\*Setup ssh server

**SSH** ([tiếng Anh](https://vi.wikipedia.org/wiki/Ti%E1%BA%BFng_Anh): ***Secure Shell***) là một [giao thức mạng](https://vi.wikipedia.org/wiki/Giao_th%E1%BB%A9c_truy%E1%BB%81n_th%C3%B4ng) dùng để thiết lập kết nối mạng một cách bảo mật. SSH hoạt động ở lớp trên trong mô hình phân lớp [TCP/IP](https://vi.wikipedia.org/wiki/TCP/IP). Các công cụ SSH (như là [OpenSSH](https://vi.wikipedia.org/wiki/OpenSSH),...) cung cấp cho người dùng cách thức để thiết lập kết nối mạng được mã hoá để tạo một kênh kết nối riêng tư.

B1: Install:

$ sudo apt-get update

$ sudo apt-get install –y openssh-server

B2: Cầu hình cho sshd:

$ sudo vi /etc/ssh/sshd\_config

OR

$ sudo gedit /etc/ssh/sshd\_config

VD: thay đổi cổng cho ssh là:

Port 22222 # mặc định sẽ là 22

MaxAuthTries 3 # chỉ số lần đăng nhập tối đa

B3: Khởi động lại sshd

$sudo systemctl restart ssh

B4: Kiểm tra trạng thái sshd

$sudo systemctl status ssh.service

+Dùng user/pass

AllowUsers <tên\_user>

+Truy cập ssh server:

$ ssh username@IP –p xxxx

-Kiểm tra ip trên ubuntu:

$ ip addr show

+Hạn chế cổng <- nmap

+Hạn chế IP

+Dùng public key:

$ ssh-keygen –t rsa –b 2048  
$ ls ~/.ssh/

$ mv ~/.ssh/id\_rsa.pub ~/.ssh/authorized\_keys

$ scp lam@hoanghunglam: /home/lam/.ssh/id\_rsa ~/.ssh/

$ ssh –i <tên\_file> <tên\_máy chủ>@<địa chỉ> -p <cổng>