OpenSSH

LAB

- Step 1: Install OpenSSH
  - apt-get install openssh-server
  - Tất cả file cấu hình được lưu ở thư mục /etc/ssh

Ssh_config	cấu hình cho ssh client
Sshd_config	cấu hình cho ssh server
Ssh_config_host_dsa_key	key mã hóa
Ssh_config_host_dsa_key.pub	
Ssh_config_host_rsa_key	
Ssh_config_host_rsa_key.pub	

LAB

- Step 2: edit /etc/ssh/sshd_config
  - cp /etc/ssh/sshd_config /etc/ssh/sshd_config.origin
  - vi /etc/ssh/sshd_config

```
Port 22
Protocol 2
PermitRootLogin yes
StrictModes yes
MaxAuthTries 3
RSAAuthentication no
PubkeyAuthentication yes
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreUserKnownHosts yes
PermitEmptyPassword no
```

LAB

- Step 3: restart OpenSSH

  - root@ubuntu:/# service ssh   restart
    * Restarting OpenBSD Secure Shell server sshd [ok]
  - root@ubuntu:/# chmod 700 /home/<USER>/.ssh

    Vi du: chmode 700 /home/thuy/.ssh
  - root@ubuntu:/# chmod 600 /home/<USER>/.ssh/authorized_keys

root@ubuntu:/# chown $<USER>:$<USER> /home/<USER>/.ssh -R

LAB

- Step 4: tạo OpenSSH private and public key
  - Login vào ubuntu bằng 1 acc của user (ví dụ login bằng account thuy)
  - Dùng lệnh “ssh-keygen -t rsa “ để tạo cặp khóa private key/public key

LAB

- thuy@ubuntu:~S ssh-keygen -t rsa

  Generating public/private rsa key pair.
  Enter file in which to save the key (/home/thuy/.ssh/id_rsa):
  Created directory ‘/home/thuy/.ssh’
  Enter passphrase (empty for no passphrase): <password >4 ký tự>
  Enter same passphrase again:
  Your identification has been saved in /home/thuy/.ssh/id_rsa.
  Your public key has been saved in /home/thuy/.ssh/id_rsa.pub.
  The key fingerprint is:
  ec:f4:3f:b5:fe:2f:de:22:6c:42:8c:38:ad:6c:5e:96 toylet@ubuntu

LAB

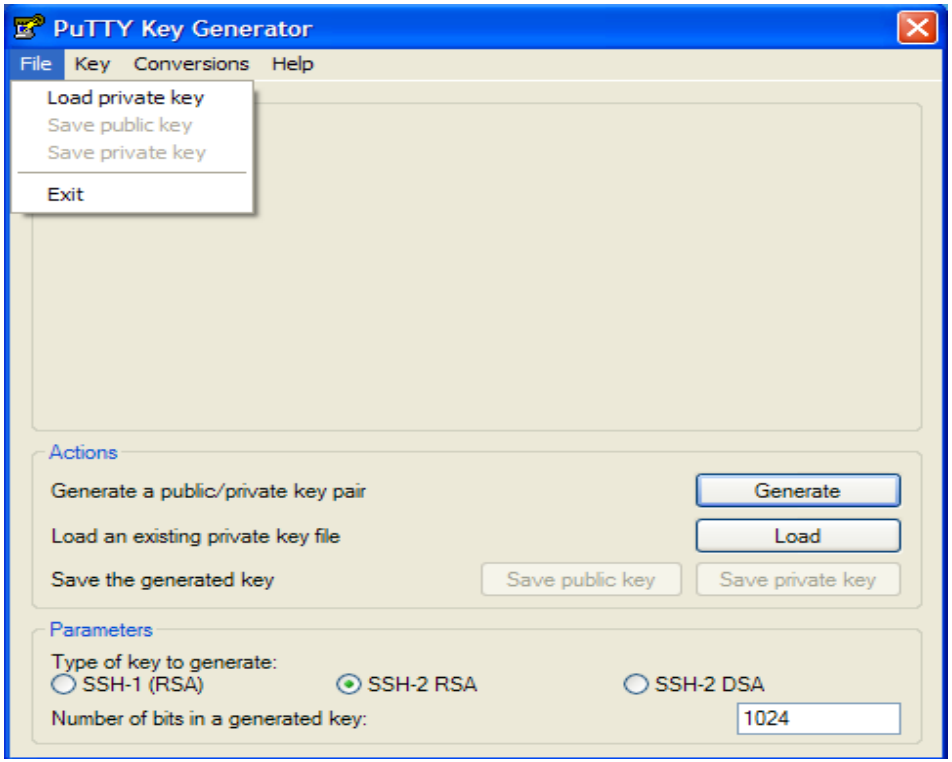
- Step 5:
  - thuy@ubuntu:~S cd /home/thuy/.ssh

    Id_rsa khóa bí mật

    Id_rsa.pub khóa công khai
- Step 6:
  - thuy@ubuntu:~S cp id_rsa.pub authorized_keys
- Step 7:
  - Copy /home/thuy/.ssh/id_rsa đến client (pc Windows)

LAB

- Step 8: Convert OpenSSH private key
  - Sử dụng chương trình puttygen trên windows
  - Load id_rsa vào puttygen

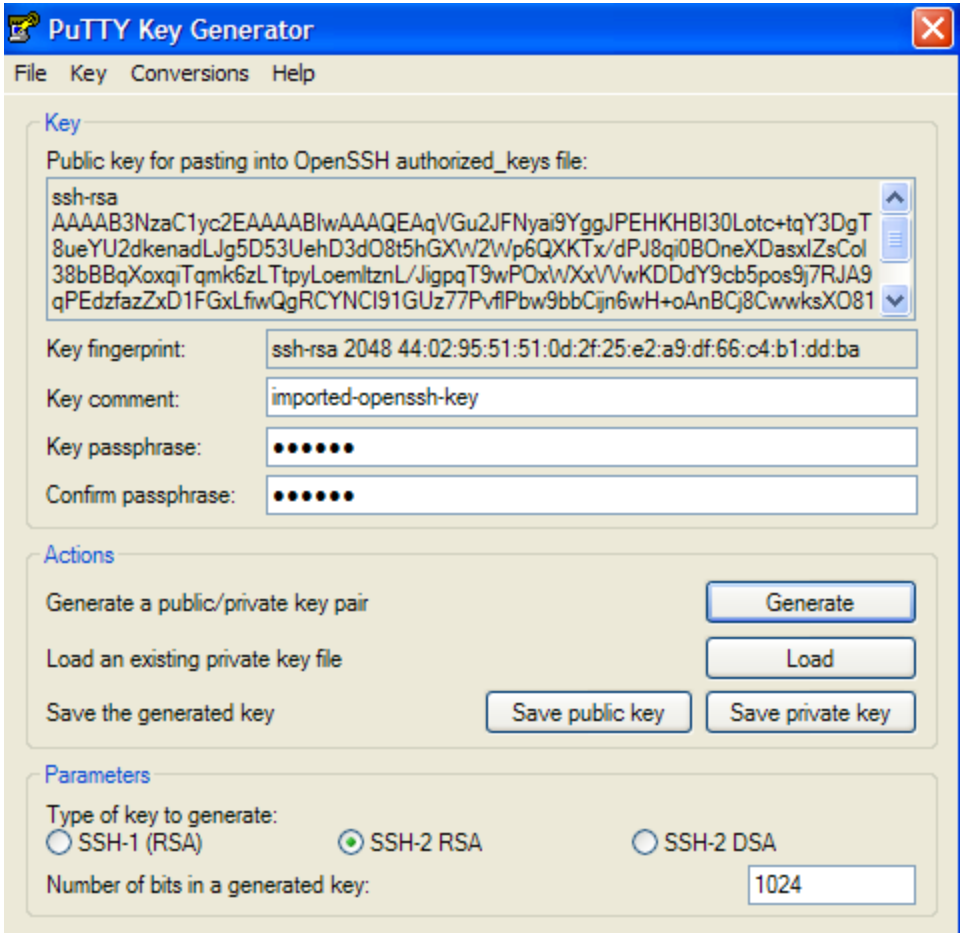


LAB

- Step 8:
  - Kích "Save private key“

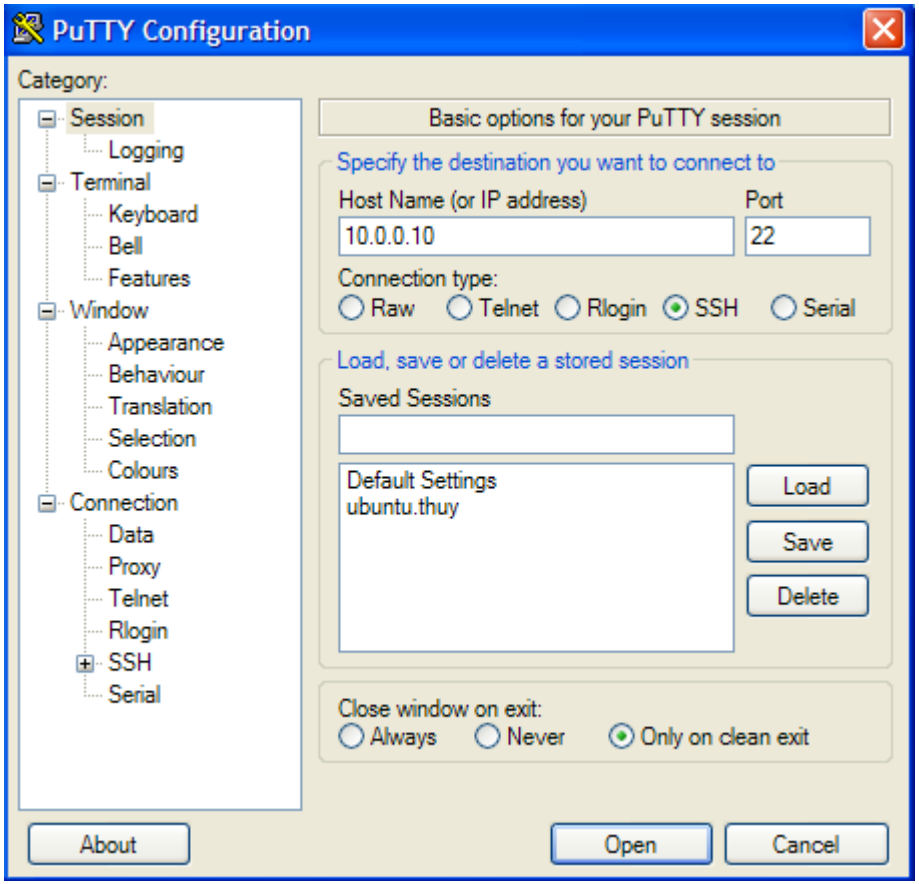
Để convert key thành

Dạng id_rsa.ppk



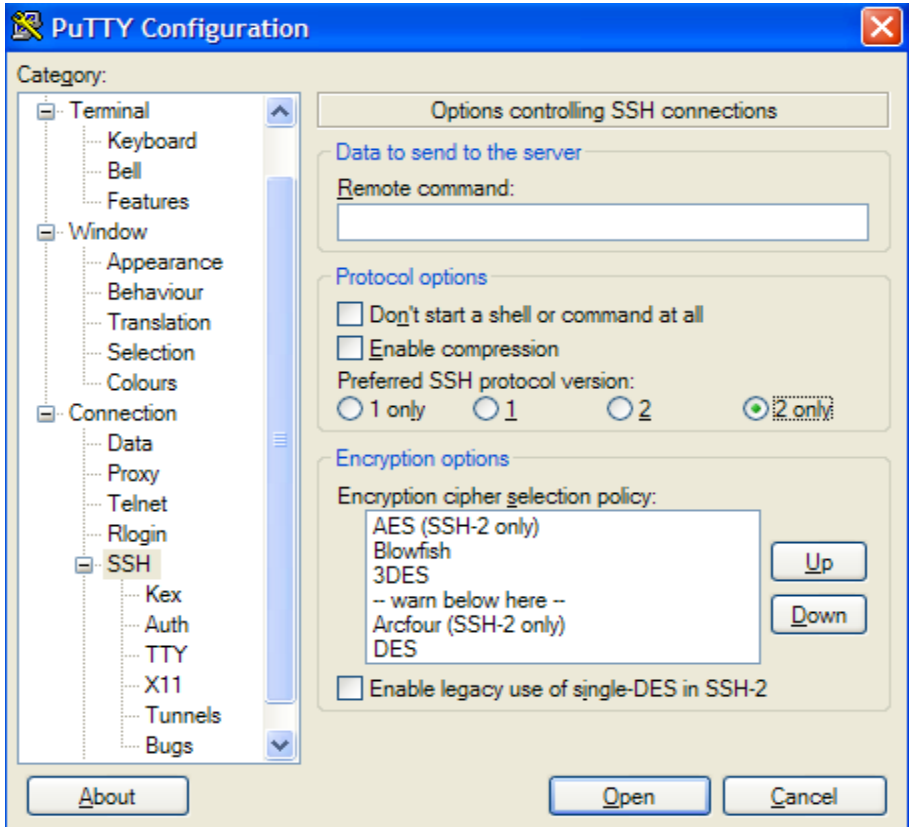
LAB

- Step 9: Login SSHserver bằng putty
  - Session
    Host name: <IP>
    Port: [22]



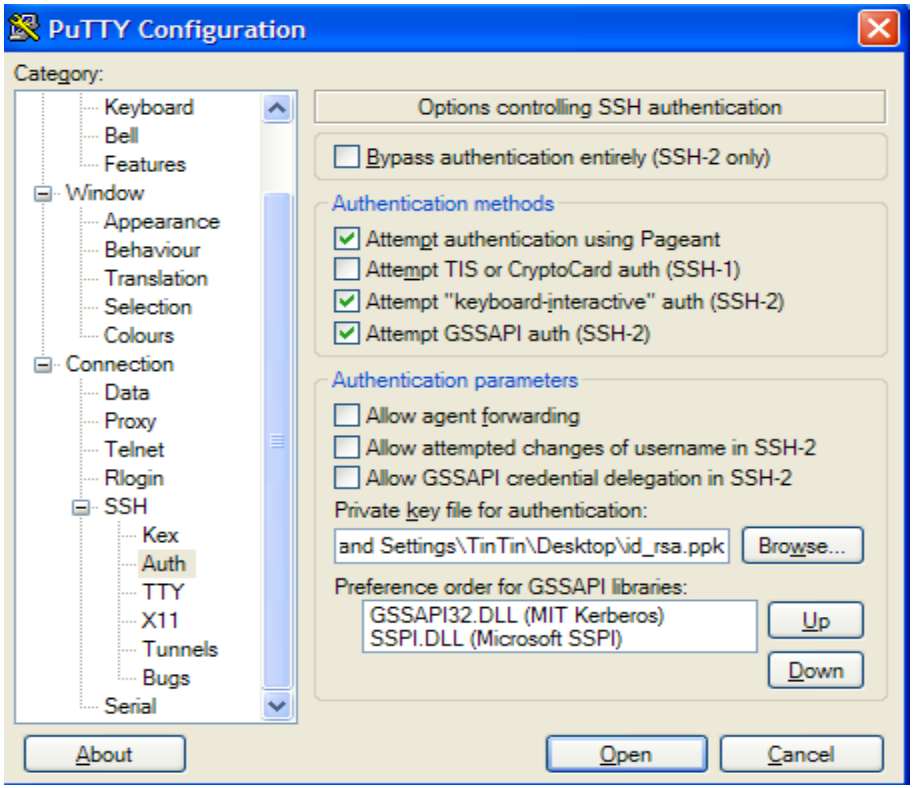
LAB

- Chọn connecttion/SSH
  - Trong mục “preferred SSH protocol version” chọn “2 only”



LAB

- Chọn SSH/Auth
  - ở tùy chọn “private key file for authentication” click Browser để load file id_rsa.ppk vừa tạo ra ở step 8



LAB

- Chọn Session/open