**Trường Đại học Thủy Lợi**

**Bộ môn Công nghệ thông tin**

****

**Đề tài: Tìm hiểu và triển khai cấu hình bảo mật SSH server trên Linux**

**Môn: Linux và mã nguồn mở**

**Giảng viên: Kiều Tuấn Dũng**

**Nhóm L25**

**1, Danh sách thành viên và công việc.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Họ và tên** | **Mã SV** | **Công việc** | **Tiến độ** |
| Nguyễn Duyên Mạnh | 175A071275 | -Tìm hiểu về cấu hình bảo mật SSH server trên Linux.  -Hướng dẫn cài đặt và bảo mật. | Hoàn thành |
| Nguyễn Thùy Linh | 175A071621 | -Cài đặt demo. |  |

**2, Nội dung nghiên cứu( tài liệu được thao khảo qua trang digitalocean.com):**

**A, Giới thiệu về SSH:**

**Khái niệm về giao thức SSH( secure shell):** Là một giao thức mạng dùng để thiết lập kết nối giữa Client và Server/VPS, giúp các quản trị viên truy cập máy chủ từ xa một cách an toàn. **SSH dùng mật khẩu để xác thực người** **dùng** trong một phiên kết nối giữa client và server. SSH hoạt động ở tầng thứ 4 trong mô hình TCP/IP. Tuy nhiên khả năng bảo mật không cao tiểm ẩn nhiều rủi rõ, đặc biệt khi làm việc với hệ thống [LAMP Stack](https://www.thuysys.com/tag/lemp-server) hay [LEMP Stack](https://www.thuysys.com/tag/lemp-server).

**SSH** làm việc thông qua 3 bước đơn giản:

* **Định danh host** - xác định định danh của hệ thống tham gia phiên làm việc SSH.
* **Mã hoá** - thiết lập kênh làm việc mã hoá.
* **Chứng thực** - xác thực người sử dụng có quyền đăng nhập hệ thống.

**Cách SSH hoạt động:**

Để thiết lập kết nối SSH, bạn cần hai thành phần: máy khách và thành phần phía máy chủ tương ứng. Máy khách SSH là một ứng dụng bạn cài đặt trên máy tính mà bạn sẽ sử dụng để kết nối với máy tính khác hoặc máy chủ. Máy khách sử dụng thông tin máy chủ từ xa được cung cấp để bắt đầu kết nối và nếu thông tin đăng nhập được xác minh, sẽ thiết lập kết nối được mã hóa.

Về phía máy chủ, có một thành phần được gọi là SSH daemon liên tục lắng nghe một cổng TCP / IP cụ thể cho các yêu cầu kết nối máy khách có thể. Khi khách hàng khởi tạo kết nối, trình nền SSH sẽ phản hồi với phần mềm và các phiên bản giao thức mà nó hỗ trợ và cả hai sẽ trao đổi dữ liệu nhận dạng của họ. Nếu thông tin đăng nhập được cung cấp là chính xác, SSH sẽ tạo một phiên mới cho môi trường phù hợp.

**Lệnh SSH có 3 phần:**

ssh {user}@{host}

SSH key command cho hệ thống biết là bạn muốn mở một kết nối được mã hóa Secure Shell Connection. **{user}** đại diện cho tài khoản người dùng bạn muốn dùng để truy cập. Ví dụ, bạn muốn truy cập user **root**, thì thay root tại đây. User root là user quản trị hệ thống với toàn quyền để chỉnh sửa bất kỳ điều gì trên hệ thống. **{host}** đại diện cho máy tính bạn muốn dùng để truy cập. Nó có thể là một địa chỉ IP**(ví dụ 244.235.23.19)** hoặc một tên miền (ví dụ, www.xyzdomain.com).

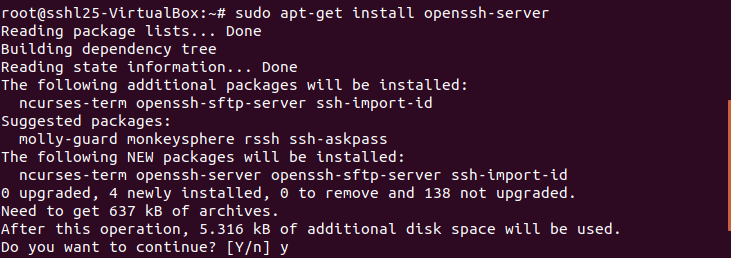
Khi bạn nhấn enter, nó sẽ hỏi bạn nhập mật khẩu tương ứng cho tài khoản. Khi bạn gõ, bạn sẽ không thấy bất kỳ dấu hiệu nào trên màn hình, nhưng nếu bạn gõ đúng mật khẩu và nhấn enter, bạn sẽ vào được hệ thống và nhận thông báo đăng nhập thành công.

**B, Cài đặt SSH server qua Ubuntu Desktop và tiến trình bảo mật:**

Tải về SSH server bằng dòng code dưới đây bằng quyền root:

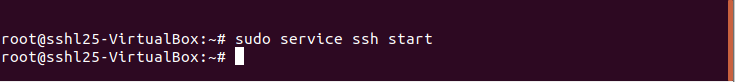
[root@fw:~]# sudo apt-get install openssh-server

[root@fw:~]# apt-get install openssh-server openssh-client



Sau khi tải về xong chúng ta dùng lệnh dưới để chạy SSH server

sudo service ssh start



Khi bạn thay đổi gì ở phần **/etc/ssh/sshd\_config hãy gõ lệnh sau để khởi động lại ssh:**

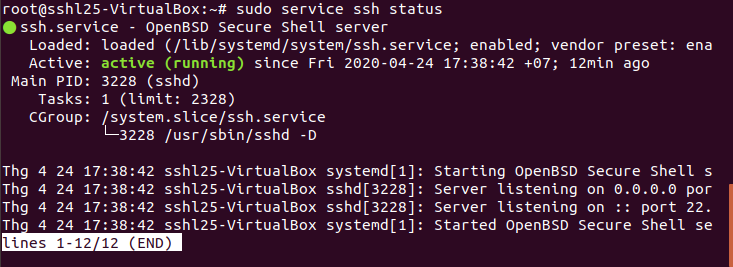
sudo service ssh restart



Để kiểm tra SSH mà chúng ta cài đã chạy hay chưa thì ta dùng:

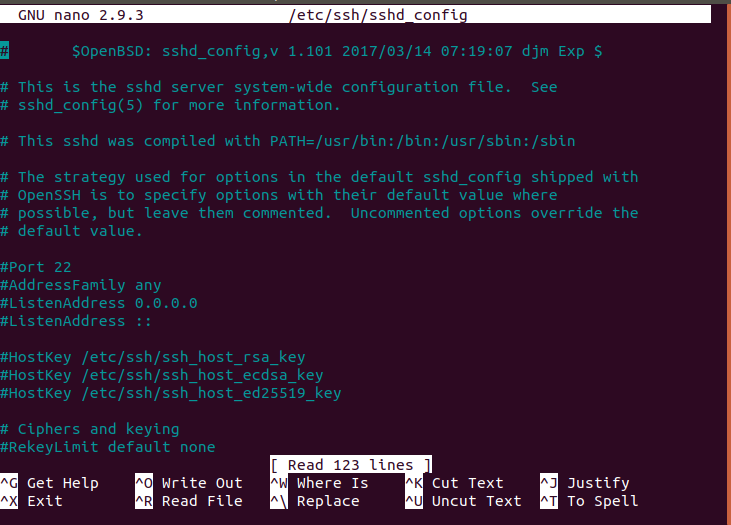
sudo service ssh status

Hiển thị **active (running)** có nghĩa là nó đang chạy.



Để thay đổi cấu hình ssh:

Sudo nano /etc/ssh/sshd\_config



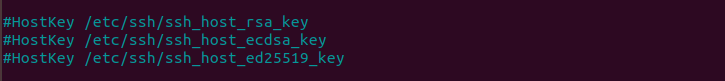
Cổng kết nối mặc định là 22:



Số lần đăng nhập tối đa là 6 lần:



Thay đổi cổng kết nối:



Ở dưới đây lần lượt là

LoginGraceTime: Thời gian đăng nhập.

PermitRootLogin: Root có thể đăng nhập hay không.

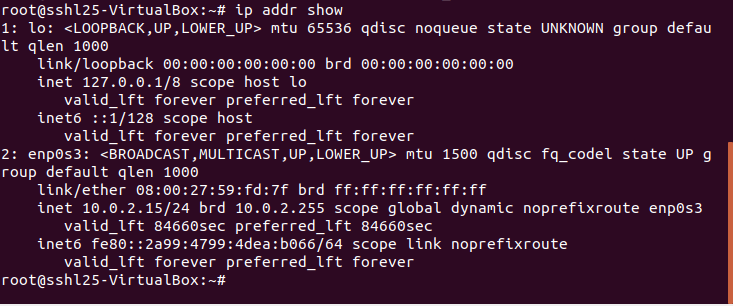
StrictModes:  từ chối một nỗ lực đăng nhập nếu mọi người đều có thể đọc được các tệp xác thực.( Điều này ngăn các nỗ lực đăng nhập khi các tệp cấu hình không an toàn.).



**Kết nối SSH với windows và với Ubuntu server:**

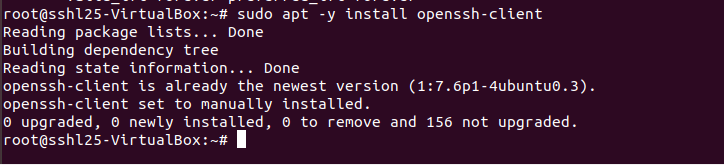
Trước hết chúng ta kiểm tra IP của máy:

Ip addr show

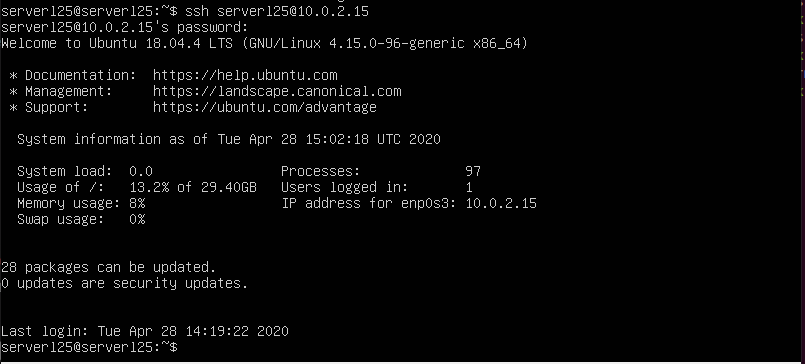


Cài đặt cấu hình SSH client cho Ubuntu:

Sudo atp –y install openssh-client



Kết nối với server thao tác như dưới:



**Sử dụng đăng nhập SSH bằng khóa(tang tính năng bảo mật):**

+Xác thực dựa trên khóa hoạt động bằng cách tạo một cặp khóa: khóa *riêng* và *khóa chung* .

+Khóa *riêng* được đặt trên máy khách và được bảo mật và giữ bí mật.

+Khóa *công khai* có thể được trao cho bất kỳ ai hoặc được đặt trên bất kỳ máy chủ nào bạn muốn truy cập.

+Khi bạn cố gắng kết nối bằng cặp khóa, máy chủ sẽ sử dụng khóa chung để tạo một thông báo cho máy khách chỉ có thể được đọc bằng khóa riêng.

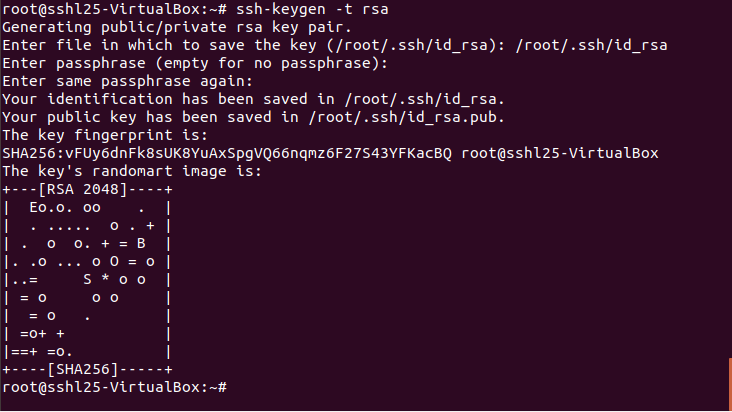
+Sau đó, máy khách sẽ gửi phản hồi thích hợp trở lại máy chủ và máy chủ sẽ biết rằng máy khách là hợp pháp.

Tạo khóa ssh:

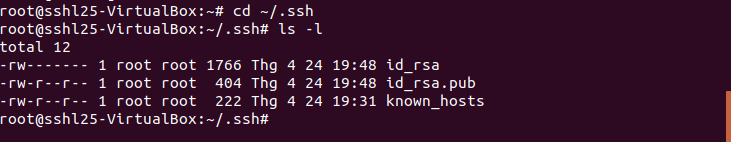
Nhập câu lệnh để thiết lập khóa:

Ssh-keygen –t rsa

Khóa của bạn được tạo tại /root/.ssh/id\_rsa



Thực hiên câu lệnh di chuyển đến ~/.ssh và kiểm tra quyền của nó bằng ls –l:



Như bạn có thể thấy, tập tin **id\_rsa** chỉ có thể đọc và ghi được cho chủ sở hữu. Đây là cách nó nên được giữ bí mật.

Các tập tin **id\_rsa.pub** có thể được chia sẻ và có quyền truy cập thích hợp cho hoạt động này.

**Bảo mật:**

Để tăng tính năng bảo mật chúng ta truy cập vào cấu hình ssh để chỉnh sửa:

Sudo nano /etc/ssh/sshd\_config

Tạo khóa để đăng nhập với cách trình bày ở trên ta vừa thực hiện.

Giao thức SSH 1 (SSH1) chứa nhiều lỗ hổng bảo mật. Thay vào đó, sử dụng giao thức 2 (SSH2) được khuyến khích.

Theo mặc định, SSH2 nên được đặt. Nếu không thì thay đổi dòng **Giao thức** để sử dụng SSH2.



Sử dụng danh sách trắng để cho phép người dùng cụ thể truy cập SSH và danh sách đen không cho phép người dùng khác, sẽ cải thiện bảo mật SSH của bạn.(nameuser1 và nameuser2 là tên tài khoản cụ thể.)



Vô hiệu hóa đăng nhập bằng root:



Ẩn người dùng đăng nhập cuối:



Theo mặc định, SSH sẽ chấp nhận các kết nối từ bất kỳ địa chỉ IP bên ngoài nào. Nếu bạn muốn hạn chế SSH chỉ cho phép kết nối từ một địa chỉ IP cụ thể, bạn có thể thêm một dòng **ListenAddress** .

Thay đổi ip ở dưới thành một ip cụ thể:



Vô hiệu hóa xác thực bằng mật khẩu:

Xác thực mật khẩu trong SSH là một rủi ro bảo mật lớn nếu người dùng của bạn đặt mật khẩu yếu.

Để tắt xác thực mật khẩu, hãy thay đổi dòng **PasswordAuthentication** để đọc:



Theo mặc định, SSH không cho phép rhosts. Các .rhoststệp chỉ định người dùng nào có thể truy cập các lệnh r (như rcpvà rsh) trên hệ thống cục bộ mà không cần mật khẩu.

Để tắt rhosts:



Xác thực dựa trên máy chủ của SSH an toàn hơn rhostsxác thực. Tuy nhiên, các máy chủ đáng tin cậy vẫn được coi là một rủi ro bảo mật.

Theo mặc định, tùy chọn **HostbasingAuthentication** bị tắt, nếu không thì thay đổi dòng sau:



"LoginGraceTime" chỉ định khoảng thời gian sau khi yêu cầu kết nối, máy chủ SSH sẽ đợi trước khi ngắt kết nối. Giá trị được đề xuất cho thời gian chờ đăng nhập là 60 giây.

Bạn có thể thay đổi giá trị này bằng cách chỉnh sửa dòng sau:



Giới hạn số lượng kết nối đồng thời tối đa vào daemon SSH có thể giúp bảo vệ máy chủ SSH của bạn khỏi một cuộc tấn công vũ phu.Bạn có thể đặt giá trị này bằng cách chỉnh sửa dòng sau thành số lượng kết nối đồng thời bạn muốn cho phép.



Tin tặc có thể sử dụng kỹ thuật chuyển tiếp cổng tới các kết nối mạng đường hầm thông qua phiên SSH để đăng nhập vào hệ thống.

Để vô hiệu hóa thay đổi này, các dòng sau:



Theo mặc định, SSH ghi lại mọi thứ. Nếu bạn muốn đăng nhập thêm thông tin như các lần đăng nhập thất bại. bạn có thể thay đổi giá trị từ INFO sang VERBOSE.

Đối với điều này thay đổi dòng sau: LogLevel VERBOSE:



Bạn sẽ muốn từ chối đăng nhập cho người dùng bằng mật khẩu trống (trống).

Theo mặc định, tùy chọn này bị vô hiệu hóa, nếu không thì thay đổi dòng sau:



SSH cho phép người dùng đặt khoảng thời gian chờ không hoạt động. Sau khi khoảng thời gian này trôi qua, người dùng nhàn rỗi sẽ tự động đăng xuất.

Bạn có thể đặt số giây bằng cách thêm dòng sau:



Khi bạn đã hoàn tất chỉnh sửa tệp / etc / ssh / sshd\_config, hãy lưu và thoát , sau đó khởi động lại máy chủ SSH:



Trình bao bọc TCP cung cấp kiểm soát truy cập dựa trên máy chủ cho các dịch vụ mạng, được sử dụng để lọc truy cập mạng vào internet.

Bạn chỉ có thể cho phép SSH từ các địa chỉ IP 192.168.1.100 và 172.16.20.10 IP bằng cách chỉnh sửa tệp /etc/hosts.allow.

sshd: 192.168.1.100 172.16.20.10



Thêm dòng sau:



**Kết nối máy thật với máy ảo qua giao thức SSH:**

