录下就有了一个.ssh的文件,这个文件里面就是你的rsa或者dsa 就是你进入的钥匙拉….不过我们后面做的不需要密钥进行登录,就要把这个文件删除了,我们要重新建一个.ssh的目录,这里是不同的. [test2@test2 ~]$ ssh-keygen -t rsa 这个就是生成密钥 有2个(例子是用rsa)Your identification has been saved in /home/test2/.ssh/id_rsa lt.==公钥The key fingerprint is:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 然后用scp /传输文件帐号@ip或者主机名: /目录 或者加-p 端口 ----SCP是有冒号的因为要做到不需要密码登录ssh ,就要将公钥public key(就是刚才作的那个id_rsa.pub)上传到服务器. 还有刚才提到一个AUTHORIZEkeysFILE .ssh/authorized_keys这个东西很重要就是要是否要登录密码进行登录ssh, 这么一个东西公钥的写法就要写成authorized_keys 当然你也可以自己改自己喜欢的,但是名字一定要互相对应好,配置对目录位置对好,为了方便也为了免去以后的麻烦,一般都按照他这个名字写,mv

id_rsa.pub authorized_keys另外注意好2个密钥的位置,都是在帐号home目录下的.ssh里面scp authorized_keys 帐号@ip或主机名:~/.ssh确认好都有密钥 然后用相应的帐号登录就不需要密码了由于authorized_keys中可能保存多个公钥所以用gt.来添加,建立类似vpn的隧道,--在几台主机之间建立一个专门的通讯隧道,可以将其他没有加密的通讯转到这里,从而将通讯加密.建立隧道ssh -2C -p 555 test@192.168.0.1 -L 5000:172.16.1.1:22 -g-2C是ssh服务通讯协议版本 为2 C 为表示压缩传输-L bind_address格式port/host/hostport-g 表示提供使用权限,即隧道提供其他主机使用从172.16.1.1的5000端口建立一个连接到192.168.0.1的ssh的555端口服务隧道,隧道自动转接22端口的包ssh XXX@172.16.1.1 -p 5000就可以连接上去或者telent xxx@172.16.1.1 5000道ssh -2C -p 555 test@192.168.0.1 -L 5000:172.16.1.1:22 -g-2C 是ssh服务通讯协议版本 为2 C 为表示压缩传输-L bind_address格式port/host/hostport-g 表示提供使用权限,即隧道提供其他主机使用从172.16.1.1的5000端口建立一个连接到192.168.0.1的ssh的555端口服务隧道,隧道自动转接22端口的包ssh XXX@172.16.1.1 -p 5000就可以连接上去或者telent xxx@172.16.1.1 5000