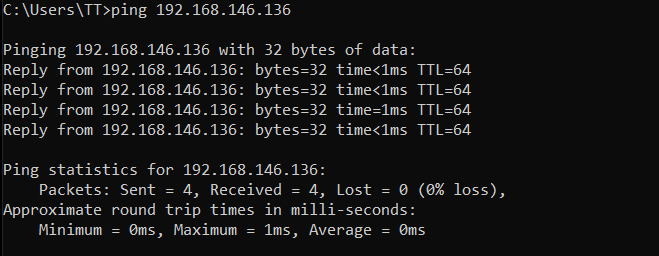
**Lab 6 : Packet filterwith iptables**

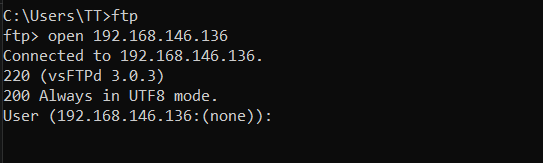
Nguyễn Văn Thắng 17110230

Nguyễn Văn Hà 17110130

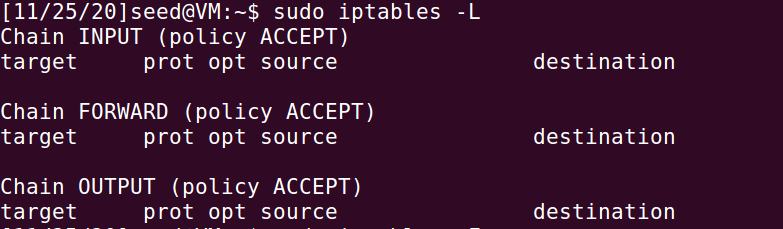
1. **Change the default policy to DROP all access to Ubuntu server,Check the result from either client machines (cannotping, web access, ftp connect..)**

* Trước khi drop

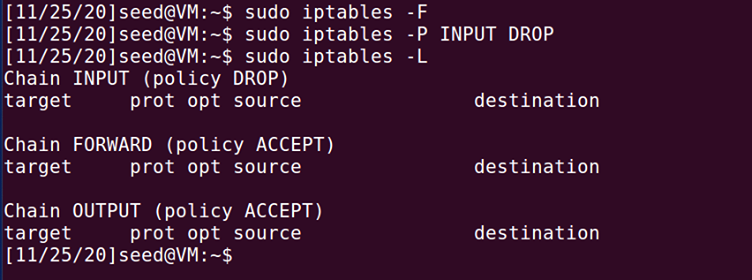




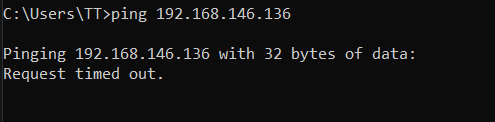
* Kiểm tra chính sách

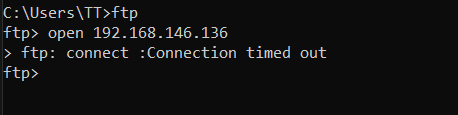


* Thay đổi chính sách chuyển từ accept sang drop để chặn máy client



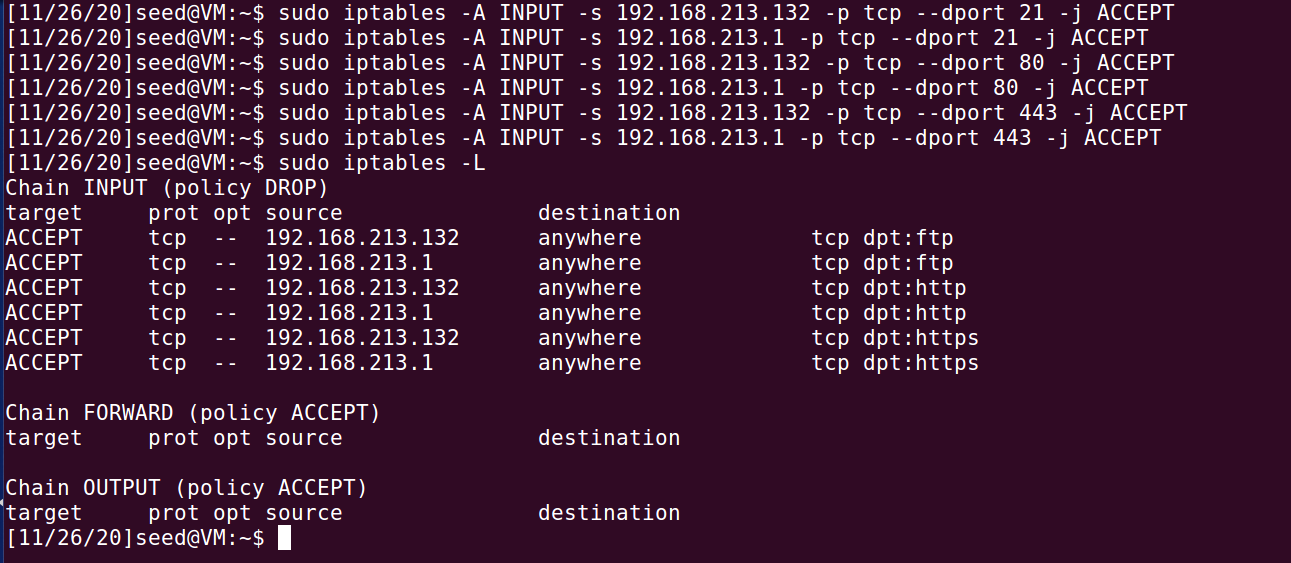
* Kết quả





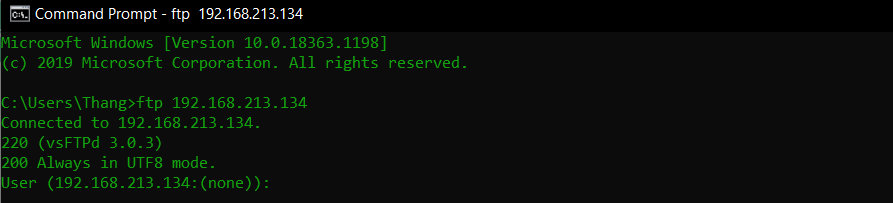
1. **Enable web and ftp access only for both clients**

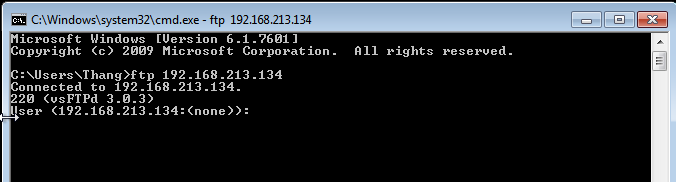
* Như câu a đã drop input thì để thực hiển mở cổng với chỉ 2 client thì ta thực hiện như sau:



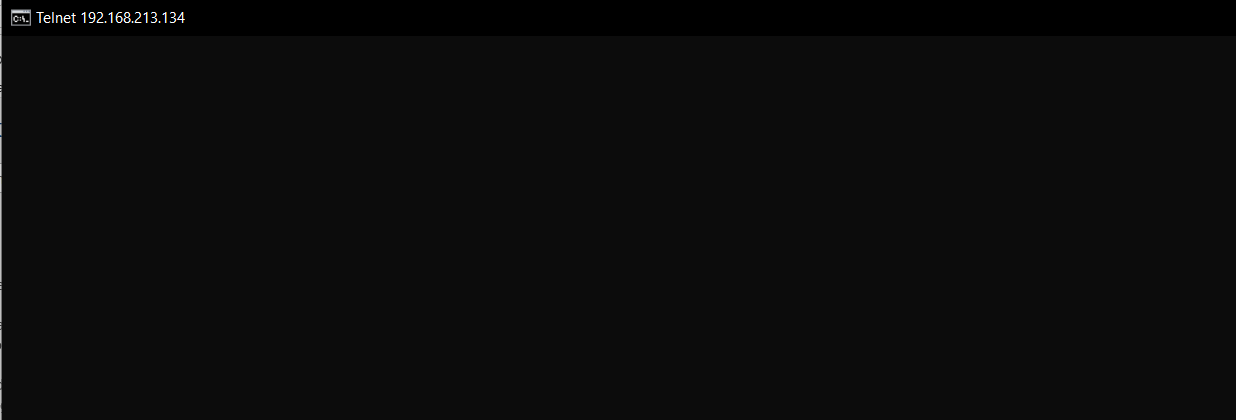
* Kết quả:

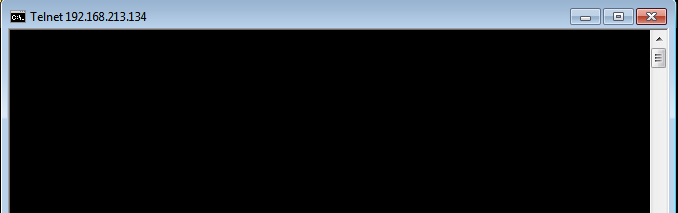
+ ftp





+ http



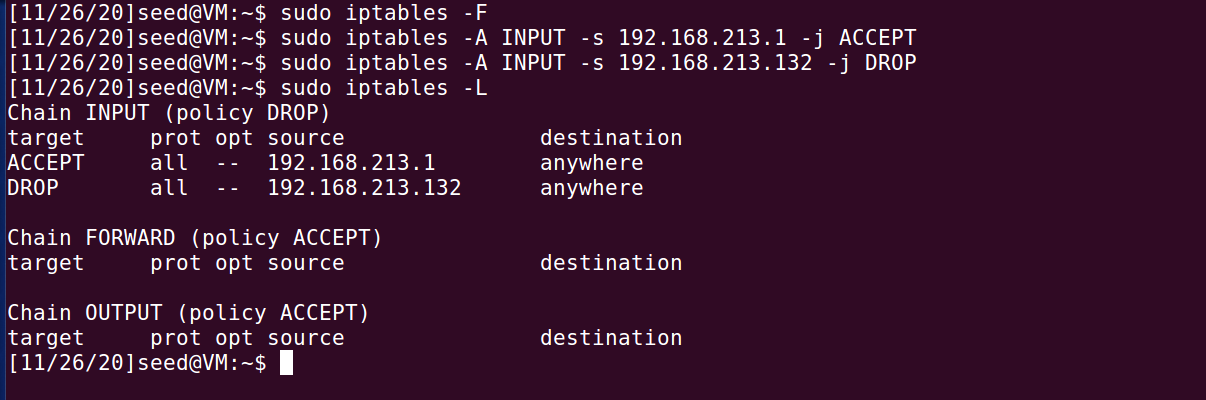


1. **Enable ping only from client 1 by:**

**+ Config DROP packets from client 2 only or**

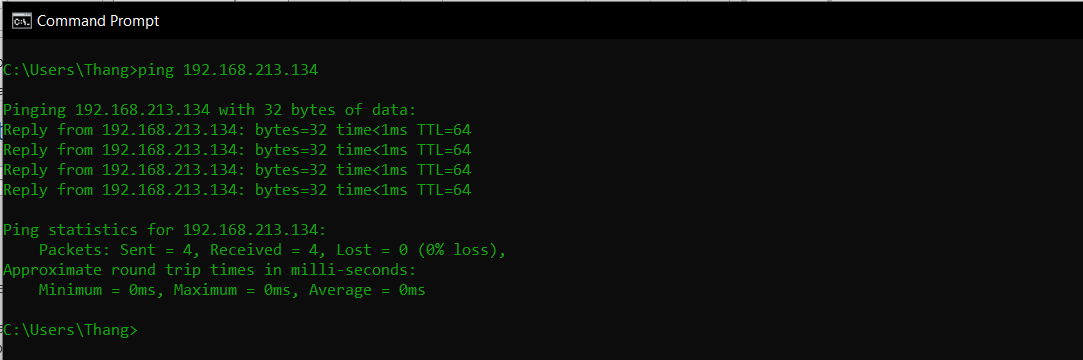
**+ Config DROP packets from subnet where client 2 machine resides by setting up blacklist option.**

* Để đặt chính sách hạn chế với 1 trong 2 client thì ta làm như sau:

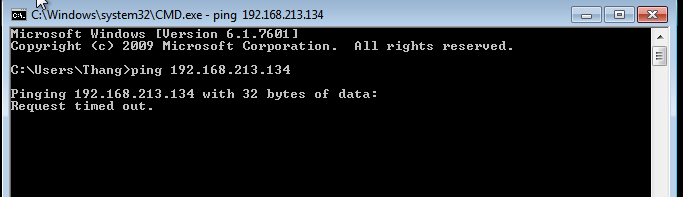


* Kết quả

+ client không hạn chế

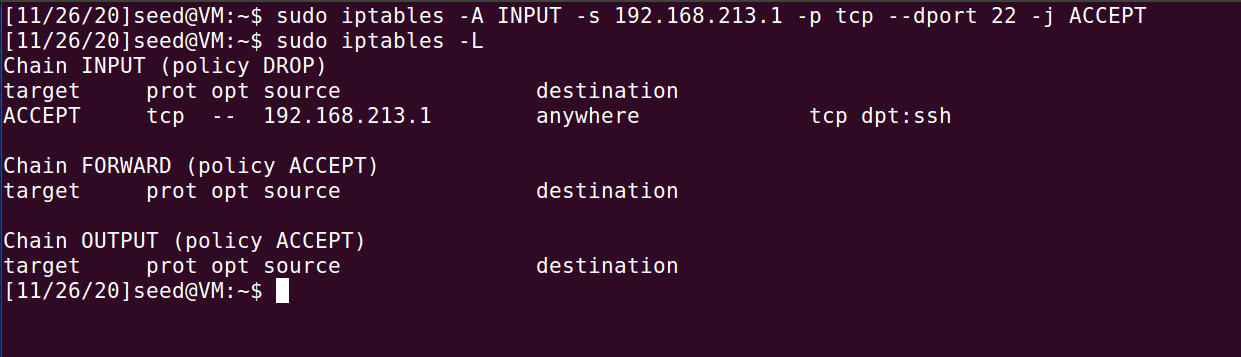


+ Client hạn chế



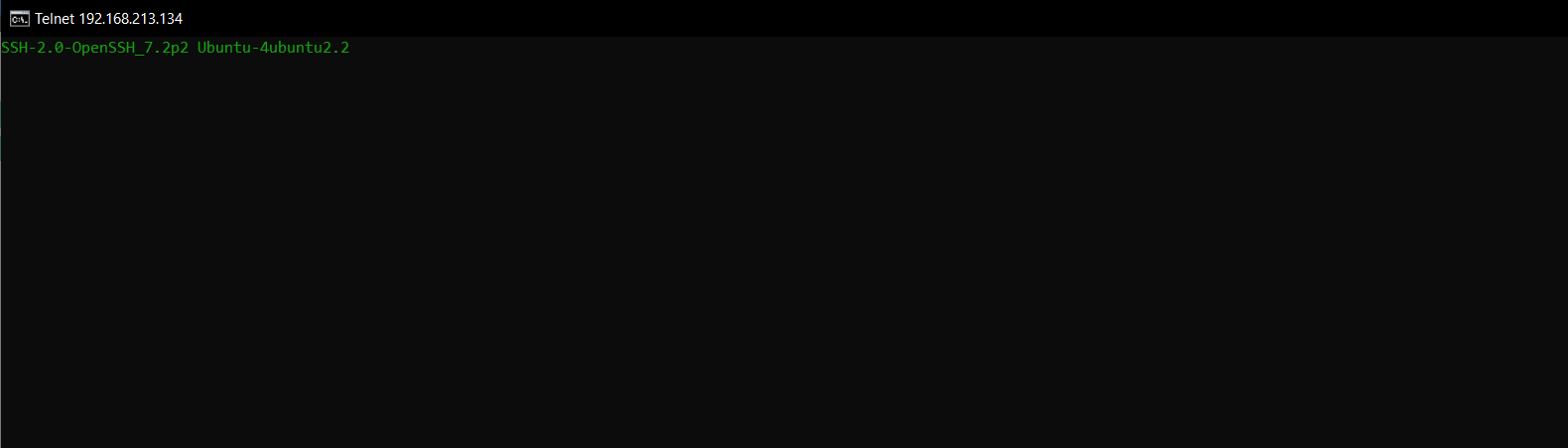
1. **Create a rule that allows SSH only from a specific IP address**

* Để thực hiện chính sách trên thì ta làm như sau:

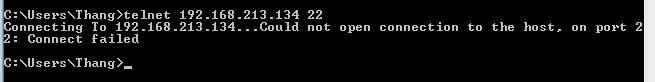


* Kết quả

+ client cho phép:

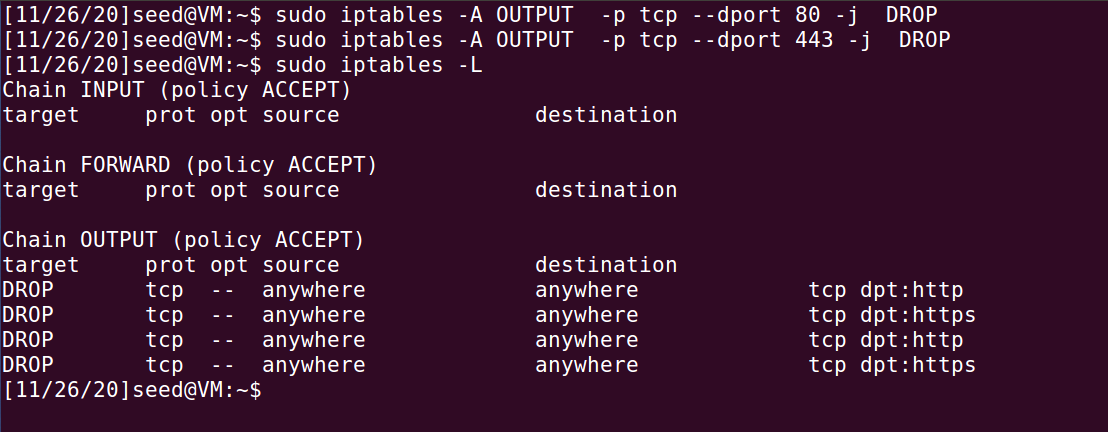


+ Client hạn chế



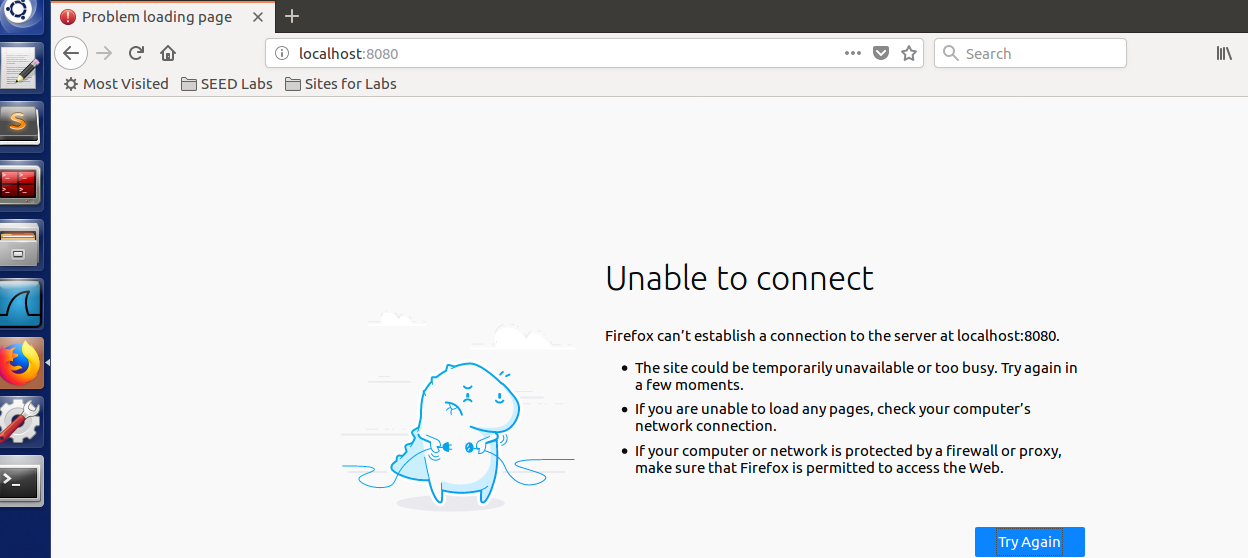
1. **Create the rules that block any HTTP and HTTPS browsing**

* Để thực hiện chính sách trên thì ta làm như sau:



* Kết quả:

+ http



+ https

