**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:**

**A, 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).

Khi mua một VPS Linux hoặc một máy chủ vật lý cài Linux thì sẽ có thông tin đăng nhập thông qua giao thức SSH gồm:

* IP máy chủ
* Tên người dùng đăng nhập, đa phần là root
* Mật khẩu của người dùng, nếu tên người dùng là root thì mật khẩu này được gọi là mật khẩu root.
* Cổng giao tiếp: 22, mặc định SSH sử dụng cổng 22.

**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

**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.

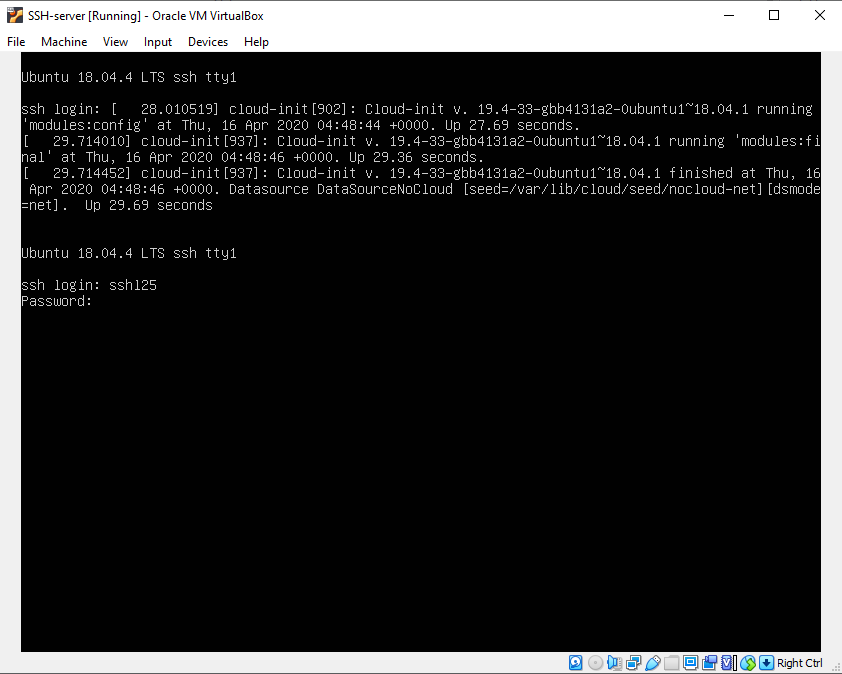
**Ưu điểm của SSH:**

**SSH** có khả năng mã hóa và truyền tải dữ liệu an toàn giữa mạng lưới host và client. Host đại diện cho máy chủ từ xa bạn muốn kết nối tới và client là máy tính của bạn dùng để truy cập tới host.

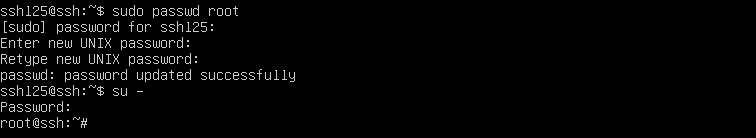
Lợi thế thứ hai là có nhiều cách khác nhau giúp việc mã hóa qua **SSH** được thực hiện hiệu quả và toàn vẹn

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

Bước 1: Cài đặt sẵn Ubuntu server, rồi thực hiện đăng nhập bằng tài khoản:



Bước 2: Tạo root và đăng nhập bằng root:



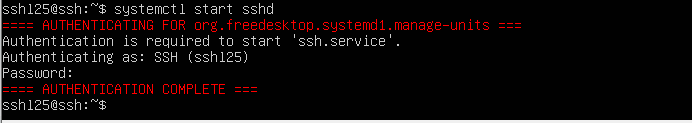
Bước 3: Tải về SSH server bằng dòng code dưới đây bằng quyền root:

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

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

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

systemctl start sshd



Kiểm tra trạng thái của server:

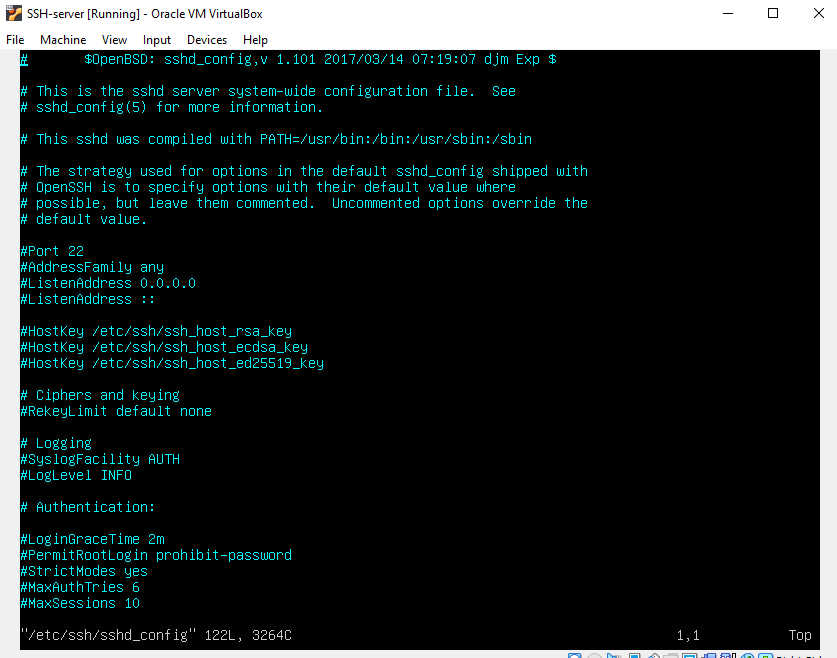
Systemctl status sshd



Bước 4: Tiếp theo chúng ta cấu hình SSH Server bằng cách mở file config ra để thay đổi:

vi /etc/ssh/sshd\_config

Sau khi thao tác dòng trên thì sẽ xuất hiện ra phần dưới:



Chú ý: muốn sửa thì phải bấm i(insert) để thực hiện sửa.

Gõ 3 dòng dưới với:

* Port 22: Cổng mặc định của SSH server.
* PermitRootLogin no: Cho phép user root đăng nhập qua kết nối SSH.
* PasswordAuthentication yes: Cho phép đăng nhập bằng password.



Bước 5: Bước tiếp theo bạn [**kiểm tra tường lửa**](https://www.thuysys.com/providers/vultr/huong-dan-su-dung-chuc-nang-firewall-o-vultr.html) đã cho phép từ ngoài truy cập vào hay chưa. Nếu chưa thì chạy cho mình thêm lệnh bên dưới.

ufw allow 22/tcp



Bước 6: Khởi động lại dịch vụ SSH server lưu lại và thay đổi:

Systemctl restart sshd

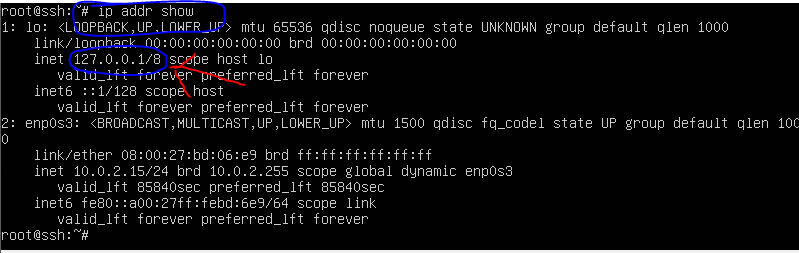


Bước 7, sử dụng SSH Client điều khiển từ xa:

Trước tiên ta cầm tìm địa chỉ ip của Ubuntu server đang dùng bằng cách truy cập root và gõ lệnh:

Ip addr show

Phần inet chính là địa chỉ IP của Ubuntu server mà ta đang dùng: IP( 127.0.0.1/8)



Ta hiển hành cài đặt SSH server trên windows:

Chọn bản phù hợp với máy tính: <https://github.com/PowerShell/Win32-OpenSSH/releases>

Tiến hành cài đặt dịch vụ Open SSH server trên windows

Mở file đã giản nén trên cmd và thực hiện câu lệnh sau để cài đặt

powershell -ExecutionPolicy ByPass -File install-sshd.ps1

