**Nội dung và hướng dẫn thực hiện bài thực hành**

**Mục đích**

* Thiết lập tường lửa để chặn truy cập telnet từ các địa chỉ không được cấp phép
* Cho phép telnet được truy cập từ các địa chỉ được chỉ định

**Yêu cầu đối với sinh viên**

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.
* Một máy chủ hoặc thiết bị mạng hỗ trợ telnet.
* Một tường lửa có khả năng thiết lập quy tắc dựa trên địa chỉ IP (VD:iptables trên linux)

**Nội dung thực hành**

# Khởi Động Lab

Chạy lab: labtainer ptit-firewall

Nhập mã sinh viên.

3 terminal xuất hiện: client1, client, server (cùng mạng LAN).

# Task 1: Cấu Hình Tường Lửa

1. Trên server, kiểm tra IP:

ip a

Ghi lại IP server và IP client cấp phép

1. Cấu hình iptables để cho phép client và chặn các IP khác trên cổng (ví dụ: 23 cho telnet):
2. sudo iptables -A INPUT -p tcp --dport 23 -s <IP client> -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 23 -j DROP

(Thay <IP client> bằng IP của client).

1. Trên client1, thử telnet:

telnet <IP server>

* + Kết quả: timed out (bị chặn).

# Task 2: Kết Nối Telnet

1. Trên **client**, telnet vào **server**:

telnet <IP server>

1. Xem file trên server:

ls

1. Thoát:

exit

# Task 3: Copy và Đọc File

1. Trên client, copy file từ server:

scp -r ubuntu@<IP server>:<path-to-file> .

* Thay <IP server> bằng IP thực tế.
* Thay <path-to-file> bằng đường dẫn file trên **server** (ví dụ: /home/ubuntu/file.txt, check bằng ls ở Task 2).
* User/pass: ubuntu/123.

1. Đọc file:

cat <file>

(Thay <file> bằng tên file vừa copy).

# Kết Thúc

stoplab