# Bài 11: Hướng dẫn cấu hình bảo mật ssh server

[chipchip](http://echip.pro/author/chipchip/) 30/12/2016 [Linux](http://echip.pro/category/linux/) [Đăng bình luận](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#respond) 732 Lượt xem

* [1 Giới thiệu.](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Gioi_thieu)
* [2 Thực hiện bảo mật SSH server.](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Thuc_hien_bao_mat_SSH_server)
* [3 Ưu điểm.](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Uu_diem)
* [4 Nhược điểm.](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Nhuoc_diem)
* [5 Hỏi đáp.](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Hoi_dap)
* [6 Bài viết khác trong cùng Series:](http://echip.pro/2016/12/30/bai-11-huong-dan-cau-hinh-bao-mat-ssh-server/#Bai_viet_khac_trong_cung_Series)

## **Giới thiệu.**

Chào các bạn! Trong [**bài trước**](http://echip.pro/2016/12/29/bai-10-huong-dan-su-dung-ssh-de-dieu-khien-may-chu-tu-xa/) mình đã giới thiệu về **SSH server** và các sử dụng đơn giản. Hôm nay mình sẽ hướng dẫn các bạn cấu hình bảo mật **SSH server**.

Chúng ta sẽ gây khó khăn cho các hacker bằng cách:

* Không cho **root** đăng nhập thông qua **SSH**.
* Thay đổi **port** mặc định của **SSH** để tránh dò quét.
* Sử dụng phương pháp xác thực bằng khóa công khai thay cho **user / password**.

Và để làm được những điều trên chúng ta cần biết:

* File cấu hình chính của **SSH server** nằm ở **/etc/ssh/sshd\_config**.
* Thư mục lưu các khóa xác thực nằm ở **~/.ssh/**.

## **Thực hiện bảo mật SSH server.**

**Bước 1**: Sử dụng trình soạn thảo bất kỳ **vi/vim**, **nano** chỉnh sửa file cấu hình **/etc/ssh/sshd\_config**.

Shell



|  |  |
| --- | --- |
| 1 | sudo nano /etc/ssh/sshd\_config |

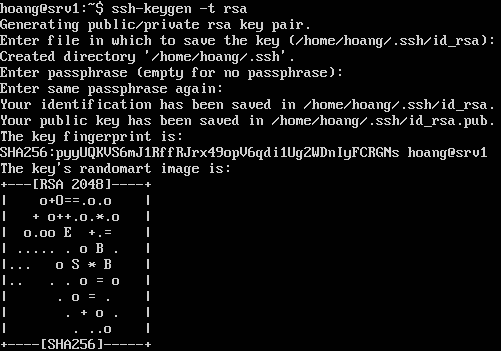
* Tại **dòng thứ 5** ta thay đổi giá trị **Port** mặc định là **22**, có thể thay là **2222** tùy bạn.
* Tại **dòng thứ 9** ta đảm bảo là đang sử dụng**Protocol 2**. Vì phiên bản cũ hơn bị lỗi bảo mật.
* Tại **dòng thứ 28** ta set **PermitRootLogin no** để không cho **root** kết nối từ **SSH**.
* Tại **dòng thứ 52** ta bỏ dấu**#** đầu dòng sau đó cho giá trị **PasswordAuthentication no**. Để tắt chức năng xác thực bằng mật khẩu.

**Bước 2**: Ta tiến hành tạo mã khóa bằng cách gõ lệnh:



|  |  |
| --- | --- |
| 1 | ssh-keygen -t rsa |

* Ở dòng **Enter file in which to save the key** bạn để mặc định nhấn enter.
* Ở dòng **Enter passphrase** bạn có thể điền ngẫu nhiên gì cũng được hoặc để trống enter luôn.

[](https://i0.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey1.png)

**Bước 3**: Ta đổi tên public key từ **id\_rsa.pub** thành **authorized\_keys** và tiến hành **chmod 600** cho nó.

[https://i0.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey2.png?resize=461%2C34](https://i2.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey2.png)

**Bước 4**: Ta copy **private key** của **SSH server** về máy **Ubuntu Desktop** bằng cách mở **terminal**trên **Ubuntu Desktop** và gõ lệnh sau:

[](https://i1.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey4.png)

**Bước 5**: Restart**SSH server** bằng lệnh:

Shell



|  |  |
| --- | --- |
| 1 | sudo systemctl restart ssh |

[https://i2.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey6.png?resize=618%2C51](https://i0.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey6.png)

**Bước 6**: Test thành quả nãy giờ thôi…

Ta thử kết nối **SSH** theo cách thông thường bằng cách gõ lệnh:

Shell



|  |  |
| --- | --- |
| 1  2 | hoang@echip-desktop:~$ ssh 192.168.1.9  ssh: connect to host 192.168.1.9 port 22: Connection refused |

Sẽ nhận được lỗi **connection refused**.

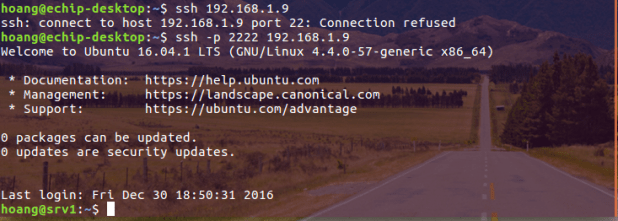
Thử kết nối bằng cách thêm option**-p 2222**:

Shell



|  |  |
| --- | --- |
| 1 | hoang@echip-desktop:~$ ssh -p 2222 192.168.1.9 |

Ta sẽ được **login** vào thẳng **user hoang** mà không cần điền mật khẩu nữa.

[](https://i2.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey5.png)

## **Ưu điểm.**

Những thiết lập trên phần nào khiến cho hacker gặp khó khăn hơn khi cố tình hack server của bạn.

* Việc thay đổi port mặc định sẽ gây khó khăn cho việc dò quét được cổng kết nối **SSH**.
* Thay đổi cơ chế xác thực người dùng từ **user / password** thành **khóa công khai** và ngăn user **root** đăng nhập qua **SSH** loại trừ khả năng bị **đoán mật khẩu** và **Brute Force Attack**.

## **Nhược điểm.**

Tuy nhiên nó cũng gây khó khăn cho chính bạn luôn vì từ giờ chỉ ai có cái key **id\_rsa** mới **SSH** vào server được.

Trong trường hợp:

* Bạn làm mất cái key**id\_rsa** nằm trong máy **Desktop** của bạn (lỡ tay xóa, cài lại hệ điều hành…) thì phải chạy lên máy chủ copy lại.
* Bạn muốn nhờ một người khác cài đặt, thiết lập dùm hệ thống thì phải copy cái key này đưa cho người đó.

## **Hỏi đáp.**

**Khóa id\_rsa có khả năng bị đánh cắp không?**

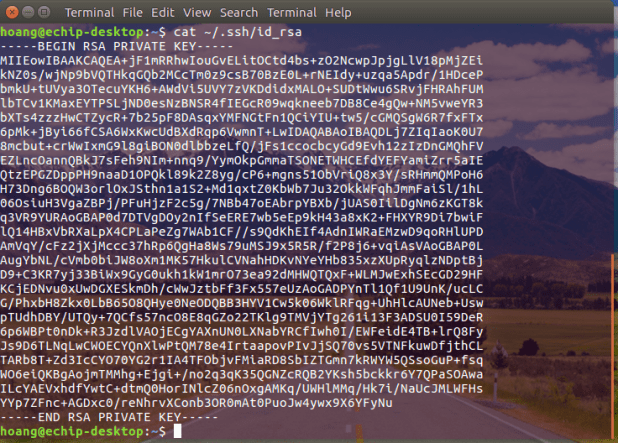
**Trả lời**: Có nhưng mà khó và hiếm. Ví dụ như họ ôm được **Laptop** hoặc **Desktop** của bạn về thì họ thành công.

**Hacker có thể tạo ra khóa id\_rsa giống của mình để đăng nhập trái phép không?**

**Trả lời**: Không thể tạo ra 1 file **id\_rsa** có nội dung giống y chang của bạn được.

**Khóa id\_rsa có nội dung gì?**

**Trả lời**: Bạn có thể xem nội dung file **id\_rsa** bằng lệnh **cat**.

[](https://i2.wp.com/echip.pro/wp-content/uploads/2016/12/sshkey7.png)

## **Bài viết khác trong cùng Series:**