TRƯỜNG ĐẠI HỌC CẦN THƠ
KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG
BỘ MÔN MẠNG MÁY TÍNH & TRUYỀN THÔNG

Quản trị Linux từ xa

Trình bày: TS. NGÔ BÁ HÙNG
Email: nbhung@cit.ctu.edu.vn

Quản trị từ xa

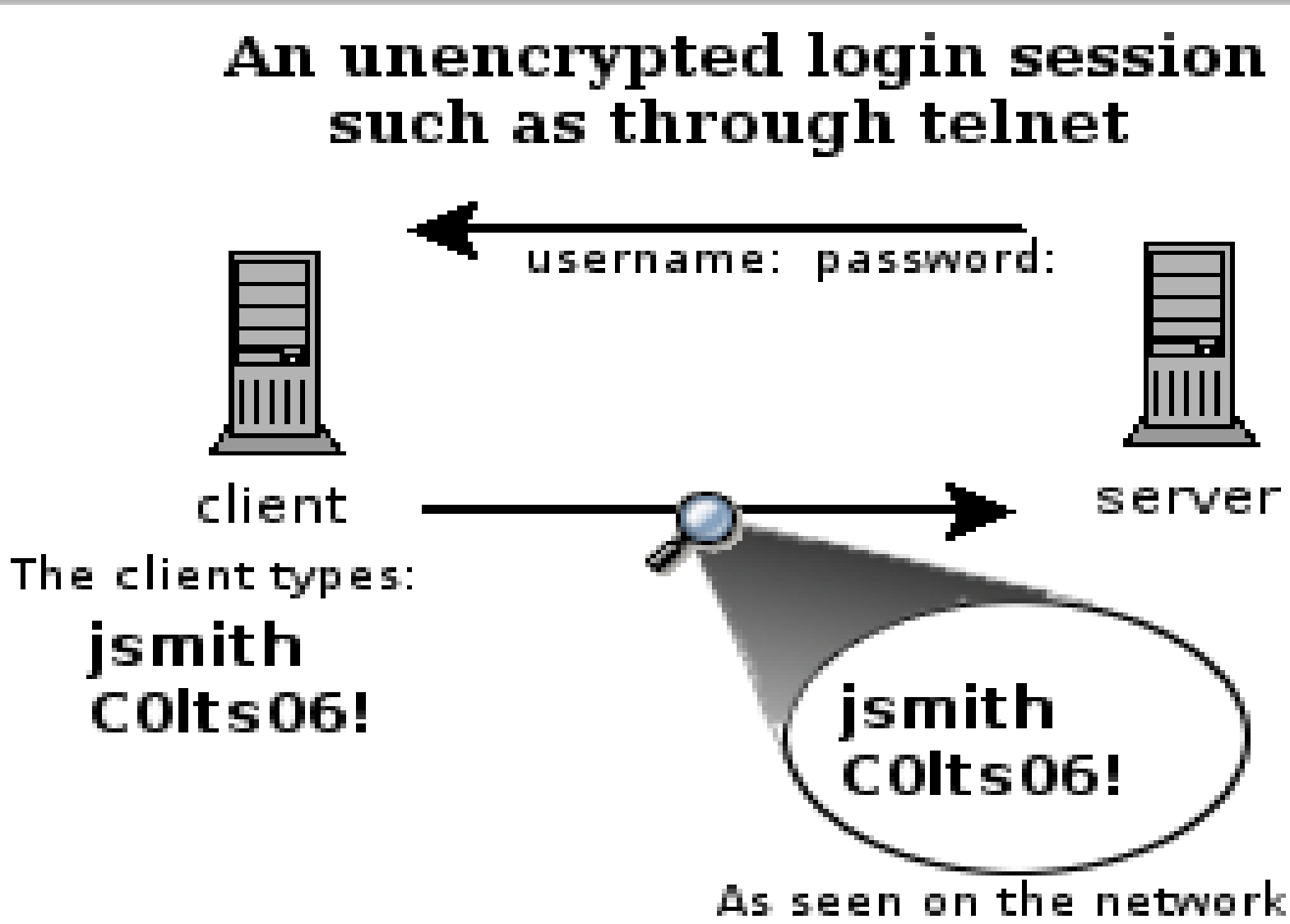
- Cần một tài khoản trên máy tính Server
- Đăng nhập từ xa
  - Đăng nhập vào Server với tài khoản đã có bằng một một phần mềm thực thi trên một máy tính trạm
  - Thực hiện các thao tác quản trị tương tự như đăng nhập trực tiếp tại server
- Copy dữ liệu giữa các máy tính
- Thực thi chương trình trên một máy tính khác

Một số phần mềm quản trị từ xa

- Cũ, không bảo mật, mật khẩu không mã hóa
  - rlogin, telnet: Đăng nhập từ xa
  - rcp, ftp: Copy dữ liệu
  - rexec: Thực thi chương trình từ xa
- An toàn, mã hóa dữ liệu chứng thực
  - Giao thức SSH (Secure SHell)
  - OpenSSH: Bộ phần mềm cài đặt SSH

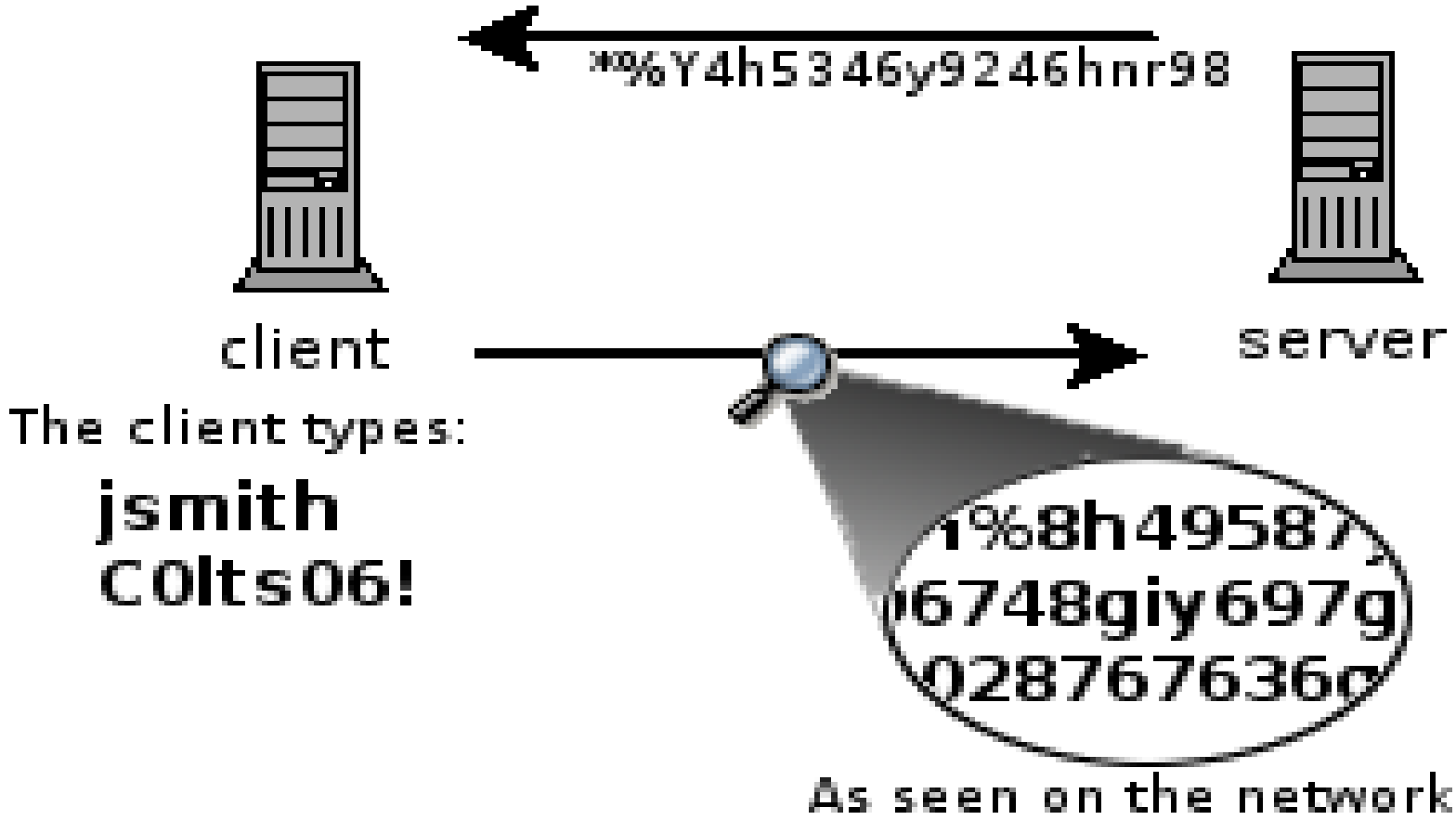
SSH (Secure SHell)

- Giao thức truy cập máy tính từ xa an toàn
- Mô hình Client-Server trên nền TCP, Cổng 22
- SSH-1 (Tatu Ylönen-University of Helsinki,1995)
  - Một giao thức cho truyền tải, chứng thực, an toàn
- SSH-2 (RFC 4251)
  - Gồm các giao thức cho truyền tải, chứng thực, nối kết
  - Sử dụng mã hóa công khai cho chứng thực người dùng và máy tính



http://support.suso.com/supki/SSH_Tutorial_for_Linux

An encrypted login session such as through SSH



http://support.suso.com/supki/SSH_Tutorial_for_Linux

Lợi điểm của SSH

- Tăng cường bảo mật nhờ
  - Kênh truyền được mã hóa
  - Chứng thực người dùng, client, server
- Cung cấp kênh giao tiếp an toàn
  - Tạo kênh giao tiếp an toàn chia sẻ cho nhiều ứng dụng giữa 2 đầu cuối, nhờ đó giảm số lượng cổng mở trên mỗi đầu cuối
  - Bổ sung cơ chế an toàn cho các giao thức không an toàn

Mã hóa công khai

- Được sử dụng trong SSH
- Cặp khóa công khai-cá nhân
- Khóa công khai (Public key):
  - Dùng để mã dữ liệu gởi
  - Có thể truyền trên kênh truyền công cộng mà không ảnh hưởng đến tính bảo mật của dữ liệu đã mã hóa
- Khóa cá nhân (Private key):
  - Dùng để giải mã dữ liệu
  - Phải giữ bí mật

OpenSSH

http://www.openssh.org/

- Bộ công cụ cài đặt SSH, license BSD
  - Server: sshd
  - Client: ssh (rlogin, telnet), scp (rcp), sftp (ftp),
  - ssh-add, ssh-agent, ssh-keysign, ssh-keyscan, ssh-keygen và sftp-server
- Hỗ trợ nhiều hệ điều hành khác nhau
  - Linux, Solaris, FreeBSD AIX HP-UX,...
  - Unix, Windows, Java, Mac OS Palm OS, ...

Cài đặt SSH

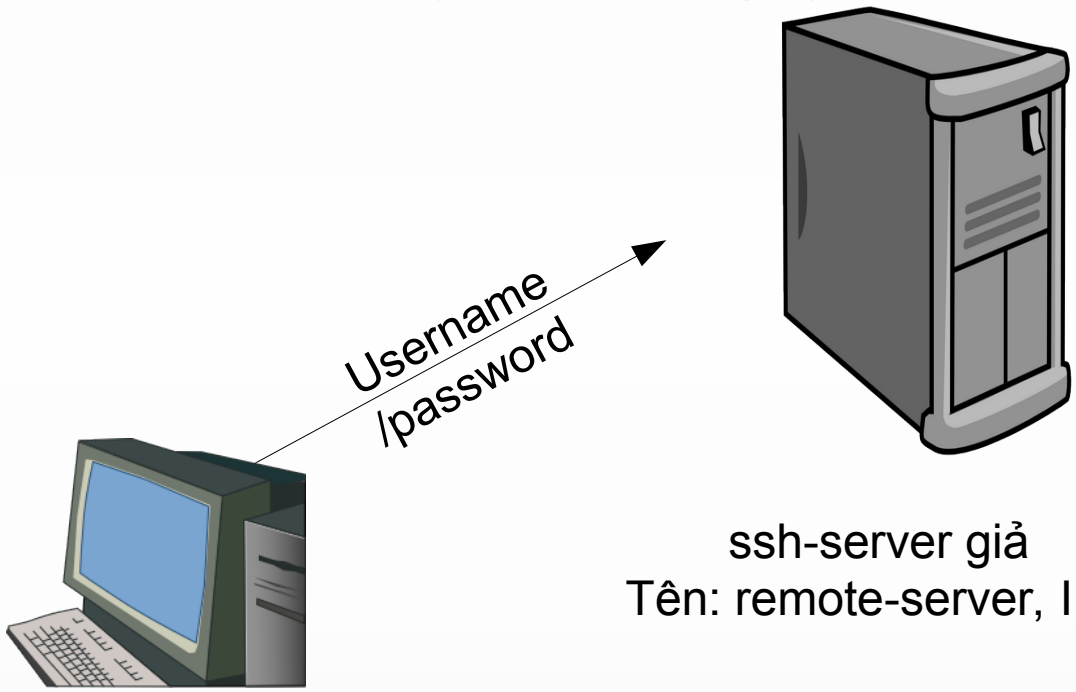
- Cài đặt SSH Server trên Ubuntu
  - sudo apt install openssh-server
- Cài đặt SSH Client trên Ubuntu
  - sudo apt install openssh-client
- Cài đặt SSH Client trên Windows
  - Download phần mềm PuTTY

Đăng nhập từ xa

- Sử dụng login name của người dùng cục bộ
  - ssh ssh-server-ip/name
- Mô tả tên người dùng đăng nhập
  - ssh -l user-name ssh-server-ip/name
  - ssh user-name@ssh-server-ip/name
- Đăng nhập với cổng khác cổng mặc định
  - ssh -l user-name ssh-server-ip/name -p port-num
- Nhập mật khẩu của người dùng trên server

Chứng thực ssh server

- Để tránh giả danh (người thứ ba ở giữa)



Chứng thực ssh server

- Mỗi ssh server có một khóa công khai để nhận dạng nó, lưu tại /etc/ssh/ssh_host_dsa_key.pub
  - Tương ứng với dâu vân tay fingerprint
    - ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub
- Gởi dấu vân tay về ssh client khi client nối kết lần đầu tiên để người dùng nhận dạng ssh server
- Lưu dấu vân tay của ssh server vào file ~/.ssh/known_hosts để những lần sau nhận dạng lại server một cách tự động

Ví dụ - chứng thực ssh server

- $ ssh www.phongchongdichhai.org.vn

  The authenticity of host 'www.phongchongdichhai.org.vn (203.162.202.138)' can't be established.

  RSA key fingerprint is cf:4a:87:66:38:2c:46:ca:2c:86:39:d5:eb:c6:a8:32.

  Are you sure you want to continue connecting (yes/no)? [Nhập yes]

Ví dụ - chứng thực ssh server

Warning: Permanently added 'www.phongchongdichhai.org.vn,203.162.202.138' (RSA) to the list of known hosts.

nbhung@www.phongchongdichhai.org.vn's password: [Nhập mật khẩu của nbhung trên server phongchongdichhai]

- Xem dấu vân tay của server phongchongdichhai
  - $ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub

    2048 cf:4a:87:66:38:2c:46:ca:2c:86:39:d5:eb:c6:a8:32

Ví dụ - chứng thực ssh server

- Xem dấu vân tay của server phongchongdichhai
  - $ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub

    2048 cf:4a:87:66:38:2c:46:ca:2c:86:39:d5:eb:c6:a8:32
- Thoát khỏi server phongchongdichhai
  - exit
- Xem dấu vân tay của các host từ xa đã nhận dạng trên máy cục bộ
  - $ssh-keygen -l -f ~/.ssh/known_hosts

    2048 cf:4a:87:66:38:2c:46:ca:2c:86:39:d5:eb:c6:a8:32

Thực hành

- Cài đặt OpenSSH server trên Ubuntu Server
- Cho biết dấu vân tay của ssh server là gì
- Đăng nhập vào một máy trạm ubuntu với tài khoản **student**
- Đăng nhập từ xa vào Ubuntu Server tài khoản user1
  - Kiểm tra dấu vân tay lưu trong máy trạm có trùng khớp với dấu vân tay của ssh server không
  - Tạo thư mục ~/.ssh

Hãy nhớ

Truy cập đến SSH Server nào thì phải khai báo tài khoản (username/password) trên server đó !

Copy từ xa

- scp user1@source-host:path-to-file
  user2@destination-host:path-to-file
- Ví dụ: Chép tập tin my-file trong thư mục hiện hành của người dùng vào thư mục data trong home của người dùng nbhung trên máy tính có địa chỉ ip là remote-host-ip:
  - scp my-file nbhung@remote-host-ip:~/data/

Thực hành

- Tạo tập tin có tên là mydata trên máy Ubuntu Desktop
- Sử dụng lệnh scp để chép tập tin này lên home của người dùng user1 trên server Ubuntu của bạn.
- Tạo tập tin là tên của bạn, copy tập tin này lên thư mục **~/nhom1** của người dùng **user1** (password=user1) trên server có địa chỉ **172.30.102.250**.

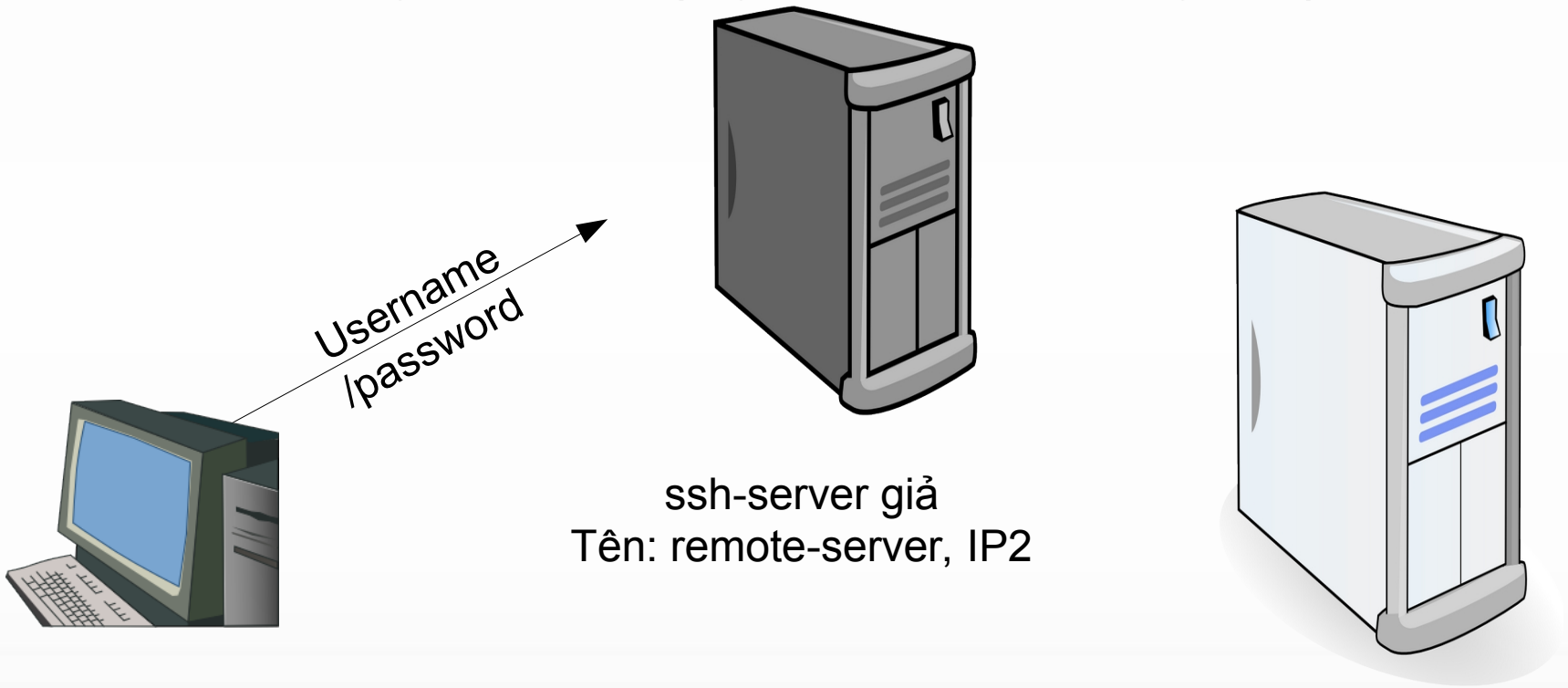
Bài giải

- touch ~/Desktop/mydata
- scp ~/Desktop/mydata user1@ip-server:~/

- touch ~/Desktop/your-name
- scp ~/Desktop/your-name user1@ip-server:~/nhom1/

Chứng thực ssh server

- Để tránh giả danh (người thứ ba ở giữa)



Chứng thực DSA

- Trên máy Ubuntu Desktop
- Tạo cặp public key – private key bằng lệnh
  - ssh-keygen -t dsa
  - ssh-keygen -t dsa -C "rusername@remoteIP -p port"
    - Thư mục/File mặc định chứa cặp khóa
      - /home/user1/.ssh/id_dsa.pub, /home/user1/.ssh/id_dsa
    - Nhập passphrase để bảo vệ khóa cá nhân
- Copy public key lên remote server và nối vào tập tin /home/user1/.ssh/authorized_keys
  - Đặt quyền 600 trên ~/.ssh/authorized_keys

Thực hành

- Mở terminal trên Ubuntu Desktop
- Tạo bộ khóa công khai và cá nhân cho user1
  - ssh-keygen -t dsa "-C user1@**172.16.23.(100+X)"**
- Đánh lệnh ssh-add
- Copy lên khóa công khai lên Ubuntu Server
  - **ssh-copy-id user1@172.16.23.(100+X)**
- Đăng nhập từ xa vào Ubuntu Server với tài khoản user1 từ máy trạm Ubuntu
  - **ssh user1@172.16.23.(100+X)**

Copy khóa công khai lên server

- Từ máy Ubuntu Desktop
  - cd ~/.ssh
  - scp id_dsa.pub user1@ssh-server:~/.ssh/user1_pub_key
- Trên Ubuntu server
  - Login vào user1
  - cd .ssh
  - touch authorized_keys
  - cat user1_pub_key >> authorized_keys

Cấu hình OpenSSH Server

- Tập tin cấu hình /etc/ssh/sshd_config
  - Port new-port-number
- Khởi động lại ssh server sau khi thay đổi cấu hình
  - **sudo systemctl restart sshd.service**
  - sudo service ssh restart
  - (sudo /etc/init.d/ssh restart)

Thực hành

- Hãy đổi cổng của ssh server thành 2222
- Khởi động lại ssh server
- Thử đăng nhập từ xa vào Ubuntu server với cổng 2222

Bài tập

- Tham khảo thêm về lệnh ssh và scp
  - ssh –help
  - man ssh
  - scp –help
  - man scp

Một số tài liệu tham khảo

- http://support.suso.com/supki/SSH_Tutorial_for_Linux
- http://kimmo.suominen.com/docs/ssh/
- http://www.inetdaemon.com/tutorials/internet/ssh/
- http://www.snailbook.com/