Giới hạn IP được SSH tới server

Vấn đề

Để giới hạn các IP có thể ssh vào server từ bên ngoài, tránh việc attacker tấn công vào hệ thống, thì trong hướng dẫn này sẽ dùng hosts.allow and hosts.deny để giải quyết việc này.

Mục tiêu

- Giới hạn được các IP được ssh vào server.

- Thêm một lớp limmit ip sau firewall.

Thực hiện

1. Allow SSH

- Mở file **/etc/hosts.allow** để mở cho các IP được phép ssh

1

vi /etc/hosts.allow

- Thêm các IP được ssh, ví dụ:

1

sshd: 10.83.33.77/32, 10.63.152.9/32, 10.12.100.11/28, 10.82.192.0/28

*(Các IP/Range phân tách nhau bởi dấu phẩy "," - lưu ý:****nhớ cho IP của mình vào kẻo bị limmit****)*

2. Deny SSH

- Mở file /etc/hosts.deny để limmit toàn bộ

1

vi /etc/hosts.deny

- Sửa dòng sshd để limmit all

1

sshd: ALL

*(Dòng này là block tất cả - trừ các IP đã allow ở trên)*