**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 hướng dẫn : 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. Khái niệm vè giao thức SSH:**

Secure Shell (SSH) là một giao thức mạng mật mã cung cấp chức năng mã hóa giữa và máy khách và máy chủ. Nó thay thế các máy khách mạng không bảo mật trước đây trong môi trường mạng.

SSH dùng mật khẩu để xác thực người dùng trong một phiên kết nối giữa client và server.

SSH server là máy chủ của chúng ta, với máy chủ chạy hệ điều hành Linux ta cần cìa openssh-server

SSH Client : là máy muốn truy cập vào SSH server của chúng ta, trên Linux có openssh-client

**b. Chức năng cụ thể của giao thức SSH:**

Dịch vụ được tạo ra nhằm thay thế cho trình Telnet vốn không có mã hóa và sử dụng kỹ thuật cryptographic để đảm bảo tất cả giao tiếp gửi tới và gửi từ server từ xa diễn ra trong tình trạng mã hóa. Nó cung cấp thuật toán để chứng thực người dùng từ xa, chuyển input từ client tới host, và relay kết quả trả về tới khách hàng.

**c. Cách SSH hoạt động:**

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

* Định danh host: Xác định danh tính của hệ thống tham gia phiên làm việc SSH
* Mã hóa: Thiết lập kênh làm việc mã hóa
* 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}**

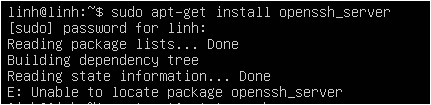
SSH key command cho hệ thống biết là bạn muốn mở một kết nối được mã hóa Secure Shell Connection. **{user}** đại diện cho tài khoản người dùng bạn muốn dùng để truy cập. Ví dụ, bạn muốn truy cập user **root**, thì thay root tại đây. User root là user quản trị hệ thống với toàn quyền để chỉnh sửa bất 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.

**d. Hướng dẫn cài đặt SSH server trên Ubuntu Desktop**

- Để cài đặt openssh-server, ta chạy dòng lệnh:

Sudo apt-get install openssh-server



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

Sudo service ssh start



- Để kiểm tra dịch vụ SSH đã chaỵ hay chưa, ta dùng lệnh:

Systemctl status ssh



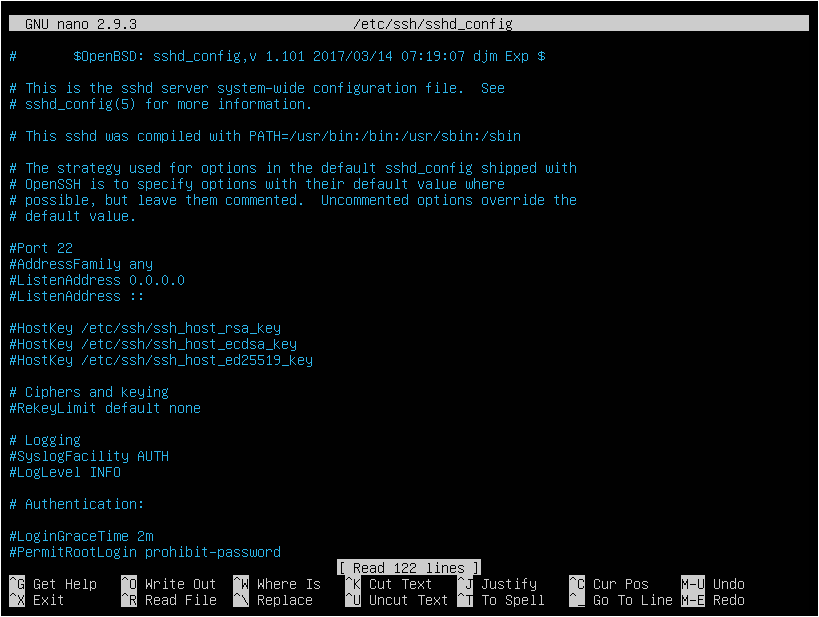
Hiển thị active (running) có nghĩa là nó đang chạy

Việc cài đặt hoàn tất.

**e. Hướng dẫn sử dụng / quản trị:**

**e.1. Thay đổi cấu hình ssh:**

Sudo nano /etc/ssh/sshd\_config



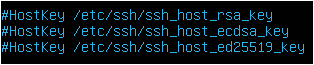
* *Cổng kết nối mặc định là 22:*



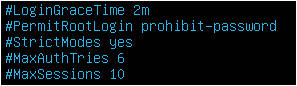
* *Số lần đăng nhập tối đa là 6 lần:*



* *Thay đổi cổng kết nối:*



* *Ở dưới đây lần lượt là:*



LoginGraceTime: Thời gian đăng nhập

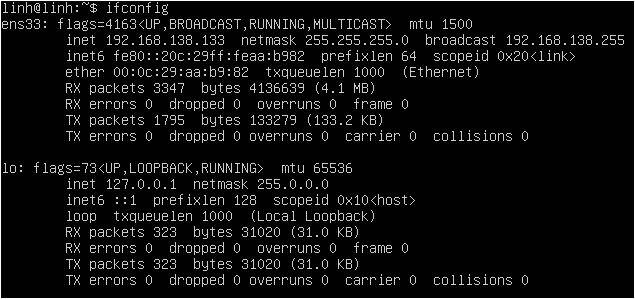
PermitRootLogin: quyền root có thể đăng nhập hay không

StrictModes: từ chối một nỗ lực đăng nhập nếu mọi người có thể đọc được các tệp xác thực.

**e.2. Kết nối SSH với windowa và với Ubuntu Server**

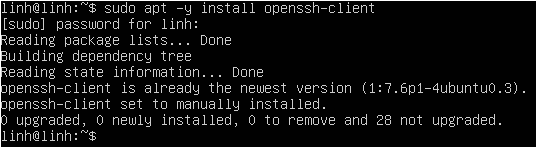
- Trước hết ta kiểm tra IP của máy:

Ifconfig

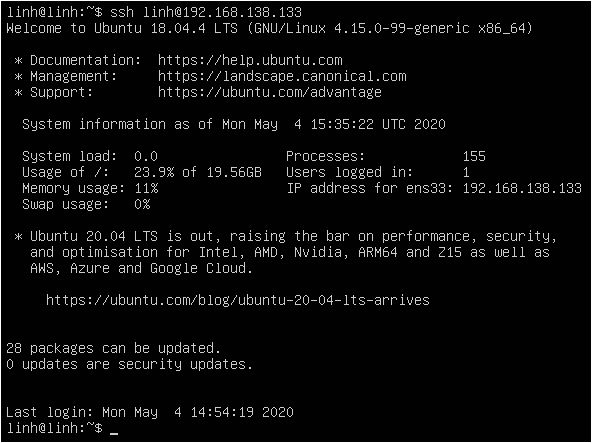


- Cài đặt cấu hình SSH client cho Ubuntu:

Sudo apt –y install openssh-client



- Kết nối với server thao tác như dưới:



**e.3. Bảo mật tệp cấu hình SSH**

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

Sudo nano /etc/ssh/sshd\_config

* Sử dụng SSH2:

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.



Vô hiệu hóa đăng nhập gốc:

Một cuộc tấn công phổ biến là cố gắng sử dụng root để đăng nhập vào máy chủ bằng SSH. Vì đây là một rủi ro bảo mật lớn, hãy vô hiệu hóa đăng nhập SSH gốc bằng cách thay đổi PermitRootLogin từ không có mật khẩu thành:



* Ẩn lần đăng nhập cuối cùng

Bạn có thể ẩn người dùng đăng nhập cuối cùng bằng cách chỉnh sửa dòng sau:



* Hạn chế đăng nhập SSH vào địa chỉ IP cụ thể

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.

Ví dụ: nếu bạn muốn chỉ chấp nhận kết nối SSH từ địa chỉ IP 192.168.1.2, bạn sẽ thêm dòng:



* Vô hiệu hóa xác thực mật khẩu

Xác thực mật khẩu trong SSH là một rủi ro bảo mật lớn nếu người dùng của bạn đặt mật khẩu yếu. Xem phần này để biết hướng dẫn về cách thiết lập xác thực khóa SSH.

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



* Vô hiệu hóa .Rhosts
* Vô hiệu hóa Rhosts:

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

Để vô hiệu hóa rhosts:



* Vô hiệu hóa xác thực dựa trên máy chủ

Xác thực dựa trên máy chủ của SSH an toàn hơn xác thực rhosts. 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:



* Đặt thời gian chờ đăng nhập Grace

"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: 

* Đặt kết nối khởi động tối đa

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. Trong ví dụ này, chúng tôi đã chọn 2:



* Vô hiệu hóa chuyển tiếp

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:



* Đăng nhập thêm thông tin

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:



* Vô hiệu hóa mật khẩu trống

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:



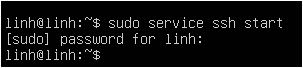
* Đặt khoảng thời gian chờ nhàn rỗi

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:



**e.3. Bảo mật kết nối SSH bằng cách trao đổi khóa để tăng tính bảo mật:**

*- Các thành phần của SSH Key:*

* Gồm 3 thành phần:

Private Key: có dạng file chứ chuỗi mã hóa được lưu trên Client, cần phải bảo mật file này cẩn thận để lấy lại Public Key

Public Key: cũng là dạng file chứ chuỗi mã hóa được lưu trên Server

Passphrase: là mật khẩu dùng để nhận diện Public Key và Private Key khi tạo SSH connection, cũng như để lấy lại Public Key

*- Cách làm việc của SSH Key:*

* Quá trình hình thành kết nối SSH sử dụng Key sẽ trải qua nhiều lớp xác thực khác nhau.
* Đầu tiên, khi SSH Client khởi tạo kết nối bạn phải nhập vào Passphrase để kiểm tra xem Private Key & Public Key có phải là một cặp hay không.
* Tiếp theo chúng sẽ được so sánh với nhau theo thuật toán riêng xem có khớp hay không. Nếu ok người dùng phải nhập đúng tài khoản được cấp trên SSH Server tương ứng với cặp khóa này. Khi đó kết nối mới được khởi tạo để bắt đầu phiên làm việc.

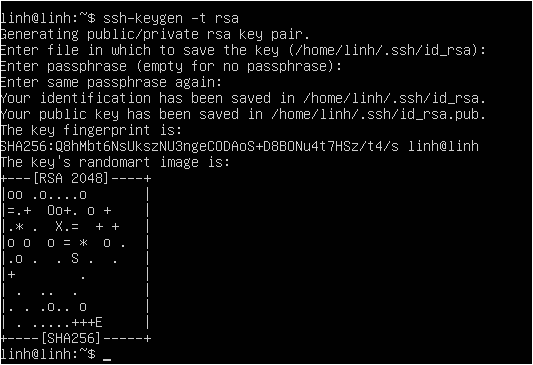
***-****Tạo private key và public key:*

Linux: dùng ssh-keygen tạo khóa, công cụ này có sẵn nên chúng ta có thể sử dụng luôn

Tạo cặp khóa cho mỗi người dùng, vì vậy hãy đăng nhập với một người dùng chung và làm việc như sau:

Ssh-keygen –t rsa

-t rsa : chỉ định thuật toán mã hóa là RSA



* Nó sẽ hỏi bạn taọ Pasphrase, nhập vào pasphrase muốn dùng. Quá trình tạo SSH keys trên Linux hoàn tất ta sẽ được hai file:

Id\_rsa: đây là file Private Key

Id\_rsa.pub: đây là file Public Key

* Mặc định mỗi user trên Linux có một Home Directory (profile) có đường dẫn home/user . Khi đăng nhập bằng user nào để tạo sshKey thì cặp khóa sinh ra nằm trong thư mục /home/user/.ssh với dấu chấm đằng trước chỉ định .ssh là thư mục ẩn.

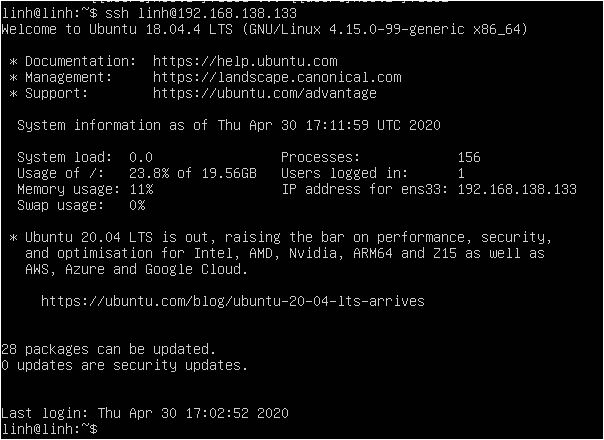
- Cách sử dụng Public Key:

* Theo mô hình ở trên, mặc định Public Key có tên và đường dẫn là : home/linh/.ssh/authorized\_keys trên server









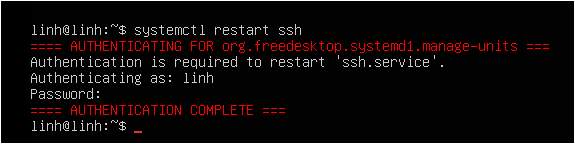
- Cấu hình SSH Key trên Server:

Tìm đến file /etc/ssh/sshd\_config để đặt "PasswordAuthentication no", nó sẽ an toàn hơn :



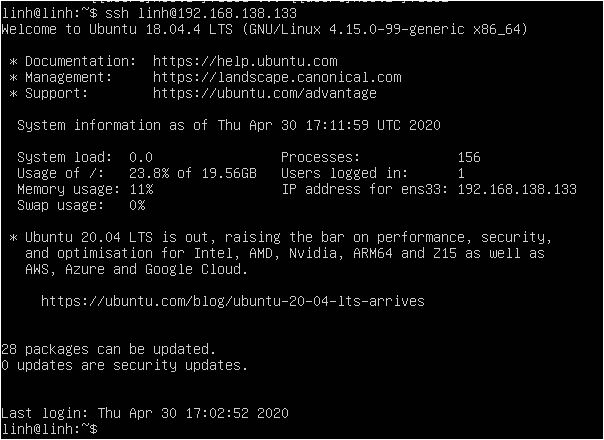


Khởi động lại hệ thống:

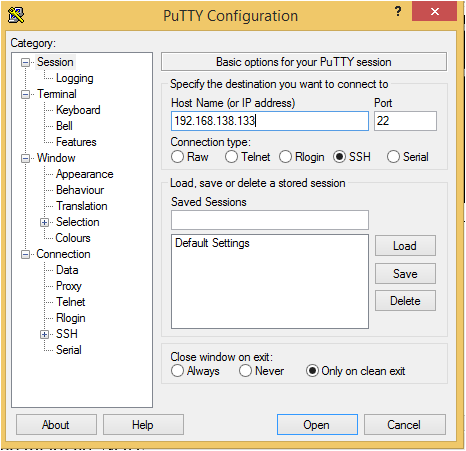
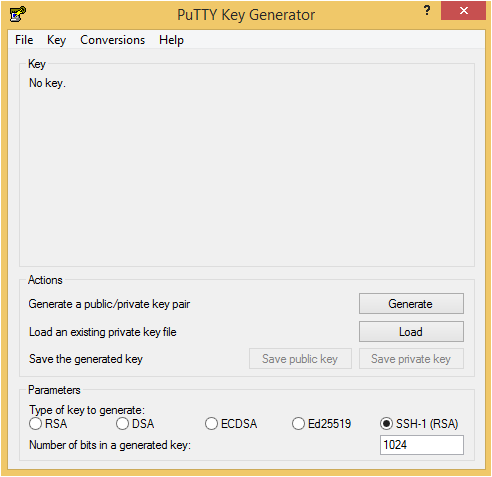


*- Sử dụng Putty để thử đăng nhập bằng SSH Key trên Linux:*

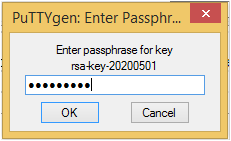
SSH sẽ tự biết lấy private key trong /home/linh/.ssh/id\_rsa trên Client để so sánh tạo kết nối với server



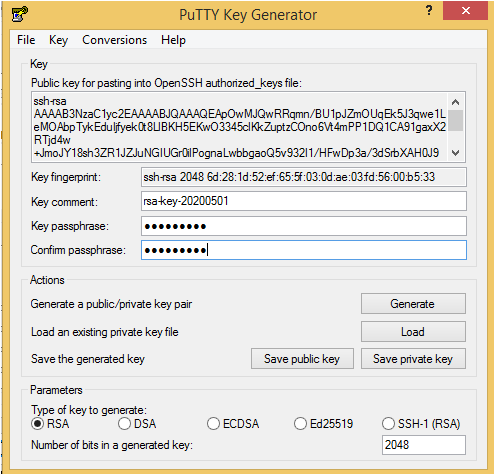
- Sử dụng PuTTy để thử đăng nhập bằng SSH Key trên Window :

* 
* 

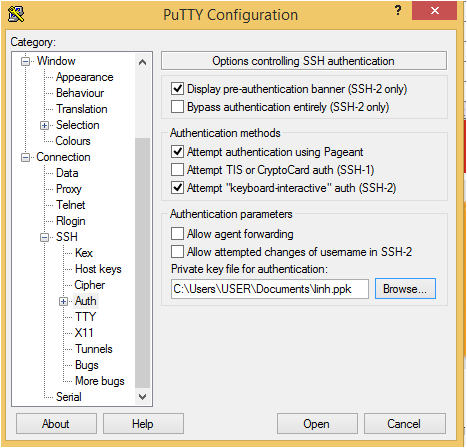
Chỉ định khóa bí mật mà bạn đã tải xuống, sau đó cụm mật khẩu được yêu cầu như sau, hãy trả lời nó.



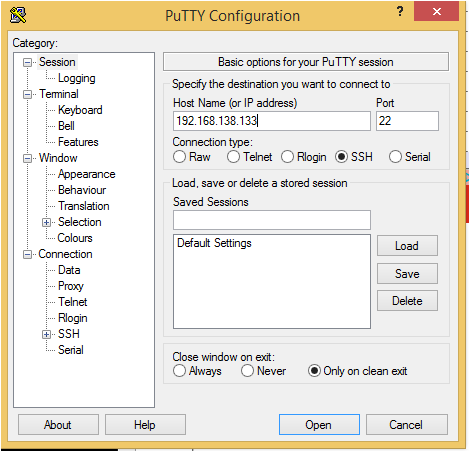
Nhấp vào nút "Save Private Key" để lưu nó trong thư mục bạn thích với bất kỳ tên tệp nào bạn thích.



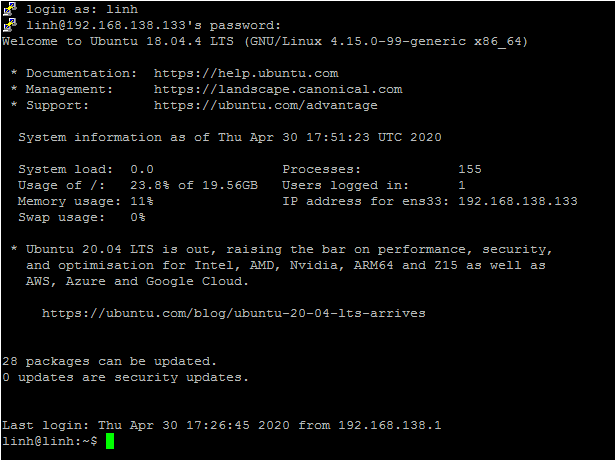
Bắt đầu Putty và mở [Kết nối] - [SSH] - [Auth] trên menu bên trái, sau đó chọn "private\_key" vừa được lưu ở trên.



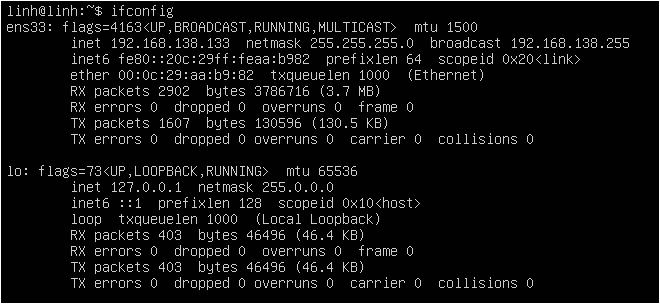
Quay lại [Session] trên menu bên trái và kết nối với máy chủ SSH.

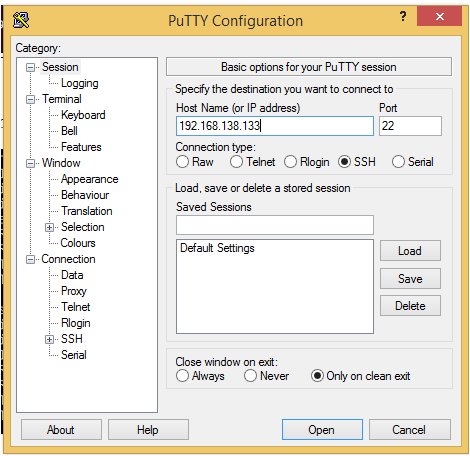


Cụm mật khẩu được yêu cầu để đăng nhập, sau đó trả lời nó. Nếu đúng, bạn có thể đăng nhập bình thường như sau:



**e.4. Kết nối máy thật với máy ảo qua giao thức SSH:**





Nếu hiện ra màn hình đen xì là bạn đã kết nối thành công:

